

H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI& S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

可靠性配置指导

新华三技术有限公司
<http://www.h3c.com>

资料版本：6W103-20190822
产品版本：Release 612x 系列

Copyright © 2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

前言

本配置指导主要介绍故障检测和快速保护倒换这两类可靠性技术的原理及具体配置。通过这些技术，您可以进行网络故障检测和诊断、出现故障时能够快速的进行业务恢复。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定






格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 以太网OAM.....	1-1
1.1 以太网OAM简介.....	1-1
1.1.1 以太网OAM主要功能	1-1
1.1.2 以太网OAM协议报文	1-1
1.1.3 以太网OAM工作流程	1-2
1.1.4 协议规范	1-3
1.2 以太网OAM配置限制和指导	1-3
1.3 以太网OAM配置任务简介	1-4
1.4 配置以太网OAM基本功能	1-4
1.5 配置以太网OAM连接检测定时器	1-4
1.5.1 功能简介	1-4
1.5.2 配置限制和指导	1-5
1.5.3 全局配置以太网OAM连接检测定时器	1-5
1.5.4 在接口上配置以太网OAM连接检测定时器	1-5
1.6 配置错误帧事件检测参数	1-5
1.6.1 配置限制和指导	1-5
1.6.2 全局配置错误帧事件检测参数	1-6
1.6.3 在接口上配置错误帧事件检测参数	1-6
1.7 配置错误帧周期事件检测参数	1-6
1.7.1 配置限制和指导	1-6
1.7.2 全局配置错误帧周期事件检测参数	1-6
1.7.3 在接口上配置错误帧周期事件检测参数	1-7
1.8 配置错误帧秒事件检测参数	1-7
1.8.1 配置限制和指导	1-7
1.8.2 全局配置错误帧秒事件检测参数	1-7
1.8.3 在接口上配置错误帧秒事件检测参数	1-7
1.9 配置对远端以太网OAM事件的响应动作	1-8
1.10 开启以太网OAM远端环回功能	1-8
1.10.1 功能简介	1-8
1.10.2 配置限制和指导	1-8
1.10.3 开启指定接口的以太网OAM远端环回功能	1-9
1.10.4 开启当前接口的以太网OAM远端环回功能	1-9
1.11 拒绝远端发起的以太网OAM远端环回	1-9

1.12 以太网OAM显示和维护	1-9
1.13 以太网OAM典型配置举例	1-10
1.13.1 以太网OAM基础配置举例	1-10

1 以太网OAM

1.1 以太网OAM简介

以太网 OAM（Operation, Administration, and Maintenance，操作、管理和维护）是一种监控网络故障的工具，主要用于解决以太网接入“最后一公里”中常见的链路问题，能够有效提高以太网的管理和维护能力，保障网络的稳定运行。用户通过在两个点到点连接的设备上启用以太网 OAM 功能，可以监控这两台设备之间的链路状态。

1.1.1 以太网OAM主要功能

以太网 OAM 的主要功能包括：

- 链路性能监测：对链路的各种性能进行监测，包括对丢包、时延和抖动等数据的衡量，以及对各类流量的统计。
- 故障侦测和告警：通过发送检测报文来探测链路的连通性，当链路出现故障时及时通知网络管理员。
- 环路测试：通过监测所发出报文的返回情况来检测链路质量和定位链路故障。

1.1.2 以太网OAM协议报文

以太网OAM工作在数据链路层，其协议报文被称为OAMPDU（OAM Protocol Data Unit，OAM协议数据单元）。以太网OAM就是通过设备之间定时交互OAMPDU来报告链路状态，使网络管理员能够对网络进行有效的管理。几种常见的OAMPDU及其作用如 [表 1-1](#) 所示。

表1-1 常见的 OAMPDU 及其作用

报文类型	中文含义	作用
Information OAMPDU	信息OAMPDU	用于将OAM实体的状态信息（包括本地信息、远端信息和自定义信息）发给远端OAM实体，以保持以太网OAM连接
Event Notification OAMPDU	事件通知OAMPDU	一般用于链路监控，对连接本端和远端OAM实体的链路上所发生的故障进行告警
Loopback Control OAMPDU	环回控制OAMPDU	主要用于远端环回控制，用来控制远端设备的OAM环回状态，该报文中带有开启或关闭环回功能的信息，根据该信息开启或关闭远端环回功能



说明

我们将开启了以太网 OAM 功能的接口称为“以太网 OAM 实体”，简称“OAM 实体”。

1.1.3 以太网OAM工作流程

1. 建立以太网OAM连接

以太网 OAM 连接的建立过程也称为 **Discovery** 阶段，即本端 OAM 实体发现远端 OAM 实体、并与之建立稳定对话的过程。

在这个过程中，相连的 OAM 实体通过交互 **Information OAMPDU** 通报各自的以太网 OAM 配置信息和本端支持的以太网 OAM 能力信息。当 OAM 实体收到远端的配置参数后，决定是否建立 OAM 连接。当两端 OAM 实体对远端环回功能、单向链路检测及链路事件等配置信息的检查都通过之后，以太网 OAM 协议开始正常工作。

以太网OAM的连接模式有两种：主动模式和被动模式。以太网OAM连接只能由主动模式的OAM实体发起，而被动模式的OAM实体只能等待远端OAM实体的连接请求；同处于被动模式下的两个OAM实体之间无法建立以太网OAM连接。在这两种模式下设备的处理能力如 [表 1-2](#) 所示。

表1-2 主动模式与被动模式的处理能力比较

处理能力	主动模式	被动模式
初始化以太网OAM Discovery过程	可以	不可以
对以太网OAM Discovery初始化过程的响应	可以	可以
发送Information OAMPDU	可以	可以
发送Event Notification OAMPDU	可以	可以
发送不携带TLV的Information OAMPDU	可以	可以
发送Loopback Control OAMPDU	可以	不可以
对Loopback Control OAMPDU的响应	可以，但需要远端为主动模式	可以

以太网 OAM 连接建立后，两端的 OAM 实体会以一定的时间间隔为周期发送 **Information OAMPDU** 来检测连接是否正常，该间隔被称为握手报文发送间隔。如果一端 OAM 实体在连接超时时间内未收到远端 OAM 实体发来的 **Information OAMPDU**，则认为 OAM 连接中断。

2. 链路监控

以太网的故障检测非常困难，特别是在网络物理通信没有中断而网络性能缓慢下降的情况下。链路监控用于在各种环境下检测和发现链路层故障，以太网OAM通过交互**Event Notification OAMPDU**来监控链路：当一端OAM实体监控到一般链路事件（其所含类型如 [表 1-3](#) 所示）时，将向其远端发送**Event Notification OAMPDU**以进行通报，管理员可以通过观察日志信息动态地掌握网络的情况。

表1-3 一般链路事件

事件类型	描述
错误帧事件（Errored Frame Event）	以设定的时间为检测窗口，在窗口期内检测到的错误帧数量如果达到或超过了检测阈值，就产生一次错误帧事件
错误帧周期事件（Errored Frame Period Event）	以收到设定数量的帧为检测窗口，在窗口期内检测到的错误帧数量如果达到或超过了检测阈值，就产生一次错误帧周期事件

事件类型	描述
错误帧秒事件（Errored Frame Seconds Event）	以设定的时间为检测窗口，在窗口期内检测到的错误帧秒（在某一秒内检测到至少一个错误帧，就称该秒为错误帧秒）数量如果达到或超过了检测阈值，就产生一次错误帧秒事件

3. 远端故障检测

在以太网OAM连接已建立的情况下，两端的OAM实体会不断交互Information OAMPDU。当设备故障或不可用导致流量中断时，故障端OAM实体会通过Information OAMPDU中的Flag域将故障信息（即紧急链路事件类型）通知给远端OAM实体。这样，管理员可以通过观察日志信息动态地了解链路状态，对相应的错误及时进行处理。紧急链路事件的类型及其对应的Information OAMPDU发送频率如表1-4所示。

表1-4 紧急链路事件

事件类型	描述	OAMPDU 发送频率
链路故障（Link Fault）	远端链路信号丢失	每秒发送一次
致命故障（Dying Gasp）	不可预知的状态发生，比如电源中断	不间断发送
紧急事件（Critical Event）	不能确定的紧急事件发生	不间断发送

4. 远端环回

远端环回是指主动模式下的 OAM 实体向远端发送除 OAMPDU 以外的所有其它报文时，远端收到报文后不按其目的地址进行转发，而是将其按原路返回给本端。远端环回只有在以太网 OAM 连接建立之后才能实现。

远端环回功能可用于检测链路质量和定位链路故障。定期进行环回检测可以及时发现网络故障，并可通过分段进行环回检测来定位故障发生的具体区域。

1.1.4 协议规范

与以太网 OAM 相关的协议规范有：

- IEEE 802.3ah: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

1.2 以太网OAM配置限制和指导

设备对收、发携带有紧急链路事件的 Information OAMPDU 的支持情况如下：

- 支持接收携带所有类型紧急链路事件的 Information OAMPDU。
- 支持发送携带链路故障事件的 Information OAMPDU。
- 仅支持在设备重启或接口被 shutdown 时发送携带致命故障事件的 Information OAMPDU，但 IRF 物理接口不支持发送该报文。
- 不支持发送携带紧急事件的 Information OAMPDU。

1.3 以太网OAM配置任务简介

以太网 OAM 配置任务如下：

- (1) [配置以太网OAM基本功能](#)
- (2) （可选）[配置以太网OAM连接检测定时器](#)
- (3) （可选）配置一般链路事件检测参数
 - [配置错误帧事件检测参数](#)
 - [配置错误帧周期事件检测参数](#)
 - [配置错误帧秒事件检测参数](#)
- (4) （可选）[配置对远端以太网OAM事件的响应动作](#)
- (5) （可选）配置以太网 OAM 远端环回功能
 - [开启以太网OAM远端环回功能](#)
 - [拒绝远端发起的以太网OAM远端环回](#)

1.4 配置以太网OAM基本功能

1. 功能简介

以太网 OAM 的连接模式分为主动和被动模式，当开启了以太网 OAM 功能之后，以太网接口开始使用预设的连接模式与其远端接口建立以太网 OAM 连接。

2. 配置限制和指导

不允许在已开启以太网 OAM 功能的接口上更改以太网 OAM 的连接模式。如需更改，请先关闭该接口上的以太网 OAM 功能。

3. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 进入二层以太网接口视图。
interface interface-type interface-number
- (3) 配置以太网 OAM 的连接模式。
oam mode { active | passive }
缺省情况下，以太网 OAM 连接模式为主动模式。
- (4) 开启以太网 OAM 功能。
oam enable
缺省情况下，以太网 OAM 功能处于关闭状态。

1.5 配置以太网OAM连接检测定时器

1.5.1 功能简介

以太网 OAM 连接建立后，两端的 OAM 实体会以一定的时间间隔为周期发送 Information OAMPDU 来检测连接是否正常，该间隔被称为握手报文发送间隔。如果一端 OAM 实体在连接超时时间内未

收到远端 OAM 实体发来的 Information OAMPDU，则认为 OAM 连接中断。通过调整握手报文发送间隔和连接超时时间，可以改变以太网 OAM 连接的检测精度。

1.5.2 配置限制和指导

用户既可在系统视图下配置对所有接口都有效的全局值，也可在接口视图下配置只对当前接口有效的接口值，后者的配置优先级较高。

由于本端 OAM 实体在连接超时后将老化与远端 OAM 实体的连接关系，导致 OAM 连接中断，因此连接超时时间必须大于握手报文发送间隔（建议为五倍或以上），否则将导致以太网 OAM 连接不稳定。

1.5.3 全局配置以太网OAM连接检测定时器

- (1) 进入系统视图。

```
system-view
```

- (2) 全局配置以太网 OAM 握手报文的发送间隔。

```
oam global timer hello interval
```

缺省情况下，以太网 OAM 握手报文发送间隔的全局值为 1000 毫秒。

- (3) 全局配置以太网 OAM 连接的超时时间。

```
oam global timer keepalive interval
```

缺省情况下，以太网 OAM 连接超时时间的全局值为 5000 毫秒。

1.5.4 在接口上配置以太网OAM连接检测定时器

- (1) 进入系统视图。

```
system-view
```

- (2) 进入二层以太网接口视图。

```
interface interface-type interface-number
```

- (3) 在接口上配置以太网 OAM 握手报文的发送间隔。

```
oam timer hello interval
```

缺省情况下，接口采用全局值。

- (4) 在接口上配置以太网 OAM 连接的超时时间。

```
oam timer keepalive interval
```

缺省情况下，接口采用全局值。

1.6 配置错误帧事件检测参数

1.6.1 配置限制和指导

用户既可在系统视图下配置对所有接口都有效的全局值，也可在接口视图下配置只对当前接口有效的接口值，后者的配置优先级较高。

1.6.2 全局配置错误帧事件检测参数

- (1) 进入系统视图。

system-view

- (2) 全局配置错误帧事件的检测窗口。

oam global errored-frame window *window-value*

缺省情况下，错误帧事件检测窗口的全局值为 1000 毫秒。

- (3) 全局配置错误帧事件的检测阈值。

oam global errored-frame threshold *threshold-value*

缺省情况下，错误帧事件检测阈值的全局值为 1 次。

1.6.3 在接口上配置错误帧事件检测参数

- (1) 进入系统视图。

system-view

- (2) 进入二层以太网接口视图。

interface *interface-type interface-number*

- (3) 在接口上配置错误帧事件的检测窗口。

oam errored-frame window *window-value*

缺省情况下，接口采用全局值。

- (4) 在接口上配置错误帧事件的检测阈值。

oam errored-frame threshold *threshold-value*

缺省情况下，接口采用全局值。

1.7 配置错误帧周期事件检测参数

1.7.1 配置限制和指导

用户既可在系统视图下配置对所有接口都有效的全局值，也可在接口视图下配置只对当前接口有效的接口值，后者的配置优先级较高。

1.7.2 全局配置错误帧周期事件检测参数

- (1) 进入系统视图。

system-view

- (2) 全局配置错误帧周期事件的检测窗口。

oam global errored-frame-period window *window-value*

缺省情况下，错误帧周期事件检测窗口的全局值为 10000000 次。

- (3) 全局配置错误帧周期事件的检测阈值。

oam global errored-frame-period threshold *threshold-value*

缺省情况下，错误帧周期事件检测阈值的全局值为 1 次。

1.7.3 在接口上配置错误帧周期事件检测参数

- (1) 进入系统视图。

system-view

- (2) 进入二层以太网接口视图。

interface *interface-type* *interface-number*

- (3) 在接口上配置错误帧周期事件的检测窗口。

oam errored-frame-period window *window-value*

缺省情况下，接口采用全局值。

- (4) 在接口上配置错误帧周期事件的检测阈值。

oam errored-frame-period threshold *threshold-value*

缺省情况下，接口采用全局值。

1.8 配置错误帧秒事件检测参数

1.8.1 配置限制和指导

用户既可在系统视图下配置对所有接口都有效的全局值，也可在接口视图下配置只对当前接口有效的接口值，后者的配置优先级较高。

在数量上，错误帧秒事件的检测阈值不应大于其检测窗口值（换算成秒），否则将不会产生错误帧秒事件。

1.8.2 全局配置错误帧秒事件检测参数

- (1) 进入系统视图。

system-view

- (2) 全局配置错误帧秒事件的检测窗口。

oam global errored-frame-seconds window *window-value*

缺省情况下，错误帧秒事件检测窗口的全局值为 60000 毫秒。

- (3) 全局配置错误帧秒事件的检测阈值。

oam global errored-frame-seconds threshold *threshold-value*

缺省情况下，错误帧秒事件检测阈值的全局值为 1 次。

1.8.3 在接口上配置错误帧秒事件检测参数

- (1) 进入系统视图。

system-view

- (2) 进入二层以太网接口视图。

interface *interface-type* *interface-number*

- (3) 在接口上配置错误帧秒事件的检测窗口。

oam errored-frame-seconds window *window-value*

缺省情况下，接口采用全局值。

- (4) 在接口上配置错误帧秒事件的检测阈值。

```
oam errored-frame-seconds threshold threshold-value
```

缺省情况下，接口采用全局值。

1.9 配置对远端以太网OAM事件的响应动作

1. 功能简介

通过本配置可以使接口在收到远端以太网 OAM 事件时除了记录日志外，还会自动断开 OAM 连接，并设置该接口的链路层状态为 **down**。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入二层以太网接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口收到远端以太网 OAM 事件时的响应动作。

```
oam remote-failure { connection-expired | critical-event | dying-gasp |  
link-fault } action error-link-down
```

缺省情况下，接口收到远端以太网 OAM 事件后仅记录日志。

1.10 开启以太网OAM远端环回功能

1.10.1 功能简介

在本端接口上开启了以太网 OAM 远端环回功能之后，该接口将向远端接口发送 Loopback Control OAMPDU，使远端进入 OAM 环回状态。然后，远端会返回本端发送来的报文（除 OAMPDU 以外），用户可以通过观察这些报文的返回情况来计算链路丢包率，以此来评判链路性能。

1.10.2 配置限制和指导

由于远端环回功能将使正常业务受到影响，因此请慎重开启该功能。

只有当接口上的以太网 OAM 连接已建立完成，且以太网 OAM 的连接模式为主动模式时，才允许在该接口上开启以太网 OAM 远端环回功能。

只有本端和远端接口都支持远端环回功能、且在全双工链路上才能实现远端环回功能。

在开启远端环回时，将引起所有数据流量的中断；当退出远端环回后，接口将自动执行一次先关闭再开启的操作。导致接口退出远端环回的原因有：关闭接口上的以太网 OAM 功能、关闭接口上的以太网 OAM 远端环回功能或 OAM 连接超时等。

如果在远端环回过程中开启了内部环回功能，远端环回将终止。有关环回功能的详细介绍，请参见“二层技术-以太网交换配置指导”中的“以太网接口”。

用户既可在用户视图或系统视图下开启指定接口的以太网 OAM 远端环回功能，也可在接口视图下开启当前接口的以太网 OAM 远端环回功能，三者的配置效果相同。

1.10.3 开启指定接口的以太网OAM远端环回功能

- (1) （可选）进入系统视图。

system-view

用户也可以在用户视图下执行以下任务。

- (2) 开启指定接口的以太网 OAM 远端环回功能。

oam remote-loopback start interface *interface-type interface-number*

缺省情况下，以太网 OAM 远端环回功能处于关闭状态。

1.10.4 开启当前接口的以太网OAM远端环回功能

- (1) 进入系统视图。

system-view

- (2) 进入二层以太网接口视图。

interface *interface-type interface-number*

- (3) 开启当前接口的以太网 OAM 远端环回功能。

oam remote-loopback start

缺省情况下，以太网 OAM 远端环回功能处于关闭状态。

1.11 拒绝远端发起的以太网OAM远端环回

1. 功能简介

由于远端环回功能会使正常业务受到影响，为了避免这种情况，用户可通过本配置使本端接口不受远端发来的 Loopback Control OAMPDU 的控制，从而拒绝其发起的以太网 OAM 远端环回。

2. 配置限制与指导

在执行本配置时若接口已处于环回状态，则该配置将从下次环回开始时生效。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入二层以太网接口视图。

interface *interface-type interface-number*

- (3) 配置接口拒绝远端发起的以太网 OAM 远端环回。

oam remote-loopback reject-request

缺省情况下，接口不拒绝远端发起的以太网 OAM 远端环回。

1.12 以太网OAM显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后以太网 OAM 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除以太网 OAM 的统计信息。

表1-5 以太网 OAM 显示和维护

操作	命令
显示以太网OAM连接的信息	display oam { local remote } [interface <i>interface-type</i> <i>interface-number</i>]
显示以太网OAM的配置信息	display oam configuration [interface <i>interface-type</i> <i>interface-number</i>]
显示以太网OAM的紧急链路事件统计信息	display oam critical-event [interface <i>interface-type</i> <i>interface-number</i>]
显示以太网OAM的一般链路事件统计信息	display oam link-event { local remote } [interface <i>interface-type</i> <i>interface-number</i>]
清除以太网OAM的报文和一般链路事件统计信息	reset oam [interface <i>interface-type</i> <i>interface-number</i>]

1.13 以太网OAM典型配置举例

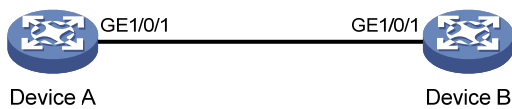
1.13.1 以太网OAM基础配置举例

1. 组网需求

- 通过在 Device A 和 Device B 上配置以太网 OAM 功能，实现二者之间链路连通性故障的自动检测。
- 通过观察 Device A 上收到错误帧的情况，来评判 Device A 与 Device B 之间的链路性能。

2. 组网图

图1-1 以太网 OAM 典型配置组网图



3. 配置步骤

(1) 配置 Device A

在接口 GigabitEthernet1/0/1 上配置以太网 OAM 的连接模式为主动模式，并开启其以太网 OAM 功能。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] oam mode active
[DeviceA-GigabitEthernet1/0/1] oam enable
```

在接口 GigabitEthernet1/0/1 上配置错误帧事件的检测窗口为 20000 毫秒，检测阈值为 10 次。

```
[DeviceA-GigabitEthernet1/0/1] oam errored-frame window 200
[DeviceA-GigabitEthernet1/0/1] oam errored-frame threshold 10
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device B

在接口 GigabitEthernet1/0/1 上配置以太网 OAM 的连接模式为被动模式，并开启其以太网 OAM 功能。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] oam mode passive
[DeviceB-GigabitEthernet1/0/1] oam enable
[DeviceB-GigabitEthernet1/0/1] quit
```

4. 验证配置

通过使用 **display oam critical-event** 命令可以显示以太网 OAM 的紧急链路事件统计信息，例如：

显示 Device A 所有接口上以太网 OAM 的紧急链路事件统计信息。

```
[DeviceA] display oam critical-event
----- [GigabitEthernet1/0/1] -----
Local link status      : UP
Event statistics
Link fault             : Not occurred
Dying gasp             : Not occurred
Critical event         : Not occurred
```

以上信息表明：Device A 与 Device B 之间的链路上尚未发生任何紧急链路事件。

通过使用 **display oam link-event** 命令可以显示以太网 OAM 的一般链路事件统计信息，例如：

显示 Device A 所有接口上以太网 OAM 的一般链路事件的本端统计信息。

```
[DeviceA] display oam link-event local
----- [GigabitEthernet1/0/1] -----
Link status: UP
OAM local errored frame event
Event time stamp       : 5789 x 100 milliseconds
Errored frame window   : 200 x 100 milliseconds
Errored frame threshold : 10 error frames
Errored frame          : 13 error frames
Error running total    : 350 error frames
Event running total    : 17 events
```

以上信息表明：从 Device A 开始运行时起，总共有 350 个错误帧，产生了 17 次错误帧事件，链路性能并不稳定。

目 录

1 CFD.....	1-1
1.1 CFD简介	1-1
1.1.1 CFD基本概念.....	1-1
1.1.2 CFD分级.....	1-2
1.1.3 MP的报文处理	1-4
1.1.4 CFD各项功能.....	1-4
1.1.5 以太网告警抑制功能.....	1-5
1.1.6 协议规范.....	1-6
1.2 CFD配置限制和指导	1-6
1.3 CFD配置任务简介	1-6
1.4 CFD配置准备	1-6
1.5 配置CFD基本功能	1-7
1.5.1 开启CFD功能.....	1-7
1.5.2 配置服务实例.....	1-7
1.5.3 配置MEP	1-7
1.5.4 配置MIP的创建规则.....	1-8
1.6 配置CFD各项功能	1-9
1.6.1 配置连续性检测功能	1-9
1.6.2 配置环回功能.....	1-10
1.6.3 配置链路跟踪功能	1-10
1.6.4 配置告警抑制功能	1-10
1.6.5 配置单向丢包测试功能	1-11
1.6.6 配置单向时延测试功能	1-11
1.6.7 配置双向时延测试功能	1-12
1.6.8 配置比特错误测试功能	1-12
1.7 配置以太网告警抑制功能.....	1-12
1.8 CFD显示和维护	1-13
1.9 CFD典型配置举例	1-14
1.9.1 CFD基础配置举例.....	1-14

1 CFD

1.1 CFD简介

CFD (Connectivity Fault Detection, 连通错误检测) 遵循 IEEE 802.1ag 的 CFM (Connectivity Fault Management, 连通错误管理) 协议和 ITU-T 的 Y.1731 协议, 是一种二层网络中基于 VLAN 的端到端 OAM (Operation, Administration, and Maintenance, 操作、管理和维护) 机制, 主要用于在二层网络中检测链路连通性, 以及在故障发生时确认故障并定位。

1.1.1 CFD基本概念

1. MD

MD (Maintenance Domain, 维护域) 是指连通错误检测所覆盖的一个网络或网络的一部分, 它以“MD 名称”来标识。

2. MA

MA (Maintenance Association, 维护集) 是 MD 的一部分, 一个 MD 可划分为一个或多个 MA。MA 以“MD 名称+MA 名称”来标识。

MA 可以服务于指定的 VLAN, 也可以不服务于任何 VLAN, 分别称为带 VLAN 属性和不带 VLAN 属性的 MA。

3. MP

MP (Maintenance Point, 维护点) 配置在接口上, 属于某个 MA, 可分为 MEP (Maintenance association End Point, 维护端点) 和 MIP (Maintenance association Intermediate Point, 维护中间点)。

MEP 确定了 MA 的边界, 以“MEP ID”来标识。MEP 具有方向性, 分为内向 MEP 和外向 MEP 两种:

- 内向 MEP 通过除其所在的接口以外的所有接口向外发送 CFD 协议报文, 即在其所属 MA 所服务的 VLAN 中进行广播。
- 外向 MEP 则直接通过其所在的接口向外发送 CFD 协议报文。

MIP 位于 MA 的内部, 不能主动发出 CFD 协议报文, 但可以处理和响应 CFD 协议报文。MIP 由设备自动创建, 可以配合 MEP 完成类似于 ping 和 tracert 的功能。

4. MEP列表

MEP 列表是同一 MA 中允许配置的本地 MEP 和需要监控的远端 MEP 的集合, 它限定了 MA 中 MEP 的选取范围, 不同设备上同一 MA 中的所有 MEP 都应包含在此列表中, 且 MEP ID 互不重复。如果 MEP 收到来自远端设备的 CCM (Continuity Check Message, 连续性检测报文) 报文所携带的 MEP 不在同一 MA 的 MEP 列表中, 就丢弃该报文。



说明

本端设备发送的 CCM 报文应当携带 RDI（Remote Defect Indication，远程故障指示）标志位，否则对端设备将无法感知某些故障。当 MA 中至少有一个本地 MEP 未学到 MEP 列表中的所有远端 MEP 时，该 MA 中的 MEP 发送的 CCM 报文将不会携带 RDI 标志位。

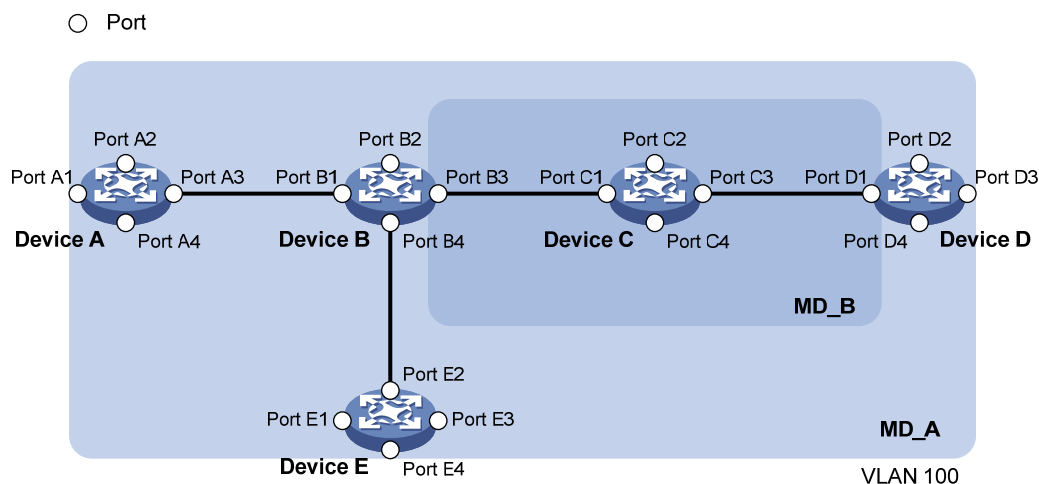
1.1.2 CFD分级

1. MD分级

为了准确定位故障点，在 MD 中引入了级别（层次）的概念。MD 共分为八级，用整数 0~7 来表示，数字越大级别越高，MD 的范围也就越大。不同 MD 之间可以相邻或嵌套，但不能交叉，且嵌套时只能由高级别 MD 向低级别 MD 嵌套，即低级别 MD 必须包含在高级别 MD 内部。

MD 的分级使得故障定位更加便利和准确，如 [图 1-1](#) 所示，有 MD_A 和 MD_B 两个 MD，MD_B 嵌套于 MD_A 中，如果在 MD_A 的边界上发现链路不通，则表明该域内的设备出现了故障，故障可能出现在 Device A~Device E 这五台设备上。此时，如果在 MD_B 的边界上也发现链路不通，则故障范围就缩小到 Device B~Device D 这三台设备上；反之，如果 MD_B 中的设备都工作正常，则至少可以确定 Device C 是没有故障的。

图1-1 两个嵌套的 MD



CFD 协议报文的交互以及相关处理都是基于 MD 的，合理的 MD 规划可以帮助网络管理员迅速定位故障点。

2. MA和MP分级

MA 的级别等于其所属 MD 的级别。

MEP 的级别等于其所属 MD 的级别。

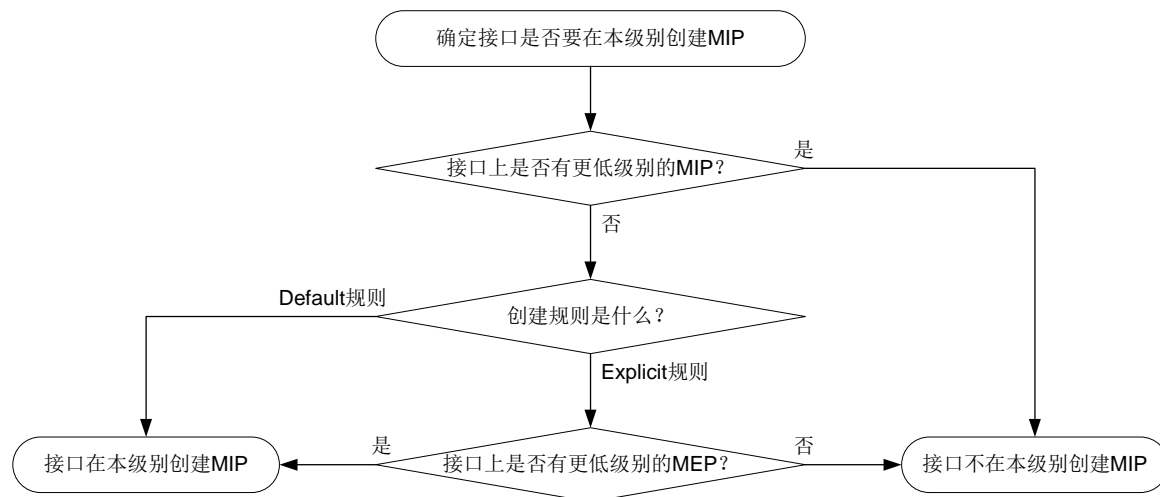
MIP 的级别由其创建规则和所属 MD 的级别共同确定。MIP 的创建规则有以下两种：

- **Default 规则：**当接口上没有更低级别的 MIP 时，在本级别创建 MIP。在此规则下，接口上即使没有配置 MEP 也可创建 MIP。

- **Explicit 规则：**当接口上没有更低级别的 MIP 且有更低级别的 MEP 时，在本级别创建 MIP。
在此规则下，接口上只有配置了更低级别的 MEP 时才可创建 MIP。

当用户在设备上指定了MIP的创建规则后，系统会在尚没有MIP的接口上，按照级别由低到高依次检查各MD中的MA，并按照 图 1-2 所示的流程来确定接口是否要在本级别创建MIP。

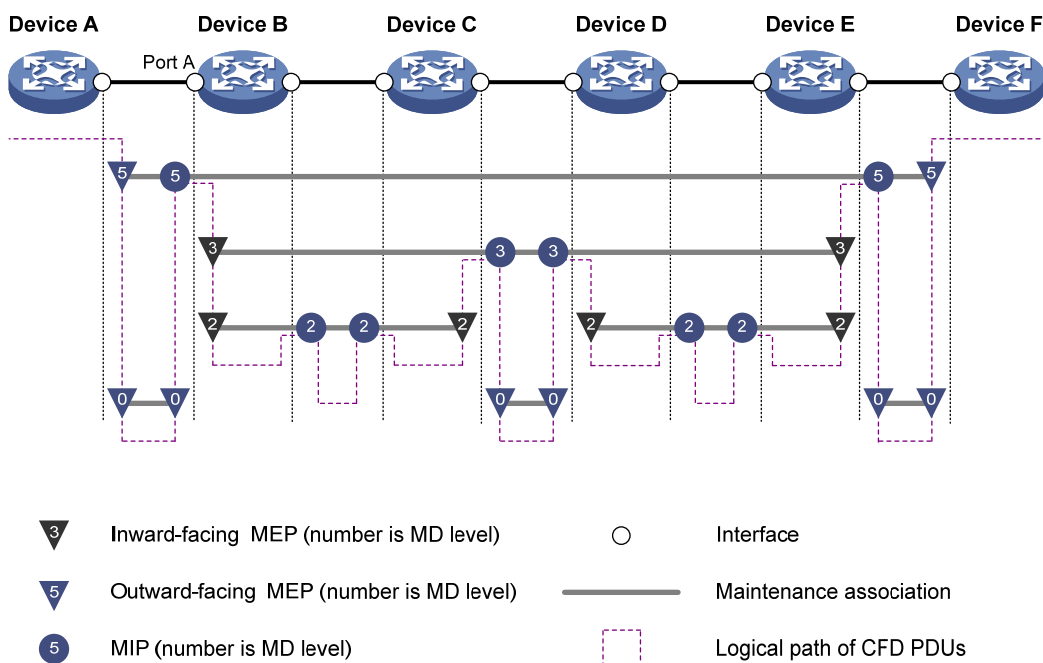
图1-2 是否创建 MIP 的确定流程



3. CFD分级示例

图 1-3 所示为CFD的一种分级配置方式，图中共有 0、2、3、5 四个级别的MD，标识号较大的MD 的级别高、控制范围广；标识号较小的MD的级别低、控制范围小。在Device A~Device F的各接口上配置了MP，譬如Device B的接口Port A上配置有：级别为 5 的MIP、级别为 3 的内向MEP、级别为 2 的内向MEP和级别为 0 的外向MEP。

图1-3 CFD 的分级配置



1.1.3 MP的报文处理

对于带 VLAN 属性的 MA，MP 仅在其所属 MA 所服务于的 VLAN 中发送的报文，报文的级别为 MP 所属 MD 的级别。

对于不带 VLAN 属性的 MA，MP 只能为外向 MEP，主要用来检测直连链路的状态。不带 VLAN 属性的外向 MEP 所发送报文的级别为该 MEP 所属 MD 的级别。

当 MEP 收到高于自己级别的报文时只转发该报文，不会进行处理；当 MEP 收到小于等于自己级别的报文时才会进行处理。

当 MIP 收到不等于自己级别的报文时只转发该报文，不会进行处理；当 MIP 收到等于自己级别的报文时才会进行处理。

1.1.4 CFD各项功能

连通错误检测的有效应用建立在合理的网络部署和配置之上，它的功能是在所配置的 MP 之间实现的。

1. 连续性检测功能

MEP 之间的连通失败可能由设备故障或配置错误造成，连续性检测（Continuity Check，CC）功能就是用来检测 MEP 之间的连通状态。该功能的实现方式是：由 MEP 周期性地发送 CCM 报文，相同 MA 的其它 MEP 接收该报文，并由此获知远端状态。若 MEP 在 3.5 个 CCM 报文发送周期内未收到远端 MEP 发来的 CCM 报文，则认为链路有问题，会输出日志报告。当 MD 中的多个 MEP 在发送 CCM 报文时，就实现了多点到多点之间的链路检测。

CCM 报文是组播报文。

2. 环回功能

环回（Loopback，LB）功能类似于 IP 层的 ping 功能，用于验证源 MEP 与目标 MP 之间的连接状态。该功能的实现方式是：由源 MEP 发送 LBM（Loopback Message，环回报文）报文给目标 MP，并根据能否收到对端反馈的 LBR（Loopback Reply，环回应答）报文来检验链路状态。

LBM 报文分为组播和单播两种报文，设备支持发送和处理单播 LBM 报文，不支持发送但可处理组播 LBM 报文；LBR 是单播报文。

3. 链路跟踪功能

链路跟踪（Linktrace，LT）功能类似于 IP 层的 tracert 功能，用于确定源 MEP 到目标 MP 的路径，其实现方式是：由源 MEP 发送 LTM（Linktrace Message，链路跟踪报文）报文给目标 MP，目标 MP 以及 LTM 报文所经过的 MIP 收到该报文后，都会发送 LTR（Linktrace Reply，链路跟踪应答）报文给源 MEP，源 MEP 则根据收到的 LTR 报文来确定到目标 MP 的路径。

LTM 报文是组播报文，LTR 报文是单播报文。

4. 告警抑制功能

告警抑制功能用来减少 MEP 故障告警的数量。如果 MEP 在 3.5 个 CCM 报文发送周期内未收到远端 MEP 发来的 CCM 报文，便立刻开始周期性地发送 AIS（Alarm Indication Signal，告警指示信号）报文，该报文的发送方向与 CCM 报文相反。其它 MEP 在收到 AIS 报文后，会抑制本端的故障告警，并继续发送 AIS 报文。此后，如果 MEP 收到了 CCM 报文，便停止发送 AIS 报文并恢复故障告警。

AIS 报文是组播报文。

5. 单向丢包测试功能

单向丢包测试（Loss Measurement, LM）功能用来检测 MEP 之间的单向丢包情况，其实现方式是：由源 MEP 发送 LMM（Loss Measurement Message, 丢包测量报文）报文给目标 MEP，目标 MEP 收到该报文后，会发送 LMR（Loss Measurement Reply, 丢包测量应答）报文给源 MEP，源 MEP 则根据两个连续的 LMR 报文来计算源 MEP 和目标 MEP 间的丢包数，即源 MEP 从收到第二个 LMR 报文开始，根据本 LMR 报文和前一个 LMR 报文的统计计数来计算源 MEP 和目标 MEP 间的丢包数。

LMM 报文和 LMR 报文都是单播报文。

6. 帧时延测试功能

帧时延测试（Delay Measurement, DM）功能用来检测 MEP 之间报文传输的时延情况，分为以下两种：

- 单向时延测试

单向时延测试功能的实现方式是：源 MEP 发送 1DM（One-way Delay Measurement, 单向时延测量）报文给目标 MEP，该报文中携带有其发送时间。目标 MEP 收到该报文后记录其接收时间，并结合其发送时间来计算并记录链路传输的时延和抖动（即时延变化值）。

1DM 报文是单播报文。

- 双向时延测试

双向时延测试功能的实现方式是：源 MEP 发送 DMM（Delay Measurement Message, 时延测量报文）报文给目标 MEP，该报文中携带有其发送时间。目标 MEP 收到该报文后记录其接收时间，然后再发送 DMR（Delay Measurement Reply, 时延测量应答）报文给源 MEP，该报文中携带有 DMM 报文的发送和接收时间，以及 DMR 报文的发送时间。源 MEP 收到 DMR 报文后记录其接收时间，并据此计算出链路传输的时延和抖动。

DMM 报文和 DMR 报文都是单播报文。

7. 比特错误测试功能

比特错误测试功能用来测试 MEP 之间的比特错误。源 MEP 发送 TST（Test, 比特错误测试）报文给目标 MEP，该报文中携带有伪随机序列或全 0 值。目标 MEP 收到该报文后，通过对报文内容进行计算比较来确定错误比特的情况。

TST 报文是单播报文。

1.1.5 以太网告警抑制功能

以太网告警抑制功能用来建立以太网端口的状态与告警抑制功能之间的联动。当设备（不一定是 MP）的端口发生了 down 事件，便立刻开始周期性地发送 EAIS（Ethernet Alarm Indication Signal, 以太网告警指示信号）报文以抑制故障告警的上报；当该端口重新 up 后，会立刻停止发送 EAIS 报文。MEP 在收到 EAIS 报文后，会抑制本端的故障告警，并继续发送 EAIS 报文。此后，如果 MEP 在 3.5 个 EAIS 报文发送周期内再未收到 EAIS 报文，则表明故障已消除，于是便停止发送 EAIS 报文并恢复故障告警。

EAIS 报文是组播报文。

1.1.6 协议规范

与 CFD 相关的协议规范有：

- IEEE 802.1ag: Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
- ITU-T Y.1731: OAM functions and mechanisms for Ethernet based networks

1.2 CFD配置限制和指导

- 在使用远端 MEP 的 MEP ID 进行其它各项 CFD 功能测试之前，必须先配置连续性检测功能；在使用远端 MEP 的 MAC 地址进行其它 CFD 各项功能测试之前，则没有此限制。
- 被生成树协议阻塞的端口通常不能收发 CFD 协议报文，但下列情况例外：
 - 如果设备上配置有外向 MEP，那么外向 MEP 所在的端口即使被生成树协议阻塞，也仍能收发 CFD 协议报文。
 - 如果设备上配置有 MIP 或内向 MEP，那么该设备上的端口即使被生成树协议阻塞，也仍能收发除 CCM 报文以外的其它 CFD 协议报文。

有关生成树协议的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”。

1.3 CFD配置任务简介

CFD 配置任务如下：

- (1) [配置CFD基本功能](#)
 - a. [开启CFD功能](#)
 - b. [配置服务实例](#)
 - c. [配置MEP](#)
 - d. [配置MIP的创建规则](#)
- (2) [配置CFD各项功能](#)
 - a. [配置连续性检测功能](#)
 - b. (可选) [配置环回功能](#)
 - c. (可选) [配置链路跟踪功能](#)
 - d. (可选) [配置告警抑制功能](#)
 - e. (可选) [配置单向丢包测试功能](#)
 - f. (可选) [配置单向时延测试功能](#)
 - g. (可选) [配置双向时延测试功能](#)
 - h. (可选) [配置比特错误测试功能](#)
- (3) (可选) [配置以太网告警抑制功能](#)

1.4 CFD配置准备

在配置 CFD 功能之前，应对网络进行如下规划：

- 对整个网络的 MD 进行分级，确定各级别 MD 的边界。

- 确定各 MD 的名称，同一 MD 内的设备使用相同的 MD 名称。
- 根据需要监控的 VLAN，确定各 MD 中的 MA。
- 确定各 MA 的名称，同一 MD 中同一 MA 内的设备使用相同的 MA 名称。
- 确定同一 MD 中同一 MA 的 MEP 列表，在不同设备上应保持相同。
- 在 MD 和 MA 的边界接口上应规划 MEP，非边界设备或接口上可规划 MIP。

1.5 配置CFD基本功能

1.5.1 开启CFD功能

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 CFD 功能。

```
cfid enable
```

缺省情况下，CFD 功能处于关闭状态。

1.5.2 配置服务实例

1. 功能简介

一个服务实例用一个整数表示，代表了一个 MD 中的一个 MA。

服务实例内的 MP 所处理报文的级别属性和 VLAN 属性分别由 MD 和 MA 来确定。其中，不带 VLAN 属性的 MA 中的 MP 也不属于任何 VLAN。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 MD。

```
cfid md md-name [ index index-value ] level level-value [ md-id { dns  
dns-name | mac mac-address subnumber | none } ]
```

- (3) 创建服务实例。

```
cfid service-instance instance-id ma-id { icc-based ma-name | integer  
ma-num | string ma-name | vlan-based [ vlan-id ] } [ ma-index index-value ]  
md md-name [ vlan vlan-id ]
```

1.5.3 配置MEP

1. 功能简介

CFD 功能主要体现在对 MEP 的各种操作上，由于 MEP 配置在服务实例上，因此服务实例所代表的 MD 的级别和 VLAN 属性就自然成为了 MEP 的属性。

2. 配置限制和指导

在一个级别上，一个接口只能成为一个不带 VLAN 属性的 MA 的 MEP，且只能为外向 MEP；而对于带 VLAN 属性的 MA，则无此限制。

当 MEP 属于不带 VLAN 属性的 MA 时, 本端 MEP 在 3.5 个 CCM 报文发送周期内未收到远端 MEP 发来的 CCM 报文, 则会将该 MEP 所在接口的链路状态置为 Down, 以便实现 RRPP、Smart Link 等协议的快速切换。

3. 配置准备

在配置 MEP 之前, 必须首先配置服务实例。

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 MEP 列表。

```
cfg meplist mep-list service-instance instance-id
```

所创建的 MEP 必须已包含在对应服务实例的 MEP 列表中。

- (3) 进入二层以太网或二层聚合接口视图。

```
interface interface-type interface-number
```

- (4) 创建 MEP。

```
cfg mep mep-id service-instance instance-id { inbound | outbound }
```

1.5.4 配置MIP的创建规则

1. 功能简介

MIP 是服务实例中的功能实体, 用来响应各种 CFD 测试报文 (如 LTM、LBM 等)。请根据网络规划配置 MIP 的创建规则, 系统将按照此规则在接口上自动创建 MIP。在配置了 MIP 的创建规则之后, 下列任一条件均可触发 MIP 的创建或删除:

- 开启或关闭 CFD 功能。
- 创建或删除接口上的 MEP。
- 端口的 VLAN 属性发生变化。
- MIP 的创建规则发生变化。

2. 配置限制和指导

由于不带 VLAN 属性的 MA 主要用来检测直连链路的状态, 因而此类 MA 无法创建 MIP。

对于带 VLAN 属性的 MA, 当接口上有同级别或更高级别的 MEP 时, 不会在该接口上生成该 MA 的 MIP。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 MIP 的创建规则。

```
cfg mip-rule { default | explicit } service-instance instance-id
```

缺省情况下, 未配置 MIP 的创建规则, 系统不自动创建 MIP。

1.6 配置CFD各项功能

1.6.1 配置连续性检测功能

1. 功能简介

连续性检测功能通过在 MEP 之间互发 CCM 报文来检测这些 MEP 之间的连通状态，从而实现链路连通性的管理。

在使用远端 MEP 的 MEP ID 进行其它各项 CFD 功能测试之前，必须先配置连续性检测功能；在使用远端 MEP 的 MAC 地址进行其它 CFD 各项功能测试之前，则没有此限制。

CCM报文中时间间隔域（Interval域）的值、CCM报文的发送间隔和远端MEP的超时时间这三者之间的关系如 [表 1-1](#) 所示。

表1-1 参数关系表

CCM 报文中时间间隔域的值	CCM 报文的发送间隔	远端 MEP 的超时时间
1	10/3毫秒	35/3毫秒
2	10毫秒	35毫秒
3	100毫秒	350毫秒
4	1秒	3.5秒
5	10秒	35秒
6	60秒	210秒
7	600秒	2100秒



说明

- CCM 报文中时间间隔域的取值范围为 1 ~ 7。对于本系列交换机，当配置该参数取值为 1 和 2 时，受设备硬件限制，可能导致连续性检测功能不稳定。

为了便于描述，下文中我们将时间间隔域小于 4 的 CCM 报文称为“高速 CCM 报文”，大于等于 4 的则称为“低速 CCM 报文”。

2. 配置限制和指导

配置 CCM 报文中时间间隔域时，需要注意：

- 同一 MA 中所有 MEP 发送的 CCM 报文中时间间隔域的值必须相同。
- 当 CCM 报文中时间间隔域的值改变后，需要等待一个新的间隔才能发送 CCM 报文。

3. 配置步骤

- 进入系统视图。

system-view

- （可选）配置 MEP 发送的 CCM 报文中时间间隔域的值。

cfd cc interval interval-value service-instance instance-id

缺省情况下，MEP 发送的 CCM 报文中时间间隔域的值为 4。

- (3) 进入二层以太网或二层聚合接口视图。

```
interface interface-type interface-number
```

- (4) 开启 MEP 的 CCM 报文发送功能。

```
cfd cc service-instance instance-id mep mep-id enable
```

缺省情况下，MEP 的 CCM 报文发送功能处于关闭状态。

1.6.2 配置环回功能

如需检查链路连通性状况，可在任意视图下执行本命令，开启环回功能。

```
cfd loopback service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ number number ]
```

1.6.3 配置链路跟踪功能

1. 功能简介

通过配置链路跟踪功能，可以查找源 MEP 到目标 MEP 之间的路径，从而实现链路故障的定位。它包括以下两种功能：

- 查找源 MEP 到目标 MEP 的路径：通过从源 MEP 发送 LTM 报文到目标 MEP，并检测回应的 LTR 报文来确定设备间的路径。
- 自动发送 LTM 报文：开启本功能后，当源 MEP 在 3.5 个 CCM 报文发送周期内未收到目标 MEP 发来的 CCM 报文，从而判定与目标 MEP 的连接出错时，将发送 LTM 报文（该 LTM 报文的目的地为目标 MEP，LTM 报文中 TTL 字段为最大值 255），通过检测回应的 LTR 报文来定位故障。

2. 配置准备

在为带 VLAN 属性的 MA 所创建的 MEP 配置链路跟踪功能之前，必须先创建该 MA 所属的 VLAN。

3. 配置步骤

- (1) 可在任意视图下执行本命令，查找源 MEP 到目标 MEP 的路径。

```
cfd linktrace service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ ttl ttl-value ] [ hw-only ]
```

- (2) 进入系统视图。

```
system-view
```

- (3) 开启自动发送 LTM 报文功能。

```
cfd linktrace auto-detection [ size size-value ]
```

缺省情况下，自动发送 LTM 报文功能处于关闭状态。

1.6.4 配置告警抑制功能

1. 功能简介

通过配置告警抑制功能可以减少 MEP 故障告警的数量。

2. 配置限制和指导

如果只开启了告警抑制功能，而没有配置 AIS 报文发送级别或者配置的级别错误，那么该 MEP 只能抑制自己的故障告警，而不会再继续向更高级别的 MD 发送 AIS 报文。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启告警抑制功能。

```
cfd ais enable
```

缺省情况下，告警抑制功能处于关闭状态。

- (3) 配置 AIS 报文的发送级别。

```
cfd ais level level-value service-instance instance-id
```

缺省情况下，未配置 AIS 报文的发送级别，服务实例中的 MEP 将无法发送 AIS 报文。

AIS 报文发送级别必须高于服务实例所在 MD 的级别。

- (4) 配置 AIS 报文的发送周期。

```
cfd ais period period-value service-instance instance-id
```

缺省情况下，AIS 报文的发送周期为 1 秒。

1.6.5 配置单向丢包测试功能

1. 功能简介

通过配置单向丢包测试功能，可以检测 MEP 之间的单向丢包情况，包括：目标 MEP 的丢包数、丢包率和平均丢包数，源 MEP 的丢包数、丢包率和平均丢包数。

2. 配置步骤

可在任意视图下执行本命令，开启单向丢包测试功能。

```
cfd slm service-instance instance-id mep mep-id { target-mac mac-address |  
target-mep target-mep-id } [ dot1p dot1p-value ] [ number number ] [ interval  
interval ]
```

1.6.6 配置单向时延测试功能

1. 功能简介

通过配置单向时延测试功能，可以检测 MEP 之间报文传输的单向时延，从而对链路的传输性能进行监测和管理。

2. 配置限制和指导

测试时要求源 MEP 和目标 MEP 的时间相同，否则时延值会出现负值或较大数值；用于单向时延变化测量时两端时间可以不同。

测试结果需在目标 MEP 上通过 **display cfd dm one-way history** 命令来显示。

3. 配置步骤

可在任意视图下执行本命令，开启单向时延测试功能。

```
cfld dm one-way service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ number number ]
```

1.6.7 配置双向时延测试功能

1. 功能简介

通过配置双向时延测试功能，可以检测 MEP 之间报文传输的双向时延、平均时延和时延变化值，从而对链路的传输性能进行监测和管理。

2. 配置步骤

可在任意视图下执行本命令，开启双向时延测试功能。

```
cfld dm two-way service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ dot1p dot1p-value ] [ number number ] [ interval interval ]
```

1.6.8 配置比特错误测试功能

1. 功能简介

通过配置比特错误测试功能，可以检测到链路上比特错误发生的情况，从而对链路的传输性能进行监测和管理。

2. 配置限制和指导

测试结果需在目标 MEP 上通过 **display cfd tst** 命令来显示。

3. 配置步骤

可在任意视图下执行本命令，开启比特错误测试功能。

```
cfld tst service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ number number ] [ length-of-test length ] [ pattern-of-test { all-zero | prbs } [ with-crc ] ]
```

1.7 配置以太网告警抑制功能

1. 配置限制和指导

以太网告警抑制功能可以配置在不支持或未配置 CFD 功能的设备上，但需要在网络中与 CFD 功能配合使用，因此需要在网络中配置 CFD 功能。

当端口加入聚合组后，可在该端口上配置以太网告警抑制功能，但不会生效；若端口在加入聚合组之前已配置以太网告警抑制功能，则该配置将立刻失效。当端口退出聚合组后，其上的以太网告警抑制功能相关配置才会生效。

在配置 EAIS 报文发送的 VLAN 范围之后，如果所配置 VLAN 与本设备所创建的 VLAN 交集为空，将不会发送 EAIS 报文；如果该交集内 VLAN 的数量大于 70、且 EAIS 报文的发送周期为 1 秒，将导致设备的 CPU 占用率很高，此时建议将 EAIS 报文的发送周期调整为 60 秒。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

- (2) 开启端口状态与 AIS 的联动功能。
`cfld ais-track link-status global`
 缺省情况下，端口状态与 AIS 联动功能处于关闭状态。
- (3) 进入二层以太网接口或二层聚合接口视图。
`interface interface-type interface-number`
- (4) 配置 EAIS 报文的发送级别。
`cfld ais-track link-status level level-value`
 缺省情况下，未配置 EAIS 报文的发送级别。
- (5) 配置 EAIS 报文的发送周期。
`cfld ais-track link-status period period-value`
 缺省情况下，未配置 EAIS 报文的发送周期。
- (6) 配置 EAIS 报文的发送 VLAN。
`cfld ais-track link-status vlan vlan-list`
 缺省情况下，EAIS 报文只在本端口的缺省 VLAN 内发送。
 EAIS 报文将在所配置 VLAN 与设备所创建 VLAN 的交集内发送。

1.8 CFD显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 CFD 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 CFD 的测试结果。

表1-2 CFD 显示和维护

操作	命令
显示MEP上AIS的配置和动态信息	<code>display cfd ais [service-instance instance-id [mep mep-id]]</code>
显示与端口状态相关联的AIS的配置和动态信息	<code>display cfd ais-track link-status [interface interface-type interface-number]</code>
显示单向时延的测试结果	<code>display cfd dm one-way history [service-instance instance-id [mep mep-id]]</code>
显示MEP上获得的LTR报文信息	<code>display cfd linktrace-reply [service-instance instance-id [mep mep-id]]</code>
显示自动发送LTM报文后收到的LTR报文信息	<code>display cfd linktrace-reply auto-detection [size size-value]</code>
显示MD的配置信息	<code>display cfd md</code>
显示MEP的属性和运行信息	<code>display cfd mep mep-id service-instance instance-id</code>
显示服务实例内的MEP列表	<code>display cfd meplist [service-instance instance-id]</code>
显示MP的信息	<code>display cfd mp [interface interface-type interface-number]</code>
显示远端MEP的信息	<code>display cfd remote-mep service-instance instance-id mep mep-id</code>

操作	命令
显示服务实例的配置信息	display cfd service-instance [<i>instance-id</i>]
显示CFD的开启状态	display cfd status
显示比特错误的测试结果	display cfd tst [service-instance <i>instance-id</i> [mep <i>mep-id</i>]]
清除单向时延的测试结果	reset cfd dm one-way history [service-instance <i>instance-id</i> [mep <i>mep-id</i>]]
清除比特错误的测试结果	reset cfd tst [service-instance <i>instance-id</i> [mep <i>mep-id</i>]]

1.9 CFD典型配置举例

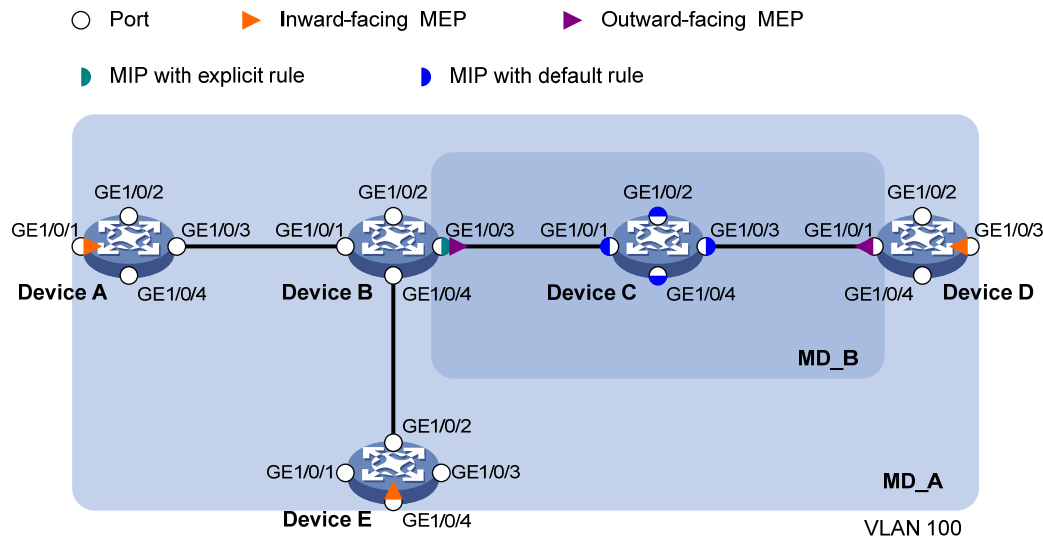
1.9.1 CFD基础配置举例

1. 组网需求

- 由五台设备组成的网络被划分为 MD_A 和 MD_B 两个 MD，其级别分别为 5 和 3，各设备的所有端口都属于 VLAN 100，且各 MD 中的 MA 均服务于该 VLAN，并假定 Device A~Device E 的 MAC 地址依次为 0010-FC01-6511、0010-FC02-6512、0010-FC03-6513、0010-FC04-6514 和 0010-FC05-6515。
- MD_A 的边界端口为 Device A 的 GigabitEthernet1/0/1、Device D 的 GigabitEthernet1/0/3 和 Device E 的 GigabitEthernet1/0/4，这些端口上都是内向 MEP；MD_B 的边界端口为 Device B 的 GigabitEthernet1/0/3 和 Device D 的 GigabitEthernet1/0/1，这些端口都是外向 MEP。
- 要求将 MD_A 的 MIP 规划在 Device B 上，并只在端口上有低级别 MEP 时配置。根据此规划，由于 Device B 的 GigabitEthernet1/0/3 上配置有 MD_B 的 MEP，因此在 Device B 上采用 Explicit 规则来创建 MD_A 的 MIP。
- 要求将 MD_B 的 MIP 规划在 Device C 上，并在其所有端口上配置。根据此规划，在 Device C 上配置 MD_B 的 MIP，且其创建规则为 Default 规则。
- 要求通过使用连续性检测功能来检测 MD_A 和 MD_B 中各 MEP 之间的连通状态，当检测到链路故障时，使用环回功能进行故障定位，并通过告警抑制功能和以太网告警抑制功能来减少故障告警的数量。
- 要求在获取到整个组网的状态后，分别使用链路跟踪功能、单向丢包测试功能、单向时延测试功能、双向时延测试功能和比特错误测试功能进行各种链路故障检测。

2. 组网图

图1-4 CFD 典型配置组网图



3. 配置步骤

(1) 配置 VLAN 和端口

请按照 [图 1-4](#) 在各设备上分别创建VLAN 100，并配置端口GigabitEthernet1/0/1～GigabitEthernet1/0/4 都属于VLAN 100。

(2) 开启 CFD 功能

在 Device A 上开启 CFD 功能。

```
<DeviceA> system-view
[DeviceA] cfd enable
```

Device B～Device E 的配置与 Device A 相似，配置过程略。

(3) 配置服务实例

在 Device A 上创建级别为 5 的 MD MD_A，并创建服务实例 1，该服务实例的 MA 以 VLAN 编号为名称，且服务于 VLAN 100。

```
[DeviceA] cfd md MD_A level 5
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 100
```

Device E 的配置与 Device A 相似，配置过程略。

在 Device B 上先创建级别为 5 的 MD MD_A，并创建服务实例 1，该服务实例的 MA 以 VLAN 编号为名称，且服务于 VLAN 100；再创建级别为 3 的 MD MD_B，并创建服务实例 2，该服务实例的 MA 以 VLAN 编号为名称，且服务于 VLAN 100。

```
[DeviceB] cfd md MD_A level 5
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 100
[DeviceB] cfd md MD_B level 3
[DeviceB] cfd service-instance 2 ma-id vlan-based md MD_B vlan 100
```

Device D 的配置与 Device B 相似，配置过程略。

在 Device C 上创建级别为 3 的 MD MD_B，并创建服务实例 2，该服务实例的 MA 以 VLAN 编号为名称，且服务于 VLAN 100。

```
[DeviceC] cfd md MD_B level 3
[DeviceC] cfd service-instance 2 ma-id vlan-based md MD_B vlan 100
```

(4) 配置 MEP

在 Device A 的服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的内向 MEP 1001。

```
[DeviceA] cfd meplist 1001 4002 5001 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

在 Device B 的服务实例 1 和 2 内分别配置 MEP 列表，在端口 GigabitEthernet1/0/3 上创建服务实例 2 内的外向 MEP 2001。

```
[DeviceB] cfd meplist 1001 4002 5001 service-instance 1
[DeviceB] cfd meplist 2001 4001 service-instance 2
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] cfd mep 2001 service-instance 2 outbound
[DeviceB-GigabitEthernet1/0/3] quit
```

在 Device D 的服务实例 1 和 2 内分别配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 2 内的外向 MEP 4001，然后在端口 GigabitEthernet1/0/3 上创建服务实例 1 内的内向 MEP 4002。

```
[DeviceD] cfd meplist 1001 4002 5001 service-instance 1
[DeviceD] cfd meplist 2001 4001 service-instance 2
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4001 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] cfd mep 4002 service-instance 1 inbound
[DeviceD-GigabitEthernet1/0/3] quit
```

在 Device E 的服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/4 上创建服务实例 1 内的内向 MEP 5001。

```
[DeviceE] cfd meplist 1001 4002 5001 service-instance 1
[DeviceE] interface gigabitethernet 1/0/4
[DeviceE-GigabitEthernet1/0/4] cfd mep 5001 service-instance 1 inbound
[DeviceE-GigabitEthernet1/0/4] quit
```

(5) 配置 MIP

在 Device B 的服务实例 1 内配置 MIP 的创建规则为 Explicit 规则。

```
[DeviceB] cfd mip-rule explicit service-instance 1
```

在 Device C 的服务实例 2 内配置 MIP 的创建规则为 Default 规则。

```
[DeviceC] cfd mip-rule default service-instance 2
```

(6) 配置连续性检测功能

在 Device A 的端口 GigabitEthernet1/0/1 上开启服务实例 1 内 MEP 1001 的 CCM 报文发送功能。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

在 Device B 的端口 GigabitEthernet1/0/3 上开启服务实例 2 内 MEP 2001 的 CCM 报文发送功能。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] cfd cc service-instance 2 mep 2001 enable
[DeviceB-GigabitEthernet1/0/3] quit
```

在 Device D 的端口 GigabitEthernet1/0/1 上开启服务实例 2 内 MEP 4001 的 CCM 报文发送功能，并在端口 GigabitEthernet1/0/3 上开启服务实例 1 内 MEP 4002 的 CCM 报文发送功能。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 4001 enable
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] cfd cc service-instance 1 mep 4002 enable
[DeviceD-GigabitEthernet1/0/3] quit
```

在 Device E 的端口 GigabitEthernet1/0/4 上开启服务实例 1 内 MEP 5001 的 CCM 报文发送功能。

```
[DeviceE] interface gigabitethernet 1/0/4
[DeviceE-GigabitEthernet1/0/4] cfd cc service-instance 1 mep 5001 enable
[DeviceE-GigabitEthernet1/0/4] quit
```

(7) 配置告警抑制功能

在 Device B 上开启告警抑制功能，并在服务实例 2 内配置 AIS 报文的发送级别为 5，发送周期为 1 秒。

```
[DeviceB] cfd ais enable
[DeviceB] cfd ais level 5 service-instance 2
[DeviceB] cfd ais period 1 service-instance 2
```

(8) 配置以太网告警抑制功能

在 Device B 上开启端口状态与 AIS 联动功能。

```
[DeviceB] cfd ais-track link-status global
```

在 Device B 的端口 GigabitEthernet1/0/3 上配置 EAIS 报文的发送级别为 5，发送周期为 60 秒，发送的 VLAN 范围为 VLAN 100。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] cfd ais-track link-status level 5
[DeviceB-GigabitEthernet1/0/3] cfd ais-track link-status period 60
[DeviceB-GigabitEthernet1/0/3] cfd ais-track link-status vlan 100
[DeviceB-GigabitEthernet1/0/3] quit
```

4. 验证配置

(1) 验证环回功能

当通过连续性检测功能检测到链路故障时，可以使用环回功能进行故障定位。譬如：

在 Device A 上启用环回功能，检查服务实例 1 内 MEP 1001 到 5001 的链路状况。

```
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 5001
Loopback to MEP 5001 with the sequence number start from 1001-43404:
Reply from 0010-fc05-6515: sequence number=1001-43404 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43405 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43406 time=5ms
```

```

Reply from 0010-fc05-6515: sequence number=1001-43407 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43408 time=5ms
Sent: 5          Received: 5          Lost: 0

```

(2) 验证链路跟踪功能

当通过连续性检测功能获取到整个组网的状态后，可以使用链路跟踪功能进行路径查找或故障定位。譬如：

在 **Device A** 的服务实例 1 内查找 MEP 1001 到 5001 的路径。

```

[DeviceA] cfd linktrace service-instance 1 mep 1001 target-mep 5001
Linktrace to MEP 5001 with the sequence number 1001-43462:
MAC address          TTL      Last MAC          Relay action
0010-fc05-6515       63      0010-fc02-6512   Hit

```

(3) 验证单向丢包测试功能

当通过连续性检测功能获取到整个组网的状态后，可以使用单向丢包测试功能检测链路状态。譬如：

在 **Device A** 上测试服务实例 1 内 MEP 1001 到 4002 的单向丢包情况。

```

[DeviceA] cfd slm service-instance 1 mep 1001 target-mep 4002
Reply from 0010-fc04-6514
Far-end frame loss: 10    Near-end frame loss: 20
Reply from 0010-fc04-6514
Far-end frame loss: 40    Near-end frame loss: 40
Reply from 0010-fc04-6514
Far-end frame loss: 0     Near-end frame loss: 10
Reply from 0010-fc04-6514
Far-end frame loss: 30    Near-end frame loss: 30

Average
Far-end frame loss: 20    Near-end frame loss: 25
Far-end frame loss rate: 25.00%    Near-end frame loss rate: 32.00%
Sent LMMs: 5    Received: 5    Lost: 0

```

(4) 验证单向时延测试功能

当通过连续性检测功能获取到整个组网的状态后，可以使用单向时延测试功能检测链路的单向时延。例如：

在 **Device A** 上测试服务实例 1 内 MEP 1001 到 4002 的单向时延。

```

[DeviceA] cfd dm one-way service-instance 1 mep 1001 target-mep 4002
5 lDMs have been sent. Please check the result on the remote device.

```

在 **Device D** 上显示服务实例 1 内 MEP 4002 上单向时延的测试结果。

```

[DeviceD] display cfd dm one-way history service-instance 1 mep 4002
Service instance: 1
MEP ID: 4002
Sent lDM total number: 0
Received lDM total number: 5
Frame delay: 10ms 9ms 11ms 5ms 5ms
Delay average: 8ms
Delay variation: 5ms 4ms 6ms 0ms 0ms
Variation average: 3ms

```

(5) 验证双向时延测试功能

当通过连续性检测功能获取到整个组网的状态后，可以使用双向时延测试功能检测链路的双向时延。例如：

在 Device A 上测试服务实例 1 内 MEP 1001 到 4002 的双向时延。

```
[DeviceA] cfd dm two-way service-instance 1 mep 1001 target-mep 4002
```

Frame delay:

Reply from 0010-fc04-6514: 2406us

Reply from 0010-fc04-6514: 2215us

Reply from 0010-fc04-6514: 2112us

Reply from 0010-fc04-6514: 1812us

Reply from 0010-fc04-6514: 2249us

Average: 2158us

Sent DMMS: 5 Received: 5 Lost: 0

Frame delay variation: 191us 103us 300us 437us

Average: 257us

(6) 验证比特错误测试功能

当通过连续性检测功能获取到整个组网的状态后，可以使用比特错误测试功能检测链路上比特错误的情况。例如：

在 Device A 上测试服务实例 1 内 MEP 1001 到 4002 的比特错误。

```
[DeviceA] cfd tst service-instance 1 mep 1001 target-mep 4002
```

5 TSTs have been sent. Please check the result on the remote device.

在 Device D 上显示服务实例 1 内 MEP 4002 上比特错误的测试结果。

```
[DeviceD] display cfd tst service-instance 1 mep 4002
```

Service instance: 1

MEP ID: 4002

Sent TST total number: 0

Received TST total number: 5

Received from 0010-fc01-6511, Bit True, sequence number 0

Received from 0010-fc01-6511, Bit True, sequence number 1

Received from 0010-fc01-6511, Bit True, sequence number 2

Received from 0010-fc01-6511, Bit True, sequence number 3

Received from 0010-fc01-6511, Bit True, sequence number 4

目 录

1 DLDP.....	1-1
1.1 DLDP简介.....	1-1
1.1.1 DLDP应用场景.....	1-1
1.1.2 DLDP基本概念.....	1-2
1.1.3 DLDP工作机制.....	1-3
1.2 DLDP配置限制和指导.....	1-5
1.3 DLDP配置任务简介.....	1-5
1.4 开启DLDP功能.....	1-6
1.5 配置Advertisement报文的发送间隔.....	1-6
1.6 配置DelayDown定时器的超时时间	1-6
1.7 配置DLDP发现单向链路后接口的关闭模式.....	1-7
1.8 配置DLDP的认证模式和密码.....	1-8
1.9 DLDP显示和维护.....	1-8
1.10 DLDP典型配置举例	1-8
1.10.1 DLDP配置举例（自动模式）	1-8
1.10.2 DLDP配置举例（手动模式）	1-12
1.10.3 DLDP配置举例（混合模式）	1-16

1 DLDP

1.1 DLDP简介

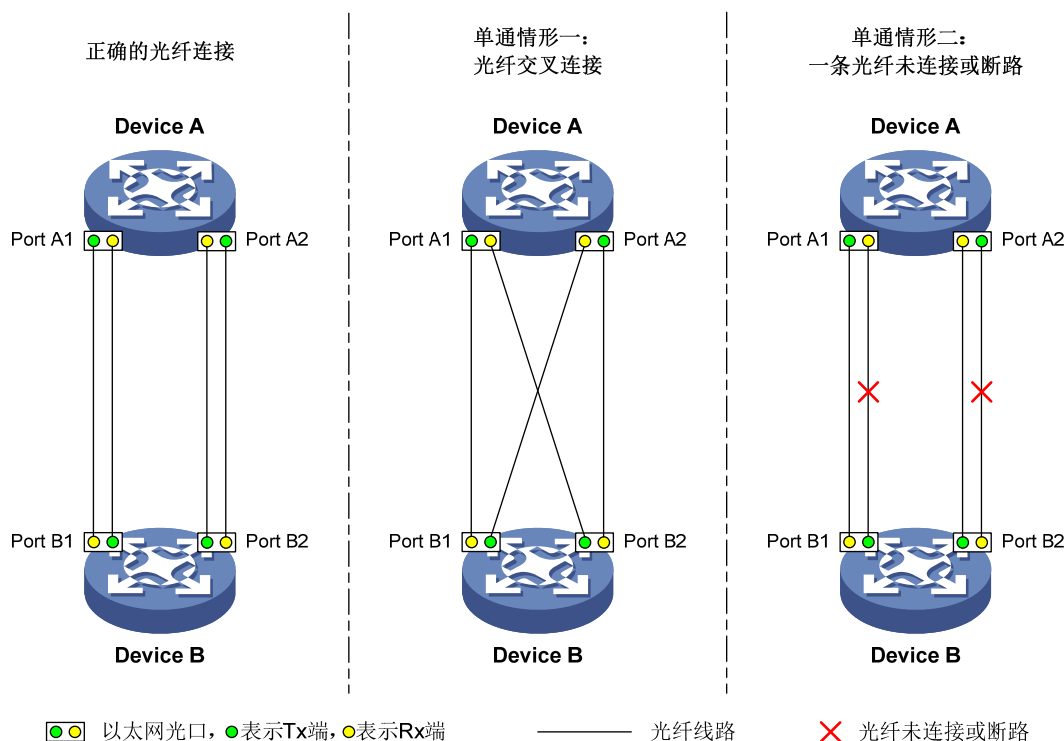
物理层的检测机制（如自动协商机制）负责进行物理信号和故障的检测，但在出现单向链路时，由于物理层仍处于连通状态，因此物理层检测机制无法发现设备间的通信异常。DLDP（Device Link Detection Protocol，设备链路检测协议）通过在链路层监控光纤或网线的链路状态，与物理层检测机制协同工作，检测链路连接是否正确、链路两端可否正常交互报文。当发现单向链路时，DLDP会根据用户配置自动关闭或由用户手工关闭相关接口，避免错误转发、环路等问题。

1.1.1 DLDP应用场景

在实际组网中，有时会出现单通现象，即一条链路上的两个端口，有且只有一端可收到另一端发来的链路层报文，此链路便称为单向链路。图 1-1 以光纤连接为例，示意了两种单通情形：一种是光纤交叉相连，另一种是一条光纤未连接或断路。

当发现单向链路时，DLDP 会根据用户配置自动关闭或由用户手工关闭相关接口，以防止网络问题的发生。

图1-1 光纤连接的两种单通情形示意图



1.1.2 DLDLP基本概念

1. DLDLP邻居状态

假设接口A和B同处一条链路上，若A能收到B发来的链路层报文，便将B称为A的DLDLP邻居，能够互相收发报文的两个接口互为邻居。DLDLP邻居的状态如 [表 1-1](#) 所示。

表1-1 DLDLP 邻居状态

状态	说明
Confirmed（确定）	链路双通时的DLDLP邻居状态
Unconfirmed（未确定）	发现新邻居但未确认链路双通时的DLDLP邻居状态

2. DLDLP接口状态

开启了DLDLP功能的接口简称DLDLP接口。DLDLP接口可以有一或多个DLDLP邻居，其状态与各DLDLP邻居的状态相关，具体如 [表 1-2](#) 所示。

表1-2 DLDLP 接口状态

状态	说明
Initial（初始）	当接口已开启DLDLP功能，但全局尚未开启DLDLP功能时的接口状态
Inactive（非活动）	当接口和全局均已开启DLDLP功能，但链路物理down时的接口状态
Bidirectional（双通）	当接口和全局均已开启DLDLP功能，且有至少一个处于确定状态下的邻居时的接口状态
Unidirectional（单通）	当接口和全局均已开启DLDLP功能，且没有处于确定状态下的邻居时的接口状态，处于此状态的接口只能收发DLDLP报文

3. DLDLP定时器

DLDLP在工作过程中使用到的定时器如 [表 1-3](#) 所示。

表1-3 DLDLP 定时器

定时器	说明
Advertisement发送定时器	Advertisement报文的发送间隔（缺省为5秒，可配）
Probe发送定时器	Probe报文的发送间隔（固定为1秒）
Echo等待定时器	对邻居进行探测时会启动此定时器，该定时器超时则删除邻居信息（固定为10秒）
邻居老化定时器	每个新邻居的加入都要建立邻居表项，当邻居处于确定状态时启动邻居老化定时器，当收到邻居的Advertisement报文时刷新邻居表项的邻居老化定时器。如果该定时器超时，则启动该邻居的加强探测定时器和Echo等待定时器。邻居老化定时器的值是Advertisement发送定时器的值的3倍
加强探测定时器	Probe报文的发送间隔（固定为1秒） 若邻居老化定时器超时，则启动该邻居的加强探测定时器并发送Probe报文，同时启动Echo等待定时器
DelayDown定时器	接口物理down时不会立即删除所有邻居，而是先启动DelayDown定时器（缺省为1秒，可配），该定时器超时后再核对接口的物理状态：若为down，则删除DLDLP邻居信息；若为up，则不进行任何处理

定时器	说明
恢复探测定时器	RecoverProbe报文的发送间隔（固定为2秒）。处于单通状态的接口会定期发送RecoverProbe报文来检测单向链路是否恢复

4. DLDP认证模式

进行DLDP认证，可以防止网络攻击和恶意探测，DLDP的认证模式如 表 1-4 所示。

表1-4 DLDP 认证模式

认证模式	DLDP 报文发送端的处理	DLDP 报文接收端的处理
不认证	将DLDP报文的认证字段置为全0	将接收的DLDP报文的认证信息与本端配置进行比较，若一致则认证通过，否则丢弃该报文
明文认证	将DLDP报文的认证字段置为明文认证密码	
MD5认证	将DLDP报文的认证字段置为用MD5算法加密后的密码摘要	

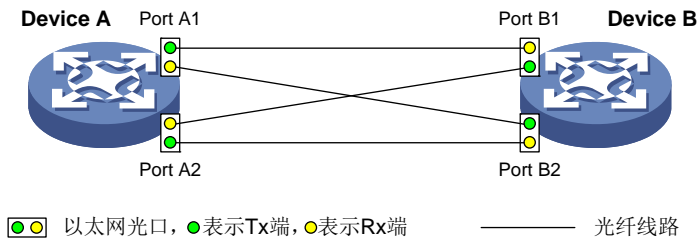
1.1.3 DLDP工作机制

1. 单邻居检测

当两台设备通过光纤或网线直接相连时，可以在这两台设备之间启用 DLDP 协议来检测单向链路，此时这两台设备的接口互为 DLDP 邻居，因此称为单邻居检测。下面分两种情况分别介绍单邻居的单向链路检测过程。

(1) 开启 DLDP 功能前链路已出现单通

图1-2 光纤交叉连接示意图



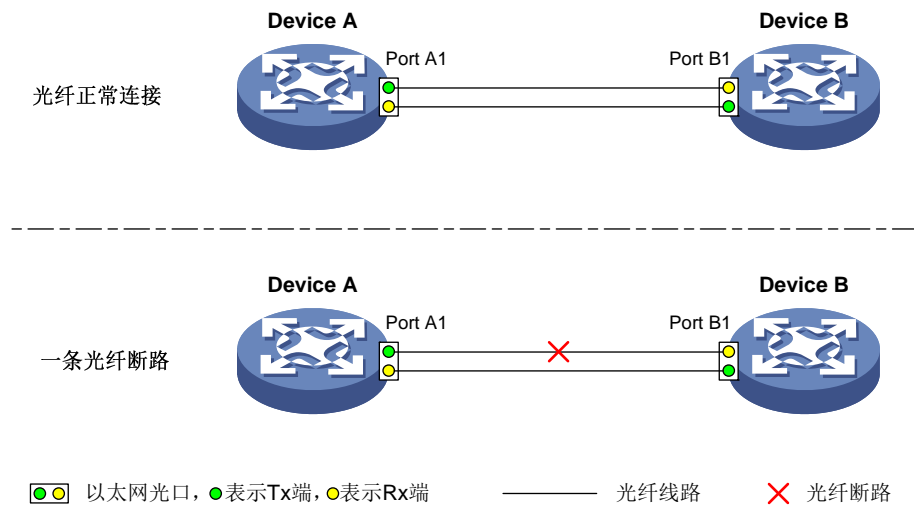
如 图 1-2 所示，在开启DLDP功能之前，Device A和Device B之间的光纤就已交叉连接。当开启DLDP功能后，处于up状态的四个接口都进入单通状态，并向外发送RecoverProbe报文。下面以Port A1 为例介绍单向链路的检测过程：

- a. Port A1 收到 Port B2 发来的 RecoverProbe 报文后，回复 RecoverEcho 报文。
- b. 由于 Port B2 无法收到 Port A1 发来的 RecoverEcho 报文，因此不会与 Port A1 建立邻居关系。
- c. Port B1 虽能收到 Port A1 发来的 RecoverEcho 报文，但由于该报文并不是回复给 Port B1 的，因此 Port B1 也不会与 Port A1 建立邻居关系。

其它三个接口上的检测过程与 Port A1 类似，这四个接口将始终处于单通状态。

(2) 开启 DLDP 功能后链路才出现单通

图1-3 一条光纤断路示意图



如 图 1-3 所示，Device A 和 Device B 通过光纤相连。在开启 DLDP 功能之后，光纤连接起初是正常的，Port A1 与 Port B1 之间的双通邻居建立过程如下：

- 处于物理 up 状态的 Port A1 先进入单通状态，向外发送 RecoverProbe 报文。
- Port B1 收到 RecoverProbe 报文后，回复 RecoverEcho 报文。
- Port A1 收到 RecoverEcho 报文后，发现该报文中携带的邻居信息与本机的相同，于是与 Port B1 建立确定的邻居关系，接口状态由单通变为双通，启动该邻居的老化定时器并定期发送 Advertisement 报文。
- Port B1 收到 Advertisement 报文后与 Port A1 建立未确定的邻居关系，为该邻居启动 Echo 等待定时器和 Probe 发送定时器，定期发送 Probe 报文。
- Port A1 收到 Probe 报文后，回复 Echo 报文。
- Port B1 收到 Echo 报文后，发现该报文中携带的邻居信息和本机保存的相同，于是将邻居状态由未确定切换为确定，接口状态则由单通切换为双通，启动该邻居的老化定时器并定期发送 Advertisement 报文。

至此，Port A1 与 Port B1 之间的双通邻居关系建立完毕。

此后，假设 Port B1 的 Rx 端突发故障而无法接收信号，该接口将物理 down 并进入非活动状态，但此时由于其 Tx 端尚能发送信号给 Port A1，因此 Port A1 还处于 up 状态。Port A1 在邻居老化定时器超时后，将启用加强探测定时器和 Echo 等待定时器，并向邻居 Port B1 发送 Probe 报文；而由于 Port A1 的 Tx 端已断路，Echo 等待定时器超时后将收不到 Port B1 回复的 Echo 报文，于是 Port A1 进入单通状态，并发送 Disable 报文通知对端。同时，Port A1 删除邻居 Port B1，并启动恢复探测定时器以检测链路是否恢复。在此过程中，Port B1 将一直处于非活动状态。



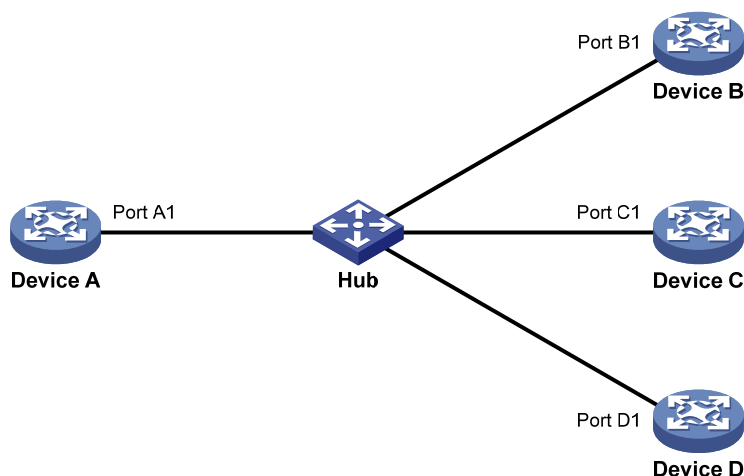
说明

当接口物理 down 之后，DLDP 将尝试发送 LinkDown 报文，对端收到此报文后会直接删除邻居表项，以缩短故障发现时间。但由于发送此报文时接口已物理 down，因此能否发送成功取决于接口的 Tx 端是否完好。

2. 多邻居检测

当多台设备通过 Hub 相连时，也可以在这些设备之间启用 DLDP 协议来检测单向链路，此时每个接口都会检测到一个以上的 DLDP 邻居，因此称为多邻居检测。在多邻居组网环境中，为了能正确检测出单向链路，要求在所有与 Hub 相连的接口上都启用 DLDP，接口一旦发现没有确定的邻居，便进入单通状态。

图1-4 多邻居组网示意图



如 图 1-4 所示，Device A~Device D 都通过一台 Hub 相连，各设备都支持 DLDP。当 Port A1、Port B1 和 Port C1 发现与 Port D1 的连接出错后，都将删除该邻居，但仍保持双通状态。

1.2 DLDP配置限制和指导

- 为确保 DLDP 功能正常工作，要保证两端设备的 DLDP 功能都处于开启状态，且 Advertisement 报文的发送间隔、DLDP 认证模式和密码都相同。
- 为确保 DLDP 功能正常工作，请将两端接口的双工模式配置为全双工、速率配置为相同的强制速率。

1.3 DLDP配置任务简介

DLDP 配置任务如下：

- (1) [开启DLDP功能](#)
- (2) （可选）[配置Advertisement报文的发送间隔](#)
- (3) （可选）[配置DelayDown定时器的超时时间](#)

- (4) (可选) [配置DLDP发现单向链路后接口的关闭模式](#)
- (5) (可选) [配置DLDP的认证模式和密码](#)

1.4 开启DLDP功能

- (1) 进入系统视图。
system-view
- (2) 全局开启 DLDP 功能。
dldp global enable
缺省情况下，DLDP 功能处于全局关闭状态。
- (3) 进入以太网接口视图。
interface interface-type interface-number
- (4) 开启接口的 DLDP 功能。
dldp enable
缺省情况下，接口上的 DLDP 功能处于关闭状态。

1.5 配置Advertisement报文的发送间隔

1. 功能简介

通过合理调整 Advertisement 报文的发送间隔，可使 DLDP 在不同的网络环境下都能够及时发现单向链路（建议采用缺省值）。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 配置 Advertisement 报文的发送间隔。
dldp interval interval
缺省情况下，Advertisement 报文的发送间隔为 5 秒。

1.6 配置DelayDown定时器的超时时间

1. 功能简介

有些接口当其 Tx 端发生故障时会引起 Rx 端光信号的抖动（表现为该接口 down 后随即又 up），为避免在这种情况下错误清除邻居信息，DLDP 会在接口物理 down 时先启动 DelayDown 定时器，该定时器超时后再核对接口的物理状态：若为 down，则删除 DLDP 邻居信息；若为 up，则不进行任何处理。

本配置将应用于所有开启了 DLDP 功能的接口上。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 配置 DelayDown 定时器的超时时间。

dldp delaydown-timer time

缺省情况下，DelayDown 定时器的超时时间为 1 秒。

1.7 配置DLDP发现单向链路后接口的关闭模式

1. 功能简介

当 DLDP 检测到单向链路时，可以采用以下方式关闭单通接口：

- 自动模式：在此模式下，若 DLDP 检测到单向链路，会自动关闭单通接口；若单向链路恢复为双向链路，则 DLDP 会自动打开被关闭的接口。
- 手动模式：在此模式下，若 DLDP 检测到单向链路，不会直接关闭单通接口，需要用户手工将其关闭；当用户想知道链路是否恢复为双向链路时，需要执行 **undo shutdown** 命令打开端口重新检测链路，若检测到链路恢复为双向链路，则接口恢复正常。当网络性能较差、设备业务量较大或 CPU 利用率较高时，都容易造成 DLDP 对单通的误判而自动关闭接口，手动模式就是为了避免这种误判而采取的一种折中方案。
- 混合模式：在此模式下，若 DLDP 检测到单向链路，则会自动关闭单通接口；当用户想知道链路是否恢复为双向链路时，需要执行 **undo shutdown** 命令打开端口重新检测链路，若检测到链路恢复为双向链路，则接口恢复正常。

2. 配置限制和指导

用户既可在系统视图下配置对所有接口都有效的关闭模式，也可在接口视图下配置只对当前接口有效的关闭模式，后者的配置优先级较高。

如果想在接口上配置以太网 OAM 远端环回功能，建议先将 DLDP 发现单向链路后接口的关闭模式配置为手动模式，否则 DLDP 收到了由本接口发出的报文后会认为出现单向链路而自动关闭接口，从而导致以太网 OAM 远端环回失败。有关以太网 OAM 远端环回的详细介绍，请参见“可靠性配置指导”中的“以太网 OAM”。

3. 全局配置DLDP发现单向链路后接口的关闭模式

- (1) 进入系统视图。

system-view

- (2) 全局配置 DLDP 发现单向链路后接口的关闭模式。

dldp unidirectional-shutdown { auto | hybrid | manual }

缺省情况下，DLDP 发现单向链路后，所有接口的关闭模式为自动模式。

4. 在接口上配置DLDP发现单向链路后接口的关闭模式

- (1) 进入系统视图。

system-view

- (2) 进入以太网接口视图。

interface interface-type interface-number

- (3) 在接口上配置 DLDP 发现单向链路后接口的关闭模式。

dldp port unidirectional-shutdown { auto | hybrid | manual }

缺省情况下，DLDP 发现单向链路后，接口的关闭模式采用全局配置。

1.8 配置DLDP的认证模式和密码

1. 功能简介

通过配置适当的 DLDP 认证模式和密码，可以防止网络攻击和恶意探测。DLDP 的认证模式包括：不认证、明文认证和 MD5 认证。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置当前设备与邻居设备间的 DLDP 认证模式。

```
dldp authentication-mode { md5 | none | simple }
```

缺省情况下，当前设备与邻居设备间的 DLDP 认证模式为不认证。

(3) 配置当前设备与邻居设备间的 DLDP 认证密码。

```
dldp authentication-password { cipher | simple } string
```

缺省情况下，未配置当前设备与邻居设备间的 DLDP 认证密码。

在配置认证模式为明文认证或 MD5 认证后若未配置认证密码，则认证模式将仍不生效。

1.9 DLDP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 DLDP 的运行情况及报文统计信息，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 DLDP 报文统计信息。

表1-5 DLDP 显示和维护

操作	命令
显示DLDP的全局配置信息和接口的DLDP信息	display dldp [interface interface-type interface-number]
显示接口的DLDP报文统计信息	display dldp statistics [interface interface-type interface-number]
清除接口的DLDP报文统计信息	reset dldp statistics [interface interface-type interface-number]

1.10 DLDP典型配置举例

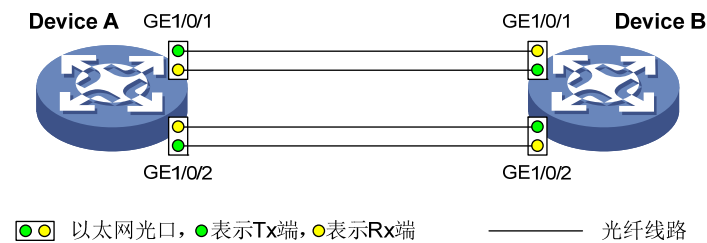
1.10.1 DLDP配置举例（自动模式）

1. 组网需求

- Device A 和 Device B 各自的接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 之间分别通过一对光纤进行连接。
- 要求通过配置 DLDP 功能，使接口上发生单向链路故障后由 DLDP 自动关闭故障接口，并在网络管理员排除故障后，故障接口自动恢复。

2. 组网图

图1-5 自动关闭单向链路配置组网图



3. 配置步骤

(1) 配置 Device A

全局开启 DLDP 功能。

```
<DeviceA> system-view
[DeviceA] dldp global enable
```

在接口 GigabitEthernet1/0/1 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

在接口 GigabitEthernet1/0/2 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

全局配置 DLDP 发现单向链路后接口的关闭模式为自动模式。

```
[DeviceA] dldp unidirectional-shutdown auto
```

(2) 配置 Device B

全局开启 DLDP 功能。

```
<DeviceB> system-view
[DeviceB] dldp global enable
```

在接口 GigabitEthernet1/0/1 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

在接口 GigabitEthernet1/0/2 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。


```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit
# 全局配置 DLDP 发现单向链路后接口的关闭模式为自动模式。
[DeviceB] dldp unidirectional-shutdown auto
```

4. 验证配置

配置完成后，通过使用 **display dldp** 命令可以查看 DLDP 的全局配置信息和接口上的 DLDP 信息。例如：

查看 Device A 上 DLDP 的全局配置信息和所有接口上的 DLDP 信息。

```
[DeviceA] display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Auto
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

Interface GigabitEthernet1/0/1
DLDP port state: Bidirectional
DLDP port unidirectional-shutdown mode: None
Number of the port's neighbors: 1
Neighbor MAC address: 0023-8956-3600
Neighbor port index: 1
Neighbor state: Confirmed
Neighbor aged time: 11s

Interface GigabitEthernet1/0/2
DLDP port state: Bidirectional
DLDP port unidirectional-shutdown mode: None
Number of the port's neighbors: 1
Neighbor MAC address: 0023-8956-3600
Neighbor port index: 2
Neighbor state: Confirmed
Neighbor aged time: 12s
```

以上信息表明，接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 上的 DLDP 接口状态均为 **Bidirectional**，说明这两个接口所在的链路均处于双通状态。

在 Device A 上配置允许日志信息输出到当前终端，且输出的日志信息最低为 6 级。

```
[DeviceA] quit
<DeviceA> terminal monitor
The current terminal is enabled to display logs.
<DeviceA> terminal logging level 6
```

此后某刻，Device A 上输出了以下日志信息：

```
<DeviceA>%Jul 11 17:40:31:089 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link
status is DOWN.
```

```
%Jul 11 17:40:31:091 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is DOWN.
%Jul 11 17:40:31:677 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is
DOWN.
%Jul 11 17:40:31:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is DOWN.
%Jul 11 17:40:38:544 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is
UP.
%Jul 11 17:40:38:836 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is
UP.
```

以上信息表明，接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的物理状态都先 down 后 up，而链路状态则都 down 后未再 up。网络管理员进行进一步检查：

查看 Device A 上 DLDP 的全局配置信息和所有接口上的 DLDP 信息。

```
<DeviceA> display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Auto
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

Interface GigabitEthernet1/0/1
DLDP port state: Unidirectional
DLDP port unidirectional-shutdown mode: None
Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
DLDP port state: Unidirectional
DLDP port unidirectional-shutdown mode: None
Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

以上信息表明，接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上的 DLDP 接口状态均为 Unidirectional，说明这两个接口所在的链路均处于单通状态。

由此可知，DLDP 在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上都检测到了单向链路，并自动关闭了这两个接口。经检查，网络管理员发现连接 Device A 和 Device B 的两对光纤被错误地进行了交叉连接，于是他将这两对光纤重新进行了正确连接。随后，Device A 上输出了以下日志信息：

```
<DeviceA>%Jul 11 17:42:57:709 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link
status is DOWN.
%Jul 11 17:42:58:603 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is
DOWN.
%Jul 11 17:43:02:342 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is
UP.
%Jul 11 17:43:02:343 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-3600, and the port
index is 1.
%Jul 11 17:43:02:344 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/1.
```

```
%Jul 11 17:43:02:353 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is UP.
%Jul 11 17:43:02:357 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is
UP.
%Jul 11 17:43:02:362 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-3600, and the port
index is 2.
%Jul 11 17:43:02:362 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/2.
%Jul 11 17:43:02:368 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is UP.
```

以上信息表明,接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的物理状态和链路状态均已 up,并各自确定了 DLDP 邻居,所在链路也变为双通状态。

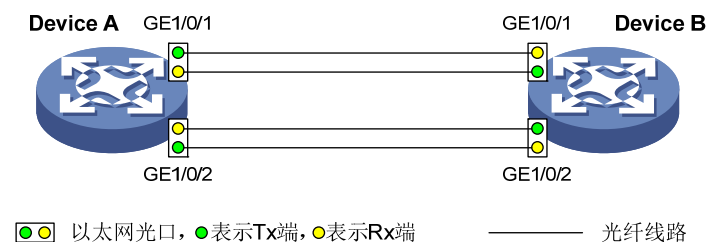
1.10.2 DLDP配置举例（手动模式）

1. 组网需求

- Device A 和 Device B 各自的接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 之间分别通过一对光纤进行连接。
- 要求通过配置 DLDP 功能,使接口上发生单向链路故障后,需要由网络管理员手工关闭和恢复故障接口。

2. 组网图

图1-6 手动关闭单向链路配置组网图



3. 配置步骤

(1) 配置 Device A

全局开启 DLDP 功能。

```
<DeviceA> system-view
[DeviceA] dldp global enable
```

在接口 GigabitEthernet1/0/1 上配置双工模式为全双工、接口速率为 1000Mbps, 并开启 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

在接口 GigabitEthernet1/0/2 上配置双工模式为全双工、接口速率为 1000Mbps, 并开启 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
# 全局配置 DLDP 发现单向链路后接口的关闭模式为手动模式。
[DeviceA] dldp unidirectional-shutdown manual
```

(2) 配置 Device B

```
# 全局开启 DLDP 功能。
<DeviceB> system-view
[DeviceB] dldp global enable
# 在接口 GigabitEthernet1/0/1 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit
# 在接口 GigabitEthernet1/0/2 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit
# 全局配置 DLDP 发现单向链路后接口的关闭模式为手动模式。
[DeviceB] dldp unidirectional-shutdown manual
```

4. 验证配置

配置完成后，通过使用 **display dldp** 命令可以查看 DLDP 的全局配置信息和接口上的 DLDP 信息。例如：

查看 Device A 上 DLDP 的全局配置信息和所有接口上的 DLDP 信息。

```
[DeviceA] display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Manual
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

Interface GigabitEthernet1/0/1
DLDP port state: Bidirectional
DLDP port unidirectional-shutdown mode: None
Number of the port's neighbors: 1
Neighbor MAC address: 0023-8956-3600
Neighbor port index: 1
```

```

Neighbor state: Confirmed
Neighbor aged time: 11s

Interface GigabitEthernet1/0/2
  DLDP port state: Bidirectional
  DLDP port unidirectional-shutdown mode: None
  Number of the port's neighbors: 1
    Neighbor MAC address: 0023-8956-3600
    Neighbor port index: 2
    Neighbor state: Confirmed
    Neighbor aged time: 12s

```

以上信息表明，接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 上的 DLDP 接口状态均为 **Bidirectional**，说明这两个接口所在的链路均处于双通状态。

在 **Device A** 上配置允许日志信息输出到当前终端，且输出的日志信息最低为 6 级。

```

[DeviceA] quit
<DeviceA> terminal monitor
The current terminal is enabled to display logs.
<DeviceA> terminal logging level 6

```

此后某刻，网络管理员在 **Device A** 上看到如下 Log 信息：

```

<DeviceA>%Jul 12 08:29:17:786 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link
status is DOWN.
%Jul 12 08:29:17:787 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is DOWN.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is
DOWN.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is DOWN.
%Jul 12 08:29:25:004 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is
UP.
%Jul 12 08:29:25:005 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is UP.
%Jul 12 08:29:25:893 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is
UP.
%Jul 12 08:29:25:894 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is UP.

```

以上信息表明，接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 的物理状态和链路状态都先 down 后 up。网络管理员进行进一步检查：

查看 **Device A** 上 DLDP 的全局配置信息和所有接口上的 DLDP 信息。

```

<DeviceA> display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Manual
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

```

```

Interface GigabitEthernet1/0/1
  DLDP port state: Unidirectional

```

```
DLDP port unidirectional-shutdown mode: None
Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

```
Interface GigabitEthernet1/0/2
```

```
DLDP port state: Unidirectional
```

```
DLDP port unidirectional-shutdown mode: None
```

```
Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

以上信息表明，接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 上的 **DLDP** 接口状态均为 **Unidirectional**，说明这两个接口所在的链路均处于单通状态。

由此可知，**DLDP** 在接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 上都检测到了单向链路，但并未关闭这两个接口。经检查，网络管理员发现连接 **Device A** 和 **Device B** 的两对光纤被错误地进行了交叉连接，于是他分别将 **Device A** 的两个接口手工关闭：

关闭接口 **GigabitEthernet1/0/1**。

```
<DeviceA> system-view
```

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] shutdown
```

Device A 上随即输出以下日志信息：

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:34:23:717 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/1 link status is DOWN.
```

```
%Jul 12 08:34:23:718 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is DOWN.
```

```
%Jul 12 08:34:23:778 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is
DOWN.
```

```
%Jul 12 08:34:23:779 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is DOWN.
```

以上信息表明，接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 的物理状态和链路状态均已变为 **down**。

关闭接口 **GigabitEthernet1/0/2**。

```
[DeviceA-GigabitEthernet1/0/1] quit
```

```
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] shutdown
```

然后，网络管理员将连接 **Device A** 和 **Device B** 的两对光纤重新进行了正确连接，检查无误后，他又分别将 **Device A** 的两个接口重新打开：

打开接口 **GigabitEthernet1/0/2**。

```
[DeviceA-GigabitEthernet1/0/2] undo shutdown
```

Device A 上随即输出以下日志信息：

```
[DeviceA-GigabitEthernet1/0/2]%Jul 12 08:46:17:677 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/2 link status is UP.
```

```
%Jul 12 08:46:17:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is UP.
```

```
%Jul 12 08:46:17:959 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-3600, and the port
index is 2.
```

```
%Jul 12 08:46:17:959 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/2.
```

以上信息表明，接口 GigabitEthernet1/0/2 的物理状态和链路状态均已 up，并确定了 DLDP 邻居，所在链路也变为双通状态。

打开接口 GigabitEthernet1/0/1。

```
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
```

Device A 上随即输出以下日志信息：

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:48:25:952 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/1 link status is UP.

%Jul 12 08:48:25:952 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-3600, and the port
index is 1.

%Jul 12 08:48:25:953 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is UP.

%Jul 12 08:48:25:953 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/1.
```

以上信息表明，接口 GigabitEthernet1/0/1 的物理状态和链路状态均已 up，并确定了 DLDP 邻居，所在链路也变为双通状态。

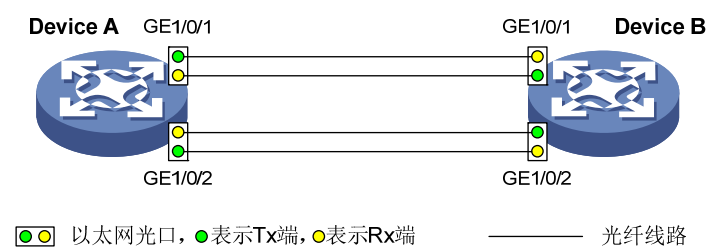
1.10.3 DLDP配置举例（混合模式）

1. 组网需求

- Device A 和 Device B 各自的接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 之间分别通过一对光纤进行连接。
- 要求通过配置 DLDP 功能，使接口上发生单向链路故障后由 DLDP 自动关闭故障接口，并在网络管理员排除故障后，手工恢复故障接口。

2. 组网图

图1-7 DLDP 配置组网图（混合模式）



3. 配置步骤

(1) 配置 Device A

全局开启 DLDP 功能。

```
<DeviceA> system-view
[DeviceA] dldp global enable
```

在接口 GigabitEthernet1/0/1 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

在接口 **GigabitEthernet1/0/2** 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

全局配置 DLDP 发现单向链路后接口的关闭模式为混合模式。

```
[DeviceA] dldp unidirectional-shutdown hybrid
```

(2) 配置 Device B

全局开启 DLDP 功能。

```
<DeviceB> system-view
[DeviceB] dldp global enable
```

在接口 **GigabitEthernet1/0/1** 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

在接口 **GigabitEthernet1/0/2** 上配置双工模式为全双工、接口速率为 1000Mbps，并开启 DLDP 功能。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

全局配置 DLDP 发现单向链路后接口的关闭模式为混合模式。

```
[DeviceB] dldp unidirectional-shutdown hybrid
```

4. 验证配置

配置完成后，通过使用 **display dldp** 命令可以查看 DLDP 的全局配置信息和接口上的 DLDP 信息。例如：

查看 Device A 上 DLDP 的全局配置信息和所有接口上的 DLDP 信息。

```
[DeviceA] display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Hybrid
DLDP delaydown-timer value: 1s
Number of enabled ports: 2
```



```
Interface GigabitEthernet1/0/1
  DLDP port state: Bidirectional
  DLDP port unidirectional-shutdown mode: None
  Number of the port's neighbors: 1
    Neighbor MAC address: 0023-8956-3600
    Neighbor port index: 1
    Neighbor state: Confirmed
    Neighbor aged time: 11s
```

```
Interface GigabitEthernet1/0/2
  DLDP port state: Bidirectional
  DLDP port unidirectional-shutdown mode: None
  Number of the port's neighbors: 1
    Neighbor MAC address: 0023-8956-3600
    Neighbor port index: 2
    Neighbor state: Confirmed
    Neighbor aged time: 12s
```

以上信息表明，接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 上的 DLDP 接口状态均为 **Bidirectional**，说明这两个接口所在的链路均处于双通状态。

在 **Device A** 上配置允许日志信息输出到当前终端，且输出的日志信息最低为 6 级。

```
[DeviceA] quit
<DeviceA> terminal monitor
The current terminal is enabled to display logs.
<DeviceA> terminal logging level 6
```

此后某刻，**Device A** 上输出了以下日志信息：

```
<DeviceA>%Jan 4 07:16:06:556 2011 DeviceA DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface
GigabitEthernet1/0/1 was deleted because the neighbor was aged. The neighbor's system MAC
is 0023-8956-3600, and the port index is 162.
%Jan 4 07:16:06:560 2011 DeviceA DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface
GigabitEthernet1/0/2 was deleted because the neighbor was aged. The neighbor's system MAC
is 0023-8956-3600, and the port index is 165.
%Jan 4 07:16:06:724 2011 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/1 changed to down.
%Jan 4 07:16:06:730 2011 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to down.
%Jan 4 07:16:06:736 2011 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/1 changed to down.
%Jan 4 07:16:06:738 2011 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/2 changed to down.
%Jan 4 07:16:07:152 2011 DeviceA DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a
unidirectional link on interface GigabitEthernet1/0/1. DLDP automatically shut down the
interface. Please manually bring up the interface.
%Jan 4 07:16:07:156 2011 DeviceA DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a
unidirectional link on interface GigabitEthernet1/0/2. DLDP automatically shut down the
interface. Please manually bring up the interface.
```

以上信息表明，接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 的物理状态与链路状态都 **down** 了。网络管理员进行进一步检查：

查看 Device A 上 DLDP 的全局配置信息和所有接口上的 DLDP 信息。

```
<DeviceA> display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Hybrid
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

Interface GigabitEthernet1/0/1
DLDP port state: Inactive
DLDP port unidirectional-shutdown mode: None
Number of the port's neighbors: 0 (Maximum number ever detected: 1)
Interface GigabitEthernet1/0/2
DLDP port state: Inactive
DLDP port unidirectional-shutdown mode: None
Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

以上信息表明,接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上的 DLDP 接口状态均为 Inactive,说明这两个接口所在的链路均处于去激活状态。

由此可知,DLDP 在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上都检测到了单向链路,且自动关闭了这两个接口。

经检查,网络管理员发现 Device B 上连接 DeviceA 的两个端口上的发光光纤被错误的进行了交叉连接。然后,网络管理员将光纤重新进行正确连接,检查无误后,再将 Device A 的两个接口重新打开:

打开接口 GigabitEthernet1/0/1。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
```

Device A 上随即输出以下日志信息:

```
[DeviceA-GigabitEthernet1/0/1]%Jan 4 07:33:26:574 2011 DeviceA IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/1 changed to up.
%Jan 4 07:33:57:562 2011 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-3600, and the port
index is 162.
%Jan 4 07:33:57:563 2011 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/1.
%Jan 4 07:33:57:590 2011 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/1 changed to up.
%Jan 4 07:33:57:609 2011 DeviceA STP/6/STP_DETECTED_TC: Instance 0's port
GigabitEthernet1/0/1 detected a topology change.
```

以上信息表明,接口 GigabitEthernet1/0/1 的物理状态和链路状态均已 up,并确定了 DLDP 邻居,所在链路也变为双通状态。

打开接口 GigabitEthernet1/0/2。

```
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface GigabitEthernet1/0/2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
```

Device A 上随即输出以下日志信息：

```
[DeviceA-GigabitEthernet1/0/2]%Jan  4 07:35:26:574 2011 DeviceA IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/2 changed to up.
%Jan  4 07:35:57:562 2011 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-3600, and the port
index is 162.
%Jan  4 07:35:57:563 2011 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/2.
%Jan  4 07:35:57:590 2011 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/2 changed to up.
%Jan  4 07:35:57:609 2011 DeviceA STP/6/STP_DETECTED_TC: Instance 0's port
GigabitEthernet1/0/2 detected a topology change.
```

以上信息表明，接口 **GigabitEthernet1/0/2** 的物理状态和链路状态均已 **up**，并确定了 **DLDP** 邻居，所在链路也变为双通状态。

目 录

1 RRPP	1-1
1.1 RRPP简介	1-1
1.1.1 RRPP组网模型.....	1-1
1.1.2 RRPP协议报文.....	1-3
1.1.3 RRPP定时器.....	1-4
1.1.4 RRPP运行机制.....	1-4
1.1.5 RRPP典型组网.....	1-5
1.1.6 协议规范.....	1-7
1.2 RRPP与硬件适配关系	1-7
1.3 RRPP配置限制和指导	1-7
1.4 RRPP配置任务简介	1-7
1.5 RRPP配置准备	1-8
1.6 创建RRPP域	1-8
1.7 配置控制VLAN.....	1-8
1.8 配置保护VLAN.....	1-9
1.9 配置RRPP环	1-9
1.9.1 配置准备.....	1-9
1.9.2 配置RRPP端口.....	1-9
1.9.3 配置RRPP节点.....	1-10
1.10 激活RRPP域.....	1-12
1.11 配置RRPP定时器.....	1-12
1.12 配置RRPP环组.....	1-13
1.13 开启RRPP的告警功能.....	1-13
1.14 RRPP显示和维护.....	1-14
1.15 RRPP典型配置举例.....	1-14
1.15.1 单环配置举例	1-14
1.15.2 相交环配置举例	1-16
1.16 RRPP常见故障处理.....	1-22
1.16.1 链路正常状态下主节点收不到Hello报文.....	1-22

1 RRPP

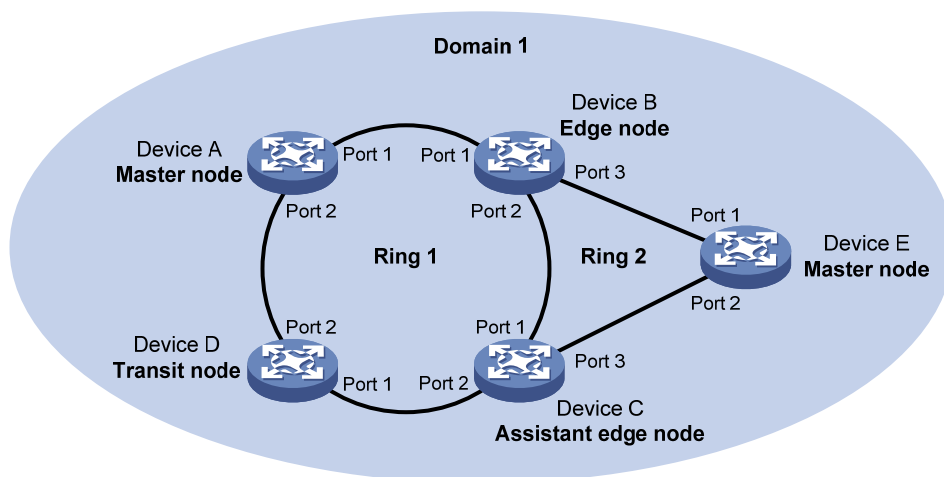
1.1 RRPP简介

RRPP（Rapid Ring Protection Protocol，快速环网保护协议）是一个专门应用于以太网环的链路层协议。当以太网环完整时它能够防止数据环路引起的广播风暴，而当以太网环上的链路断开时它能迅速恢复环网上各个节点之间的通信链路。与生成树协议相比，RRPP 的收敛速度更快，且收敛时间与环网上节点数无关，可应用于网络直径较大的网络。

1.1.1 RRPP组网模型

如 图 1-1 所示，RRPP将以太网环上的设备划分为不同角色的节点，各节点之间通过收发和处理RRPP协议报文来检测环网状态、传递环网拓扑变化信息。

图1-1 RRPP 组网示意图



1. RRPP域

域 ID 是 RRPP 域的唯一标识，一个 RRPP 域由具有相同域 ID 和控制 VLAN、且相互连通的设备构成。一个 RRPP 域包含以下元素：主环、子环、控制 VLAN、主节点、传输节点、边缘节点、辅助边缘节点、主端口、副端口、公共端口和边缘端口等。

如 图 1-1 所示，Domain 1 就是一个RRPP域，它包含了两个RRPP环Ring 1 和Ring 2，RRPP环上的所有节点属于这个RRPP域。

2. RRPP环

一个环形连接的以太网拓扑称为一个 RRPP 环。RRPP 环分为主环和子环，环的角色可以通过指定 RRPP 环的级别来设定：主环的级别为 0，子环的级别为 1。一个 RRPP 域可以由单个 RRPP 环构成，也可以由一个主环和若干个子环共同构成。RRPP 环有以下两种状态：

- 健康状态：整个环网的物理链路是连通的。
- 断裂状态：环网中某处物理链路断开。

如 图 1-1 所示，RRPP域Domain 1 中包含了两个RRPP环Ring 1 和Ring 2。Ring 1 和Ring 2 的级别分别配置为 0 和 1，则Ring 1 为主环，Ring 2 为子环。

3. 控制VLAN和保护VLAN

控制 VLAN 和保护 VLAN 是相对而言的：

- 控制 VLAN：用来传输 RRPP 协议报文。设备上接入 RRPP 环的端口都属于控制 VLAN，且只有接入 RRPP 环的端口可加入此 VLAN。每个 RRPP 域都有两个控制 VLAN：主控制 VLAN 和子控制 VLAN。主环的控制 VLAN 简称主控制 VLAN，子环的控制 VLAN 简称子控制 VLAN。配置时只需指定主控制 VLAN，系统会自动将主控制 VLAN 的 VLAN ID+1 作为子控制 VLAN。同一 RRPP 域中所有子环的控制 VLAN 都相同，且主控制 VLAN 和子控制 VLAN 的接口上都不允许配置 IP 地址。
- 保护 VLAN：用来传输数据报文。保护 VLAN 中既可包含 RRPP 端口，也可包含非 RRPP 端口。

4. 节点角色

RRPP 环上的每台设备都称为一个节点。节点角色由用户指定，分为以下几种：

- 主节点：每个环上有且仅有一个主节点。主节点是环网状态主动检测机制的发起者，也是网络拓扑发生改变后执行操作的决策者。
- 传输节点：主环上除主节点以外的其它所有节点，以及子环上除主节点、子环与主环相交节点以外的其它所有节点都为传输节点。传输节点负责监测自己的直连 RRPP 链路的状态，并把链路变化通知主节点，然后由主节点来决策如何处理。
- 边缘节点：是一种同时位于主环和子环上的特殊节点，它在主环上是主节点或传输节点，而在子环上是边缘节点。
- 辅助边缘节点：也是一种同时位于主环和子环上的特殊节点，它主环上是主节点或传输节点，而在子环上是辅助边缘节点。辅助边缘节点与边缘节点成对使用，用于检测主环完整性和进行环路预防。

如 图 1-1 所示，Ring 1 为主环，Ring 2 为子环。Device A 为 Ring 1 的主节点，Device B、Device C 和 Device D 为 Ring 1 的传输节点；Device E 为 Ring 2 的主节点，Device B 为 Ring 2 的边缘节点，Device C 为 Ring 2 的辅助边缘节点。

5. 端口角色

- 主端口和副端口

在主节点和传输节点接入 RRPP 环的各自两个端口中，一个为主端口，另一个为副端口。端口角色由用户指定。

主节点的主端口和副端口在功能上有所区别：主端口用来发送 Hello 报文，副端口用来接收 Hello 报文。当 RRPP 环处于健康状态时，副端口在逻辑上阻塞保护 VLAN，只允许控制 VLAN 的报文通过；当 RRPP 环处于断裂状态时，副端口将解除保护 VLAN 的阻塞状态，转发保护 VLAN 的报文。

传输节点的主端口和副端口在功能上没有区别，都用于 RRPP 环上协议报文和数据报文的传输。

如 图 1-1 所示，Device A 为 Ring 1 的主节点，Port 1 和 Port 2 分别为其在 Ring 1 上的主端口与副端口；Device B、Device C 和 Device D 为 Ring 1 的传输节点，它们各自的 Port 1 和 Port 2 分别为本节点在 Ring 1 上的主端口和副端口。

- 公共端口和边缘端口

公共端口是边缘节点和辅助边缘节点上接入主环的端口，即边缘节点和辅助边缘节点分别在主环上配置的两个端口。边缘端口是边缘节点和辅助边缘节点上只接入子环的端口。

端口的角色由用户指定。如 [图 1-1](#) 所示，Device B、Device C同时位于Ring 1 和Ring 2 上，Device B和Device C各自的端口Port 1 和Port 2 是接入主环的端口，因此是公共端口。Device B和Device C各自的Port 3 只接入子环，因此是边缘端口。

6. RRPP环组

RRPP 环组是为了减少 Edge-Hello 报文的收发数量,在边缘节点或辅助边缘节点上配置的一组子环的集合。这些子环的边缘节点都配置在同一台设备上，同样辅助边缘节点也都配置在同一台设备上。而且边缘节点或辅助边缘节点所在子环对应的主环链路相同，也就是说这些子环边缘节点的 Edge-Hello 报文都走相同的路径到达辅助边缘节点。

在边缘节点上配置的环组称为边缘节点环组，在辅助边缘节点上配置的环组称为辅助边缘节点环组。边缘节点环组内最多允许有一个子环发送 Edge-Hello 报文。

1.1.2 RRPP协议报文

RRPP协议报文的类型及其作用如 [表 1-1](#) 所示。

表1-1 RRPP 报文类型及其作用

报文类型	说明
Hello	也称Health报文，由主节点发起，对网络进行环路完整性检测
Link-Down	由传输节点、边缘节点或者辅助边缘节点发起，在这些节点的自身端口down时向主节点通知环路断裂
Common-Flush-FDB	由主节点发起，在RRPP环迁移到断裂状态时通知传输节点、边缘节点和辅助边缘节点更新各自MAC地址表项和ARP/ND表项。FDB是Forwarding Database（转发数据库）的缩写
Complete-Flush-FDB	由主节点发起，在RRPP环迁移到健康状态时通知传输节点、边缘节点和辅助边缘节点更新各自MAC地址表项和ARP/ND表项，同时通知传输节点解除临时阻塞端口的阻塞状态
Edge-Hello	由边缘节点发起并由辅助边缘节点接收，对边缘节点与辅助边缘节点之间的主环链路进行检测
Major-Fault	由辅助边缘节点发起，在辅助边缘节点与边缘节点之间的主环链路不连通时，向边缘节点报告主环链路故障



说明

子环的协议报文在主环中被当作数据报文传送，子环的 Common-Flush-FDB 和 Complete-Flush-FDB 协议报文在主环中会被主环的节点上送 CPU 处理，而主环的协议报文则只能在主环中传送。

1.1.3 RRPP定时器

RRPP 在检测以太网环的链路状况时所使用的定时器如下：

1. Hello定时器

规定了主节点从主端口发送 Hello 报文的周期。

2. Fail定时器

规定了主节点从主端口发出 Hello 报文到副端口收到该报文的最大时延。在该定时器超时前，若主节点在副端口上收到了自己从主端口发出的 Hello 报文，主节点认为环网处于健康状态；否则，主节点认为环网处于断裂状态。

在同一 RRPP 域中，传输节点会通过收到的 Hello 报文来学习主节点上的 Fail 定时器，以保证环网上各节点上 Fail 定时器的取值一致。

1.1.4 RRPP运行机制

1. 轮询机制

轮询机制是 RRPP 环的主节点主动检测环网健康状态的机制。

主节点以 Hello 定时器为周期从主端口发送 Hello 报文，依次经过各传输节点在环上传播。如果环路是健康的，主节点的副端口将在 Fail 定时器超时前收到该报文，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 Fail 定时器超时前无法收到 Hello 报文，主节点将解除保护 VLAN 在副端口的阻塞状态，同时发送 Common-Flush-FDB 报文通知所有传输节点，使其更新各自的 MAC 地址表项和 ARP/ND 表项。

2. 链路down告警机制

当传输节点、边缘节点或者辅助边缘节点发现自己任何一个属于 RRPP 域的端口 down 时，都会立刻发送 Link-Down 报文给主节点。主节点收到 Link-Down 报文后立刻解除保护 VLAN 在其副端口的阻塞状态，并发送 Common-Flush-FDB 报文通知所有传输节点、边缘节点和辅助边缘节点，使其更新各自的 MAC 地址表项和 ARP/ND 表项。各节点更新表项后，数据流将切换到正常的链路上。

3. 环路恢复

传输节点、边缘节点或者辅助边缘节点上属于 RRPP 域的端口重新 up 后，主节点可能会隔一段时间才能发现环路恢复。这段时间对于保护 VLAN 来说，网络有可能形成一个临时环路，从而产生广播风暴。

为了避免这种情况，非主节点在发现自己接入环网的端口重新 up 后，立即将其临时阻塞（只阻塞保护 VLAN 的流量，其它 VLAN 不阻塞，且允许控制 VLAN 的报文通过），在确信不会引起环路后，才解除该端口的阻塞状态。

4. 主环链路down，多归属子环广播风暴抑制机制

如 [图 1-5](#) 所示，假设 Ring 1 为主环，Ring 2 和 Ring 3 为子环。当边缘节点和辅助边缘节点之间的两条主环链路均处于 down 状态时，子环 Ring 2 和 Ring 3 的主节点会放开各自的副端口，导致 Device B、Device C、Device E 和 Device F 之间形成环路，从而产生广播风暴。

为了防止该环路的产生，在此种情况下边缘节点会临时阻塞边缘端口，在确信不会引起环路后，才解除该边缘端口的阻塞状态。

5. 环组机制

在边缘节点配置的 RRPP 环组内，只有域 ID 和环 ID 最小的激活子环才发送 Edge-Hello 报文。在辅助边缘节点环组内，任意激活子环收到 Edge-Hello 报文会通知给其它激活子环。这样在边缘节点/辅助边缘节点上分别对应配置 RRPP 环组后，只有一个子环发送/接收 Edge-Hello 报文，减少了对设备 CPU 的冲击。

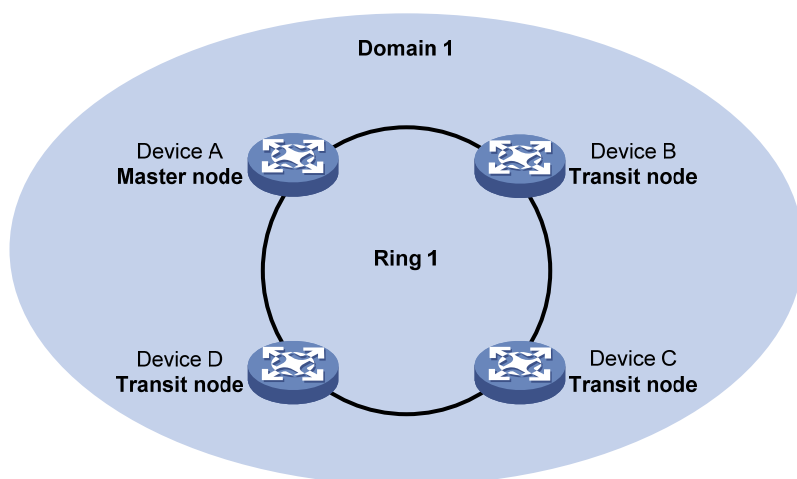
如 图 1-5 所示，Device B 和 Device C 分别为 Ring 2 和 Ring 3 的边缘节点和辅助边缘节点。Device B 和 Device C 都需要频繁收发 Edge-Hello 报文（若配置更多子环的情况，将会收发大量的 Edge-Hello 报文）。为减少 Edge-Hello 报文的收发数量，将边缘节点 Device B 上的 Ring 2 和 Ring 3 配置到一个环组，而将辅助边缘节点 Device C 上的 Ring 2 和 Ring 3 也配置到一个环组。这样在各环都激活的情况下，就只有 Device B 上的 Ring 2 发送 Edge-Hello 报文了。

1.1.5 RRPP 典型组网

1. 单环

如 图 1-2 所示，网络拓扑中只有一个环，此时只需定义一个 RRPP 域。

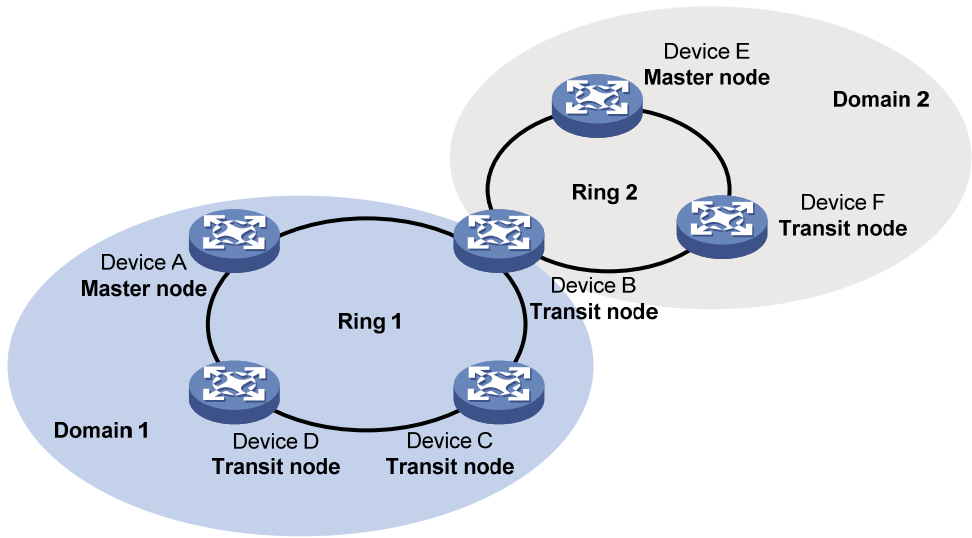
图1-2 单环示意图



2. 相切环

如 图 1-3 所示，网络拓扑中有两个或两个以上的环，各环之间只有一个公共节点，此时需针对每个环单独定义一个 RRPP 域。

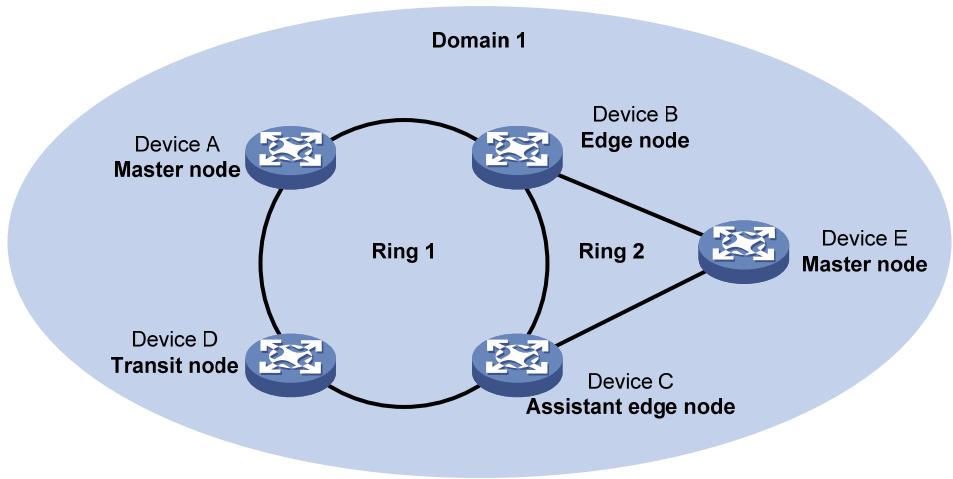
图1-3 相切环示意图



3. 相交环

如 图 1-4 所示，网络拓扑中有两个或两个以上的环，各环之间有两个公共节点，此时只需定义一个 RRPP域，选择其中一个环为主环，其它环为子环。

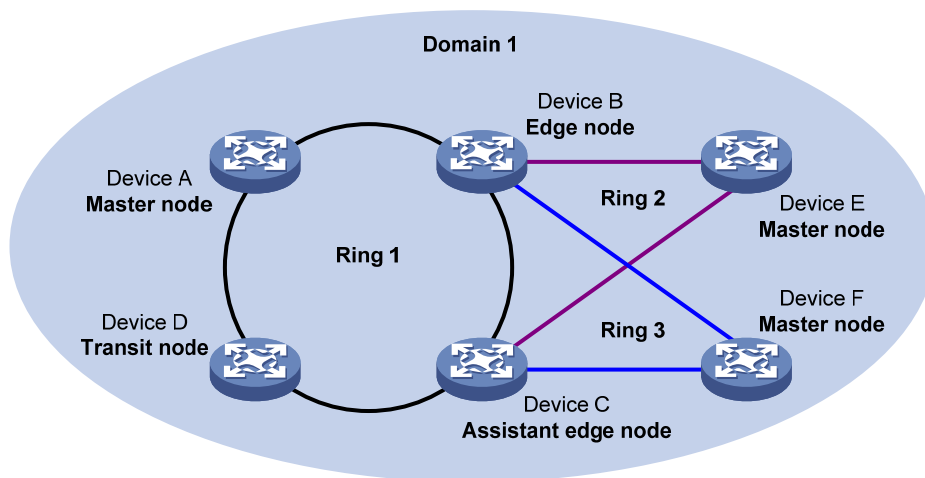
图1-4 相交环示意图



4. 双归属环

如 图 1-5 所示，网络拓扑中有两个或两个以上的环，各环之间有两个公共节点，且这两个公共节点都相同，此时可以只定义一个 RRPP域，选择其中一个环为主环，其它环为子环。

图1-5 双归属环示意图



1.1.6 协议规范

与 RRPP 相关的协议规范有：

- RFC 3619: Extreme Networks' Ethernet Automatic Protection Switching (EAPS) Version 1

1.2 RRPP与硬件适配关系

S5110V2-SI、S5000E-X 和 S5000V3-EI 系列交换机不支持 RRPP 功能。

1.3 RRPP配置限制和指导

由于 RRPP 没有自动选举机制，只有当环网中各节点的配置都正确时，才能真正实现环网的检测和保护，因此请保证配置的准确性。

用户可以根据业务规划情况先划分出 RRPP 域，再确定各 RRPP 域的控制 VLAN 和保护 VLAN，然后根据流量路径确定每个 RRPP 域内的环以及环上的节点角色。

1.4 RRPP配置任务简介

RRPP 配置任务如下：

- (1) [创建RRPP域](#)
欲指定为 RRPP 节点的设备均需进行本配置。
- (2) [配置控制VLAN](#)
RRPP 域内的所有节点均需进行本配置。
- (3) [配置保护VLAN](#)
RRPP 域内的所有节点均需进行本配置。
- (4) [配置RRPP环](#)
 - a. [配置RRPP端口](#)

各节点欲接入 RRPP 环的端口均需进行本配置。

b. [配置RRPP节点](#)

RRPP 域内的所有节点均需进行本配置。

(5) [激活RRPP域](#)

RRPP 域内的所有节点均需进行本配置。

(6) (可选) [配置RRPP定时器](#)

RRPP 域内的主节点均需进行本配置。

(7) (可选) [配置RRPP环组](#)

RRPP 域内的边缘节点和辅助边缘节点均需进行本配置。

(8) (可选) [开启RRPP的告警功能](#)

1.5 RRPP配置准备

配置 RRPP 之前，需先搭建好以太网环形拓扑的组网环境。

1.6 创建RRPP域

1. 功能简介

创建 RRPP 域时需要指定域 ID，域 ID 用来唯一标识一个 RRPP 域，在同一 RRPP 域内的所有节点上应配置相同的域 ID。

2. 配置限制和指导

本任务需要在所有欲指定为 RRPP 节点的设备上执行。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 创建 RRPP 域，并进入 RRPP 域视图。

```
rrpp domain domain-id
```

1.7 配置控制VLAN

1. 配置限制和指导

- 本任务需要在 RRPP 域内的所有节点上执行。
- 在同一 RRPP 域内的所有节点上应配置相同的控制 VLAN。用户只需配置主控制 VLAN，子控制 VLAN 由系统自动分配，其 VLAN ID 为主控制 VLAN 的 VLAN ID + 1。因此，在配置控制 VLAN 时请选取两个连续的、尚未创建的 VLAN，否则将导致配置失败。
- 请勿将接入 RRPP 环的端口的缺省 VLAN 配置为控制 VLAN。
- 控制 VLAN 内不能运行 QinQ 和 VLAN 映射功能，否则 RRPP 协议报文将无法收发。
- 配置好 RRPP 环之后不再允许用户删除或修改主控制 VLAN。主控制 VLAN 只能通过 **undo control-vlan** 命令删除，不能通过 **undo vlan** 命令删除。

- 如果要在未配置 RRPP 功能的设备上透传 RRPP 协议报文，应保证该设备上只有接入 RRPP 环的那两个端口允许该 RRPP 环所对应控制 VLAN 的报文通过，而其它端口都不允许其通过；否则，其它 VLAN 的报文可能通过透传进入控制 VLAN，从而对 RRPP 环产生冲击。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 RRPP 域视图。

```
rrpp domain domain-id
```

- (3) 配置 RRPP 域的主控制 VLAN。

```
control-vlan vlan-id
```

1.8 配置保护VLAN

1. 配置限制和指导

本任务需要在 RRPP 域内的所有节点上执行。

RRPP 端口允许通过的 VLAN 都应该被 RRPP 域保护，在同一 RRPP 域内的所有节点上应配置相同的保护 VLAN。

2. 配置准备

配置保护 VLAN 前需要配置 MST 域，配置关于保护 VLAN 的 VLAN 映射表，关于 MST 域的详细介绍，请参考“二层技术-以太网交换配置指导”中的“生成树”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 RRPP 域视图。

```
rrpp domain domain-id
```

- (3) 配置 RRPP 域的保护 VLAN。

```
protected-vlan reference-instance instance-id-list
```

1.9 配置RRPP环

配置 RRPP 环时，首先要对各节点上欲接入 RRPP 环的端口（简称 RRPP 端口）进行必要的配置，然后再配置 RRPP 环上的各节点。

1.9.1 配置准备

配置 RRPP 环之前必须先配置控制 VLAN 和保护 VLAN。

1.9.2 配置RRPP端口

1. 配置限制和指导

本任务需要在各节点欲接入 RRPP 环的端口上执行。

不建议在 RRPP 端口上开启以太网 OAM 远端环回功能，因为可能引起短时间的广播风暴。有关此功能的详细介绍，请参见“可靠性配置指导”中的“以太网 OAM”。

建议在 RRPP 端口上使用 **link-delay** 命令将端口的物理连接状态 up/down 抑制时间配置为 0 秒（即不抑制），以提高 RRPP 的拓扑变化收敛速度。有关 **link-delay** 命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“以太网接口”。

请勿将一个端口同时加入聚合组和 RRPP 环，否则该端口在 RRPP 环中将不会生效。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入二层以太网或二层聚合接口视图。

```
interface interface-type interface-number
```

- (3) 配置端口的链路类型为 Trunk 类型。

```
port link-type trunk
```

缺省情况下，端口的链路类型为 Access 类型。

本命令的详细介绍请参见“二层技术-以太网交换命令参考”中的“VLAN”。

- (4) 配置 Trunk 端口允许保护 VLAN 的报文通过。

```
port trunk permit vlan { vlan-id-list | all }
```

缺省情况下，Trunk 端口只允许 VLAN 1 的报文通过。

由于 RRPP 端口将自动允许控制 VLAN 的报文通过，因此无需配置 RRPP 端口允许控制 VLAN 的报文通过。

本命令的详细介绍请参见“二层技术-以太网交换命令参考”中的“VLAN”。

- (5) 关闭生成树协议。

```
undo stp enable
```

缺省情况下，端口上的生成树协议处于开启状态。

本命令的详细介绍请参见“二层技术-以太网交换命令参考”中的“生成树”。

1.9.3 配置RRPP节点

1. 配置限制和指导

本任务需要在 RRPP 域内的各节点上执行。

如果一台设备处于同一 RRPP 域的多个 RRPP 环上，则该设备在子环上的节点角色只能是边缘节点或辅助边缘节点。

在配置边缘节点或辅助边缘节点时，必须先配置主环再配置子环。

2. 配置主节点

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 RRPP 域视图。

```
rrpp domain domain-id
```

- (3) 指定当前设备为主节点，并指定主端口和副端口。

```
ring ring-id node-mode master [ primary-port interface-type  
interface-number ] [ secondary-port interface-type interface-number ]  
level level-value
```

3. 配置传输节点

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 RRPP 域视图。

```
rrpp domain domain-id
```

- (3) 指定当前设备为传输节点，并指定主端口和副端口。

```
ring ring-id node-mode transit [ primary-port interface-type  
interface-number ] [ secondary-port interface-type interface-number ]  
level level-value
```

4. 配置边缘节点

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 RRPP 域视图。

```
rrpp domain domain-id
```

- (3) 指定当前设备为主环的主节点或传输节点，并指定主端口和副端口。

```
ring ring-id node-mode { master | transit } [ primary-port interface-type  
interface-number ] [ secondary-port interface-type interface-number ]  
level level-value
```

- (4) 指定当前设备为子环的边缘节点，并指定边缘端口。

```
ring ring-id node-mode edge [ edge-port interface-type  
interface-number ]
```

5. 配置辅助边缘节点

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 RRPP 域视图。

```
rrpp domain domain-id
```

- (3) 指定当前设备为主环的主节点或传输节点，并指定主端口和副端口。

```
ring ring-id node-mode { master | transit } [ primary-port interface-type  
interface-number ] [ secondary-port interface-type interface-number ]  
level level-value
```

- (4) 指定当前设备为子环的辅助边缘节点，并指定边缘端口。

```
ring ring-id node-mode assistant-edge [ edge-port interface-type  
interface-number ]
```

1.10 激活RRPP域

1. 配置限制和指导

本任务需要在 RRPP 域内的所有节点上执行。

只有当 RRPP 协议和 RRPP 环都开启之后，当前设备的 RRPP 域才能被激活。

在一台设备上开启子环之前必须先开启主环，而关闭主环之前也必须先关闭所有子环，否则系统将提示出错。

为避免子环的 Hello 报文在主环上形成环路，在子环的主节点上开启子环之前，请先在主环的主节点上开启主环。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 RRPP 协议。

```
rrpp enable
```

缺省情况下，RRPP 协议处于关闭状态。

- (3) 进入 RRPP 域视图。

```
rrpp domain domain-id
```

- (4) 开启 RRPP 环。

```
ring ring-id enable
```

缺省情况下，RRPP 环处于关闭状态。

1.11 配置RRPP定时器

1. 配置限制和指导

本任务需要在 RRPP 域内的主节点上执行。

Fail 定时器不得小于 Hello 定时器的 3 倍。

在双归属环组网中，为避免主环故障时出现临时环路，应确保子环主节点与主环主节点上的 Fail 定时器之差大于子环主节点上 Hello 定时器的 2 倍。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 RRPP 域视图。

```
rrpp domain domain-id
```

- (3) 配置 Hello 和 Fail 定时器。

```
timer hello-timer hello-value fail-timer fail-value
```

缺省情况下，Hello 定时器为 1 秒，Fail 定时器为 3 秒。

1.12 配置RRPP环组

1. 功能简介

通过把具有相同边缘节点/辅助边缘节点配置的一组子环加入环组中，可以减少 Edge-Hello 报文的收发数量。

2. 配置限制和指导

- 本任务需要在 RRPP 域内的边缘节点和辅助边缘节点上执行。
- 一个子环只能属于一个环组，且配置在边缘节点和辅助边缘节点上的环组中所包含的子环必须相同，否则环组不能正常工作。
- 加入环组的子环的边缘节点应配置在同一台设备上；同样地，辅助边缘节点也应配置在同一台设备上，而且边缘节点/辅助边缘节点所对应的主环链路应相同。
- 设备在一个环组内所有子环上应具有相同的类型：边缘节点或辅助边缘节点。
- 边缘节点环组及其对应的辅助边缘节点环组的配置和激活状态必须相同。
- 同一环组中的子环所对应主环的链路必须相同；若主环链路本身的配置就不同，或由于修改配置而导致不同，环组都将不能正常运行。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 RRPP 环组，并进入 RRPP 环组视图。

```
rrpp ring-group ring-group-id
```

- (3) 将子环加入 RRPP 环组。

```
domain domain-id ring ring-id-list
```

缺省情况下，RRPP 环组内不存在子环。

1.13 开启RRPP的告警功能

1. 功能简介

开启 RRPP 的告警功能后，指定事件发生时系统会产生相应类型的告警信息。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 RRPP 的告警功能。

```
snmp-agent trap enable rrpp [ major-fault | multi-master | ring-fail |  
ring-recover ] *
```

缺省情况下，RRPP 的告警功能处于关闭状态。

1.14 RRPP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 RRPP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 RRPP 报文统计信息。

表1-2 RRPP 显示和维护

操作	命令
显示RRPP的摘要信息	display rrpp brief
显示RRPP环组的配置信息	display rrpp ring-group [<i>ring-group-id</i>]
显示RRPP报文的统计信息	display rrpp statistics domain <i>domain-id</i> [ring <i>ring-id</i>]
显示RRPP的详细信息	display rrpp verbose domain <i>domain-id</i> [ring <i>ring-id</i>]
清除RRPP报文的统计信息	reset rrpp statistics domain <i>domain-id</i> [ring <i>ring-id</i>]

1.15 RRPP典型配置举例

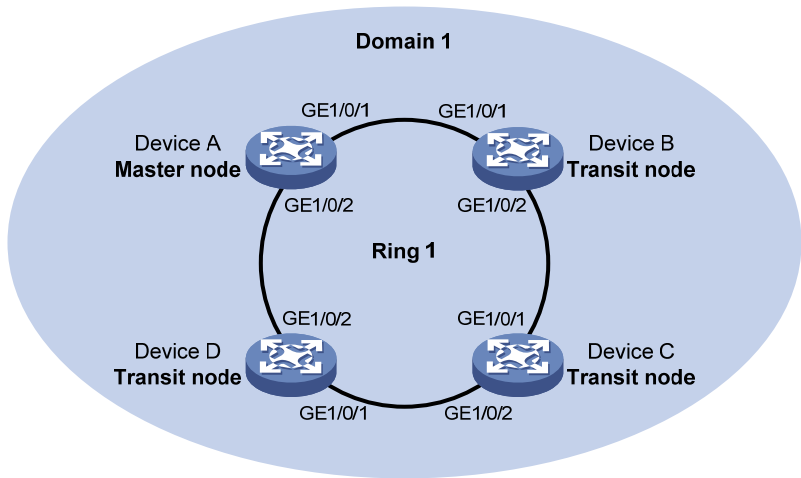
1.15.1 单环配置举例

1. 组网需求

- Device A~Device D 构成 RRPP 域 1，该域的主控制 VLAN 为 VLAN 4092，保护 VLAN 为 VLAN 1~30。
- Device A、Device B、Device C 和 Device D 构成主环 Ring 1。Device A 为主环的主节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为主、副端口；Device B、Device C 和 Device D 为主环的传输节点，其各自的 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为主、副端口。

2. 组网图

图1-6 单环配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的主控制 VLAN，并将 MSTI 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

配置本设备为主环 Ring 1 的主节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并开启该环。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

开启 RRPP 协议。

```
[DeviceA] rrpp enable
```

(2) 配置 Device B

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1～30 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的主控制 VLAN，并将 MSTI 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并开启该环。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit
```

开启 RRPP 协议。

```
[DeviceB] rrpp enable
```

(3) 配置 Device C

Device C 的配置与 Device B 相似，配置过程略。

(4) 配置 Device D

Device D 的配置与 Device B 相似，配置过程略。

4. 验证配置

配置完成后，用户可以使用 **display** 命令显示各设备上 RRPP 的配置和运行情况。

1.15.2 相交环配置举例

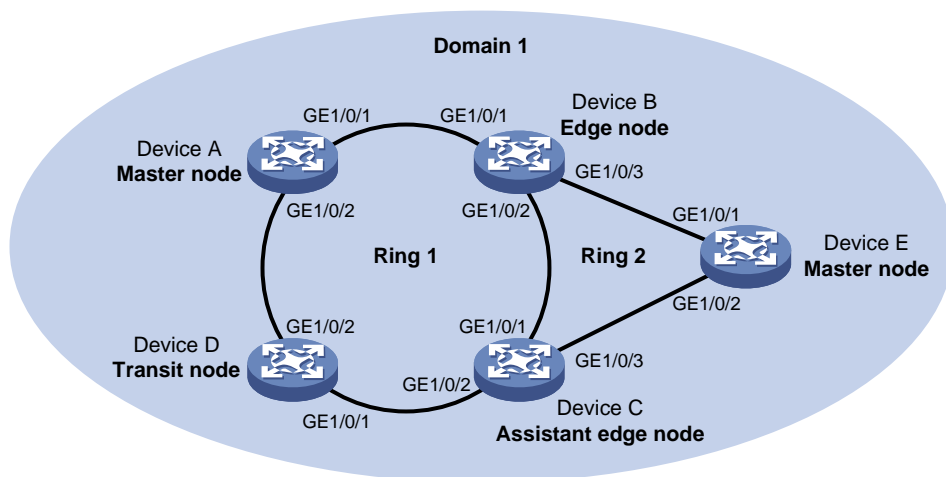
1. 组网需求

- Device A～Device E 构成 RRPP 域 1，该域的主控制 VLAN 为 VLAN 4092，保护 VLAN 为 VLAN 1～30。
- Device A、Device B、Device C 和 Device D 构成主环 Ring 1；Device B、Device C 和 Device E 构成子环 Ring 2。
- Device A 为主环的主节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为主、副端口；Device E 为子环的主节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为主、副端口；

Device B 为主环的传输节点和子环的边缘节点，GigabitEthernet1/0/3 为边缘端口；Device C 为主环的传输节点和子环的辅助边缘节点，GigabitEthernet1/0/3 为边缘端口；Device D 为主环的传输节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为主、副端口。

2. 组网图

图1-7 相交环配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的主控制 VLAN，并将 MSTI 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

配置本设备为主环 Ring 1 的主节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并开启该环。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

开启 RRPP 协议。

```
[DeviceA] rrpp enable
```

(2) 配置 Device B

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] link-delay 0
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的主控制 VLAN，并将 MSTI 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
```

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
# 配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为
GigabitEthernet1/0/2，并开启该环。
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
# 配置本设备为子环 Ring 2 的边缘节点，边缘端口为 GigabitEthernet1/0/3，并开启该环。
[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 2 enable
[DeviceB-rrpp-domain1] quit
# 开启 RRPP 协议。
[DeviceB] rrpp enable
```

(3) 配置 Device C

```
# 创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
# 分别在端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上配置物
理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk
端口且允许 VLAN 1~30 通过。
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] link-delay 0
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/3] quit
# 创建 RRPP 域 1，将 VLAN 4092 配置为该域的主控制 VLAN，并将 MSTI 1 所映射的 VLAN
配置为该域的保护 VLAN。
[DeviceC] rrpp domain 1
[DeviceC-rrpp-domain1] control-vlan 4092
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并开启该环。

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

```
[DeviceC-rrpp-domain1] ring 1 enable
```

配置本设备为子环 Ring 2 的辅助边缘节点，边缘端口为 GigabitEthernet1/0/3，并开启该环。

```
[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
```

```
[DeviceC-rrpp-domain1] ring 2 enable
```

```
[DeviceC-rrpp-domain1] quit
```

开启 RRPP 协议。

```
[DeviceC] rrpp enable
```

(4) 配置 Device D

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceD> system-view
```

```
[DeviceD] vlan 1 to 30
```

```
[DeviceD] stp region-configuration
```

```
[DeviceD-mst-region] instance 1 vlan 1 to 30
```

```
[DeviceD-mst-region] active region-configuration
```

```
[DeviceD-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceD] interface gigabitethernet 1/0/1
```

```
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

```
[DeviceD-GigabitEthernet1/0/1] quit
```

```
[DeviceD] interface gigabitethernet 1/0/2
```

```
[DeviceD-GigabitEthernet1/0/2] link-delay 0
```

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
```

```
[DeviceD-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的主控制 VLAN，并将 MSTI 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceD] rrpp domain 1
```

```
[DeviceD-rrpp-domain1] control-vlan 4092
```

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并开启该环。

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

```
[DeviceD-rrpp-domain1] ring 1 enable
```

```
[DeviceD-rrpp-domain1] quit
```


开启 RRPP 协议。

```
[DeviceD] rrpp enable
```

(5) 配置 Device E

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceE> system-view
```

```
[DeviceE] vlan 1 to 30
```

```
[DeviceE] stp region-configuration
```

```
[DeviceE-mst-region] instance 1 vlan 1 to 30
```

```
[DeviceE-mst-region] active region-configuration
```

```
[DeviceE-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceE] interface gigabitethernet 1/0/1
```

```
[DeviceE-GigabitEthernet1/0/1] link-delay 0
```

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
```

```
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

```
[DeviceE-GigabitEthernet1/0/1] quit
```

```
[DeviceE] interface gigabitethernet 1/0/2
```

```
[DeviceE-GigabitEthernet1/0/2] link-delay 0
```

```
[DeviceE-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
```

```
[DeviceE-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的主控制 VLAN，并将 MSTI 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceE] rrpp domain 1
```

```
[DeviceE-rrpp-domain1] control-vlan 4092
```

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

配置本设备为子环 Ring 2 的主节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并开启该环。

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 1
```

```
[DeviceE-rrpp-domain1] ring 2 enable
```

```
[DeviceE-rrpp-domain1] quit
```

开启 RRPP 协议。

```
[DeviceE] rrpp enable
```

4. 验证配置

配置完成后，用户可以使用 **display** 命令显示各设备上 RRPP 的配置和运行情况。

1.16 RRPP常见故障处理

1.16.1 链路正常状态下主节点收不到Hello报文

1. 故障现象

在链路正常状态下，主节点收不到 Hello 报文，主节点放开副端口。

2. 故障分析

可能的原因有：

- RRPP 环上有节点没有开启 RRPP 协议。
- 在同一 RRPP 环上的节点的域 ID 或控制 VLAN 不同。
- RRPP 环上的端口处于非正常状态。

3. 处理过程

- 使用 **display rrpp brief** 命令显示各个节点是否都配置并开启了 RRPP 协议。如果没有则使用 **rrpp enable** 和 **ring enable** 命令开启 RRPP 协议和 RRPP 环。
- 使用 **display rrpp brief** 命令显示各节点的域 ID 和控制 VLAN 是否相同。如果不相同，则需重新设置为相同。
- 使用 **display rrpp verbose** 命令显示各个节点各个环的端口链路状态。
- 在各个节点上使用 **debugging rrpp** 命令显示端口是否有 Hello 报文的接收或发送，如果没有则说明有报文丢失。

目 录

1 ERPS.....	1-1
1.1 ERPS简介	1-1
1.1.1 ERPS组网模型.....	1-1
1.1.2 ERPS实例.....	1-2
1.1.3 ERPS协议报文.....	1-2
1.1.4 ERPS协议状态.....	1-3
1.1.5 ERPS定时器.....	1-4
1.1.6 ERPS运行机制.....	1-4
1.1.7 ERPS典型组网.....	1-7
1.1.8 协议规范.....	1-10
1.2 ERPS配置限制和指导	1-10
1.3 ERPS配置任务简介	1-10
1.4 ERPS配置准备	1-11
1.5 全局使能ERPS	1-11
1.6 配置ERPS环	1-12
1.6.1 创建ERPS环.....	1-12
1.6.2 配置ERPS环成员端口.....	1-12
1.6.3 配置控制VLAN.....	1-13
1.6.4 配置保护VLAN.....	1-14
1.6.5 配置ERPS节点角色.....	1-14
1.7 在实例中使能ERPS协议	1-15
1.8 配置ERPS环发送报文的目的MAC地址所携带的环号	1-15
1.9 配置R-APS报文级别	1-15
1.10 配置ERPS定时器.....	1-16
1.11 配置ERPS非回切模式.....	1-16
1.12 配置ERPS倒换模式.....	1-17
1.13 配置子环关联环	1-17
1.14 开启互联节点Flush透传功能.....	1-18
1.15 配置ERPS环成员端口的Track联动	1-18
1.16 清除ERPS环上FS/MS模式的配置.....	1-18
1.17 ERPS显示和维护.....	1-19
1.18 ERPS典型配置举例.....	1-19
1.18.1 单环配置举例	1-19

1.18.2 单子环配置举例	1-28
1.18.3 单环多实例负载分担配置举例	1-41
1.19 ERPS常见故障处理.....	1-51
1.19.1 Owner节点收不到故障节点发送的SF报文.....	1-51

1 ERPS

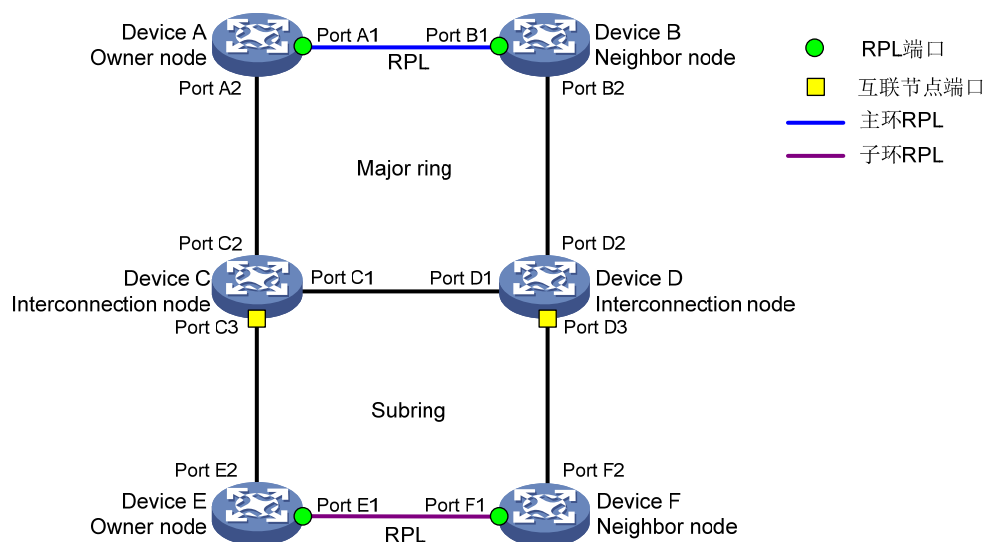
1.1 ERPS简介

ERPS（Ethernet Ring Protection Switching，以太网环保护倒换）是具备高可靠性和稳定性的以太网环链路层技术。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环发生链路故障时能迅速恢复环网上各个节点之间的通信通路，具备较高的收敛速度。

1.1.1 ERPS组网模型

如 图 1-1 所示，ERPS采用环形组网。

图1-1 ERPS 的基本组网模型



1. ERPS环

一个环形连接的以太网网络拓扑称为一个ERPS环。ERPS环分为主环和子环，缺省情况下，ERPS环为主环，可手工配置ERPS环为子环。一个ERPS环可以由单个主环构成，也可以由多个环网构成，在多个环网中可以有多主环和多个子环。如 图 1-1，Device A、Device B、Device C、Device D四个节点所围成的封闭环路为主环Major ring。子环Subring是由Device C与Device E、Device E与Device F、Device F与Device D这三段链路所够成，是个不封闭环。

2. 环保护链路

ERPS环由许多节点组成。某些节点之间使用RPL（Ring Protection Link，环保护链路）对环网进行保护，防止环路产生。如 图 1-1，Device A与Device B、Device E与Device F间的链路就是RPL。

3. 节点角色

ERPS 环上的每台设备都称为一个节点。节点角色由用户的配置来决定，分为下列几种：

- **Owner 节点：**主节点，负责阻塞和放开本节点上位于 RPL 上的端口，防止形成环路，从而进行链路倒换。

- **Neighbor 节点：**邻居节点，RPL 上和 Owner 节点相连的节点，协同 Owner 节点阻塞和放开本节点上位于 RPL 上的端口，进行链路倒换。
- **Interconnection 节点：**互联节点，多环模型中连接多个环的节点，互联节点属于子环，主环无互联节点。在子环互联节点之间的链路的协议报文上送模式中，子环的协议报文在互联节点终结，数据报文不被终结。有关协议报文的介绍，请参见“[1.1.3 ERPS协议报文](#)”。
- **Normal 节点：**普通节点，除了上述介绍的三种节点之外的所有节点都为 Normal 节点。Normal 节点负责接收和转发链路中的协议报文和数据报文。

每个节点上都有两种成员端口 port0 和 port1，这两种端口在功能上没有区别，都用于 ERPS 环上协议报文和数据报文的传输。

如 [图 1-1](#)，在主环上Device A是Owner节点，Device B是Neighbor节点，在子环上Device E是Owner节点，Device F是Neighbor节点。Device C和Device D是Interconnection节点。

4. 端口类型

ERPS 环成员端口类型由用户的配置来决定，分为以下三种：

- **RPL 端口：**RPL 两端的端口。
- **Interconnection 端口：**互联节点端口是负责连接子环和主环的端口。
- **Normal 端口：**Normal 端口为缺省端口类型，可以接收和转发链路中的协议报文和数据报文，不具备特殊功能。

如 [图 1-1](#)所示，Device A、Device B、Device E和Device F上的端口Port A1、Port B1、Port E1 和 Port F1 为RPL端口。Device C和Device D上的端口Port C3 和Port D3 为Interconnection端口。其余端口为Normal端口。

1.1.2 ERPS实例

ERPS 组网中一个环可以支持多个实例，每个实例都是一个逻辑环。每个实例中有自己的协议通道和数据通道，以及 Owner 节点；每个实例作为一个独立的协议实体，维护各自的状态和数据。

不同环 ID 的报文通过目的 MAC 地址来区分（目的 MAC 地址的最后一个字节表示环 ID）；具有相同环 ID 报文，通过其携带的 VLAN ID 来区分其所属的 ERPS 实例，即报文中的环 ID 和 VLAN ID 唯一确定一个实例。

1.1.3 ERPS协议报文

R-APS（Ring Automatic Protection Switching，环网自动保护倒换）报文是 ERPS 的协议报文。协议提供了 R-APS 报文级别的设置功能。节点不处理 R-APS 报文级别比自己大的报文。同一环上同一实例内的节点 R-APS 报文级别必须相同。

ERPS协议报文的类型及其作用如 [表 1-1](#) 所示。

表1-1 ERPS 报文类型及其作用

报文类型	说明
(NR, RB)（No Request, RPL Block，链路恢复，RPL阻塞）报文	由Owner节点在Idle状态下发送，通知其它节点RPL端口被阻塞。其它节点收到(NR, RB)报文后放开自身的无故障端口，更新各自MAC地址表项。链路稳定在Idle状态下时，Owner节点周期性发送(NR, RB)报文

报文类型	说明
NR (No Request, 链路恢复) 报文	当链路故障恢复后, 由恢复端口所在节点发送, Owner节点收到NR报文后启动WTR定时器, 在恢复端口所在节点收到(NR, RB)报文后停止发送NR报文
SF (Signal Fail, 信号失败) 报文	当链路出现信号收发失败时, 由故障端口所在节点发送, Owner和Neighbor节点收到SF报文后, 放开各自的RPL端口。故障未消除前, 故障端口所在节点周期性发送SF报文
MS (Manual Switch, 手工倒换) 报文	由配置MS模式的节点发送, 配置MS模式的端口被阻塞, 其它节点收到MS报文后放开自身无故障端口, 更新各自MAC地址表项。链路在MS状态下, MS报文周期性发送
FS (Forced Switch, 强制倒换) 报文	由配置FS模式的节点发送, 配置FS模式的端口被阻塞, 其它节点收到FS报文后放开自身所有端口, 更新各自MAC地址表项。链路在FS状态下, FS报文周期性发送
Flush (泛洪) 报文	如果子环拓扑有变化, 互联节点以广播形式发送Flush报文通知主环刷新MAC地址表项



说明

主环和子环的协议报文只能在自己的环内传输, 子环上除 Flush 报文以外的其它协议报文在互联节点被终结。

子环的数据报文可以透传至主环。

1.1.4 ERPS协议状态

ERPS 定义了以下六种状态:

- **Init 状态:** 环端口不完整时 (非互联节点的端口数量小于 2 或互联节点的端口数量小于 1), 处于 Init 状态。
- **Idle 状态:** 环初始化过后进入到稳定状态, 当 Owner 节点进入 Idle 状态后, 其它节点随之进入 Idle 状态。其中, Owner 节点和 Neighbor 节点的 RPL 端口为阻塞状态, 即 RPL 不通; Owner 节点定时发送(NR, RB)报文。
- **Protection 状态:** 当环网某段链路出现故障, 环路经过保护倒换, 最终稳定到的状态。Owner 节点和 Neighbor 节点的 RPL 端口放开, 即 RPL 放开, 保证整个环网仍然是通的。当链路中某个节点进入 Protection 状态后, 其它节点随之进入 Protection 状态。
- **MS 状态:** MS 状态下可以手动倒换流量转发路径。当对链路中某个节点进行 MS 操作后, 其它节点随之进入 MS 状态。
- **FS 状态:** FS 状态下可以强制倒换流量转发路径。当对链路中某个节点进行 FS 操作后, 其它节点随之进入 FS 状态。
- **Pending 状态:** Pending 状态是一个不稳定的状态, 是各状态在进行跳转时的一个过渡状态。环路正常时, 处于 Idle 状态; 链路发生故障后, 处于 Protection 状态。

1.1.5 ERPS定时器

1. Hold-off定时器

该定时器在端口检测到链路故障时启动，延迟故障上报的速度。当链路出现故障后，等待 Hold-off 超时后，如果故障依然存在，再上报。从而给服务层提供修复链路的机会，避免不必要的故障上报。该定时器的时长会影响链路故障上报的速度，影响故障发生时链路的倒换性能。

2. Guard定时器

该定时器在端口检测到链路恢复时启动，用于防止环网上转发延时导致的原 R-APS 消息残留对网络造成不必要的震荡。在此定时器超时前，接口不再处理所有 R-APS 报文。该定时器对多点故障时的链路恢复性能有影响。

3. WTR定时器

回切模式下，该定时器在 Owner 节点在 Protection 状态收到 NR 报文时启动，用于防止环网上存在间歇性故障链路导致网络频繁震荡。在此定时器超时前，RPL 保持转发，故障恢复点维持临时阻塞，期间，如果 Owner 节点收到 SF 报文，说明环网中还存在故障链路，该定时器直接关闭，RPL 仍然保持转发。否则，该定时器超时后，Owner 节点阻塞 RPL 端口，发送(NR, RB)报文通知故障恢复节点，放开临时阻塞的端口，同时刷新 MAC 地址表项。

4. WTB定时器

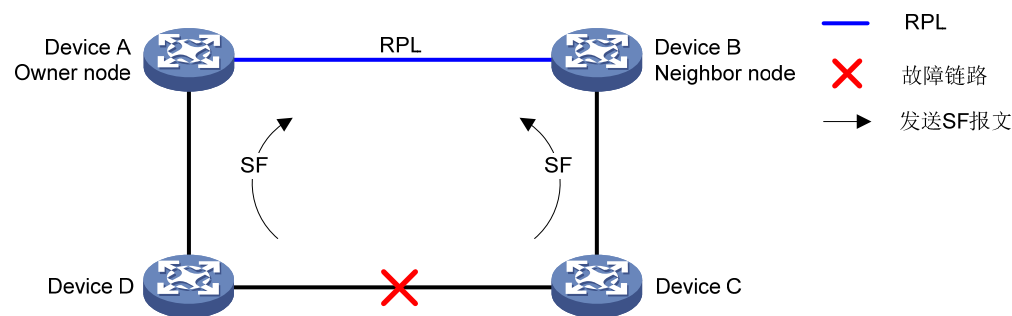
回切模式下，该定时器在 Owner 节点在 MS 或者 FS 状态收到 NR 报文时启动，用于防止环网上的 RPL 端口由于网络震荡而反复被阻塞、放开。在此定时器超时前，RPL 保持转发，故障节点发送 NR 报文。期间，如果 Owner 节点再次收到 SF 报文，说明环网中还存在故障链路，该定时器直接关闭，RPL 仍然保持转发。否则，该定时器超时后，Owner 节点阻塞 RPL，发送(NR, RB)报文通知临时阻塞点放开，同时刷新 MAC 地址表项。

1.1.6 ERPS运行机制

ERPS 采用 ITU-T G.8032/Y.1344 中定义的连续性检测进行链路双向转发检测，能够定位故障点并检测故障是单向还是双向的。ERPS 通过通告的消息来判断链路的状态，并作出相应的处理。ERPS 的控制报文类型主要有 SF 和 NR，如果检测到链路出现信号收发失败，就发送 SF 消息；检测到链路恢复，就发送 NR 消息。如果检测到链路状态变化，连续发三个报文，之后的报文每隔 5 秒发送一次。

1. 链路down告警机制

图1-2 链路故障

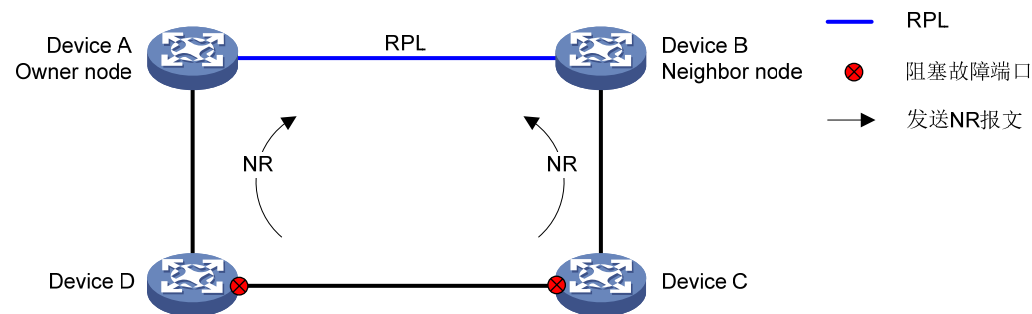


当链路中的节点发现自己任何一个属于 ERPS 环的端口 down 时，都会阻塞故障端口并立刻发送 SF 报文通知链路上其它节点发生了故障，其它节点在收到此报文后放开非故障阻塞端口，并刷新 MAC 地址表项。

如 图 1-2 所示，当 Device C 和 Device D 之间的链路发生故障，Device C 和 Device D 检测到链路故障，阻塞故障端口，并且周期性的发送 SF 消息，Device A 和 Device B 收到 SF 消息后，放开之前阻塞的 RPL 端口，业务倒换到 RPL，整个环完成了保护倒换。

2. 链路恢复机制

图1-3 故障链路恢复



当故障链路恢复后，先阻塞之前处于故障状态的端口，启动 Guard 定时器并发送 NR 报文通知 Owner 节点故障链路已恢复。Owner 节点在收到 NR 报文后，启动 WTR 定时器，如果定时器在超时前，没有收到 SF 报文，则当定时器超时后，Owner 节点阻塞 RPL 端口，并向外周期性的发送(NR, RB) 报文；故障恢复节点在收到(NR, RB)报文后放开临时阻塞的故障恢复端口；Neighbor 节点收到(NR, RB)报文后阻塞 RPL 端口，链路恢复。

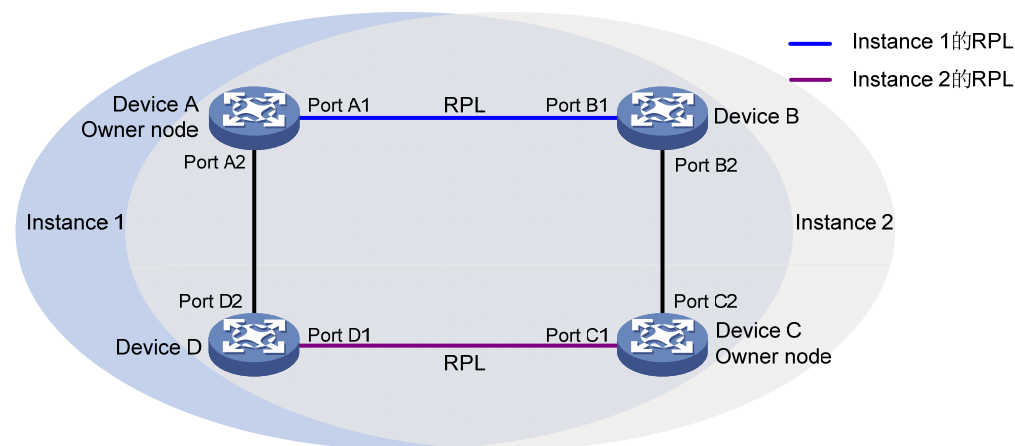
如 图 1-3 所示，当 Device C 和 Device D 检测到它们之间的链路恢复后，临时阻塞之前处于故障状态的端口，发送 NR 消息。Device A（Owner 节点）收到 NR 消息后，启动 WTR 定时器，定时器超时之后，阻塞 RPL 端口，并向外发送(NR, RB)报文。Device C 和 Device D 收到(NR, RB)消息之后，放开临时阻塞的故障恢复端口；Device B（Neighbor 节点）在收到(NR, RB)报文后阻塞 RPL 端口。链路恢复到发生故障前的状态。

Owner 节点在链路的恢复处理中，有如下两种方式。

- 回切模式(Revertive behaviour)：Owner 节点在故障消除收到 NR 报文后，会启动 WTR/WTB 定时器。在定时器超时之前，如果 Owner 节点没有收到 SF 报文，就倒换端口状态，阻塞 RPL 端口，清除 MAC 地址表项，发送(NR, RB)报文，其它节点放开非故障的阻塞端口，清除各自 MAC 地址表项。定时器超时后，倒换回 Idle 状态。
- 非回切模式(Non-revertive behaviour)：Owner 收到 NR 报文后，不执行任何动作，保持之前设置的端口状态。

3. 多实例与负载分担机制

图1-4 多实例负载分担



在同一个环网中，可能同时存在多个 VLAN 的数据流量，ERPS 可以实现流量的负载分担，即不同 VLAN 的流量沿不同的路径进行转发。

ERPS 环网中可分为控制 VLAN 和保护 VLAN：

- 控制 VLAN：用来传递 ERPS 协议报文。每个 ERPS 实例都有自己的控制 VLAN。
- 保护 VLAN：与控制 VLAN 相对，保护 VLAN 用来传输数据报文。每个 ERPS 实例都有自己的保护 VLAN，保护 VLAN 通过配置生成树实例来实现。

通过在同一个环网上配置多个 ERPS 实例，不同 ERPS 实例发送不同 VLAN 的流量，实现不同 VLAN 的数据流量在该环网中的拓扑不同，从而达到负载分担的目的。

如 图 1-4 所示，Instance 1 和 Instance 2 为 ERPS 一个环内配置的两个实例，两个实例的 RPL 不同，Device A 和 Device B 之间的链路为 Instance 1 的 RPL，Device A 为 Instance 1 的 Owner 节点；Device C 和 Device D 之间的链路为 Instance 2 的 RPL，Device C 为 Instance 2 的 Owner 节点。通过配置，不同的实例 RPL 阻塞不同的 VLAN，从而实现单环的负载分担。

4. 手动可配置机制

ERPS 支持两个级别的手动配置，即 MS 和 FS。

- MS 允许用户选取当前环实例内的配置 MS 模式的 ERPS 环成员端口作为阻塞端口。用户在该端口所在节点配置 `erps switch manual` 命令后，该节点会向外发送 MS 消息。其它节点收到 MS 消息后会主动放开各自节点上的 ERPS 环成员端口，最终会稳定在整个链路上只有 MS 配置的端口被阻塞的状态。需要注意的是，MS 状态可以响应链路事件，允许根据链路事件倒换到相应的状态：MS 状态下，如果有其它链路出现故障，故障所在节点会向外发送 SF 报文，其它节点在收到 SF 报文后会放开各自节点上的 ERPS 环成员端口，包括 MS 配置阻塞端口。此时链路可正常倒换到保护状态。
- FS 作用与 MS 类似，不同的是 FS 状态下，各节点不会响应链路故障事件，始终维持 FS 状态不变。

5. 链路检测联动机制

当链路上的中间传输设备或传输链路发生故障（如光纤链路发生单通、错纤、丢包等故障）以及故障排除时，ERPS 本身无法感知到这个变化，ERPS 环的成员端口需要通过专门的链路检测协议来检测端口的链路状态，当链路检测协议检测到故障发生或故障恢复时就通知 ERPS 进行链路倒换。

ERPS 环实例的成员端口通过 Track 项与链路检测协议进行联动，目前仅支持与 CFD（Connectivity Fault Detection，连通错误检测）的连续性检测功能联动。当端口与 CFD 连续性检测功能联动时，CFD 按照检测 VLAN 和检测端口来通知故障检测事件，只有当 CFD 检测的 VLAN 与端口所在 ERPS 环实例的控制 VLAN 或保护 VLAN 一致时，才响应此事件。有关 Track 项和 CFD 连续性检测功能的详细介绍，请分别参见“可靠性配置指导”中的“Track”和“CFD”。

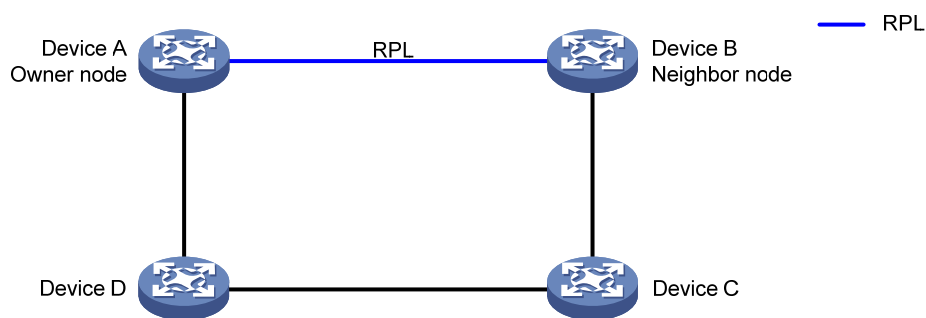
1.1.7 ERPS典型组网

ERPS 的正常运行依赖于用户正确的配置。下面介绍几种典型的组网。

1. 单环

如 图 1-5 所示，网络拓扑中只有一个环，此时只需定义一个 ERPS 环。

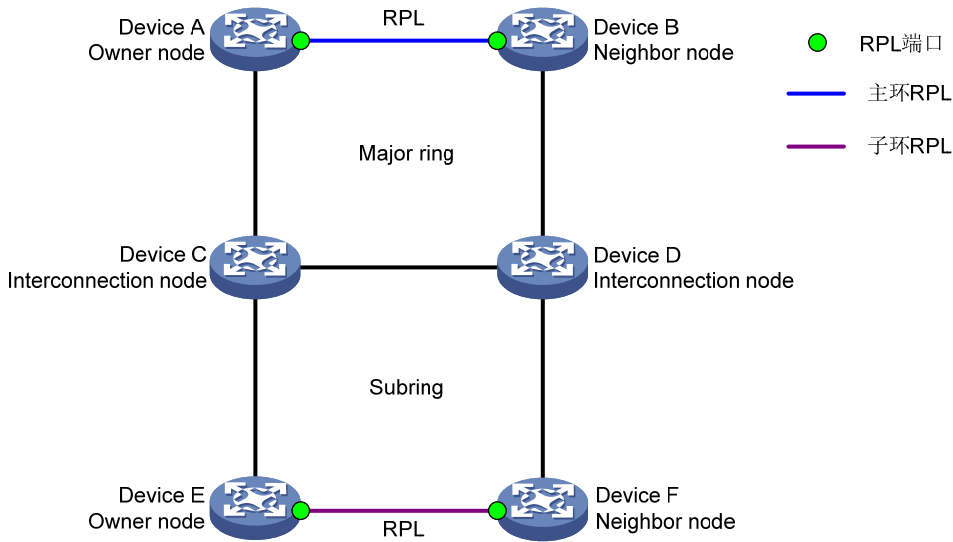
图1-5 单环示意图



2. 单子环

如 图 1-6 所示，网络拓扑中有两个环，两环之间有两个公共节点，选择其中一个环为主环，另一个环为子环。

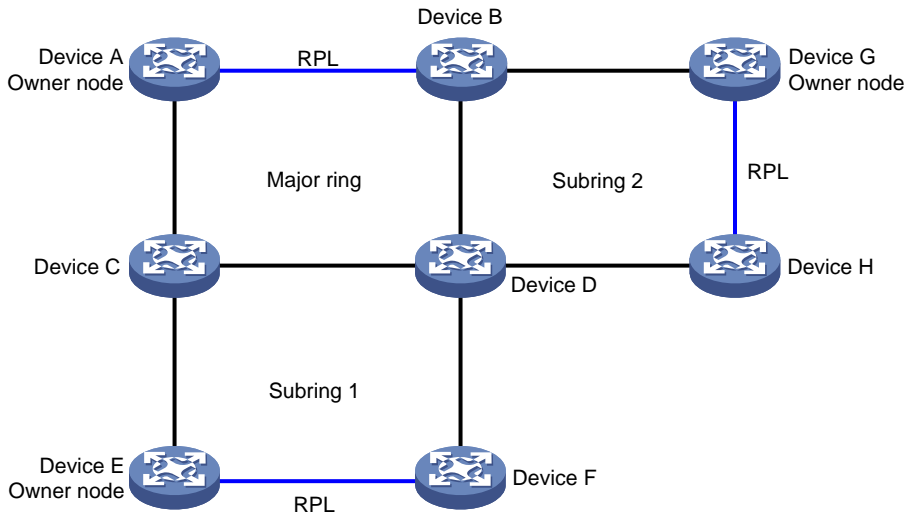
图1-6 单子环示意图



3. 多子环连接主环

如 图 1-7 所示，网络拓扑中有三个或三个以上的环，每个子环与主环之间有两个公共节点。

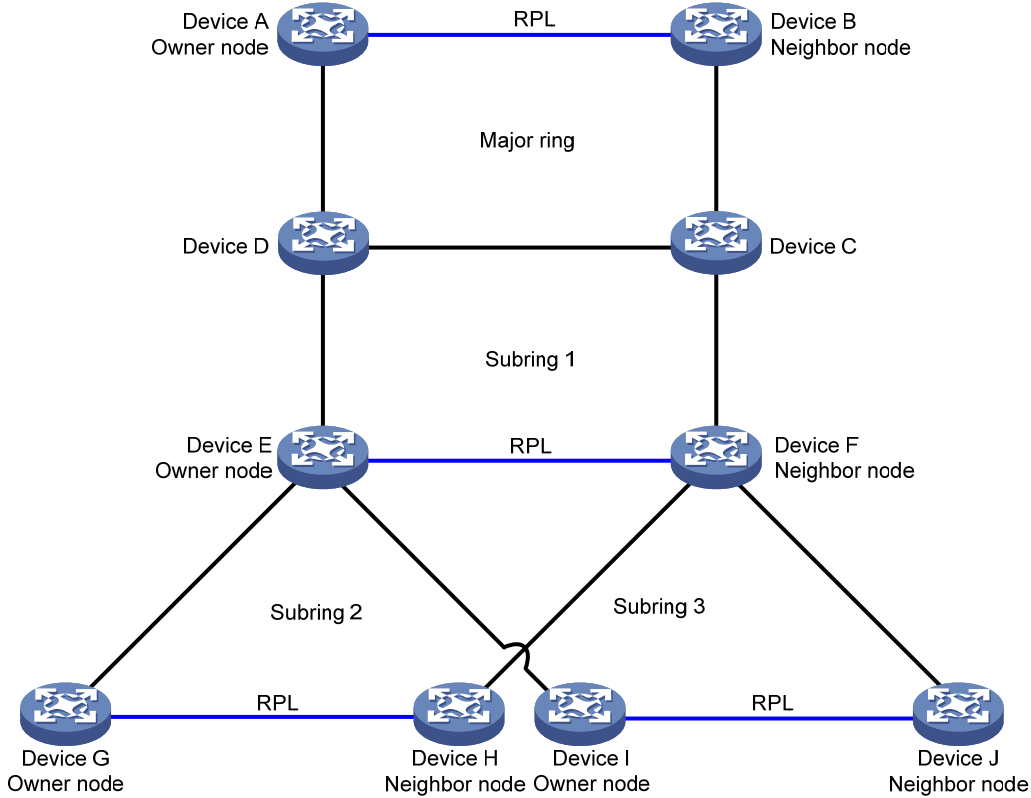
图1-7 多子环连接主环示意图



4. 子环连接单一子环

如 图 1-8 所示，网络拓扑中有三个或三个以上的环，在单子环拓扑的基础上，多个子环和子环 1 之间有两个公共节点。

图1-8 子环连接单一子环示意图



5. 子环连接多环

如 图 1-9, 图 1-10 所示, 网络拓扑中有三个或三个以上的环, 在单子环拓扑的基础上, 至少有一个子环与其它两个环各有一个公共节点, 分为以下两种情况。

图1-9 子环连接多环（子环 2 与主环、子环 1 同时相连）示意图

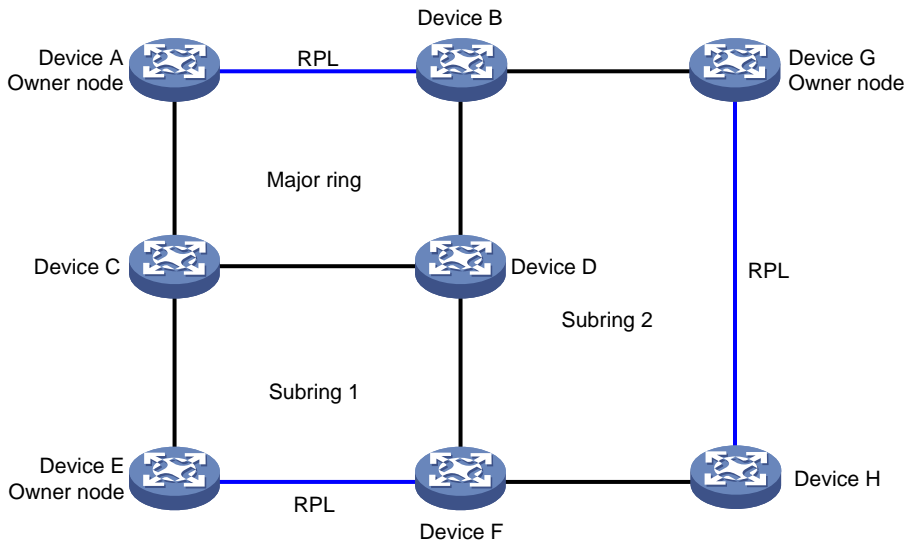
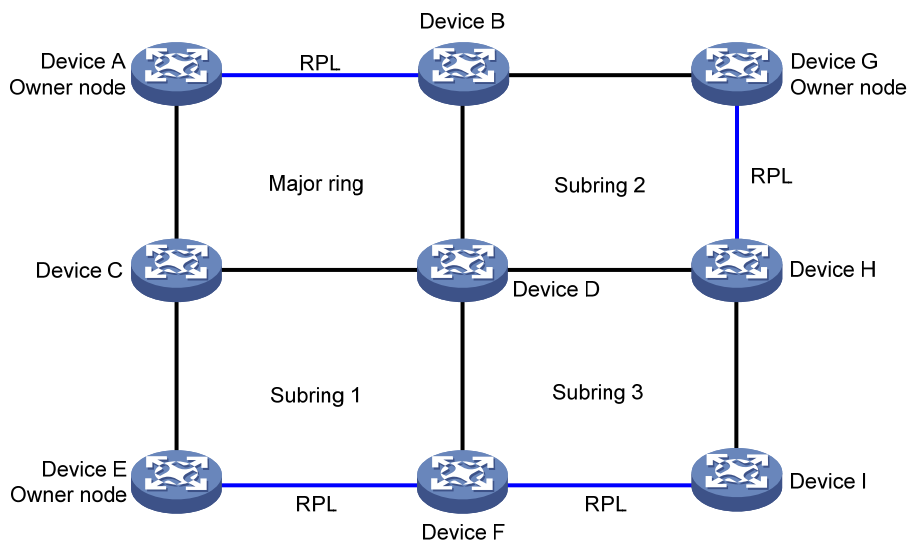


图1-10 子环连接多环（子环 3 与子环 1、子环 2 同时相连）示意图



1.1.8 协议规范

与 ERPS 相关的协议规范有：

- ITU-T G.8032: Recommendation ITU-T G.8032/Y.1344, Ethernet ring protection switching.
- IEEE 802.1D: IEEE Std 802.1D™-2004, IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Bridges.
- IEEE 802.3: IEEE Std 802.3-2008, IEEE Standard for Information technology.

1.2 ERPS配置限制和指导

由于 ERPS 没有自动选举机制，只有当环网中各节点的配置都正确时，才能真正实现环网的检测和保护，因此请保证配置的准确性。

1.3 ERPS配置任务简介

ERPS 配置任务如下：

(1) [全局使能ERPS](#)

欲指定为 ERPS 节点的设备均需进行本配置。

(2) [配置ERPS环](#)

ERPS 环上所有节点均需进行本配置。

a. [创建ERPS环](#)

b. [配置ERPS环成员端口](#)

c. [配置控制VLAN](#)

d. [配置保护VLAN](#)

e. [配置ERPS节点角色](#)

(3) [在实例中使能ERPS协议](#)

ERPS 环上所有节点均需进行本配置。

- (4) (可选) [配置ERPS环发送报文的目的MAC地址所携带的环号](#)

ERPS 环上所有节点均需进行本配置。

- (5) (可选) [配置R-APS报文级别](#)

ERPS 环上所有节点均需进行本配置。

- (6) (可选) [配置ERPS定时器](#)

ERPS 环上所有节点均需进行 Guard 定时器和 Hold-Off 定时器配置。

ERPS 环上 Owner 节点均需进行 WTR 定时器配置。

- (7) (可选) [配置ERPS非回切模式](#)

ERPS 环上 Owner 节点均需进行本配置。

- (8) (可选) [配置ERPS倒换模式](#)

ERPS 环上需要阻塞端口的节点均需进行本配置。

- (9) (可选) [配置子环关联环](#)

ERPS 环上 Interconnection 节点均需进行本配置。

- (10) (可选) [开启互联节点Flush透传功能](#)

ERPS 环上 Interconnection 节点均需进行本配置。

- (11) (可选) [配置ERPS环成员端口的Track联动](#)

- (12) (可选) [清除ERPS环上FS/MS模式的配置 ERPS典型配置举例](#)

1.4 ERPS配置准备

配置 ERPS 之前，需要完成以下任务：

- 搭建以太网环形拓扑的组网环境。
- 根据网络拓扑情况划分出 ERPS 环，接着根据业务规划情况划分出 ERPS 实例，再确定各 ERPS 实例的控制 VLAN 和保护 VLAN，然后根据流量路径确定每个 ERPS 环的实例内的各个节点角色。

1.5 全局使能ERPS

1. 配置限制和指导

本任务需要在所有欲指定为 ERPS 节点的设备上执行。

只有全局和实例都使能 ERPS 协议，ERPS 功能才能生效。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 全局使能 ERPS 协议。

```
erps enable
```

缺省情况下，ERPS 协议未全局使能。

1.6 配置ERPS环

1.6.1 创建ERPS环

1. 配置限制和指导

本任务需要在 ERPS 环上所有节点上执行。

创建 ERPS 环时需要指定环 ID，环 ID 用来唯一标识一个 ERPS 环，在同一 ERPS 环上的所有节点上应配置相同的环 ID。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 ERPS 环，并进入 ERPS 环视图。

```
erps ring ring-id
```

- (3) （可选）配置环为子环。

```
ring-type sub-ring
```

缺省情况下，ERPS 环为主环。

1.6.2 配置ERPS环成员端口

1. 配置限制和指导

本任务需要在各节点欲接入 ERPS 环的端口上执行。

由于 ERPS 环成员端口将自动允许控制 VLAN 的报文通过，因此无需配置 ERPS 环成员端口允许控制 VLAN 的报文通过。

不建议在 ERPS 环成员端口上启用以太网 OAM 远端环回功能，否则可能引起短时间的广播风暴。有关 OAM 的详细介绍，请参见“可靠性配置指导”中的“以太网 OAM”。

建议在 ERPS 环成员端口上通过 **link-delay** 命令将端口的物理连接状态 up/down 抑制时间配置为 0 秒（即不抑制），以提高 ERPS 的拓扑变化收敛速度。有关 **link-delay** 命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“以太网接口”。

ERPS 环成员端口必须为 Trunk 类型。

请勿将一个端口同时加入聚合组和 ERPS 环，否则该端口在 ERPS 环中将不会生效，也无法使用 **display erps detail** 命令查看到。

2. 配置ERPS环成员端口属性

- (1) 进入系统视图。

```
system-view
```

- (2) 进入二层以太网或二层聚合接口视图。

```
interface interface-type interface-number
```

- (3) 配置端口的链路类型为 Trunk 类型。

```
port link-type trunk
```

缺省情况下，端口的链路类型为 Access 类型。

本命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“VLAN”。

- (4) 配置 Trunk 端口允许保护 VLAN 的报文通过。

```
port trunk permit vlan { vlan-id-list | all }
```

缺省情况下，Trunk 端口只允许 VLAN 1 的报文通过。

本命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“VLAN”。

- (5) 关闭生成树协议。

```
undo stp enable
```

缺省情况下，端口上的生成树协议处于开启状态。

本命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“生成树”。

3. 配置ERPS环成员端口

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ERPS 环视图。

```
erps ring ring-id
```

- (3) 配置 ERPS 环成员端口。

```
{ port0 | port1 } interface interface-type interface-number
```

缺省情况下，ERPS 环无成员端口。

1.6.3 配置控制VLAN

1. 配置限制和指导

- 本任务需要在 ERPS 环上所有节点上执行。
- 控制 VLAN 必须为设备上尚未创建的 VLAN。
- 同一 ERPS 实例内的所有节点上应配置相同的控制 VLAN。
- 请勿将接入 ERPS 环当前实例的端口的缺省 VLAN 配置为控制 VLAN。
- 控制 VLAN 内不能运行 QinQ 和 VLAN 映射功能，否则 ERPS 协议报文将无法正确收发。
- 控制 VLAN 必须在配置 ERPS 实例之后才可配置，但在实例使能之后不可以修改控制 VLAN。
- 如果要在未配置 ERPS 功能的设备上透传 ERPS 协议报文，应保证该设备上只有接入 ERPS 环当前实例的那两个端口允许该 ERPS 环当前实例所对应控制 VLAN 的报文通过，而其它端口都不允许其通过；否则，其它端口的报文可能通过透传进入控制 VLAN，从而对 ERPS 环实例产生冲击。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ERPS 环视图。

```
erps ring ring-id
```

- (3) 进入 ERPS 实例视图。

```
instance instance-id
```

- (4) 配置 ERPS 环的控制 VLAN。

```
control-vlan vlan-id
```

1.6.4 配置保护VLAN

1. 配置限制和指导

本任务需要在 ERPS 环上所有节点上执行。

同一 ERPS 环实例内的所有节点上应配置相同的保护 VLAN。

在配置负载分担时，不同 ERPS 实例的保护 VLAN 必须不同。

2. 配置准备

配置保护 VLAN 前需要配置 MST 域，并配置关于保护 VLAN 的 VLAN 映射表，关于 MST 域的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ERPS 环视图。

```
erps ring ring-id
```

- (3) 进入 ERPS 实例视图。

```
instance instance-id
```

- (4) 配置 ERPS 实例的保护 VLAN。

```
protected-vlan reference-instance instance-id-list
```

1.6.5 配置ERPS节点角色

1. 配置限制和指导

本任务需要在 ERPS 环上各节点上执行。

同一个环上配置节点角色过程中不能同时出现两个 Owner 节点，否则不能保证配置完成后 Owner 节点功能正常。

当配置节点为 **interconnection** 时，当前的环必须是子环。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ERPS 环视图。

```
erps ring ring-id
```

- (3) 进入 ERPS 实例视图。

```
instance instance-id
```

- (4) 配置 ERPS 节点角色。

```
node-role { { owner | neighbor } rpl | interconnection } { port0 | port1 }
```

缺省情况下，节点为 Normal 节点。

1.7 在实例中使能ERPS协议

1. 配置限制和指导

本任务需要在 ERPS 环上所有节点上执行。

当存在控制 VLAN 和保护 VLAN 时，实例才能使能 ERPS 协议。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ERPS 环视图。

```
erps ring ring-id
```

- (3) 进入 ERPS 实例视图。

```
instance instance-id
```

- (4) 在 ERPS 实例使能 ERPS 协议。

```
instance enable
```

缺省情况下，ERPS 实例中的 ERPS 协议处于关闭状态。

1.8 配置ERPS环发送报文的目的MAC地址所携带的环号

1. 功能简介

不同环 ID 的报文通过目的 MAC 地址来区分（目的 MAC 地址的最后一个字节表示环 ID）。

2. 配置限制和指导

本任务需要在 ERPS 环上所有节点上执行。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ERPS 环视图。

```
erps ring ring-id
```

- (3) 配置 ERPS 环发送报文的目的 MAC 地址所携的环号为当前环号。

```
r-aps ring-mac
```

缺省情况下，R-APS 报文目的 MAC 地址的最后一个字节为 1。

1.9 配置R-APS报文级别

1. 配置限制和指导

本任务需要在 ERPS 环上所有节点上执行。

同一环上相同实例内的节点 R-APS 报文级别必须相同。

本节点不处理 R-APS 报文级别比自己大的 R-APS 报文。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 进入 ERPS 环视图。
erps ring *ring-id*
- (3) 进入 ERPS 实例视图。
instance *instance-id*
- (4) 配置 R-APS 报文级别。
r-aps level *level-value*
缺省情况下，R-APS 报文级别为 7。

1.10 配置ERPS定时器

1. 配置限制和指导

Guard 定时器和 Hold-Off 定时器需要在 ERPS 环上所有节点上配置。
WTR 定时器需要在 ERPS 环上 Owner 节点上配置。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 进入 ERPS 环视图。
erps ring *ring-id*
- (3) 进入 ERPS 实例视图。
instance *instance-id*
- (4) 配置 Guard 定时器。
timer guard *guard-value*
缺省情况下，Guard 定时器的值为 500 毫秒。
- (5) 配置 Hold-Off 定时器。
timer hold-off *hold-off-value*
缺省情况下，Hold-off 定时器的值为 0 毫秒。
- (6) 配置 WTR 定时器。
timer wtr *wtr-value*
缺省情况下，WTR 定时器的值为 5 分钟。

1.11 配置ERPS非回切模式

1. 功能简介

如果用户不想因为故障节点恢复而引起链路再次切换，可以配置 ERPS 非回切模式，维持当前 ERPS 环拓扑结构，使数据转发路径保持不变。

2. 配置限制和指导

本任务需要在 ERPS 环上 Owner 节点上执行。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ERPS 环视图。

```
erps ring ring-id
```

- (3) 进入 ERPS 实例视图。

```
instance instance-id
```

- (4) 配置实例为非回切模式。

```
revertive-operation non-revertive
```

缺省情况下，为回切模式。

1.12 配置ERPS倒换模式

1. 配置限制和指导

本任务需要在 ERPS 环上需要阻塞端口的节点上执行。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 ERPS 倒换模式。

```
erps switch { force | manual } ring ring-id instance instance-id { port0 | port1 }
```

缺省情况下，未配置 ERPS 倒换模式。

1.13 配置子环关联环

1. 功能简介

多环模型中，当某个子环的拓扑变换需要被其它环感知时，需要配置将该子环与指定环进行关联。

2. 配置限制和指导

本任务需要在 ERPS 环上互联系节点上执行。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ERPS 子环视图。

```
erps ring ring-id
```

- (3) 进入 ERPS 实例视图。

```
instance instance-id
```

- (4) 配置子环关联环。

```
sub-ring connect ring ring-id instance instance-id
```

缺省情况下，子环无关联环。

1.14 开启互联节点Flush透传功能

1. 功能简介

多环模型中，子环的拓扑发生变化时，会发送 Flush 报文，当开启互联节点的 Flush 透传功能后，子环的 Flush 报文才透传至其所关联的环中，从而使得所关联的环快速刷新 MAC 地址表项，提高收敛速度。

2. 配置限制和指导

本任务需要在 ERPS 环上互联节点上执行。

开启互联节点 Flush 透传功能时必须同时配置互联节点上的子环与其它环相关联。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启互联节点 Flush 透传功能。

```
erps tcn-propagation
```

缺省情况下，Flush 透传功能处于关闭状态。

1.15 配置ERPS环成员端口的Track联动

1. 配置限制和指导

在配置端口与 Track 项联动之前，必须保证该端口已加入相应的 ERPS 环实例。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入二层以太网或二层聚合接口视图。

```
interface interface-type interface-number
```

- (3) 配置 ERPS 环成员端口的 Track 联动。

```
port erps ring ring-id instance instance-id track track-entry-index
```

缺省情况下，未配置 ERPS 环成员端口与 Track 联动。

1.16 清除ERPS环上FS/MS模式的配置

1. 功能简介

通过本功能可将非回切模式的 ERPS 环返回到回切模式，但不清除非回切模式配置。

如果用户清除了 ERPS 环上 FS/MS 模式的配置，当故障链路恢复时，Owner 节点可跳过 WTR 定时器的超时等待，直接启动链路恢复倒换。

2. 配置步骤

- (1) 进入系统视图。
`system-view`
- (2) 清除 ERPS 环上 FS/MS 模式的配置。
`erps clear ring ring-id instance instance-id`

1.17 ERPS显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 ERPS 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 ERPS 报文统计信息。

表1-2 ERPS 显示和维护

操作	命令
显示ERPS的摘要信息	<code>display erps</code>
显示ERPS的详细信息	<code>display erps detail ring ring-id [instance instance-id]</code>
显示ERPS报文的统计信息	<code>display erps statistics [ring ring-id [instance instance-id]]</code>
清除ERPS报文的统计信息	<code>reset erps statistics ring ring-id [instance instance-id]</code>

1.18 ERPS典型配置举例

1.18.1 单环配置举例

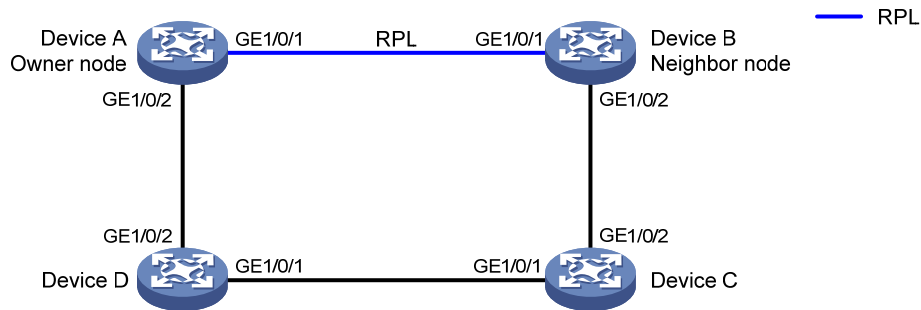
1. 组网需求

如 [图 1-11](#) 所示，为了解决单环上网络环路的问题，在环上各节点配置ERPS相关命令。

- Device A~Device D 构成 ERPS 环 1，该环的控制 VLAN 为 VLAN 100，保护 VLAN 为 VLAN 1~30。
- Device A 为 ERPS 环的 Owner 节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为 ERPS 环 1 的成员端口 port0 和 port1 端口，port0 为 RPL 端口。
- Device B 为 ERPS 环的 Neighbor 节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为 ERPS 环 1 的成员端口 port0 和 port1 端口，port0 为 RPL 端口。
- Device C 和 Device D 为 ERPS 环的 Normal 节点，其各自的 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为 ERPS 环 1 的成员端口 port0 和 port1 端口。

2. 组网图

图1-11 单环配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

创建 ERPS 环 1。

```
[DeviceA] erps ring 1
```

配置 ERPS 环成员端口。

```
[DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2
```

配置 ERPS 环发送报文的目的 MAC 地址所携带的环号。

```
[DeviceA-erps-ring1] r-aps ring-mac
```

创建 ERPS 实例 1。


```

[DeviceA-erps-ring1] instance 1
# 配置节点角色。
[DeviceA-erps-ring1-inst1] node-role owner rpl port0
# 配置控制 VLAN。
[DeviceA-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。
[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit
[DeviceA-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 1，该 MA 服务于 VLAN 1。
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
# 在服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的外向 MEP 1001，并使能其 CCM 报文发送功能。
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 2，该 MA 服务于 VLAN 2。
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
# 在服务实例 2 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 2 内的外向 MEP 2001，并使能其 CCM 报文发送功能。
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
# 创建与服务实例 1 中 MEP 1001 的 CFD 连续性检测功能关联的 Track 项 1。
[DeviceA] track 1 cfd cc service-instance 1 mep 1001
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
# 创建与服务实例 2 中 MEP 2001 的 CFD 连续性检测功能关联的 Track 项 2。
[DeviceA] track 2 cfd cc service-instance 2 mep 2001
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
```

使能 ERPS 协议。

```
[DeviceA] erps enable
```

(2) 配置 Device B

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
```

创建 ERPS 环 1。

```
[DeviceB] erps ring 1
```

配置 ERPS 环成员端口。

```
[DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2
```

配置 ERPS 环发送报文的目的 MAC 地址所携带的环号。

```
[DeviceB-erps-ring1] r-aps ring-mac
```

创建 ERPS 实例 1。

```
[DeviceB-erps-ring1] instance 1
```

配置节点角色。

```
[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0
```

配置控制 VLAN。

```
[DeviceB-erps-ring1-inst1] control-vlan 100
```

配置保护 VLAN。

```
[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1
```

实例 1 使能 ERPS 协议。

```

[DeviceB-erps-ring1-inst1] instance enable
[DeviceB-erps-ring1-inst1] quit
[DeviceB-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 1，该 MA 服务于 VLAN 1。
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
# 在服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的外向
MEP 1002，并使能其 CCM 报文发送功能。
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceB-GigabitEthernet1/0/1] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 3，该 MA 服务于 VLAN 3。
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
# 在服务实例 3 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 3 内的外向
MEP 3002，并使能其 CCM 报文发送功能。
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable
[DeviceB-GigabitEthernet1/0/2] quit
# 创建与服务实例 1 中 MEP 1002 的 CFD 连续性检测功能关联的 Track 项 1。
[DeviceB] track 1 cfd cc service-instance 1 mep 1002
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 1 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit
# 创建与服务实例 3 中 MEP 3002 的 CFD 连续性检测功能关联的 Track 项 2。
[DeviceB] track 2 cfd cc service-instance 3 mep 3002
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 2 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit
# 使能 ERPS 协议。
[DeviceB] erps enable

```

(3) 配置 Device C

```

# 创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。
<DeviceC> system-view

```

```

[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
# 分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1～30 通过。
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
# 创建 ERPS 环 1。
[DeviceC] erps ring 1
# 配置 ERPS 环成员端口。
[DeviceC-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceC-erps-ring1] port1 interface gigabitethernet 1/0/2
# 配置 ERPS 环发送报文的目的 MAC 所携带的环号。
[DeviceC-erps-ring1] r-aps ring-mac
# 创建 ERPS 实例 1。
[DeviceC-erps-ring1] instance 1
# 配置控制 VLAN。
[DeviceC-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。
[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceC-erps-ring1-inst1] instance enable
[DeviceC-erps-ring1-inst1] quit
[DeviceC-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 3，该 MA 服务于 VLAN 3。
[DeviceC] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
# 在服务实例 3 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 3 内的外向 MEP 3001，并使能其 CCM 报文发送功能。
[DeviceC] cfd meplist 3001 3002 service-instance 3

```

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3001 enable
[DeviceC-GigabitEthernet1/0/2] quit
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 4，该 MA 服务于 VLAN 4。

```
[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

在服务实例 4 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 4 内的外向 MEP 4001，并使能其 CCM 报文发送功能。

```
[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
[DeviceC-GigabitEthernet1/0/1] quit
```

创建与服务实例 3 中 MEP 3001 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceC] track 1 cfd cc service-instance 3 mep 3001
```

配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

创建与服务实例 4 中 MEP 4001 的 CFD 连续性检测功能关联的 Track 项 2。

```
[DeviceC] track 2 cfd cc service-instance 4 mep 4001
```

配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

使能 ERPS 协议。

```
[DeviceC] erps enable
```

(4) 配置 Device D

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

```

[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
# 创建 ERPS 环 1。
[DeviceD] erps ring 1
# 配置 ERPS 环成员端口。
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2
# 配置 ERPS 环发送报文的目的 MAC 所携带的环号。
[DeviceD-erps-ring1] r-aps ring-mac
# 创建 ERPS 实例 1。
[DeviceD-erps-ring1] instance 1
# 配置控制 VLAN。
[DeviceD-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceD-erps-ring1-inst1] instance enable
[DeviceD-erps-ring1-inst1] quit
[DeviceD-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 2，该 MA 服务于 VLAN 2。
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
# 在服务实例 2 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 2 内的外向
MEP 2002，并使能其 CCM 报文发送功能。
[DeviceD] cfd meplist 2001 2002 service-instance 2
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceD-GigabitEthernet1/0/2] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 4，该 MA 服务于 VLAN 4。
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
# 在服务实例 4 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 4 内的外向
MEP 4002，并使能其 CCM 报文发送功能。
[DeviceD] cfd meplist 4001 4002 service-instance 4
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound

```

```
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
[DeviceD-GigabitEthernet1/0/1] quit
# 创建与服务实例 2 中 MEP 2002 的 CFD 连续性检测功能关联的 Track 项 1。
[DeviceD] track 1 cfd cc service-instance 2 mep 2002
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 1 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
# 创建与服务实例 4 中 MEP 4002 的 CFD 连续性检测功能关联的 Track 项 2。
[DeviceD] track 2 cfd cc service-instance 4 mep 4002
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 2 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
# 使能 ERPS 协议。
[DeviceD] erps enable
```

4. 验证配置

Device A 上的 ERPS 环 1 的运行情况。

```
[DeviceA] display erps detail ring 1
Ring ID                : 1
Port0                  : GigabitEthernet1/0/1
Port1                  : GigabitEthernet1/0/2
Subring                : No
Default MAC            : No

Instance ID            : 1
Node role               : Owner
Node state              : Idle
Connect(ring/instance): -
Control VLAN           : 100
Protected VLAN         : Reference-instance 1
Guard timer            : 500 ms
Hold-off timer         : 0 ms
WTR timer              : 5 min
Revertive operation    : Revertive
Enable status          : Yes, Active status : Yes
R-APS level            : 7
Port                   PortRole           PortStatus
-----
Port0                   RPL               Block
Port1                   Non-RPL            Up
```

本节点为 Owner 节点，ERPS 环处于 Idle 状态，RPL 端口阻塞，非 RPL 端口放开。

1.18.2 单子环配置举例

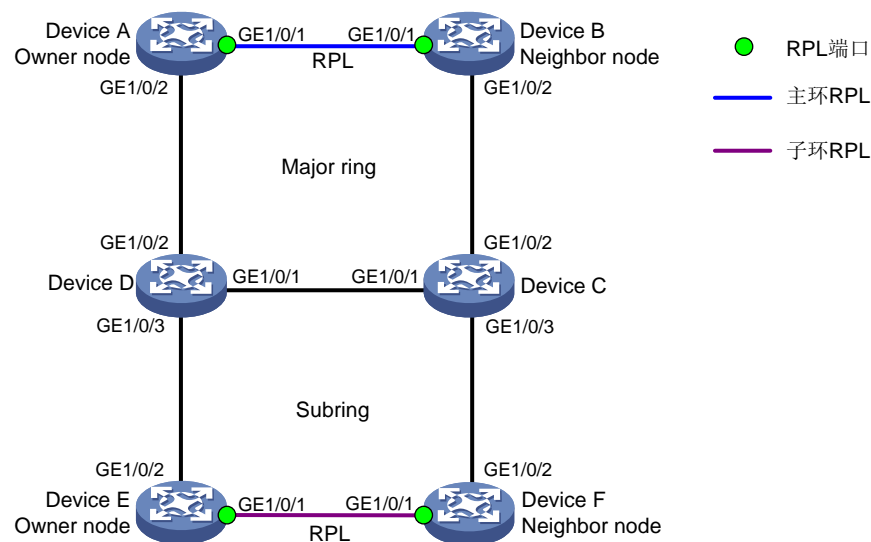
1. 组网需求

如 图 1-12，为了解决子环与主环配合时，子环上出现网络环路的问题，在环上各节点配置ERPS相关命令。

- Device A~Device D 构成 ERPS 主环，该环的控制 VLAN 为 VLAN 100，保护 VLAN 为 VLAN 1~30。Device C、Device D、Device E、Device F 构成子环，该环的控制 VLAN 为 VLAN 200，保护 VLAN 为 VLAN 1~30。
- Device A 为主环的 Owner 节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为 ERPS 环 1 的成员端口 port0 和 port1 端口，port0 为 RPL 端口。
- Device B 为主环的 Neighbor 节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为 ERPS 环 1 的成员端口 port0 和 port1 端口，port0 为 RPL 端口。
- Device C 和 Device D 为 Interconnection 节点，其各自的 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为 ERPS 环 1 的成员端口 port0 和 port1 端口，GigabitEthernet1/0/3 为 Interconnection 端口。
- Device E 为子环的 Owner 节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为 ERPS 环 1 的成员端口 port0 和 port1 端口，port0 为 RPL 端口。
- Device F 为子环的 Neighbor 节点，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为 ERPS 环 1 的成员端口 port0 和 port1 端口，port0 为 RPL 端口。

2. 组网图

图1-12 相交环配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
```



```

[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
# 分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑
制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1～
30 通过。

[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
# 创建 ERPS 环 1。

[DeviceA] erps ring 1
# 配置 ERPS 环成员端口。

[DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2
# 创建 ERPS 实例 1。

[DeviceA-erps-ring1] instance 1
# 配置节点角色。

[DeviceA-erps-ring1-inst1] node-role owner rpl port0
# 配置控制 VLAN。

[DeviceA-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。

[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。

[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit
[DeviceA-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。

[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 1，该 MA 服务于 VLAN 1。

[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
# 在服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的外向
MEP 1001，并使能其 CCM 报文发送功能。

[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound

```

```
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 2，该 MA 服务于 VLAN 2。

```
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
```

在服务实例 2 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 2 内的外向 MEP 2001，并使其 CCM 报文发送功能。

```
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

创建与服务实例 1 中 MEP 1001 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceA] track 1 cfd cc service-instance 1 mep 1001
```

配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
```

创建与服务实例 2 中 MEP 2001 的 CFD 连续性检测功能关联的 Track 项 2。

```
[DeviceA] track 2 cfd cc service-instance 2 mep 2001
```

配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
```

使能 ERPS 协议。

```
[DeviceA] erps enable
```

(2) 配置 Device B

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

```

[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
# 创建 ERPS 环 1。
[DeviceB] erps ring 1
# 配置 ERPS 环成员端口。
[DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2
# 创建 ERPS 实例 1。
[DeviceB-erps-ring1] instance 1
# 配置节点角色。
[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0
# 配置控制 VLAN。
[DeviceB-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。
[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceB-erps-ring1-inst1] instance enable
[DeviceB-erps-ring1-inst1] quit
[DeviceB-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 1，该 MA 服务于 VLAN 1。
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
# 在服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的外向
MEP 1002，并使能其 CCM 报文发送功能。
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceB-GigabitEthernet1/0/1] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 3，该 MA 服务于 VLAN 3。
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
# 在服务实例 3 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 3 内的外向
MEP 3002，并使能其 CCM 报文发送功能。
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable
[DeviceB-GigabitEthernet1/0/2] quit

```

创建与服务实例 1 中 MEP 1002 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceB] track 1 cfd cc service-instance 1 mep 1002
```

配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
```

```
[DeviceB-GigabitEthernet1/0/1] undo shutdown
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

创建与服务实例 3 中 MEP 3002 的 CFD 连续性检测功能关联的 Track 项 2。

```
[DeviceB] track 2 cfd cc service-instance 3 mep 3002
```

配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
```

```
[DeviceB-GigabitEthernet1/0/2] undo shutdown
```

```
[DeviceB-GigabitEthernet1/0/2] quit
```

使能 ERPS 协议。

```
[DeviceB] erps enable
```

(3) 配置 Device C

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceC> system-view
```

```
[DeviceC] vlan 1 to 30
```

```
[DeviceC] stp region-configuration
```

```
[DeviceC-mst-region] instance 1 vlan 1 to 30
```

```
[DeviceC-mst-region] active region-configuration
```

```
[DeviceC-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1，GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
```

```
[DeviceC-GigabitEthernet1/0/1] link-delay 0
```

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

```
[DeviceC] interface gigabitethernet 1/0/2
```

```
[DeviceC-GigabitEthernet1/0/2] link-delay 0
```

```
[DeviceC-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
```

```
[DeviceC-GigabitEthernet1/0/2] quit
```

```
[DeviceC] interface gigabitethernet 1/0/3
```

```
[DeviceC-GigabitEthernet1/0/3] link-delay 0
```

```
[DeviceC-GigabitEthernet1/0/3] undo stp enable
```

```
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
```

```
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
```

```

[DeviceC-GigabitEthernet1/0/3] quit
# 创建 ERPS 环 1.
[DeviceC] erps ring 1
# 配置 ERPS 环成员端口。
[DeviceC-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceC-erps-ring1] port1 interface gigabitethernet 1/0/2
# 创建 ERPS 实例。
[DeviceC-erps-ring1] instance 1
# 配置控制 VLAN。
[DeviceC-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。
[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceC-erps-ring1-inst1] instance enable
[DeviceC-erps-ring1-inst1] quit
[DeviceC-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 3，该 MA 服务于 VLAN 3。
[DeviceC] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
# 在服务实例 3 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 3 内的外向
MEP 3001，并使能其 CCM 报文发送功能。
[DeviceC] cfd meplist 3001 3002 service-instance 3
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3001 enable
[DeviceC-GigabitEthernet1/0/2] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 4，该 MA 服务于 VLAN 4。
[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
# 在服务实例 4 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 4 内的外向
MEP 4001，并使能其 CCM 报文发送功能。
[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
[DeviceC-GigabitEthernet1/0/1] quit
# 创建与服务实例 3 中 MEP 3001 的 CFD 连续性检测功能关联的 Track 项 1。
[DeviceC] track 1 cfd cc service-instance 3 mep 3001
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 1 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown

```

```

[DeviceC-GigabitEthernet1/0/2] quit
# 创建与服务实例 4 中 MEP 4001 的 CFD 连续性检测功能关联的 Track 项 2。
[DeviceC] track 2 cfd cc service-instance 4 mep 4001
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 2 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
# 创建 ERPS 环 2。
[DeviceC] erps ring 2
# 配置 ERPS 环成员端口。
[DeviceC-erps-ring2] port0 interface gigabitethernet 1/0/3
# 配置当前环为子环。
[DeviceC-erps-ring2] ring-type sub-ring
# 创建 ERPS 实例 1。
[DeviceC-erps-ring2] instance 1
# 配置节点角色。
[DeviceC-erps-ring2-inst1] node-role interconnection port0
# 配置控制 VLAN。
[DeviceC-erps-ring2-inst1] control-vlan 110
# 配置保护 VLAN。
[DeviceC-erps-ring2-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceC-erps-ring2-inst1] instance enable
[DeviceC-erps-ring2-inst1] quit
[DeviceC-erps-ring2] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 5，该 MA 服务于 VLAN 5。
[DeviceC] cfd service-instance 5 ma-id vlan-based md MD_A vlan 5
# 在服务实例 5 内配置 MEP 列表，在端口 GigabitEthernet1/0/3 上创建服务实例 5 内的外向
MEP 5001，并使能其 CCM 报文发送功能。
[DeviceC] cfd meplist 5001 5002 service-instance 5
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] cfd mep 5001 service-instance 5 outbound
[DeviceC-GigabitEthernet1/0/3] cfd cc service-instance 5 mep 5001 enable
[DeviceC-GigabitEthernet1/0/3] quit
# 创建与服务实例 5 中 MEP 5001 的 CFD 连续性检测功能关联的 Track 项 1。
[DeviceC] track 1 cfd cc service-instance 5 mep 5001
# 配置 ERPS 环 2 实例 1 的端口 GigabitEthernet1/0/3 通过 Track 项 1 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port erps ring 2 instance 1 track 1
[DeviceC-GigabitEthernet1/0/3] undo shutdown
[DeviceC-GigabitEthernet1/0/3] quit

```

使能 ERPS 协议。

```
[DeviceC] erps enable
```

(4) 配置 Device D

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceD> system-view
```

```
[DeviceD] vlan 1 to 30
```

```
[DeviceD] stp region-configuration
```

```
[DeviceD-mst-region] instance 1 vlan 1 to 30
```

```
[DeviceD-mst-region] active region-configuration
```

```
[DeviceD-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1，GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceD] interface gigabitethernet 1/0/1
```

```
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

```
[DeviceD-GigabitEthernet1/0/1] quit
```

```
[DeviceD] interface gigabitethernet 1/0/2
```

```
[DeviceD-GigabitEthernet1/0/2] link-delay 0
```

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
```

```
[DeviceD-GigabitEthernet1/0/2] quit
```

```
[DeviceD] interface gigabitethernet 1/0/3
```

```
[DeviceD-GigabitEthernet1/0/3] link-delay 0
```

```
[DeviceD-GigabitEthernet1/0/3] undo stp enable
```

```
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
```

```
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
```

```
[DeviceD-GigabitEthernet1/0/3] quit
```

创建 ERPS 环 1。

```
[DeviceD] erps ring 1
```

配置 ERPS 环成员端口。

```
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
```

```
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2
```

创建 ERPS 实例 1。

```
[DeviceD-erps-ring1] instance 1
```

配置控制 VLAN。

```
[DeviceD-erps-ring1-inst1] control-vlan 100
```

配置保护 VLAN。

```
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1
```

实例 1 使能 ERPS 协议。

```
[DeviceD-erps-ring1-inst1] instance enable
```

```
[DeviceD-erps-ring1-inst1] quit
```

```

[DeviceD-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 2，该 MA 服务于 VLAN 2。
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
# 在服务实例 2 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 2 内的外向 MEP 2002，并使其 CCM 报文发送功能。
[DeviceD] cfd meplist 2001 2002 service-instance 2
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceD-GigabitEthernet1/0/2] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 4，该 MA 服务于 VLAN 4。
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
# 在服务实例 4 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 4 内的外向 MEP 4002，并使其 CCM 报文发送功能。
[DeviceD] cfd meplist 4001 4002 service-instance 4
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
[DeviceD-GigabitEthernet1/0/1] quit
# 创建与服务实例 2 中 MEP 2002 的 CFD 连续性检测功能关联的 Track 项 1。
[DeviceD] track 1 cfd cc service-instance 2 mep 2002
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
# 创建与服务实例 4 中 MEP 4002 的 CFD 连续性检测功能关联的 Track 项 2。
[DeviceD] track 2 cfd cc service-instance 4 mep 4002
# 配置 ERPS 环 1 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
# 创建 ERPS 环 2。
[DeviceD] erps ring 2
# 配置 ERPS 环成员端口。
[DeviceD-erps-ring2] port0 interface gigabitethernet 1/0/3
# 配置当前环为子环。
[DeviceD-erps-ring2] ring-type sub-ring

```


创建 ERPS 实例 1。

```
[DeviceD-erps-ring2] instance 1
```

配置节点角色。

```
[DeviceD-erps-ring2-inst1] node-role interconnection port0
```

配置控制 VLAN。

```
[DeviceD-erps-ring2-inst1] control-vlan 110
```

配置保护 VLAN。

```
[DeviceD-erps-ring2-inst1] protected-vlan reference-instance 1
```

实例 1 使能 ERPS 协议。

```
[DeviceD-erps-ring2-inst1] instance enable
```

```
[DeviceD-erps-ring2-inst1] quit
```

```
[DeviceD-erps-ring2] quit
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 6，该 MA 服务于 VLAN 6。

```
[DeviceD] cfd service-instance 6 ma-id vlan-based md MD_A vlan 6
```

在服务实例 6 内配置 MEP 列表，在端口 GigabitEthernet1/0/3 上创建服务实例 6 内的外向 MEP 6002，并使能其 CCM 报文发送功能。

```
[DeviceD] cfd meplist 6001 6002 service-instance 6
```

```
[DeviceD] interface gigabitethernet 1/0/3
```

```
[DeviceD-GigabitEthernet1/0/3] cfd mep 6002 service-instance 6 outbound
```

```
[DeviceD-GigabitEthernet1/0/3] cfd cc service-instance 6 mep 6002 enable
```

```
[DeviceD-GigabitEthernet1/0/3] quit
```

创建与服务实例 6 中 MEP 6002 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceD] track 1 cfd cc service-instance 6 mep 6002
```

配置 ERPS 环 2 实例 1 的端口 GigabitEthernet1/0/3 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceD] interface gigabitethernet 1/0/3
```

```
[DeviceD-GigabitEthernet1/0/3] port erps ring 2 instance 1 track 1
```

```
[DeviceD-GigabitEthernet1/0/3] undo shutdown
```

```
[DeviceD-GigabitEthernet1/0/3] quit
```

使能 ERPS 协议。

```
[DeviceD] erps enable
```

(5) 配置 Device E

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceE> system-view
```

```
[DeviceE] vlan 1 to 30
```

```
[DeviceE] stp region-configuration
```

```
[DeviceE-mst-region] instance 1 vlan 1 to 30
```

```
[DeviceE-mst-region] active region-configuration
```

```
[DeviceE-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceE] interface gigabitethernet 1/0/1
```

```
[DeviceE-GigabitEthernet1/0/1] link-delay 0
```

```

[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] link-delay 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] quit
# 创建 ERPS 环 2。
[DeviceE] erps ring 2
# 配置 ERPS 环成员端口。
[DeviceE-erps-ring2] port0 interface gigabitethernet 1/0/1
[DeviceE-erps-ring2] port1 interface gigabitethernet 1/0/2
# 配置当前环为子环。
[DeviceE-erps-ring2] ring-type sub-ring
# 创建 ERPS 实例 1。
[DeviceE-erps-ring2] instance 1
# 配置节点角色。
[DeviceE-erps-ring2-inst1] node-role owner rpl port0
# 配置控制 VLAN。
[DeviceE-erps-ring2-inst1] control-vlan 110
# 配置保护 VLAN。
[DeviceE-erps-ring2-inst1] protected-vlan reference-interface 1
# 实例 1 使能 ERPS 协议。
[DeviceE-erps-ring2-inst1] instance enable
[DeviceE-erps-ring2-inst1] quit
[DeviceE-erps-ring2] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceE] cfd enable
[DeviceE] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 6，该 MA 服务于 VLAN 6。
[DeviceE] cfd service-instance 6 ma-id vlan-based md MD_A vlan 6
# 在服务实例 6 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 1 内的外向
MEP 6001，并使能其 CCM 报文发送功能。
[DeviceE] cfd meplist 6001 6002 service-instance 6
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] cfd mep 6001 service-instance 6 outbound
[DeviceE-GigabitEthernet1/0/2] cfd cc service-instance 6 mep 6001 enable
[DeviceE-GigabitEthernet1/0/2] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 7，该 MA 服务于 VLAN 7。
[DeviceE] cfd service-instance 7 ma-id vlan-based md MD_A vlan 7
# 在服务实例 7 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 7 内的外向
MEP 7001，并使能其 CCM 报文发送功能。

```

```
[DeviceE] cfd meplist 7001 7002 service-instance 7
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] cfd mep 7001 service-instance 7 outbound
[DeviceE-GigabitEthernet1/0/1] cfd cc service-instance 7 mep 7001 enable
[DeviceE-GigabitEthernet1/0/1] quit
```

创建与服务实例 6 中 MEP 6001 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceE] track 1 cfd cc service-instance 6 mep 6001
```

配置 ERPS 环 2 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port erps ring 2 instance 1 track 1
[DeviceE-GigabitEthernet1/0/2] undo shutdown
[DeviceE-GigabitEthernet1/0/2] quit
```

创建与服务实例 7 中 MEP 7001 的 CFD 连续性检测功能关联的 Track 项 2。

```
[DeviceE] track 2 cfd cc service-instance 7 mep 7001
```

配置 ERPS 环 2 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port erps ring 2 instance 1 track 2
[DeviceE-GigabitEthernet1/0/1] undo shutdown
[DeviceE-GigabitEthernet1/0/1] quit
```

使能 ERPS 协议。

```
[DeviceE] erps enable
```

(6) 配置 Device F

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceF> system-view
[DeviceF] vlan 1 to 30
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 1 to 30
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] link-delay 0
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/1] quit
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] link-delay 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/2] quit
```

创建 ERPS 环 2。

```
[DeviceF] erps ring 2
```

配置 ERPS 环成员端口。

```
[DeviceF-erps-ring2] port0 interface gigabitethernet 1/0/1
```

```
[DeviceF-erps-ring2] port1 interface gigabitethernet 1/0/2
```

配置当前环为子环。

```
[DeviceF-erps-ring2] ring-type sub-ring
```

创建 ERPS 实例 1。

```
[DeviceF-erps-ring2] instance 1
```

配置节点角色。

```
[DeviceF-erps-ring2-inst1] node-role neighbor rpl port0
```

配置控制 VLAN。

```
[DeviceF-erps-ring2-inst1] control-vlan 110
```

配置保护 VLAN。

```
[DeviceF-erps-ring2-inst1] protected-vlan reference-instance 1
```

实例 1 使能 ERPS 协议。

```
[DeviceF-erps-ring2-inst1] instance enable
```

```
[DeviceF-erps-ring2-inst1] quit
```

```
[DeviceF-erps-ring2] quit
```

使能 CFD 功能，并创建级别为 5 的 MD MD_A。

```
[DeviceF] cfd enable
```

```
[DeviceF] cfd md MD_A level 5
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 5，该 MA 服务于 VLAN 5。

```
[DeviceF] cfd service-instance 5 ma-id vlan-based md MD_A vlan 5
```

在服务实例 5 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 1 内的外向 MEP 5002，并使能其 CCM 报文发送功能。

```
[DeviceF] cfd meplist 5001 5002 service-instance 5
```

```
[DeviceF] interface gigabitethernet 1/0/2
```

```
[DeviceF-GigabitEthernet1/0/2] cfd mep 5002 service-instance 5 outbound
```

```
[DeviceF-GigabitEthernet1/0/2] cfd cc service-instance 5 mep 5002 enable
```

```
[DeviceF-GigabitEthernet1/0/2] quit
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 7，该 MA 服务于 VLAN 7。

```
[DeviceF] cfd service-instance 7 ma-id vlan-based md MD_A vlan 7
```

在服务实例 7 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 7 内的外向 MEP 7002，并使能其 CCM 报文发送功能。

```
[DeviceF] cfd meplist 7001 7002 service-instance 7
```

```
[DeviceF] interface gigabitethernet 1/0/1
```

```
[DeviceF-GigabitEthernet1/0/1] cfd mep 7002 service-instance 7 outbound
```

```
[DeviceF-GigabitEthernet1/0/1] cfd cc service-instance 7 mep 7002 enable
```

```
[DeviceF-GigabitEthernet1/0/1] quit
```

创建与服务实例 5 中 MEP 5002 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceF] track 1 cfd cc service-instance 5 mep 5002
```

配置 ERPS 环 2 实例 1 的端口 GigabitEthernet1/0/2 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] port erps ring 2 instance 1 track 1
[DeviceF-GigabitEthernet1/0/2] undo shutdown
[DeviceF-GigabitEthernet1/0/2] quit
# 创建与服务实例 7 中 MEP 7002 的 CFD 连续性检测功能关联的 Track 项 2。
[DeviceF] track 2 cfd cc service-instance 7 mep 7002
# 配置 ERPS 环 2 实例 1 的端口 GigabitEthernet1/0/1 通过 Track 项 2 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] port erps ring 2 instance 1 track 2
[DeviceF-GigabitEthernet1/0/1] undo shutdown
[DeviceF-GigabitEthernet1/0/1] quit
# 使能 ERPS 协议。
[DeviceF] erps enable
```

4. 验证配置

Device A 上的 ERPS 环 1 的运行情况。

```
[Device A] display erps detail ring 1
Ring ID           : 1
Port0             : GigabitEthernet1/0/1
Port1             : GigabitEthernet1/0/2
Subring           : Yes
Default MAC       : No

Instance ID       : 1
Node role          : Owner
Node state         : Idle
Connect(ring/instance): -
Control VLAN      : 100
Protected VLAN    : Reference-instance 1
Guard timer       : 500 ms
Hold-off timer    : 0 ms
WTR timer         : 5 min
Revertive operation : Revertive
Enable status     : Yes, Active status : Yes
R-APS level       : 7
Port              PortRole          PortStatus
-----
Port0              RPL              Block
Port1              Non-RPL          Up
```

本节点为 Owner 节点，ERPS 环处于 Idle 状态，RPL 端口阻塞，非 RPL 端口放开。

1.18.3 单环多实例负载分担配置举例

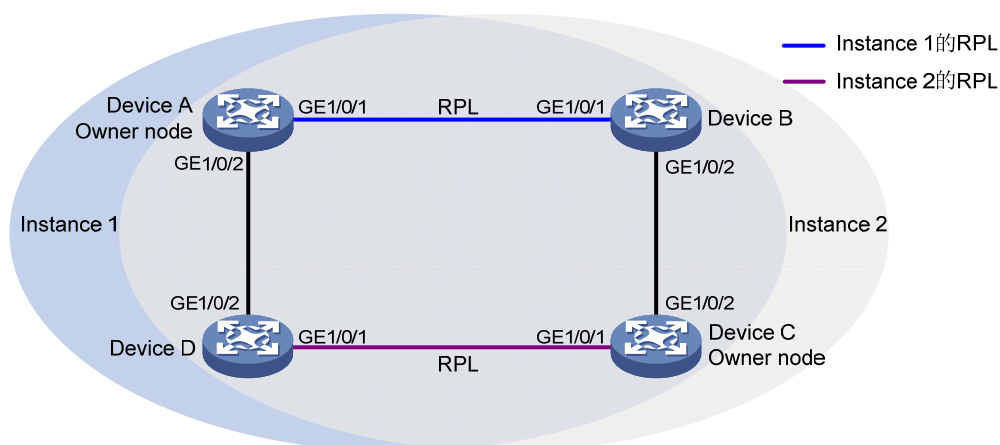
1. 组网需求

为了更高效得利用网络资源，使环网上不同链路的流量负载比较均匀，可以通过在环网上各节点配置 ERPS 协议，使得不同的 VLAN 流量走不同的链路。

- Device A、Device B、Device C 和 Device D 构成 ERPS 环 1，在该环上配置两个实例。
- Instance 1 的 Owner 节点为 Device A，RPL 为 Device A 和 Device B 之间的链路，控制 VLAN 为 VLAN 100，保护 VLAN 为 VLAN 1~30。
- Instance 2 的 Owner 节点为 Device C，其 RPL 为 Device C 和 Device D 之间的链路，控制 VLAN 为 VLAN 110，保护 VLAN 为 VLAN 31~60。

2. 组网图

图1-13 单环多实例负载分担配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 1~60，将 VLAN 1~30 映射到 MSTI 1 上，VLAN 31~60 映射到 MSTI 2 上，并激活 MST 域的配置。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 60
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] instance 2 vlan 31 to 60
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~60 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
```

```

[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceA-GigabitEthernet1/0/2] quit
# 创建 ERPS 环 1。
[DeviceA] erps ring 1
# 配置 ERPS 环成员端口。
[DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2
# 创建 ERPS 实例 1。
[DeviceA-erps-ring1] instance 1
# 配置节点角色。
[DeviceA-erps-ring1-inst1] node-role owner rpl port0
# 配置控制 VLAN。
[DeviceA-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。
[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit
[DeviceA-erps-ring1] quit
# 创建 ERPS 实例 2。
[DeviceA-erps-ring1] instance 2
# 配置控制 VLAN。
[DeviceA-erps-ring1-inst2] control-vlan 110
# 配置保护 VLAN。
[DeviceA-erps-ring1-inst2] protected-vlan reference-instance 2
# 实例 2 使能 ERPS 协议。
[DeviceA-erps-ring1-inst2] instance enable
[DeviceA-erps-ring1-inst2] quit
[DeviceA-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 1，该 MA 服务于 VLAN 1。
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
# 在服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的外向
MEP 1001，并使能其 CCM 报文发送功能。
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 2，该 MA 服务于 VLAN 2。
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2

```

在服务实例 2 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 2 内的外向 MEP 2001，并使其 CCM 报文发送功能。

```
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

创建与服务实例 1 中 MEP 1001 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceA] track 1 cfd cc service-instance 1 mep 1001
```

配置 ERPS 环 1 实例 1 和实例 2 的端口 GigabitEthernet1/0/1 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
```

创建与服务实例 2 中 MEP 2001 的 CFD 连续性检测功能关联的 Track 项 2。

```
[DeviceA] track 2 cfd cc service-instance 2 mep 2001
```

配置 ERPS 环 1 实例 1 和实例 2 的端口 GigabitEthernet1/0/2 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
```

使能 ERPS 协议。

```
[DeviceA] erps enable
```

(2) 配置 Device B

创建 VLAN 1~60，将 VLAN 1~30 映射到 MSTI 1 上，VLAN 31~60 映射到 MSTI 2 上，并激活 MST 域的配置。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 60
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] instance 2 vlan 31 to 60
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~60 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
```



```

[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceB-GigabitEthernet1/0/2] quit
# 创建 ERPS 环 1
[DeviceB] erps ring 1
# 配置 ERPS 环成员端口。
[DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2
# 创建 ERPS 实例 1。
[DeviceB-erps-ring1] instance 1
# 配置节点角色。
[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0
# 配置控制 VLAN。
[DeviceB-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。
[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceB-erps-ring1-inst1] instance enable
[DeviceB-erps-ring1-inst1] quit
[DeviceB-erps-ring1] quit
# 创建 ERPS 实例 2。
[DeviceB-erps-ring1] instance 2
# 配置控制 VLAN。
[DeviceB-erps-ring1-inst2] control-vlan 110
# 配置保护 VLAN。
[DeviceB-erps-ring1-inst2] protected-vlan reference-instance 2
# 实例 2 使能 ERPS 协议。
[DeviceB-erps-ring1-inst2] instance enable
[DeviceB-erps-ring1-inst2] quit
[DeviceB-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 1，该 MA 服务于 VLAN 1。
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
# 在服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的外向
MEP 1002，并使能其 CCM 报文发送功能。
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound

```

```
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceB-GigabitEthernet1/0/1] quit
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 3，该 MA 服务于 VLAN 3。

```
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
```

在服务实例 3 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 3 内的外向 MEP 3002，并使其 CCM 报文发送功能。

```
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable
[DeviceB-GigabitEthernet1/0/2] quit
```

创建与服务实例 1 中 MEP 1002 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceB] track 1 cfd cc service-instance 1 mep 1002
```

配置 ERPS 环 1 实例 1 和实例 2 的端口 GigabitEthernet1/0/1 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit
```

创建与服务实例 3 中 MEP 3002 的 CFD 连续性检测功能关联的 Track 项 2。

```
[DeviceB] track 2 cfd cc service-instance 3 mep 3002
```

配置 ERPS 环 1 实例 1 和实例 2 的端口 GigabitEthernet1/0/2 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit
```

使能 ERPS 协议。

```
[DeviceB] erps enable
```

(3) 配置 Device C

创建 VLAN 1~60，将 VLAN 1~30 都映射到 MSTI 1 上，将 VLAN 31~60 都映射到 MSTI 2 上，并激活 MST 域的配置。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 60
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] instance 2 vlan 31 to 60
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置物理连接状态 up/down 抑制时间为 0 秒（即不抑制），关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~60 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
```

```

[DeviceC-GigabitEthernet1/0/1] link-delay 0
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceC-GigabitEthernet1/0/2] quit
# 创建 ERPS 环 1。
[DeviceC] erps ring 1
# 配置 ERPS 环成员端口。
[DeviceC-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceC-erps-ring1] port1 interface gigabitethernet 1/0/2
# 创建 ERPS 实例 1。
[DeviceC-erps-ring1] instance 1
# 配置控制 VLAN。
[DeviceC-erps-ring1-inst1] control-vlan 100
# 配置保护 VLAN。
[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1
# 实例 1 使能 ERPS 协议。
[DeviceC-erps-ring1-inst1] instance enable
[DeviceC-erps-ring1-inst1] quit
[DeviceC-erps-ring1] quit
# 创建 ERPS 实例 2。
[DeviceC-erps-ring1] instance 2
# 配置节点角色。
[DeviceC-erps-ring1-inst2] node-role owner rpl port0
# 配置控制 VLAN。
[DeviceC-erps-ring1-inst2] control-vlan 110
# 配置保护 VLAN。
[DeviceC-erps-ring1-inst2] protected-vlan reference-instance 2
# 实例 2 使能 ERPS 协议。
[DeviceC-erps-ring1-inst2] instance enable
[DeviceC-erps-ring1-inst2] quit
[DeviceC-erps-ring1] quit
# 使能 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 3，该 MA 服务于 VLAN 3。
[DeviceC] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
# 在服务实例 3 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 3 内的外向
MEP 3001，并使能其 CCM 报文发送功能。

```

```
[DeviceC] cfd meplist 3001 3002 service-instance 3
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3001 enable
[DeviceC-GigabitEthernet1/0/2] quit
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 4，该 MA 服务于 VLAN 4。

```
[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

在服务实例 4 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 4 内的外向 MEP 4001，并使其 CCM 报文发送功能。

```
[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
[DeviceC-GigabitEthernet1/0/1] quit
```

创建与服务实例 3 中 MEP 3001 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceC] track 1 cfd cc service-instance 3 mep 3001
```

配置 ERPS 环 1 实例 1 和实例 2 的端口 GigabitEthernet1/0/2 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

创建与服务实例 4 中 MEP 4001 的 CFD 连续性检测功能关联的 Track 项 2。

```
[DeviceC] track 2 cfd cc service-instance 4 mep 4001
```

配置 ERPS 环 1 实例 1 和实例 2 的端口 GigabitEthernet1/0/1 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

使能 ERPS 协议。

```
[DeviceC] erps enable
```

(4) 配置 Device D

创建 VLAN 1~60，将 VLAN 1~30 都映射到 MSTI 1 上，将 VLAN 31~60 都映射到 MSTI 2 上，并激活 MST 域的配置。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 60
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] instance 2 vlan 31 to 60
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

分别在端口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 上配置物理连接状态 **up/down** 抑制时间为 **0** 秒（即不抑制），关闭生成树协议，并将端口配置为 **Trunk** 端口且允许 **VLAN 1～60** 通过。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceD-GigabitEthernet1/0/2] quit
```

创建 **ERPS** 环 1。

```
[DeviceD] erps ring 1
```

配置 **ERPS** 环成员端口。

```
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2
```

创建 **ERPS** 实例 1。

```
[DeviceD-erps-ring1] instance 1
```

配置控制 **VLAN**。

```
[DeviceD-erps-ring1-inst1] control-vlan 100
```

配置保护 **VLAN**。

```
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1
```

实例 1 使能 **ERPS** 协议。

```
[DeviceD-erps-ring1-inst1] instance enable
[DeviceD-erps-ring1-inst1] quit
[DeviceD-erps-ring1-inst1] quit
```

创建 **ERPS** 实例 2。

```
[DeviceD-erps-ring1] instance 2
```

配置节点角色。

```
[DeviceD-erps-ring1-inst2] node-role neighbor rpl port0
```

配置控制 **VLAN**。

```
[DeviceD-erps-ring1-inst2] control-vlan 110
```

配置保护 **VLAN**。

```
[DeviceD-erps-ring1-inst2] protected-vlan reference-instance 2
```

实例 2 使能 **ERPS** 协议。

```
[DeviceD-erps-ring1-inst2] instance enable
[DeviceD-erps-ring1-inst2] quit
[DeviceD-erps-ring1-inst2] quit
```

使能 **CFD** 功能，并创建级别为 **5** 的 **MD MD_A**。

```
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 2，该 MA 服务于 VLAN 2。

```
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
```

在服务实例 2 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 2 内的外向 MEP 2002，并使其 CCM 报文发送功能。

```
[DeviceD] cfd meplist 2001 2002 service-instance 2
```

```
[DeviceD] interface gigabitethernet 1/0/2
```

```
[DeviceD-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
```

```
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
```

```
[DeviceD-GigabitEthernet1/0/2] quit
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 4，该 MA 服务于 VLAN 4。

```
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

在服务实例 4 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 4 内的外向 MEP 4002，并使其 CCM 报文发送功能。

```
[DeviceD] cfd meplist 4001 4002 service-instance 4
```

```
[DeviceD] interface gigabitethernet 1/0/1
```

```
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound
```

```
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
```

```
[DeviceD-GigabitEthernet1/0/1] quit
```

创建与服务实例 2 中 MEP 2002 的 CFD 连续性检测功能关联的 Track 项 1。

```
[DeviceD] track 1 cfd cc service-instance 2 mep 2002
```

配置 ERPS 环 1 实例 1 和实例 2 的端口 GigabitEthernet1/0/2 通过 Track 项 1 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceD] interface gigabitethernet 1/0/2
```

```
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
```

```
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 1
```

```
[DeviceD-GigabitEthernet1/0/2] undo shutdown
```

```
[DeviceD-GigabitEthernet1/0/2] quit
```

创建与服务实例 4 中 MEP 4002 的 CFD 连续性检测功能关联的 Track 项 2。

```
[DeviceD] track 2 cfd cc service-instance 4 mep 4002
```

配置 ERPS 环 1 实例 1 和实例 2 的端口 GigabitEthernet1/0/1 通过 Track 项 2 与 CFD 的连续性检测功能联动，并重新开启该端口。

```
[DeviceD] interface gigabitethernet 1/0/1
```

```
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
```

```
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 2
```

```
[DeviceD-GigabitEthernet1/0/1] undo shutdown
```

```
[DeviceD-GigabitEthernet1/0/1] quit
```

使能 ERPS 协议。

```
[DeviceD] erps enable
```

4. 验证配置

Device A 上的 ERPS 环 1 的运行情况。

```
[Device A] display erps detail ring 1
```

```
Ring ID           : 1
Port0             : GigabitEthernet1/0/1
Port1             : GigabitEthernet1/0/2
Subring           : No
```

```

Default MAC          : No

Instance ID          : 1
Node role             : Owner
Node state            : Idle
Connect(ring/instance): -
Control VLAN          : 100
Protected VLAN        : Reference-instance 1
Guard timer           : 500 ms
Hold-off timer        : 0 ms
WTR timer             : 5 min
Revertive operation   : Revertive
Enable status          : Yes, Active status : Yes
R-APS level           : 7
Port                  PortRole                PortStatus
-----
Port0                  RPL                    Block
Port1                  Non-RPL                 Up

Instance ID          : 2
Node role             : Normal
Node state            : Idle
Connect(ring/instance): -
Control VLAN          : 100
Protected VLAN        : Reference-instance 2
Guard timer           : 500 ms
Hold-off timer        : 0 ms
WTR timer             : 5 min
Revertive operation   : Revertive
Enable status          : Yes, Active status : Yes
R-APS level           : 7
Port                  PortRole                PortStatus
-----
Port0                  Non-RPL                 Up
Port1                  Non-RPL                 Up

```

本节点在 Instance 1 中为 Owner 节点，ERPS 环处于 Idle 状态，RPL 端口阻塞，非 RPL 端口放开。
在 Instance 2 中为 Normal 节点，ERPS 环处于 Idle 状态，非 RPL 端口放开。

1.19 ERPS常见故障处理

1.19.1 Owner节点收不到故障节点发送的SF报文

1. 故障现象

故障节点和 Owner 节点间链路正常，但 Owner 节点收不到故障节点发送的 SF 报文，RPL 端口保持阻塞。

2. 故障分析

可能的原因有：

- ERPS 环上有节点没有使能 ERPS 协议。
- 在同一 ERPS 环上的节点的环 ID 或相同实例的控制 VLAN ID 不同。
- ERPS 环上的端口处于非正常状态。

3. 处理过程

- 使用 **display erps** 命令查看各个节点是否都配置并使能了 ERPS 协议。如果没有则使用 **erps enable** 命令使能 ERPS 协议。
- 使用 **display erps detail** 命令查看各个环各个节点的端口链路状态，如果端口处于关闭状态，则先打开端口。
- 使用 **debugging erps** 命令，在各个节点上打开调试信息开关，并查看各个节点报文以及状态是否倒换正常。
- 配置同一 ERPS 环上的节点的环 ID 或相同实例的控制 VLAN ID 相同。

目 录

1 Smart Link	1-1
1.1 Smart Link简介	1-1
1.1.1 Smart Link应用场景.....	1-1
1.1.2 Smart Link概念介绍.....	1-2
1.1.3 Smart Link运行机制.....	1-2
1.1.4 Smart Link和Monitor Link的端口检测联动	1-3
1.1.5 Smart Link和Track的链路检测联动	1-3
1.2 Smart Link与硬件适配关系	1-4
1.3 Smart Link配置限制和指导	1-4
1.4 Smart Link配置任务简介	1-4
1.5 配置Smart Link设备	1-4
1.5.1 配置准备.....	1-4
1.5.2 配置Smart Link组的保护VLAN.....	1-4
1.5.3 配置Smart Link组的成员端口.....	1-5
1.5.4 配置Smart Link抢占功能.....	1-5
1.5.5 开启发送Flush报文功能.....	1-5
1.5.6 配置Smart Link与Track联动	1-6
1.6 开启相关设备接收Flush报文功能	1-6
1.7 Smart Link显示和维护	1-7
1.8 Smart Link典型配置举例	1-7
1.8.1 单Smart Link组配置举例.....	1-7
1.8.2 多Smart Link组负载分担配置举例.....	1-12
1.8.3 Smart Link与Track联动配置举例	1-16

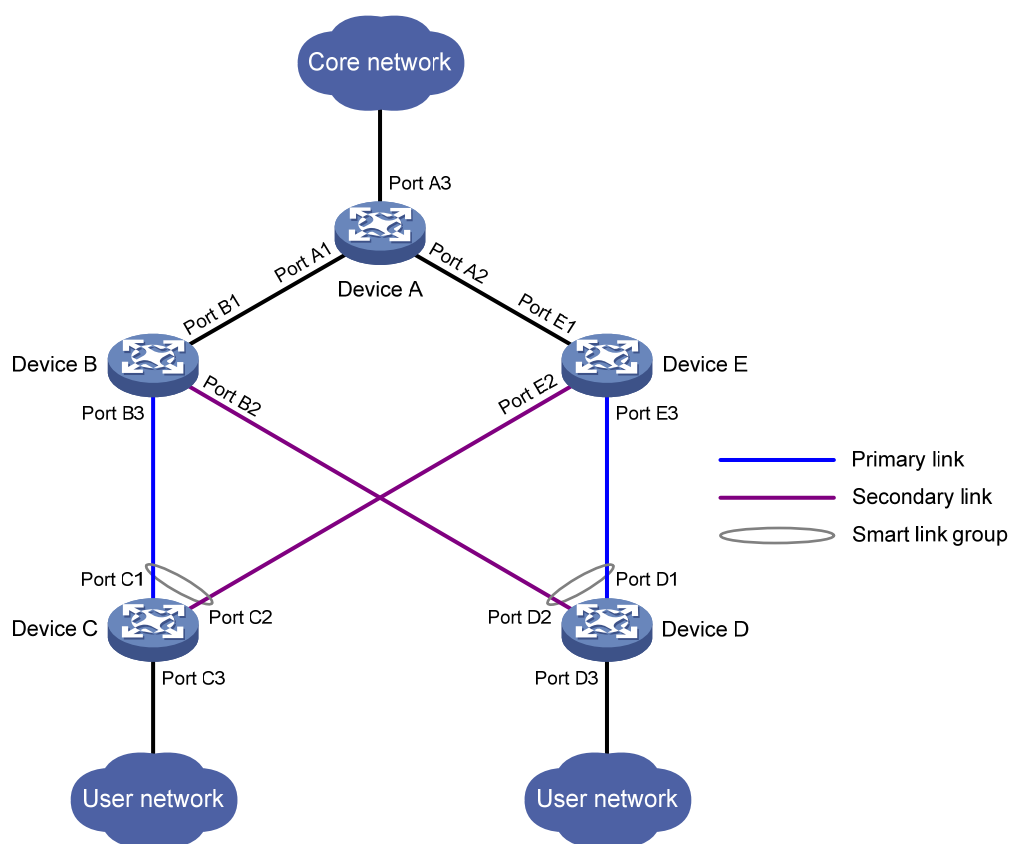
1 Smart Link

1.1 Smart Link简介

1.1.1 Smart Link应用场景

Smart Link用于双上行组网中实现主备链路的冗余备份，并提供亚秒级的快速链路切换。如 [图 1-1](#) 所示，在Device C和Device D上采用Smart Link功能，可以实现主用上行链路故障时，将流量快速切换到备用上行链路。

图1-1 Smart Link 应用场景示意图



Smart Link 组网中，设备分为以下角色：

- **Smart Link 设备：**具有双上行链路的设备，如 Device C 和 Device D。Smart Link 设备要求支持 Smart Link 功能、且配置了 Smart Link 组和从指定控制 VLAN 发送 Flush 报文功能。
- **相关设备：**Smart Link 设备连接的上行设备，如 Device A、Device B 和 Device E。相关设备要求支持 Smart Link 功能、在实际应用中为配合 Smart Link 设备而需开启从指定控制 VLAN 接收 Flush 报文功能。当上行链路切换后，相关设备会根据接收到的 Flush 报文刷新 MAC 地址转发表项和 ARP/ND 表项。

1.1.2 Smart Link概念介绍

1. Smart Link组

Smart Link 组也叫灵活链路组，每个组内只包含两个成员端口——主端口和从端口。正常情况下，只有一个端口处于转发（ACTIVE）状态，另一个端口被阻塞，处于待命（STANDBY）状态。当处于转发状态的端口出现链路故障（包括端口 down、以太网 OAM 检测到的单向链路等）时，Smart Link 组会自动将该端口阻塞，并将原阻塞的处于待命状态的端口切换到转发状态。

如 [图 1-1](#) 所示，Device C 上的端口 Port C1 和 Port C2 组成了一个 Smart Link 组，其中 Port C1 处于转发状态，而 Port C2 处于待命状态；Device D 上的端口 Port D1 和 Port D2 组成了一个 Smart Link 组，其中 Port D1 处于转发状态，而 Port D2 处于待命状态。

2. 主端口/从端口

主端口和从端口是 Smart Link 组中的两种成员端口。当 Smart Link 组中的两个端口都处于 up 状态时，主端口将优先进入转发状态，而从端口将保持待命状态。当主端口所在链路发生故障时，从端口将切换为转发状态。

如 [图 1-1](#) 所示，Device C 和 Device D 上的端口 Port C1 和 Port D1 为主端口，Port C2 和 Port D2 为从端口。

3. 主链路/从链路

我们把主端口所在的链路称为主链路，从端口所在的链路称为从链路。

4. Flush 报文

当 Smart Link 组发生链路切换时，原有的 MAC 地址转发表项和 ARP/ND 表项将不适用于新的拓扑网络，需要更新网络中的所有设备。这时，Smart Link 组通过发送 Flush 报文通知其它设备进行 MAC 地址转发表项和 ARP/ND 表项的刷新操作。Flush 报文是普通的组播数据报文，会被阻塞的接收端口丢弃。

5. 保护 VLAN

保护 VLAN 就是 Smart Link 组要保护的那些 VLAN，同一端口上不同的 Smart Link 组保护不同的 VLAN。端口在保护 VLAN 上的转发状态由端口在其所属 Smart Link 组内的状态决定。

6. 发送控制 VLAN

发送控制 VLAN 是用于发送 Flush 报文的 VLAN。当发生链路切换时，设备（如 [图 1-1](#) 中的 Device C 和 Device D）会在发送控制 VLAN 内发送 Flush 报文。

7. 接收控制 VLAN

接收控制 VLAN 是用于接收并处理 Flush 报文的 VLAN。当发生链路切换时，设备（如 [图 1-1](#) 中的 Device A、Device B 和 Device E）接收并处理属于接收控制 VLAN 的 Flush 报文，进行 MAC 地址转发表项和 ARP/ND 表项的刷新操作。

1.1.3 Smart Link 运行机制

1. 链路备份

在 [图 1-1](#) 所示的组网中，Device C 的端口 Port C1 所在的链路是主链路，Port C2 所在的链路是从链路。正常情况下，Port C1 处于转发状态，Port C2 处于待命状态。当主链路出现故障时，Port C1

将自动阻塞并切换到待命状态，Port C2 将切换到转发状态。当端口切换到转发状态时，系统会输出日志信息通知用户。

2. 网络拓扑变更

当 Smart Link 发生链路切换时，网络中各设备上的 MAC 地址转发表项和 ARP/ND 表项可能已经不是最新状态。为了保证报文的正确发送，需要由 Smart Link 设备在新的链路上发送 Flush 报文，且要求上行的设备识别 Smart Link 的 Flush 报文并进行更新 MAC 地址转发表项和 ARP/ND 表项的处理。

3. 抢占模式

在图 1-1 所示的组网中，Device C 的端口 Port C1 所在的链路是主链路，Port C2 所在的链路是从链路。当主链路出现故障时，Port C1 将自动阻塞并切换到待命状态，Port C2 则从待命状态切换到转发状态。当主链路恢复后：

- 在非抢占模式下，Port C1 仍将维持在阻塞状态，不进行链路状态切换，从而保持流量稳定。只有等下一次链路切换时，该端口才会重新切换回转发状态。
- 在抢占模式下，当符合抢占条件时，Port C2 将自动阻塞并切换到待命状态，而 Port C1 则切换回转发状态。

4. 负载分担

在同一个环网中，可能同时存在多个 VLAN 的数据流量，Smart Link 可以实现流量的负载分担，即不同 VLAN 的流量沿不同 Smart Link 组所确定的路径进行转发。

通过把一个端口配置为多个 Smart Link 组的成员端口（每个 Smart Link 组的保护 VLAN 不同），并使该端口在不同 Smart Link 组中的转发状态不同，这样就能实现不同 VLAN 的数据流量的转发路径不同，从而达到负载分担的目的。

每个 Smart Link 组的保护 VLAN 是通过引用 MSTI（Multiple Spanning Tree Instance，多生成树实例）来实现的。有关 MSTI 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”。

1.1.4 Smart Link和Monitor Link的端口检测联动

当上游设备的上行链路发生故障以及故障恢复时，下游设备上的 Smart Link 无法感知到这个变化。Monitor Link 则可以通过监控上游设备的上行端口，根据其 up/down 状态的变化来触发下行端口 up/down 状态的变化，从而触发下游设备上的 Smart Link 进行链路切换。有关 Monitor Link 的详细介绍，请参见“可靠性配置指导”中的“Monitor Link”。

1.1.5 Smart Link和Track的链路检测联动

当上行链路上的中间传输设备或传输链路发生故障（如光纤链路发生单通、错纤、丢包等故障）以及故障排除时，Smart Link 本身无法感知到这个变化，Smart Link 组的成员端口需要通过专门的链路检测协议来检测端口的链路状态，当链路检测协议检测到故障发生或故障恢复时就通知 Smart Link 进行链路切换。

Smart Link 组的成员端口通过 Track 项与链路检测协议进行联动，目前仅支持与 CFD（Connectivity Fault Detection，连通错误检测）的连续性检测功能联动。当端口与 CFD 连续性检测功能联动时，CFD 按照检测 VLAN 和检测端口来通知故障检测事件，只有当端口所在 Smart Link 组的控制 VLAN 与检测 VLAN 一致时，才响应此事件。有关 Track 项和 CFD 连续性检测功能的详细介绍，请分别参见“可靠性配置指导”中的“Track”和“CFD”。

1.2 Smart Link与硬件适配关系

S5110V2-SI、S5000E-X 和 S5000V3-EI 系列交换机不支持 Smart Link 特性。

1.3 Smart Link配置限制和指导

请勿将一个端口同时加入聚合组和 Smart Link 组，否则该端口在 Smart Link 组中将不会生效，也无法使用 **display smart-link group** 命令查看到。

1.4 Smart Link配置任务简介

Smart Link 配置任务如下：

- (1) [配置Smart Link设备](#)
 - a. [配置Smart Link组的保护VLAN](#)
 - b. [配置Smart Link组的成员端口](#)
 - c. [（可选）配置Smart Link抢占功能](#)
 - d. [（可选）开启发送Flush报文功能](#)
 - e. [（可选）配置Smart Link与Track联动](#)
- (2) [开启相关设备接收Flush报文功能](#)

1.5 配置Smart Link设备

1.5.1 配置准备

如果欲配置某端口为 Smart Link 组的成员端口（主端口或从端口）：

- 请先手工关闭该端口，并待 Smart Link 组配置完成后再开启该端口，以避免形成环路，导致广播风暴；
- 请关闭该端口的生成树协议、RRPP 功能和 ERPS 功能。

1.5.2 配置Smart Link组的保护VLAN

1. 配置准备

配置保护 VLAN 前需要配置 MST 域，并配置关于保护 VLAN 的 VLAN 映射表，关于 MST 域的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 Smart Link 组，并进入 Smart Link 组视图。

```
smart-link group group-id
```

- (3) 配置 Smart Link 组的保护 VLAN。

```
protected-vlan reference-instance instance-id-list
```

1.5.3 配置Smart Link组的成员端口

1. 配置限制和指导

可在 Smart Link 组视图或接口视图下配置 Smart Link 组的成员端口，各视图下的配置效果相同。

2. Smart Link组视图下的配置

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Smart Link 组视图。

```
smart-link group group-id
```

- (3) 配置 Smart Link 组的成员端口。

```
port interface-type interface-number { primary | secondary }
```

缺省情况下，Smart Link 组中没有成员端口。

3. 接口视图下的配置

- (1) 进入系统视图。

```
system-view
```

- (2) 进入二层以太网或二层聚合接口视图。

```
interface interface-type interface-number
```

- (3) 配置 Smart Link 组的成员端口。

```
port smart-link group group-id { primary | secondary }
```

缺省情况下，接口不是 Smart Link 组的成员端口。

1.5.4 配置Smart Link抢占功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Smart Link 组视图。

```
smart-link group group-id
```

- (3) 配置 Smart Link 组的抢占模式。

```
preemption mode { role | speed [ threshold threshold-value ] }
```

缺省情况下，Smart Link 组为非抢占模式。

- (4) 配置抢占延时。

```
preemption delay delay
```

缺省情况下，抢占延时为 1 秒。

抢占延时在配置了 Smart Link 组的抢占模式后才会生效。

1.5.5 开启发送Flush报文功能

1. 配置限制和指导

- 需要为不同的 Smart Link 组配置不同的控制 VLAN。
- 需要配置保证控制 VLAN 存在，且 Smart Link 组的端口允许控制 VLAN 的报文通过。

- 某 Smart Link 组的控制 VLAN 应同时为该 Smart Link 组的保护 VLAN，且不要将已配置为控制 VLAN 的 VLAN 删除，否则会影响 Flush 报文的发送。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Smart Link 组视图。

```
smart-link group group-id
```

- (3) 开启发送 Flush 报文的功能。

```
flush enable [ control-vlan vlan-id ]
```

缺省情况下，发送 Flush 报文的功能处于开启状态，且控制 VLAN 为 VLAN 1。

1.5.6 配置Smart Link与Track联动

1. 功能简介

Smart Link 组的成员端口通过 Track 项与链路检测协议进行联动，目前仅支持与 CFD 的连续性检测功能联动。

2. 配置准备

在配置端口与 Track 项联动之前，必须保证该端口已加入相应的 Smart Link 组。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入二层以太网或二层聚合接口视图。

```
interface interface-type interface-number
```

- (3) 配置 Smart Link 组的成员端口与 Track 项联动。

```
port smart-link group group-id track track-entry-number
```

缺省情况下，Smart Link 组的成员端口未与 Track 项联动。

1.6 开启相关设备接收Flush报文功能

1. 配置限制和指导

并非需要在相关设备的所有端口上都开启接收 Flush 报文功能，只需要在处于从 Smart Link 设备到其目的设备主、从链路上的端口的所有控制 VLAN 上开启此功能。

配置时需要注意的是：

- 如果控制 VLAN 尚未配置，设备将对收到的 Flush 报文不做处理而直接转发。
- 在相关设备上配置的接收处理 Flush 报文的控制 VLAN 和在 Smart Link 设备上配置的发送控制 VLAN 要相同，若不同，相关设备将对收到的 Flush 报文将不做处理而直接转发。
- 不要将已配置为控制 VLAN 的 VLAN 删除，否则会影响 Flush 报文的处理。
- 请确保控制 VLAN 存在，且开启了接收 Flush 报文功能的端口要允许控制 VLAN 的报文通过。

2. 配置准备

配置相关设备时，建议在其与 Smart Link 组的成员端口相连的端口上关闭生成树协议，以免由于网络拓扑改变时端口状态尚未迁移到 Forwarding 而导致 Flush 报文被丢弃。

3. 配置步骤

- (1) 进入系统视图。
`system-view`
- (2) 进入二层以太网或二层聚合接口视图。
`interface interface-type interface-number`
- (3) 开启接收 Flush 报文的功能。
`smart-link flush enable [control-vlan vlan-id-list]`
缺省情况下，接收 Flush 报文的功能处于关闭状态。

1.7 Smart Link显示和维护

在完成上述配置后，在任意视图下执行 `display` 命令可以显示配置后 Smart Link 的运行情况以及 Flush 报文的统计信息，通过查看显示信息验证配置的效果。
在用户视图下执行 `reset` 命令可以清除 Flush 报文的统计信息。

表1-1 Smart Link 显示和维护

操作	命令
显示设备收到的Flush报文信息	<code>display smart-link flush</code>
显示Smart Link组的信息	<code>display smart-link group { group-id all }</code>
清除Flush报文的统计信息	<code>reset smart-link statistics</code>

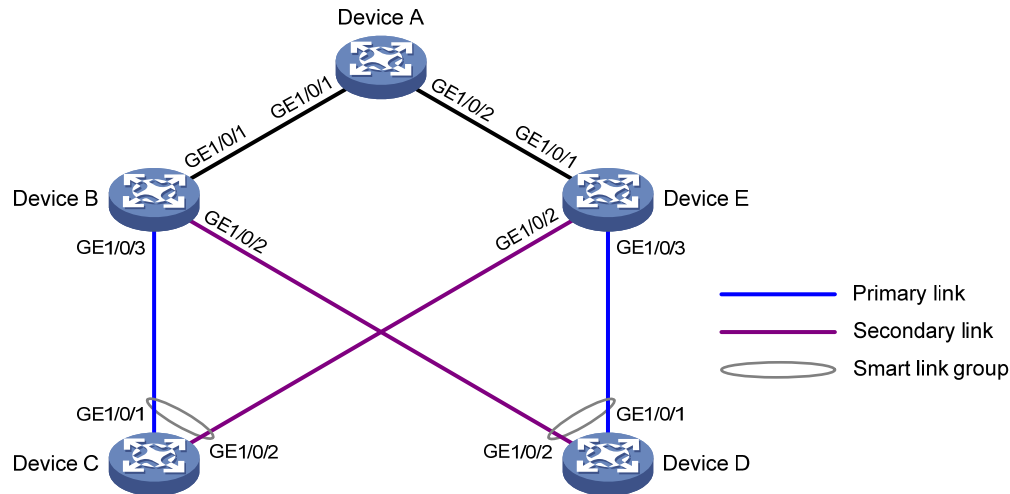
1.8 Smart Link典型配置举例

1.8.1 单Smart Link组配置举例

- 1. 组网需求
 - 在 [图 1-2](#) 所示的组网中，Device C和Device D为Smart Link设备，Device A、Device B和Device E为相关设备。Device C和Device D上VLAN 1~30 的流量分别双上行到Device A。
 - 通过配置，在 Device C 和 Device D 上分别实现双上行链路的灵活备份。

2. 组网图

图1-2 单 Smart Link 组配置组网图



3. 配置步骤

(1) 配置 Device C

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

分别关闭端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，在这两个端口上分别关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

创建 Smart Link 组 1，并配置其保护 VLAN 为 MSTI 1 所映射的 VLAN。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

配置 Smart Link 组 1 的主端口为 GigabitEthernet1/0/1，从端口为 GigabitEthernet1/0/2。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

在 Smart Link 组 1 中开启发送 Flush 报文的功能，并指定发送 Flush 报文的控制 VLAN 为 VLAN 10。

```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

重新开启端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

(2) 配置 Device D

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

分别关闭端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，在这两个端口上分别关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] shutdown
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] shutdown
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

创建 Smart Link 组 1，并配置其保护 VLAN 为 MSTI 1 所映射的 VLAN。

```
[DeviceD] smart-link group 1
[DeviceD-smlk-group1] protected-vlan reference-instance 1
```

配置 Smart Link 组 1 的主端口为 GigabitEthernet1/0/1，从端口为 GigabitEthernet1/0/2。

```
[DeviceD-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceD-smlk-group1] port gigabitethernet 1/0/2 secondary
```

在 Smart Link 组 1 中开启发送 Flush 报文的功能，并指定发送 Flush 报文的控制 VLAN 为 VLAN 20。

```
[DeviceD-smlk-group1] flush enable control-vlan 20
[DeviceD-smlk-group1] quit
```

重新开启端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo shutdown
```

```
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

(3) 配置 Device B

创建 VLAN 1~30。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

将端口 **GigabitEthernet1/0/1** 配置为 Trunk 端口且允许 VLAN 1~30 通过，在该端口上开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 20。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

将端口 **GigabitEthernet1/0/2** 配置为 Trunk 端口且允许 VLAN 1~30 通过，在该端口上关闭生成树协议并开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 20。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 20
[DeviceB-GigabitEthernet1/0/2] quit
```

将端口 **GigabitEthernet1/0/3** 配置为 Trunk 端口且允许 VLAN 1~30 通过，在该端口上关闭生成树协议并开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

(4) 配置 Device E

创建 VLAN 1~30。

```
<DeviceE> system-view
[DeviceE] vlan 1 to 30
```

将端口 **GigabitEthernet1/0/1** 配置为 Trunk 端口且允许 VLAN 1~30 通过，在该端口上开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 20。

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceE-GigabitEthernet1/0/1] quit
```

将端口 **GigabitEthernet1/0/2** 配置为 Trunk 端口且允许 VLAN 1~30 通过，在该端口上关闭生成树协议并开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10。

```
[DeviceE] interface gigabitethernet 1/0/2
```

```
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceE-GigabitEthernet1/0/2] quit
```

将端口 **GigabitEthernet1/0/3** 配置为 **Trunk** 端口且允许 **VLAN 1~30** 通过，在该端口上关闭生成树协议并开启接收 **Flush** 报文的功能，并指定接收 **Flush** 报文的控制 **VLAN** 为 **VLAN 20**。

```
[DeviceE] interface gigabitethernet 1/0/3
[DeviceE-GigabitEthernet1/0/3] port link-type trunk
[DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/3] undo stp enable
[DeviceE-GigabitEthernet1/0/3] smart-link flush enable control-vlan 20
[DeviceE-GigabitEthernet1/0/3] quit
```

(5) 配置 Device A

创建 **VLAN 1~30**。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

分别将端口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 配置为 **Trunk** 端口且允许 **VLAN 1~30** 通过，在这些端口上开启接收 **Flush** 报文的功能，并指定接收 **Flush** 报文的控制 **VLAN** 为 **VLAN 10** 和 **20**。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

4. 验证配置

通过使用 **display smart-link group** 命令可以查看设备上 **Smart Link** 组的信息：

显示 **Device C** 上 **Smart Link** 组的信息。

```
[DeviceC] display smart-link group 1
```

Smart link group 1 information:

```
Device ID       : 000f-e23d-5af0
Preemption mode : None
Preemption delay: 1(s)
Control VLAN    : 10
Protected VLAN  : Reference Instance 1
```

Member	Role	State	Flush-count	Last-flush-time
GE1/0/1	PRIMARY	ACTIVE	5	16:45:20 2012/04/21
GE1/0/2	SECONDARY	STANDBY	1	16:37:20 2012/04/21

通过使用 **display smart-link flush** 命令可以查看设备上收到的 **Flush** 报文信息：

显示 Device B 上收到的 Flush 报文信息。

```
[DeviceB] display smart-link flush
Received flush packets                : 5
Receiving interface of the last flush packet : GigabitEthernet1/0/3
Receiving time of the last flush packet   : 16:50:21 2012/04/21
Device ID of the last flush packet       : 000f-e23d-5af0
Control VLAN of the last flush packet    : 10
```

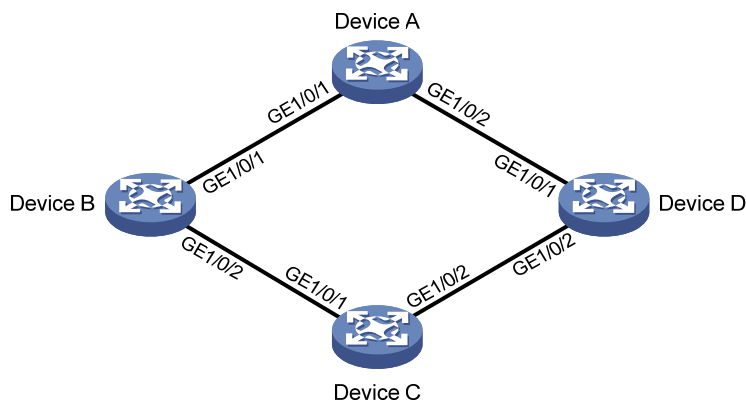
1.8.2 多Smart Link组负载分担配置举例

1. 组网需求

- 在图 1-3 所示的组网中，Device C 为 Smart Link 设备，Device A、Device B 和 Device D 为相关设备。Device C 上 VLAN 1~200 的流量通过 Device B 和 Device D 双上行到 Device A。
- 通过配置，在 Device C 上实现双上行链路的灵活备份和负载分担：VLAN 1~100 的流量经 Device B 向 Device A 转发，VLAN 101~200 的流量经 Device D 向 Device A 转发。

2. 组网图

图1-3 多 Smart Link 组负载分担配置组网图



3. 配置步骤

(1) 配置 Device C

创建 VLAN 1~200，分别将 VLAN 1~100 映射到 MSTI 1、VLAN 101~200 映射到 MSTI 2 上，并激活 MST 域的配置。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

分别关闭端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，在这两个端口上分别关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~200 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/2] quit
```

创建 Smart Link 组 1，并配置其保护 VLAN 为 MSTI 1 所映射的 VLAN。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

配置 Smart Link 组 1 的主端口为 GigabitEthernet1/0/1，从端口为 GigabitEthernet1/0/2。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

在 Smart Link 组 1 中配置抢占模式为角色抢占模式；开启发送 Flush 报文的功能，并指定发送 Flush 报文的控制 VLAN 为 VLAN 10。

```
[DeviceC-smlk-group1] preemption mode role
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

创建 Smart Link 组 2，并配置其保护 VLAN 为 MSTI 2 所映射的 VLAN。

```
[DeviceC] smart-link group 2
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

配置 Smart Link 组 2 的主端口为 GigabitEthernet1/0/2，从端口为 GigabitEthernet1/0/1。

```
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 primary
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 secondary
```

在 Smart Link 组 2 中配置抢占模式为角色抢占模式；开启发送 Flush 报文的功能，并指定发送 Flush 报文的控制 VLAN 为 VLAN 110。

```
[DeviceC-smlk-group2] preemption mode role
[DeviceC-smlk-group2] flush enable control-vlan 110
[DeviceC-smlk-group2] quit
```

重新开启端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

(2) 配置 Device B

创建 VLAN 1~200。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口且允许 VLAN 1~200 通过，在该端口上开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 110。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/1] quit
```

将端口 **GigabitEthernet1/0/2** 配置为 **Trunk** 端口且允许 **VLAN 1~200** 通过，在该端口上关闭生成树协议并开启接收 **Flush** 报文的功能，并指定接收 **Flush** 报文的控制 **VLAN** 为 **VLAN 10** 和 **110**。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/2] quit
```

(3) 配置 Device D

创建 **VLAN 1~200**。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 200
```

将端口 **GigabitEthernet1/0/1** 配置为 **Trunk** 端口且允许 **VLAN 1~200** 通过，在该端口上开启接收 **Flush** 报文的功能，并指定接收 **Flush** 报文的控制 **VLAN** 为 **VLAN 10** 和 **110**。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/1] quit
```

将端口 **GigabitEthernet1/0/2** 配置为 **Trunk** 端口且允许 **VLAN 1~200** 通过，在该端口上关闭生成树协议并开启接收 **Flush** 报文的功能，并指定接收 **Flush** 报文的控制 **VLAN** 为 **VLAN 10** 和 **110**。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/2] quit
```

(4) 配置 Device A

创建 **VLAN 1~200**。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
```

分别将端口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2** 配置为 **Trunk** 端口且允许 **VLAN 1~200** 通过，在这些端口上开启接收 **Flush** 报文的功能，并指定接收 **Flush** 报文的控制 **VLAN** 为 **VLAN 10** 和 **110**。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
```

```
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/2] quit
```

4. 验证配置

通过使用 **display smart-link group** 命令可以查看设备上 Smart Link 组的信息：

显示 Device C 上 Smart Link 组的信息。

```
[DeviceC] display smart-link group all
```

Smart link group 1 information:

```
Device ID       : 000f-e23d-5af0
Preemption mode : Role
Preemption delay: 1(s)
Control VLAN    : 10
Protected VLAN  : Reference Instance 1
```

Member	Role	State	Flush-count	Last-flush-time
GE1/0/1	PRIMARY	ACTIVE	5	16:45:20 2012/04/21
GE1/0/2	SECONDARY	STANDBY	1	16:37:20 2012/04/21

Smart link group 2 information:

```
Device ID       : 000f-e23d-5af0
Preemption mode : Role
Preemption delay: 1(s)
Control VLAN    : 110
Protected VLAN  : Reference Instance 2
```

Member	Role	State	Flush-count	Last-flush-time
GE1/0/2	PRIMARY	ACTIVE	5	16:45:20 2012/04/21
GE1/0/1	SECONDARY	STANDBY	1	16:37:20 2012/04/21

通过使用 **display smart-link flush** 命令可以查看设备上收到的 Flush 报文信息：

显示 Device B 上收到的 Flush 报文信息。

```
[DeviceB] display smart-link flush
```

```
Received flush packets           : 5
Receiving interface of the last flush packet : GigabitEthernet1/0/2
Receiving time of the last flush packet      : 16:25:21 2012/04/21
Device ID of the last flush packet          : 000f-e23d-5af0
Control VLAN of the last flush packet       : 10
```

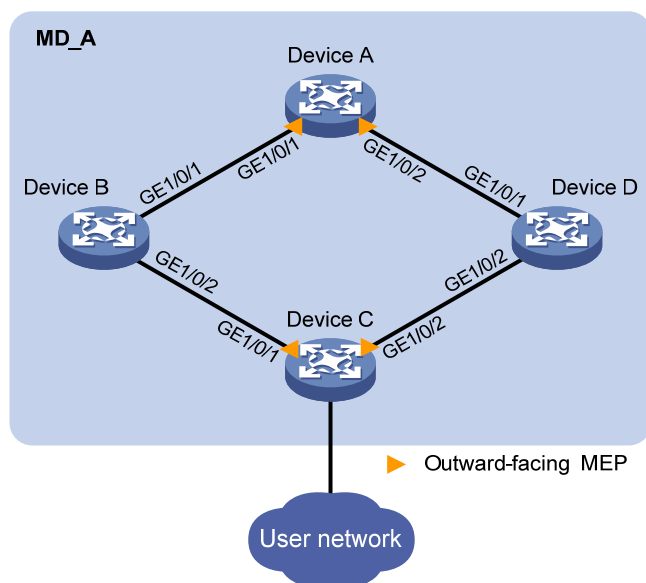

1.8.3 Smart Link与Track联动配置举例

1. 组网需求

- 在图 1-4 所示的组网中，Device A~Device D 组成级别为 5 的 MD MD_A；Device C 为 Smart Link 设备，Device A、Device B 和 Device D 为相关设备。Device C 上 VLAN 1~200 的流量通过 Device B 和 Device D 双上行到 Device A。
- 配置 Smart Link 与 Track 联动，通过将端口与 CFD 连续性检测功能的联动以实现：在正常情况下，VLAN 1~100 的流量经 Device C 上 Smart Link 组 1 的主端口 GigabitEthernet1/0/1 向 Device A 转发，VLAN 101~200 的流量经 Device C 上 Smart Link 组 2 的主端口 GigabitEthernet1/0/2 向 Device A 转发；当 Device C 与 Device A 之间的链路发生故障时，原本由各 Smart Link 组的主端口转发的流量能够快速切换到从端口，并在故障排除后再切换回主端口。

2. 组网图

图1-4 Smart Link 与 Track 联动配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 1~200。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
```

分别将端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 配置为 Trunk 端口且允许 VLAN 1~200 通过，在这些端口上开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 110。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/1] quit
```

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/2] quit
```

开启 CFD 功能，并创建级别为 5 的 MD MD_A。

```
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 1，该 MA 服务于 VLAN 10。

```
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 10
```

在服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的外向 MEP 1002，并开启其 CCM 报文发送功能。

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 2，该 MA 服务于 VLAN 110。

```
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 110
```

在服务实例 2 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 2 内的外向 MEP 2002，并开启其 CCM 报文发送功能。

```
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

(2) 配置 Device B

创建 VLAN 1~200。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口且允许 VLAN 1~200 通过，在该端口上开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 110。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/1] quit
```

将端口 GigabitEthernet1/0/2 配置为 Trunk 端口且允许 VLAN 1~200 通过，在该端口上关闭生成树协议并开启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 110。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
```

```
[DeviceB-GigabitEthernet1/0/2] quit
```

(3) 配置 Device C

创建 VLAN 1~200，分别将 VLAN 1~100 映射到 MSTI 1、VLAN 101~200 映射到 MSTI 2 上，并激活 MST 域的配置。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

分别关闭端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，在这两个端口上分别关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~200 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/2] quit
```

创建 Smart Link 组 1，并配置其保护 VLAN 为 MSTI 1 所映射的 VLAN。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

配置 Smart Link 组 1 的主端口为 GigabitEthernet1/0/1，从端口为 GigabitEthernet1/0/2。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

在 Smart Link 组 1 中配置抢占模式为角色抢占模式；开启发送 Flush 报文的功能，并指定发送 Flush 报文的控制 VLAN 为 VLAN 10。

```
[DeviceC-smlk-group1] preemption mode role
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

创建 Smart Link 组 2，并配置其保护 VLAN 为 MSTI 2 所映射的 VLAN。

```
[DeviceC] smart-link group 2
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

配置 Smart Link 组 2 的主端口为 GigabitEthernet1/0/2，从端口为 GigabitEthernet1/0/1。

```
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 primary
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 secondary
```

在 Smart Link 组 2 中配置抢占模式为角色抢占模式；开启发送 Flush 报文的功能，并指定发送 Flush 报文的控制 VLAN 为 VLAN 110。

```
[DeviceC-smlk-group2] preemption mode role
```

```

[DeviceC-smlk-group2] flush enable control-vlan 110
[DeviceC-smlk-group2] quit
# 开启 CFD 功能，并创建级别为 5 的 MD MD_A。
[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 1，该 MA 服务于 VLAN 10。
[DeviceC] cfd service-instance 1 ma-id vlan-based md MD_A vlan 10
# 在服务实例 1 内配置 MEP 列表，在端口 GigabitEthernet1/0/1 上创建服务实例 1 内的外向
MEP 1001，并开启其 CCM 报文发送功能。
[DeviceC] cfd meplist 1001 1002 service-instance 1
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] quit
# 在 MD_A 中创建以 VLAN 编号为 MA 名称的服务实例 2，该 MA 服务于 VLAN 110。
[DeviceC] cfd service-instance 2 ma-id vlan-based md MD_A vlan 110
# 在服务实例 2 内配置 MEP 列表，在端口 GigabitEthernet1/0/2 上创建服务实例 2 内的外向
MEP 2001，并开启其 CCM 报文发送功能。
[DeviceC] cfd meplist 2001 2002 service-instance 2
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceC-GigabitEthernet1/0/2] quit
# 创建与服务实例 1 中 MEP 1001 的 CFD 连续性检测功能关联的 Track 项 1。
[DeviceC] track 1 cfd cc service-instance 1 mep 1001
# 配置 Smart Link 组 1 的主端口 GigabitEthernet1/0/1 通过 Track 项 1 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track 1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
# 创建与服务实例 2 中 MEP 2001 的 CFD 连续性检测功能关联的 Track 项 2。
[DeviceC] track 2 cfd cc service-instance 2 mep 2001
# 配置 Smart Link 组 2 的主端口 GigabitEthernet1/0/2 通过 Track 项 2 与 CFD 的连续性检测
功能联动，并重新开启该端口。
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port smart-link group 2 track 2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit

```

(4) 配置 Device D

```

# 创建 VLAN 1~200。
<DeviceD> system-view
[DeviceD] vlan 1 to 200
# 将端口 GigabitEthernet1/0/1 配置为 Trunk 端口且允许 VLAN 1~200 通过，在该端口上开
启接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 110。

```

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/1] quit
```

将端口 **GigabitEthernet1/0/2** 配置为 **Trunk** 端口且允许 **VLAN 1~200** 通过，在该端口上关闭生成树协议并开启接收 **Flush** 报文的功能，并指定接收 **Flush** 报文的控制 **VLAN** 为 **VLAN 10** 和 **110**。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/2] quit
```

4. 验证配置

假设连接 **Device A** 与 **Device B** 的光纤发生了单通故障，通过使用 **display smart-link group** 命令可以查看设备上 **Smart Link** 组的信息：

显示 **Device C** 上 **Smart Link** 组的信息。

```
[DeviceC] display smart-link group all
Smart link group 1 information:
Device ID       : 000f-e23d-5af0
Preemption mode : Role
Preemption delay: 1(s)
Control VLAN    : 10
Protected VLAN  : Reference Instance 1
```

Member	Role	State	Flush-count	Last-flush-time
GE1/0/1	PRIMARY	DOWN	5	16:45:20 2012/04/21
GE1/0/2	SECONDARY	ACTIVE	1	16:37:20 2012/04/21

```
Smart link group 2 information:
Device ID       : 000f-e23d-5af0
Preemption mode : Role
Preemption delay: 1(s)
Control VLAN    : 110
Protected VLAN  : Reference Instance 2
```

Member	Role	State	Flush-count	Last-flush-time
GE1/0/2	PRIMARY	ACTIVE	5	16:45:20 2012/04/21
GE1/0/1	SECONDARY	STANDBY	1	16:37:20 2012/04/21

由此可见，**Smart Link** 组 1 的主端口 **GigabitEthernet1/0/1** 处于故障状态，而从端口 **GigabitEthernet1/0/2** 则处于转发状态。

目 录

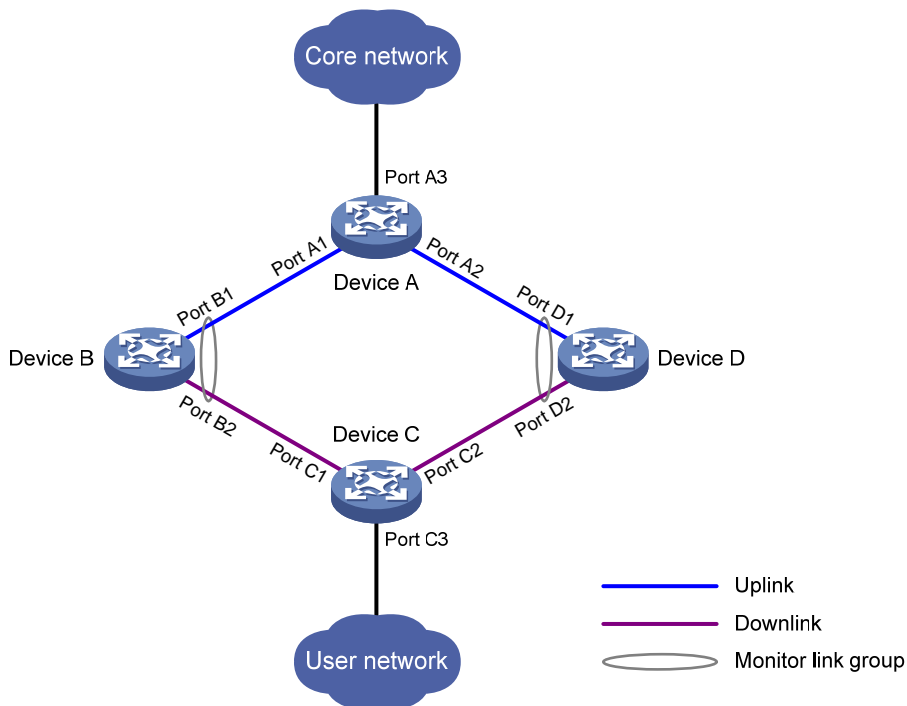
1 Monitor Link	1-1
1.1 Monitor Link简介	1-1
1.2 Monitor Link配置限制和指导	1-1
1.3 Monitor Link配置任务简介	1-2
1.4 全局开启Monitor Link协议	1-2
1.5 创建Monitor Link组	1-2
1.6 配置Monitor Link组的成员接口	1-2
1.6.1 配置限制和指导	1-2
1.6.2 在Monitor Link组视图下配置Monitor Link组的成员接口	1-3
1.6.3 在接口视图下配置Monitor Link组的成员接口	1-3
1.7 配置触发Monitor Link组状态切换的上行接口阈值	1-3
1.8 配置Monitor Link组下行接口的回切延时	1-3
1.9 Monitor Link显示和维护	1-4
1.10 Monitor Link典型配置举例	1-4
1.10.1 Monitor Link基础配置举例	1-4

1 Monitor Link

1.1 Monitor Link简介

Monitor Link 是一种接口联动方案，通过监控设备的上行接口，根据其 up/down 状态的变化来触发下行接口 up/down 状态的变化，从而触发下游设备上的拓扑协议进行链路的切换。

图1-1 Monitor Link 应用场景示意图



每个 Monitor Link 组都由上行接口和下行接口这两种成员接口组成，一个 Monitor Link 组可以有多个上行接口或下行接口，但一个接口只能属于一个 Monitor Link 组。

- 上行接口是被监控的接口，其所在链路被称为上行链路。
- 下行接口是监控接口，其所在链路被称为下行链路。

如 图 1-1 所示，Device B 的接口 Port B1 和 Port B2 组成了一个 Monitor Link 组，其中 Port B1 为上行接口，该接口所在的链路为上行链路；Port B2 为下行接口，该接口所在的链路为下行链路。Device D 上的情形也与 Device B 类似。

每个 Monitor Link 组独立进行上行接口的监控和下行接口的联动。当 Monitor Link 组中状态为 up 的上行接口个数低于上行接口阈值时，Monitor Link 组就处于 down 状态，并将强制使其所有下行接口的状态都变为 down；而状态为 up 的上行接口个数大于或等于上行接口阈值时，Monitor Link 组的状态就恢复为 up，并使其所有下行接口的状态都恢复为 up。

1.2 Monitor Link配置限制和指导

- 请勿通过接口开关命令来干预 Monitor Link 组中下行接口的状态。

- 通过延时回切机制可以避免由于 Monitor Link 组上行链路震荡而导致的下行链路频繁切换。当 Monitor Link 组的上行接口恢复为 up 状态并维持了一段时间之后,下行接口才恢复为 up 状态,这段时间就称为 Monitor Link 组下行接口的回切延时。

1.3 Monitor Link配置任务简介

Monitor Link 配置任务如下:

- (1) [全局开启Monitor Link协议](#)
- (2) [创建Monitor Link组](#)
- (3) [配置Monitor Link组的成员接口](#)
- (4) (可选) [配置触发Monitor Link组状态切换的上行接口阈值](#)
- (5) (可选) [配置Monitor Link组下行接口的回切延时](#)

1.4 全局开启Monitor Link协议

1. 功能简介

全局开启 Monitor Link 协议后,Monitor Link 组才会生效;全局关闭 Monitor Link 协议后,所有 Monitor Link 组失效,之前由 Monitor Link 协议联动触发更改状态为 down 的下行接口将恢复联动触发前的状态。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 全局开启 Monitor Link 协议。
undo monitor-link disable
缺省情况下, Monitor Link 协议处于全局开启状态。

1.5 创建Monitor Link组

- (1) 进入系统视图。
system-view
- (2) 创建 Monitor Link 组,并进入 Monitor Link 组视图。
monitor-link group group-id

1.6 配置Monitor Link组的成员接口

1.6.1 配置限制和指导

- 一个接口只能属于一个 Monitor Link 组。
- 建议先配置 Monitor Link 的上行接口,以避免下行接口出现不必要的 down/up 状态变化。
- 如果已将一个聚合组的选中端口配置为 Monitor Link 组的下行接口,请勿再将该聚合组的非选中端口配置为该 Monitor Link 组的上行接口。

- 不允许将一个聚合接口及其所对应聚合组的成员端口加入同一个 Monitor Link 组中。
- 可在 Monitor Link 组视图或接口视图下配置 Monitor Link 组的成员接口，各视图下的配置效果相同。可配置为 Monitor Link 组成员接口的接口包括二层以太网接口、二层聚合接口。

1.6.2 在Monitor Link组视图下配置Monitor Link组的成员接口

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Monitor Link 组视图。

```
monitor-link group group-id
```

- (3) 配置 Monitor Link 组的成员接口。

```
port interface-type interface-number { downlink | uplink }
```

缺省情况下，Monitor Link 组中不存在成员接口。

1.6.3 在接口视图下配置Monitor Link组的成员接口

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口为 Monitor Link 组的成员接口。

```
port monitor-link group group-id { downlink | uplink }
```

缺省情况下，接口不是 Monitor Link 组的成员接口。

1.7 配置触发Monitor Link组状态切换的上行接口阈值

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Monitor Link 组视图。

```
monitor-link group group-id
```

- (3) 配置触发 Monitor Link 组状态切换的上行接口阈值。

```
uplink up-port-threshold number-of-port
```

缺省情况下，触发 Monitor Link 组状态切换的上行接口阈值为 1。

1.8 配置Monitor Link组下行接口的回切延时

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Monitor Link 组视图。

```
monitor-link group group-id
```

- (3) 配置 Monitor Link 组下行接口的回切延时。

downlink up-delay *delay*

缺省情况下，Monitor Link 组下行接口的回切延时为 0 秒，即上行接口 up 后，下行接口立刻恢复为 up 状态。

1.9 Monitor Link显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 Monitor Link 组的运行情况。

表1-1 Monitor Link 显示和维护

操作	命令
显示Monitor Link组的信息	display monitor-link group { <i>group-id</i> all }

1.10 Monitor Link典型配置举例

1.10.1 Monitor Link基础配置举例

1. 组网需求

- 在 图 1-2 所示的组网中，Device C为Smart Link设备，Device A、Device B和Device D为相关设备。Device C上VLAN 1～30 的流量通过Smart Link组双上行到Device A。
- 通过配置，在 Device C 上实现双上行链路的灵活备份，并且当 Device A 与 Device B（或 Device D）之间出现链路故障时，Device C 能够感知到这个故障并完成其上行链路的切换。

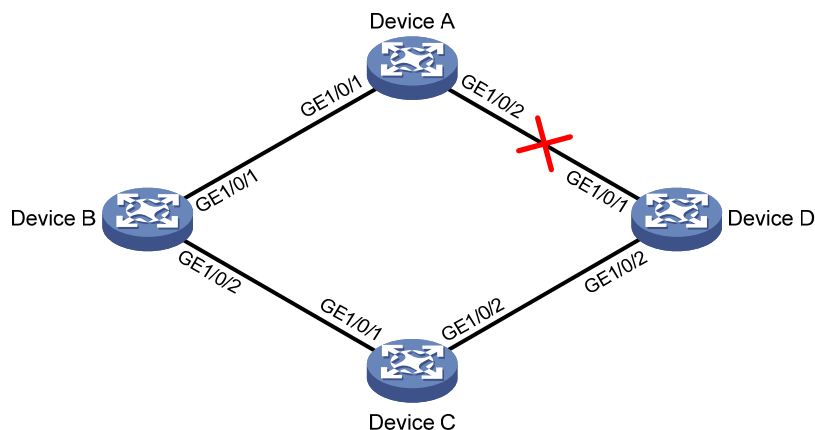


说明

有关 Smart Link 的详细介绍和配置，请参见“可靠性配置指导”中的“Smart Link”。

2. 组网图

图1-2 Monitor Link 典型配置组网图



3. 配置步骤

(1) 配置 Device C

创建 VLAN 1~30，将这些 VLAN 都映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

分别关闭端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，在这两个端口上分别关闭生成树协议，并将端口配置为 Trunk 端口且允许 VLAN 1~30 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

创建 Smart Link 组 1，并配置其保护 VLAN 为 MSTI 1 所映射的 VLAN。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

配置 Smart Link 组 1 的主端口为 GigabitEthernet1/0/1，从端口为 GigabitEthernet1/0/2。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

在 Smart Link 组 1 中使能发送 Flush 报文的功能。

```
[DeviceC-smlk-group1] flush enable
[DeviceC-smlk-group1] quit
```

重新开启端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

(2) 配置 Device A

创建 VLAN 1~30。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

分别将端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 配置为 Trunk 端口且允许 VLAN 1~30 通过，并在这些端口上都使能接收 Flush 报文的功能。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable
[DeviceA-GigabitEthernet1/0/2] quit
```

(3) 配置 Device B

创建 VLAN 1~30。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

分别将端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 配置为 Trunk 端口且允许 VLAN 1~30 通过，在端口 GigabitEthernet1/0/2 上关闭生成树协议，并在这些端口上都使能接收 Flush 报文的功能。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable
[DeviceB-GigabitEthernet1/0/2] quit
```

创建 Monitor Link 组 1，并配置该组的上行接口为 GigabitEthernet1/0/1，下行接口为 GigabitEthernet1/0/2。

```
[DeviceB] monitor-link group 1
[DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceB-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceB-mtlk-group1] quit
```

(4) 配置 Device D

创建 VLAN 1~30。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
```

分别将端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 配置为 Trunk 端口且允许 VLAN 1~30 通过，在端口 GigabitEthernet1/0/2 上关闭生成树协议，并在这些端口上都使能接收 Flush 报文的功能。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable
[DeviceD-GigabitEthernet1/0/1] quit
```

```

[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable
[DeviceD-GigabitEthernet1/0/2] quit
# 创建 Monitor Link 组 1，并配置该组的上行接口为 GigabitEthernet1/0/1，下行接口为
GigabitEthernet1/0/2。
[DeviceD] monitor-link group 1
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceD-mtlk-group1] quit

```

4. 验证配置

通过使用 **display monitor-link group** 命令可以查看各设备上 Monitor Link 组的信息。例如当 Device A 的端口 GigabitEthernet1/0/2 由于链路故障而 down 掉时：

显示 Device B 上 Monitor Link 组 1 的信息。

```

[DeviceB] display monitor-link group 1
Monitor link group 1 information:
  Group status      : UP
  Downlink up-delay: 0(s)
  Last-up-time      : 16:38:26 2012/4/21
  Last-down-time    : 16:37:20 2012/4/21
  Up-port-threshold: 1

```

Member	Role	Status
GE1/0/1	UPLINK	UP
GE1/0/2	DOWNLINK	UP

显示 Device D 上 Monitor Link 组 1 的信息。

```

[DeviceD] display monitor-link group 1
Monitor link group 1 information:
  Group status      : DOWN
  Downlink up-delay: 0(s)
  Last-up-time      : 16:37:20 2012/4/21
  Last-down-time    : 16:38:26 2012/4/21
  Up-port-threshold: 1

```

Member	Role	Status
GE1/0/1	UPLINK	DOWN
GE1/0/2	DOWNLINK	DOWN

目 录

1 VRRP	1-1
1.1 VRRP简介	1-1
1.2 VRRP备份组	1-2
1.3 VRRP标准协议模式	1-2
1.3.1 VRRP标准协议模式典型组网	1-2
1.3.2 虚拟IP地址和IP地址拥有者	1-3
1.3.3 备份组中路由器的优先级	1-3
1.3.4 备份组中路由器的工作方式	1-3
1.3.5 备份组中路由器的认证方式	1-3
1.3.6 VRRP定时器	1-4
1.3.7 Master路由器选举	1-4
1.3.8 VRRP监视功能	1-4
1.3.9 VRRP应用	1-5
1.4 VRRP负载均衡模式	1-6
1.4.1 虚拟MAC地址的分配	1-7
1.4.2 虚拟转发器	1-9
1.5 协议规范	1-11
1.6 配置IPv4 VRRP	1-11
1.6.1 IPv4 VRRP配置限制和指导	1-11
1.6.2 IPv4 VRRP配置任务简介	1-11
1.6.3 配置IPv4 VRRP的工作模式	1-12
1.6.4 配置使用的IPv4 VRRP版本	1-12
1.6.5 配置IPv4 VRRP备份组	1-12
1.6.6 配置IPv4 VRRP报文的相关属性	1-14
1.6.7 配置虚拟转发器监视功能	1-15
1.6.8 配置IPv4 VRRPv3 版本的路由器发送VRRP报文的模式	1-16
1.6.9 配置IPv4 VRRP Master路由器定时发送免费ARP报文	1-16
1.6.10 配置IPv4 VRRP成员备份组关联管理备份组功能	1-17
1.6.11 开启告警功能	1-18
1.6.12 IPv4 VRRP显示和维护	1-18
1.7 配置IPv6 VRRP	1-19
1.7.1 IPv6 VRRP配置限制和指导	1-19
1.7.2 IPv6 VRRP配置任务简介	1-19

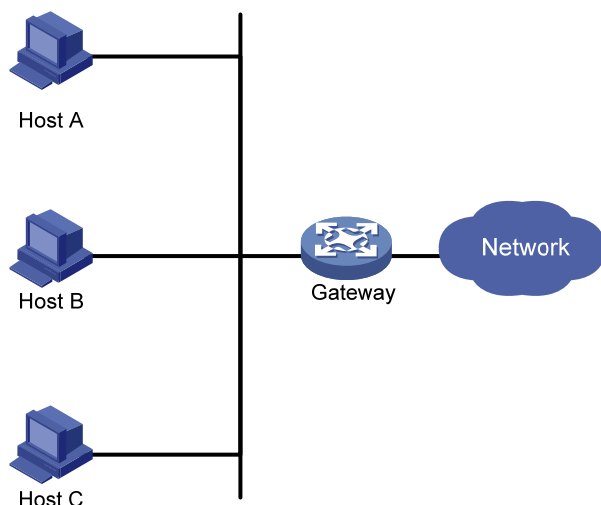
1.7.3 配置IPv6 VRRP的工作模式.....	1-19
1.7.4 配置IPv6 VRRP备份组.....	1-19
1.7.5 配置虚拟转发器监视功能.....	1-21
1.7.6 配置IPv6 VRRP报文的相关属性.....	1-22
1.7.7 配置IPv6 VRRP Master路由器定时发送ND报文.....	1-22
1.7.8 配置IPv6 VRRP成员备份组关联管理备份组功能.....	1-23
1.7.9 IPv6 VRRP显示和维护.....	1-24
1.8 IPv4 VRRP典型配置举例.....	1-24
1.8.1 VRRP单备份组配置举例.....	1-24
1.8.2 多个VLAN中的VRRP备份组配置举例.....	1-27
1.8.3 VRRP负载均衡模式配置举例.....	1-30
1.9 IPv6 VRRP典型配置举例.....	1-39
1.9.1 VRRP单备份组配置举例.....	1-39
1.9.2 多个VLAN中的VRRP备份组配置举例.....	1-42
1.9.3 VRRP负载均衡模式配置举例.....	1-45
1.10 VRRP常见故障处理.....	1-54
1.10.1 出现配置错误的提示.....	1-54
1.10.2 同一个备份组内出现多个Master路由器.....	1-54
1.10.3 VRRP的状态频繁转换.....	1-55

1 VRRP

1.1 VRRP简介

通常，同一网段内的所有主机上都存在一个相同的默认网关。主机发往其它网段的报文将通过默认网关进行转发，从而实现主机与外部网络的通信。如 [图 1-1](#) 所示，当默认网关发生故障时，本网段内所有主机将无法与外部网络通信。

图1-1 局域网组网方案



默认网关为用户的配置操作提供了方便，但是对网关设备提出了很高的稳定性要求。增加网关是提高链路可靠性的常见方法，此时如何在多个出口之间进行选路就成为需要解决的问题。

VRRP (Virtual Router Redundancy Protocol, 虚拟路由器冗余协议) 可以解决这个问题，VRRP 功能将可以承担网关功能的一组路由器加入到备份组中，形成一台虚拟路由器，并为该虚拟路由器指定虚拟 IP 地址。VRRP 通过选举机制决定哪台路由器承担转发任务。局域网内的主机仅需要知道这台虚拟路由器的虚拟 IP 地址，并将其设置为网关的 IP 地址即可。局域网内的主机通过这台虚拟路由器与外部网络进行通信。

VRRP 在提高可靠性的同时，简化了主机的配置。在具有组播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台路由器出现故障时仍然提供高可靠的链路，有效避免单一链路发生故障后网络中断的问题。

设备支持两种工作模式的 VRRP：

- 标准协议模式：基于RFC实现的VRRP，详细介绍请参见“[1.3 VRRP标准协议模式](#)”。
- 负载均衡模式：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，详细介绍请参见“[1.4 VRRP负载均衡模式](#)”。

VRRP 包括 VRRPv2 和 VRRPv3 两个版本，VRRPv2 版本只支持 IPv4 VRRP，VRRPv3 版本支持 IPv4 VRRP 和 IPv6 VRRP。

1.2 VRRP备份组

VRRP 将局域网内的可以承担网关功能的一组路由器划分在一起，组成一个备份组。备份组由一台 **Master** 路由器和多台 **Backup** 路由器组成，对外相当于一台虚拟路由器。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台虚拟路由器的 IP 地址，并将其设置为网关的 IP 地址即可。局域网内的主机通过这台虚拟路由器与外部网络进行通信。

管理员在路由器的某个三层接口上创建 VRRP 备份组后，该路由器就可成功添加到 VRRP 备份组中。



说明

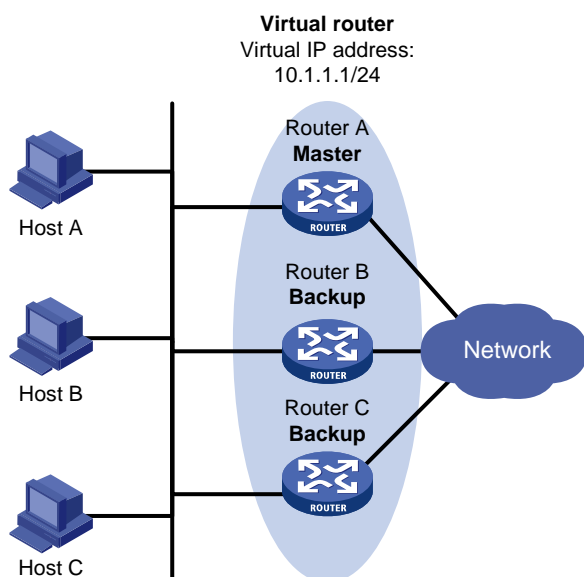
同一台设备的不同接口如果指定了相同备份组编号的 VRRP 备份组，这些接口仍然属于不同的 VRRP 备份组。

1.3 VRRP标准协议模式

1.3.1 VRRP标准协议模式典型组网

VRRP标准协议模式典型组网如 [图 1-2](#) 所示，Router A、Router B和Router C组成一台虚拟路由器。此虚拟路由器有自己的IP地址，由用户手工指定。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，当**Master**路由器发生故障时，取代**Master**路由器继续履行网关职责，从而保证局域网内的主机可不间断地与外部网络进行通信。

图1-2 VRRP 组网示意图



1.3.2 虚拟IP地址和IP地址拥有者

虚拟路由器的 IP 地址可以是备份组所在网段中未被分配的 IP 地址，也可以和备份组内的某个路由器的接口 IP 地址相同。接口 IP 地址与虚拟 IP 地址相同的路由器被称为 IP 地址拥有者。在同一个 VRRP 备份组中，只能存在一个 IP 地址拥有者。

1.3.3 备份组中路由器的优先级

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。

VRRP 优先级的取值范围为 0 到 255（数值越大表明优先级越高），可配置的范围是 1 到 254，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 地址拥有者。当路由器为 IP 地址拥有者时，其优先级始终为 255。因此，当备份组内存在 IP 地址拥有者时，只要其工作正常，则为 Master 路由器。

1.3.4 备份组中路由器的工作方式

备份组中的路由器具有以下两种工作方式：

- 非抢占方式：在该方式下只要 Master 路由器未出现故障，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。非抢占方式可以避免频繁地切换 Master 路由器。
- 抢占方式：在该方式下 Backup 路由器一旦发现自己的优先级比当前 Master 路由器的优先级高，就会触发 Master 路由器的重新选举，并最终取代原有的 Master 路由器。抢占方式可以确保承担转发任务的 Master 路由器始终是备份组中优先级最高的路由器。

1.3.5 备份组中路由器的认证方式

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，防止非法用户构造报文攻击备份组内的路由器。VRRP 提供了两种认证方式：

- 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，将其丢弃。
- 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 VRRP 报文中。收到 VRRP 报文的路由器会利用本地配置的认证字和 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合法的 VRRP 报文；否则认为接收到的报文是一个非法报文，然后将其丢弃。

在一个安全的网络中，用户也可以不设置认证方式。



说明

VRRPv3 版本的 IPv4 VRRP 和 IPv6 VRRP 均不支持对 VRRP 报文进行认证。

1.3.6 VRRP定时器

1. 偏移时间

偏移时间（Skew_Time）用来避免 Master 路由器出现故障时，备份组中的多个 Backup 路由器在同一时刻同时转变为 Master 路由器，导致备份组中存在多台 Master 路由器。

Skew_Time 的值不可配置，其计算方法与使用的 VRRP 协议版本有关：

- 使用 VRRPv2 版本（RFC 3768）时，计算方法为： $(256 - \text{路由器在备份组中的优先级}) / 256$
- 使用 VRRPv3 版本（RFC 5798）时，计算方法为： $((256 - \text{路由器在备份组中的优先级}) \times \text{VRRP 通告报文的发送时间间隔}) / 256$

2. VRRP通告报文发送间隔定时器

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。

用户可以通过命令行来调整 Master 路由器发送 VRRP 通告报文的发送间隔。如果 Backup 路由器在等待了 $3 \times \text{发送间隔} + \text{Skew_Time}$ 后，依然未收到 VRRP 通告报文，则认为自己是 Master 路由器，并向本组其它路由器发送 VRRP 通告报文，重新进行 Master 路由器的选举。

3. VRRP抢占延迟定时器

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），在抢占方式下，Backup 路由器接收到优先级低于本地优先级的 VRRP 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 + Skew_Time 后，才会对外发送 VRRP 通告报文通过 Master 路由器选举取代原来的 Master 路由器。

1.3.7 Master路由器选举

备份组中的路由器根据优先级确定自己在备份组中的角色。路由器加入备份组后，初始处于 Backup 状态：

- 如果等待 $3 \times \text{发送间隔} + \text{Skew_Time}$ 后还未收到 VRRP 通告报文，则转换为 Master 状态；
- 如果在 $3 \times \text{发送间隔} + \text{Skew_Time}$ 内收到优先级大于或等于自己优先级的 VRRP 通告报文，则保持 Backup 状态；
- 如果在 $3 \times \text{发送间隔} + \text{Skew_Time}$ 内收到优先级小于自己优先级的 VRRP 通告报文，且路由器工作在非抢占方式，则保持 Backup 状态；否则，路由器抢占成为 Master 路由器。

通过上述步骤选举出的 Master 路由器启动 VRRP 通告报文发送间隔定时器，定期向外发送 VRRP 通告报文，通知备份组内的其它路由器自己工作正常；Backup 路由器则启动定时器等待 VRRP 通告报文的到来。

由于网络故障原因造成备份组中存在多台 Master 路由器时，这些 Master 路由器会根据优先级和 IP 地址选举出一个 Master 路由器：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；如果优先级相同，则 IP 地址大的成为 Master 路由器。

1.3.8 VRRP监视功能

VRRP 监视功能通过 NQA（Network Quality Analyzer，网络质量分析）、BFD（Bidirectional Forwarding Detection，双向转发检测）等监测 Master 路由器和上行链路的状态，并通过 Track 功能在 VRRP 设备状态和 NQA/BFD 之间建立关联：

- 监视上行链路，根据上行链路的状态，改变路由器的优先级。当 **Master** 路由器的上行链路出现故障，局域网内的主机无法通过网关访问外部网络时，被监视 **Track** 项的状态变为 **Negative**，**Master** 路由器的优先级降低指定的数值。使得当前的 **Master** 路由器不是组内优先级最高的路由器，而其它路由器成为 **Master** 路由器，保证局域网内主机与外部网络的通信不会中断。
- 在 **Backup** 路由器上监视 **Master** 路由器的状态。当 **Master** 路由器出现故障时，监视 **Master** 路由器状态的 **Backup** 路由器能够迅速成为 **Master** 路由器，以保证通信不会中断。

被监视 **Track** 项的状态由 **Negative** 变为 **Positive** 或 **Notready** 后，对应的路由器优先级会自动恢复。**Track** 项的详细介绍，请参见“可靠性配置指导”中的“**Track**”。

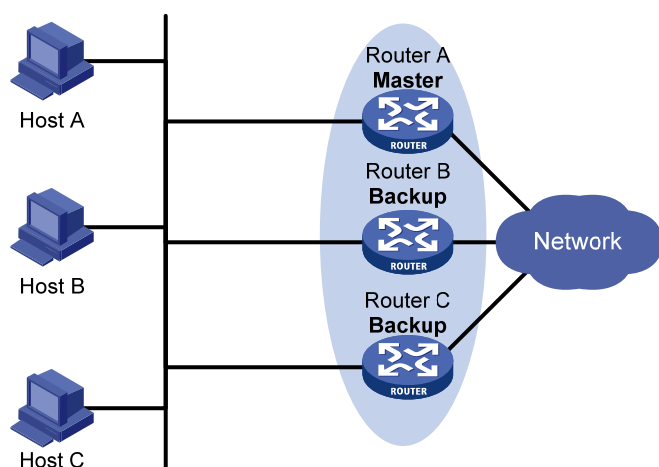
VRRP 监视功能只能工作在抢占方式下，用以保证只有优先级最高的路由器才能成为 **Master** 路由器。

1.3.9 VRRP应用

1. 主备备份

主备备份方式表示转发任务仅由**Master**路由器承担。当**Master**路由器出现故障时，才会从其它**Backup**路由器选举出一个接替工作。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 1-3](#) 中所示（以IPv4 VRRP为例）。

图1-3 主备备份 VRRP



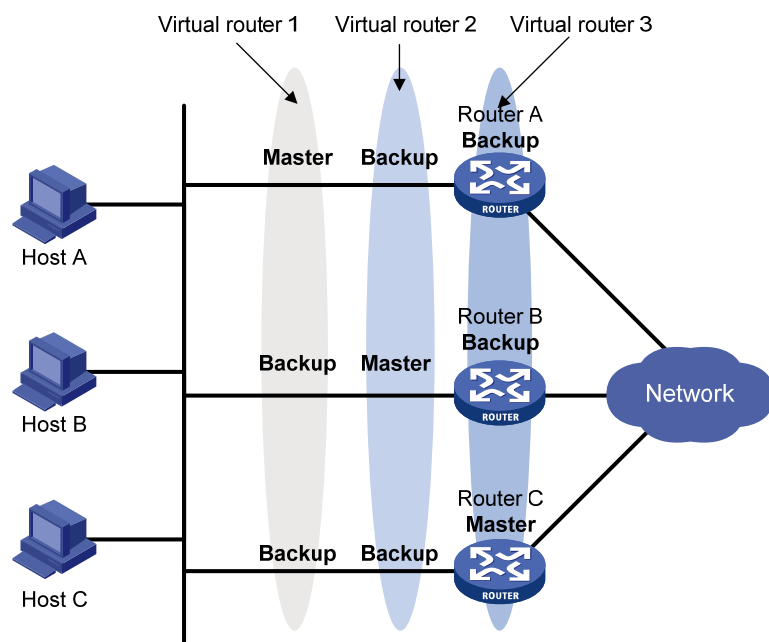
初始情况下，**Router A** 为 **Master** 路由器并承担转发任务，**Router B** 和 **Router C** 是 **Backup** 路由器且都处于就绪监听状态。如果 **Router A** 发生故障，则备份组内处于 **Backup** 状态的 **Router B** 和 **Router C** 路由器将根据优先级选出一台新的 **Master** 路由器，这台新 **Master** 路由器继续向网络内的主机提供网关服务。

2. 负载分担

一台路由器可加入多个备份组，在不同备份组中有不同的优先级，使得该路由器可以在一个备份组中作为 **Master** 路由器，在其它的备份组中作为 **Backup** 路由器。

负载分担方式是指多台路由器同时承担网关的功能，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台**Master**路由器和若干台**Backup**路由器，各备份组的**Master**路由器各不相同，如 [图 1-4](#) 中所示。

图1-4 负载分担 VRRP



同一台路由器同时加入多个 VRRP 备份组，在不同备份组中有不同的优先级。

在 [图 1-4](#) 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缺省网关分别设置为虚拟路由器 1、虚拟路由器 2 和虚拟路由器 3。在配置优先级时，需要确保备份组 1 中，Router A 的优先级最高；备份组 2 中，Router B 的优先级最高；备份组 3 中，Router C 的优先级最高。

1.4 VRRP 负载均衡模式

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台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 备份组中的每台路由器都对应一个虚拟 MAC 地址；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，备份组中的每台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台路由器之间的负载分担，

避免了标准协议模式下 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。

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。VRRP 负载均衡模式还在此基础上，增加了新的工作机制。

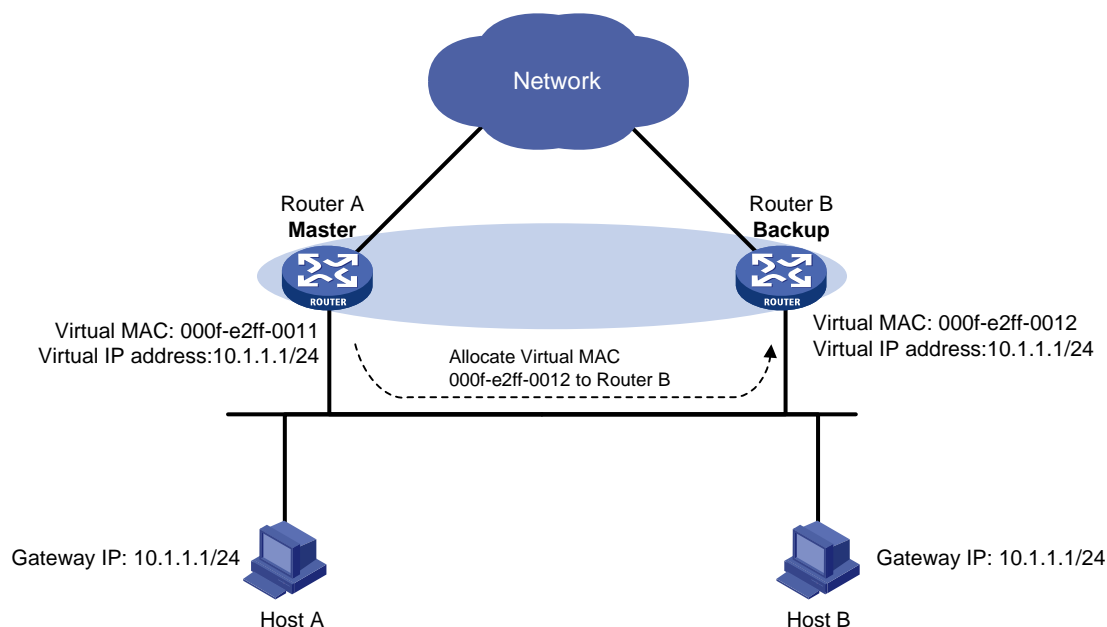
1.4.1 虚拟MAC地址的分配

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，从而实现流量在多台路由器之间分担。备份组中的 Backup 路由器不会应答主机的 ARP/ND 请求。

以 IPv4 网络为例，VRRP 负载均衡模式的具体工作过程为：

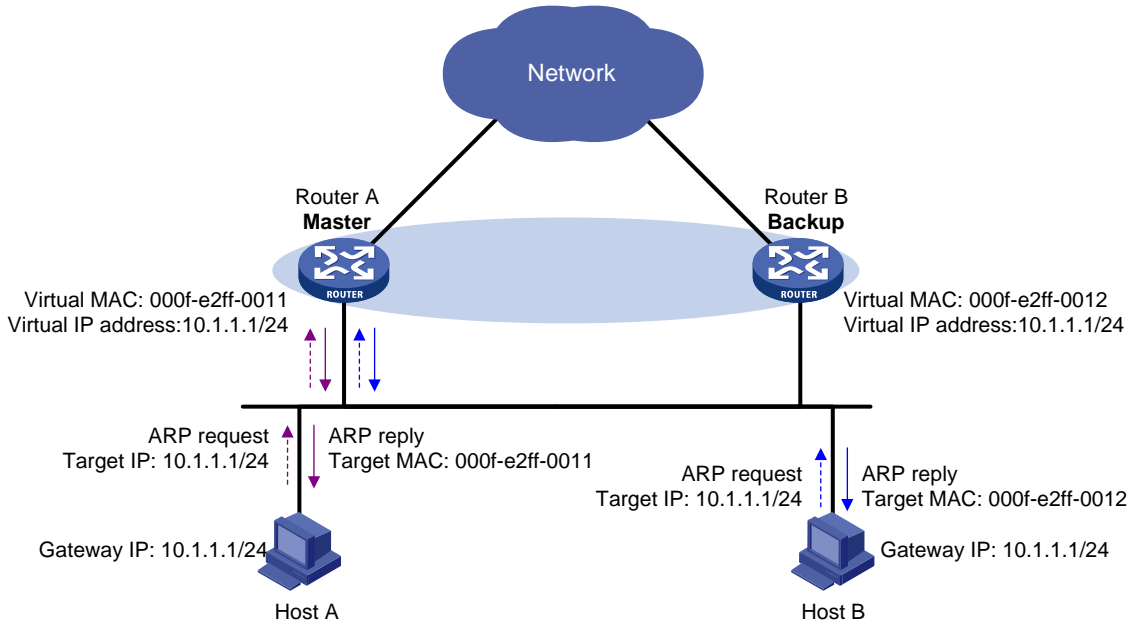
- (1) Master 路由器为备份组中的路由器（包括 Master 自身）分配虚拟 MAC 地址。如 图 1-5 所示，虚拟 IP 地址为 10.1.1.1/24 的备份组中，Router A 作为 Master 路由器，Router B 作为 Backup 路由器。Router A 为自己分配的虚拟 MAC 地址为 000f-e2ff-0011，为 Router B 分配的虚拟 MAC 地址为 000f-e2ff-0012。

图1-5 Master 分配虚拟 MAC 地址



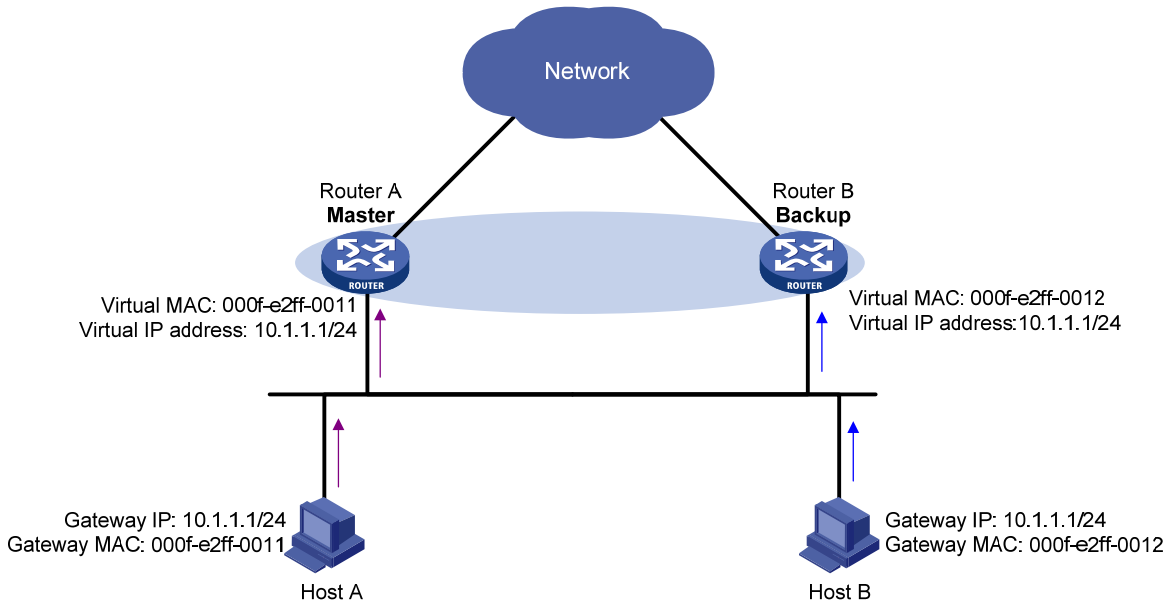
- (2) Master 路由器接收到主机发送的目标 IP 地址为虚拟 IP 地址的 ARP 请求后，根据负载均衡算法使用不同的虚拟 MAC 地址应答主机的 ARP 请求。如 图 1-6 所示，Host A 发送 ARP 请求获取网关 10.1.1.1 对应的 MAC 地址时，Master 路由器（即 Router A）使用 Router A 的虚拟 MAC 地址应答该请求；Host B 发送 ARP 请求获取网关 10.1.1.1 对应的 MAC 地址时，Master 路由器使用 Router B 的虚拟 MAC 地址应答该请求。

图1-6 Master 应答 ARP 请求



(3) 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 1-7](#) 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1-7 主机通过不同路由器转发流量



当 Master 路由器收到 ARP 请求报文后，发出的 ARP 应答报文中以太网报文头部中的源 MAC 地址和 ARP 报文内容的源 MAC 地址不一致。这样，就需要对和 VRRP 备份组配合使用的二层设备做如下限制：

- 不能开启 ARP 报文源 MAC 地址一致性检查功能；
- 如果开启了 ARP Detection 功能，不能开启 ARP 报文有效性检查功能的源 MAC 地址检查模式。

关于“ARP 报文源 MAC 地址一致性检查”和“ARP Detection”功能的介绍，请参见“安全使用指导”中的“ARP 攻击防御”。

1.4.2 虚拟转发器

1. 虚拟转发器的创建

虚拟 MAC 地址的分配，实现了不同主机将流量发送给备份组中不同的路由器。为了使备份组中的路由器能够转发主机发送的流量，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。

虚拟转发器的创建过程为：

- (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 地址对应虚拟转发器的 VF Owner（Virtual Forwarder Owner，虚拟转发器拥有者）。
- (2) VF Owner 将虚拟转发器的信息通告给备份组内其它的路由器。
- (3) 备份组内的路由器接收到虚拟转发器信息后，在本地创建对应的虚拟转发器。

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，还需要创建其它路由器通告的虚拟 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虚拟转发器的转发能力。权重值越高，虚拟转发器的转发能力越强。当权重低于一定的值——失效下限时，虚拟转发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，动态虚拟转发器），负责转发流量；其它虚拟转发器处于 Listening 状态，称为 LVF（Listening Virtual Forwarder，监听虚拟转发器），监听 AVF 的状态，不转发流量。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：

- 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 地址对应的虚拟转发器之间形成备份关系。当为主机转发流量的虚拟转发器或其对应的路由器出现故障后，可以由其它路由器上备份的虚拟转发器接替其为主机转发流量。

图1-8 虚拟转发器

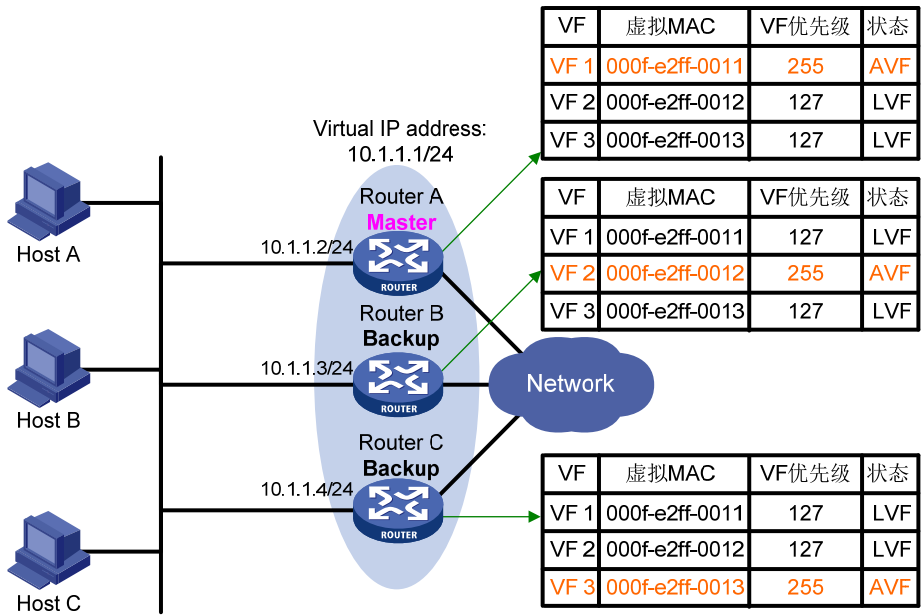


图 1-8 举例说明了备份组中每台路由器上的虚拟转发器信息及其备份关系。Master路由器Router A 为自己、Router B和Router C分配的虚拟MAC地址分别为 000f-e2ff-0011、000f-e2ff-0012 和 000f-e2ff-0013。这些虚拟MAC地址对应的虚拟转发器分别为VF 1、VF 2和VF 3。在Router A、Router B和Router C上都创建了这三个虚拟转发器，并形成备份关系。例如，Router A、Router B和Router C上的VF 1 互相备份：

- 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+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。
- 当 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。如果 LVF 的优先级相同，则 LVF 所在设备接口 MAC 地址大的成为 AVF。

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假设变成 AVF 后的优先级，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、BFD 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。

1.5 协议规范

与 VRRP 相关的协议规范有：

- RFC 3768: Virtual Router Redundancy Protocol (VRRP)
- RFC 5798: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

1.6 配置IPv4 VRRP

1.6.1 IPv4 VRRP配置限制和指导

- 在聚合组的成员端口上配置 VRRP 不生效。
- 每台路由器都需要配置一致的功能，才能形成一个 VRRP 备份组。

1.6.2 IPv4 VRRP配置任务简介

IPv4 VRRP 配置任务如下：

- (1) [配置IPv4 VRRP的工作模式](#)
- (2) (可选) [配置使用的IPv4 VRRP版本](#)
- (3) [配置IPv4 VRRP备份组](#)
- (4) (可选) [配置IPv4 VRRP报文的相关属性](#)
- (5) (可选) [配置虚拟转发器监视功能](#)

本配置仅在 VRRP 负载均衡模式下生效。

- (6) (可选) [配置IPv4 VRRPv3 版本的路由器发送VRRP报文的模式](#)
- (7) (可选) [配置IPv4 VRRP Master路由器定时发送免费ARP报文](#)
- (8) (可选) [配置IPv4 VRRP成员备份组关联管理备份组功能](#)
- (9) (可选) [开启告警功能](#)

1.6.3 配置IPv4 VRRP的工作模式

1. 配置限制和指导

配置 VRRP 的工作模式后，路由器上所有的 IPv4 VRRP 备份组都工作在指定的模式。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 VRRP 工作模式。

- 配置 VRRP 工作在标准协议模式。

```
undo vrrp mode
```

- 配置 VRRP 工作在负载均衡模式。

```
vrrp mode load-balance [ version-8 ]
```

缺省情况下，VRRP 工作在标准协议模式。

1.6.4 配置使用的IPv4 VRRP版本

1. 功能简介

IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本。通过本配置，可以指定接口上 IPv4 VRRP 使用的版本。

2. 配置限制和指导

IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本必须一致，否则备份组无法正常工作。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置使用的 VRRP 版本。

```
vrrp version version-number
```

缺省情况下，IPv4 VRRP 使用 VRRPv3 版本。

1.6.5 配置IPv4 VRRP备份组

1. 功能简介

只有创建备份组，并为备份组配置虚拟 IP 地址后，备份组才能正常工作。如果接口连接多个子网，则可以为一个备份组配置多个虚拟 IP 地址，以便实现不同子网中路由器的备份。

关闭 VRRP 备份组功能通常用于暂时禁用备份组，但还需要再次开启该备份组的场景。关闭备份组后，该备份组的状态为 **Initialize**，并且该备份组所有已存在的配置保持不变。在关闭状态下还可以对备份进行配置。备份组再次被开启后，基于最新的配置，从 **Initialize** 状态重新开始运行。

2. 配置限制和指导

限制项	说明
最大备份组及虚拟IP地址数目	负载均衡模式下，设备支持备份组最大数量为 $\text{MaxVRNum}/N$ ，其中 MaxVRNum 为标准协议模式下支持配置备份组的最大数量， N 为VRRP备份组内设备数量
备份组的虚拟IP地址	<p>VRRP工作在标准协议模式时，备份组的虚拟IP地址可以是备份组所在网段中未被分配的IP地址，也可以和备份组内的某个路由器的接口IP地址相同</p> <p>VRRP工作在负载均衡模式时，备份组的虚拟IP地址可以是备份组所在网段中未被分配的IP地址，但不能与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地址拥有者</p> <p>如果没有为备份组配置虚拟IP地址，但为备份组进行了其它配置（如优先级、抢占方式等），则该备份组会存在于设备上，并处于Inactive状态，此时备份组不起作用</p> <p>建议将备份组的虚拟IP地址和备份组中设备下行接口的IP地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络</p>
IP地址拥有者	<p>路由器作为IP地址拥有者时，建议不要采用接口的IP地址（即备份组的虚拟IP地址）与相邻的路由器建立OSPF邻居关系，即不要通过<code>network</code>命令在该接口上开启OSPF。<code>network</code>命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“OSPF”</p> <p>删除IP地址拥有者上的VRRP备份组，将导致地址冲突。建议先修改配置了备份组的接口的IP地址，再删除该接口上的VRRP备份组，以避免地址冲突</p> <p>IP地址拥有者的优先级始终为255，无需用户配置；IP地址拥有者始终工作在抢占方式</p> <p>路由器在某个备份组中作为IP地址拥有者时，如果在该路由器上执行<code>vrrp vrid track priority reduced</code>或<code>vrrp vrid track switchover</code>命令来配置该备份组监视指定的Track项，则该配置不会生效。该路由器不再作为IP地址拥有者后，监视指定的Track项功能的配置才会生效</p>
VRRP关联Track项状态	被监视Track项的状态由Negative变为Positive或Notready后，对应的路由器优先级会自动恢复或故障恢复后的原Master路由器会重新抢占为Master状态

3. 创建备份组，并配置备份组的虚拟IP地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 创建备份组，并配置备份组的虚拟IP地址。

```
vrrp vrid virtual-router-id virtual-ip virtual-address
```

4. 配置备份组的相关参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置路由器在备份组中的优先级。

```
vrrp vrid virtual-router-id priority priority-value
```

缺省情况下，路由器在备份组中的优先级为 100。

- (4) 配置备份组中的路由器工作在抢占方式，并配置抢占延迟时间。

```
vrrp vrid virtual-router-id preempt-mode [ delay delay-value ]
```

缺省情况下，备份组中的路由器工作在抢占方式，抢占延迟时间为 0 厘秒。

- (5) 配置监视指定的 Track 项。

```
vrrp vrid virtual-router-id track track-entry-number  
{ forwarder-switchover member-ip ip-address | priority reduced  
[ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }
```

缺省情况下，未指定被监视的 Track 项。

5. 关闭备份组

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 关闭 VRRP 备份组。

```
vrrp vrid virtual-router-id shutdown
```

1.6.6 配置IPv4 VRRP报文的相关属性

1. 配置限制和指导

- 一个接口上的不同备份组可以设置不同的认证方式和认证字；加入同一备份组的路由器需要设置相同的认证方式和认证字。
- 使用 VRRPv3 时，认证方式和认证字的相关配置不会生效。
- 使用 VRRPv2 时，备份组中的所有路由器必须配置相同的 VRRP 通告报文发送间隔。
- 使用 VRRPv3 时，备份组中的路由器上配置的 VRRP 通告报文发送间隔可以不同。Master 路由器根据自身配置的报文发送间隔定时发送通告报文，并在通告报文中携带 Master 路由器上配置的发送间隔；Backup 路由器接收到 Master 路由器发送的通告报文后，记录报文中携带的 Master 路由器通告报文发送间隔，如果在 $3 \times \text{发送间隔} + \text{Skew_Time}$ 内未收到 Master 路由器发送的 VRRP 通告报文，则认为 Master 路由器出现故障，重新选举 Master 路由器。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置备份组发送和接收 VRRP 报文的认证方式和认证字。

```
vrrp vrid virtual-router-id authentication-mode { md5 | simple } { cipher  
| plain } string
```

缺省情况下，不进行认证。

- (4) 配置备份组中 Master 路由器发送 VRRP 通告报文的发送间隔。

```
vrrp vrid virtual-router-id timer advertise adver-interval
```

缺省情况下，备份组中 Master 路由器发送 VRRP 通告报文的发送间隔为 100 厘秒。

建议配置 VRRP 通告报文的发送间隔大于 100 厘秒，否则会对系统的稳定性产生影响。

- (5) 为 VRRP 备份组指定源接口，该源接口用来代替 IPv4 VRRP 备份组所在接口进行该备份组 VRRP 报文的收发。

```
vrrp vrid virtual-router-id source-interface interface-type  
interface-number
```

缺省情况下，未指定备份组的源接口，VRRP 报文通过 VRRP 备份组所在接口进行收发。

- (6) 启动对 VRRP 报文 TTL 域的检查。

```
vrrp check-ttl enable
```

缺省情况下，检查 VRRP 报文的 TTL 域。

- (7) 退回系统视图。

```
quit
```

- (8) 配置 VRRP 报文的 DSCP 优先级。

```
vrrp dscp dscp-value
```

缺省情况下，VRRP 报文的 DSCP 优先级为 48。

DSCP 用来体现报文自身的优先等级，决定报文传输的优先程度。

1.6.7 配置虚拟转发器监视功能

1. 功能简介

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 负载均衡模式下虚拟转发器监视功能才会起作用。

VRRP 工作在负载均衡模式时，如果通过 Track 功能在虚拟转发器和 NQA/BFD 之间建立联动，当 Track 项的状态变为 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 项的状态由 Negative 变为 Positive 或 Notready 后，路由器中所有虚拟转发器的权重会自动恢复。

2. 配置限制和指导

- 缺省情况下，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。当监视的上行链路出现故障时，配置的权重降低数额需保证 VF Owner 的权重低于失效下限，即权重降低的数额大于 245，其它的虚拟转发器才能接替 VF Owner 成为 AVF。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置虚拟转发器监视指定的 Track 项。

```
vrrp vrid virtual-router-id track track-entry-number  
{ forwarder-switchover member-ip ip-address | priority reduced  
[ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }
```

缺省情况下，未指定虚拟转发器监视的 Track 项。

1.6.8 配置IPv4 VRRPv3 版本的路由器发送VRRP报文的模式

1. 功能简介

缺省情况下，VRRPv3 版本的路由器能够识别 VRRPv2 报文，而 VRRPv2 版本的路由器无法识别 VRRPv3 报文。通过配置本功能，使 VRRPv3 版本的路由器能够发送 VRRPv2 报文，从而与 VRRPv2 版本的路由器互相通信。该命令通常用于防止在网络中所有的路由器从 VRRPv2 版本升级成 VRRPv3 版本的过程中，由于 VRRPv2 版本的路由器无法识别 VRRPv3 报文而造成存在多台 Master 路由器的情况。

2. 配置限制和指导

- 该命令只配置 VRRP 报文的发送模式。对于接收模式，VRRPv3 版本的路由器既识别 VRRPv2 的报文，也识别 VRRPv3 的报文，所以并不受该功能控制。
- 配置了 VRRP 认证功能之后，如果发送的是 VRRPv2 报文，则会携带配置的认证信息。如果发送的是 VRRPv3 报文，则不会携带配置的认证信息。
- VRRPv3 发送版本号是 2 的 VRRP 报文时，报文中携带的 VRRP 通告报文发送时间间隔必须是 100 厘秒的整数倍，可能与 **vrrp vrid timer advertise** 命令设置的时间间隔不同。具体介绍请参见 **vrrp vrid timer advertise** 命令。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 IPv4 VRRPv3 版本的路由器发送 VRRP 报文的模式。

```
vrrp vrid virtual-router-id vrrpv3-send-packet { v2-only | v2v3-both }
```

缺省情况下，IPv4 VRRPv3 版本的路由器只发送 VRRPv3 版本的报文。

1.6.9 配置IPv4 VRRP Master路由器定时发送免费ARP报文

1. 功能简介

配置本功能后，Master 路由器定时发送免费 ARP 报文用来保证下游设备的 MAC 地址表项能够定时刷新。

2. 配置限制和指导

- 该命令只在 VRRP 标准模式下生效。
- 重复执行本命令修改免费 ARP 报文的发送时间间隔，修改后的时间间隔在下一个发送时间间隔生效。

- 为了防止设备在同一时间发送大量免费 ARP 报文，当设备同时作为多个 VRRP 备份组的 Master 路由器时，在这些 VRRP 备份组中 Master 路由器会在执行本命令后的 *interval/2* 到 *interval* 时间内随机发送第一个免费 ARP 报文。
- 如果设备上配置了大量的 VRRP 备份组，同时又配置了很小的免费 ARP 报文发送时间间隔，那么免费 ARP 报文的实际发送时间间隔可能会远远高于用户配置的时间间隔。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv4 VRRP Master 路由器定时发送免费 ARP。

```
vrrp send-gratuitous-arp [ interval interval ]
```

缺省情况下，IPv4 VRRP Master 路由器不会定时发送免费 ARP 功能报文。

1.6.10 配置IPv4 VRRP成员备份组关联管理备份组功能

1. 功能简介

设备上配置多个 VRRP 备份组承担流量转发时，因为每个 VRRP 备份组都需要单独维护自己的状态机，所以会产生大量 VRRP 报文，对网络和 CPU 性能都造成大量负荷。通过将 VRRP 备份组分为管理备份组和成员备份组，当成员备份组关联管理备份组后，成员备份组就不再发送 VRRP 通告报文进行设备间的主备协商，其设备主备状态与管理备份组保持一致，从而大大减少了 VRRP 通告报文对网络带宽和 CPU 处理性能的影响。

2. 配置限制和指导

- VRRP 管理备份组需要配置路由器在备份组中的优先级、抢占方式及监视功能等功能，保证可以正常选举出 Master 设备，VRRP 成员备份组不需要配置上述功能。
- 在 VRRP 标准协议模式和负载均衡模式下均可配置成员备份组关联管理备份组功能，但只有在 VRRP 标准协议模式下配置才会起作用。
- VRRP 备份组无法同时作为管理备份组和成员备份组。
- 如果 VRRP 备份组所关联的管理备份组不存在，则该 VRRP 备份组始终处于 Inactive 状态。
- 如果 VRRP 备份组在关联管理备份组前处于 Inactive 或 Initialize 状态，关联的管理备份组处于除 Inactive 状态的其他状态，则关联之后该 VRRP 备份组状态保持不变。
- 由于成员备份组不主动发送 VRRP 报文，可能导致下游设备上的 MAC 表项不正确，建议同时配置 **vrrp send-gratuitous-arp** 命令配置 IPv4 VRRP Master 路由器定时发送免费 ARP 报。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 IPv4 VRRP 管理备份组。

```
vrrp vrid virtual-router-id name name
```


缺省情况下，未配置 VRRP 管理备份组。

- (4) 退回系统视图。

quit

- (5) 进入接口视图。

interface *interface-type interface-number*

- (6) 配置 IPv4 VRRP 成员备份组关联管理备份组。

vrrp vrid *virtual-router-id* **follow** *name*

缺省情况下，未配置 IPv4 VRRP 成员备份组关联的管理备份组。

1.6.11 开启告警功能

1. 功能简介

开启 VRRP 的告警功能后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 开启 VRRP 的告警功能。

snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

缺省情况下，VRRP 的告警功能处于开启状态。

1.6.12 IPv4 VRRP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IPv4 VRRP 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 IPv4 VRRP 统计信息。

表1-1 IPv4 VRRP 显示和维护

操作	命令
显示IPv4 VRRP备份组的状态信息	display vrrp [interface <i>interface-type interface-number</i> [vrid <i>virtual-router-id</i>]] [verbose]
显示IPv4 VRRP管理备份组及成员备份组关联信息	display vrrp binding [interface <i>interface-type interface-number</i> [vrid <i>virtual-router-id</i>] name <i>name</i>]
显示IPv4 VRRP备份组的统计信息	display vrrp statistics [interface <i>interface-type interface-number</i> [vrid <i>virtual-router-id</i>]]
清除IPv4 VRRP备份组的统计信息	reset vrrp statistics [interface <i>interface-type interface-number</i> [vrid <i>virtual-router-id</i>]]

1.7 配置IPv6 VRRP

1.7.1 IPv6 VRRP配置限制和指导

- 在聚合组的成员端口上配置 IPv6 VRRP 不生效。
- 每台路由器都需要配置一致的功能，才能形成一个 IPv6 VRRP 备份组。

1.7.2 IPv6 VRRP配置任务简介

IPv6 VRRP 配置任务如下：

- (1) [配置IPv6 VRRP的工作模式](#)
- (2) [配置IPv6 VRRP备份组](#)
- (3) （可选）[配置虚拟转发器监视功能](#)
本配置仅在 VRRP 负载均衡模式下生效。
- (4) （可选）[配置IPv6 VRRP报文的相关属性](#)
- (5) （可选）[配置IPv6 VRRP Master路由器定时发送ND报文](#)
- (6) （可选）[配置IPv6 VRRP成员备份组关联管理备份组功能](#)

1.7.3 配置IPv6 VRRP的工作模式

1. 配置限制和指导

配置 VRRP 的工作模式后，路由器上所有的 IPv6 VRRP 备份组都工作在该模式。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 配置 VRRP 工作模式。
 - 配置 VRRP 工作在标准协议模式。
undo vrrp ipv6 mode
 - 配置 VRRP 工作在负载均衡模式。
vrrp ipv6 mode load-balance缺省情况下，VRRP 工作在标准协议模式。

1.7.4 配置IPv6 VRRP备份组

1. 功能简介

只有创建备份组，并为备份组配置虚拟 IPv6 地址后，备份组才能正常工作。可以为一个备份组配置多个虚拟 IPv6 地址。

关闭 IPv6 VRRP 备份组功能通常用于暂时禁用备份组，但还需要再次开启该备份组的场景。关闭备份组后，该备份组的状态为 **Initialize**，并且该备份组所有已存在的配置保持不变。在关闭状态下还可以对备份进行配置。备份组再次被开启后，基于最新的配置，从 **Initialize** 状态重新开始运行。

2. 配置限制和指导

限制项	说明
最大备份组及虚拟IP地址数目	负载均衡模式下设备支持备份组最大数量为MaxVRNum/N，其中MaxVRNum为标准协议模式下支持配置备份组的最大数量，N为VRRP备份组内设备数量
备份组的虚拟IP地址	<p>VRRP工作在负载均衡模式时，虚拟IPv6地址不能与VRRP备份组中路由器的接口IPv6地址相同，即负载均衡模式的VRRP备份组中不能存在IP地址拥有者</p> <p>如果没有为备份组配置虚拟IPv6地址，但是为备份组进行了其它配置（如优先级、抢占方式等），则该备份组会存在于设备上，并处于Inactive状态，此时备份组不起作用</p> <p>建议将备份组虚拟IPv6地址和备份组中设备下行接口的IPv6地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络</p>
IP地址拥有者	<p>路由器作为IP地址拥有者时，建议不要采用接口的IPv6地址（即备份组的虚拟IPv6地址）与相邻的路由器建立OSPFv3邻居关系，即不要通过ospfv3 area命令在该接口上开启OSPF。ospfv3 area命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“OSPFv3”</p> <p>删除IP地址拥有者上的VRRP备份组，将导致地址冲突。建议先修改IP地址拥有者的接口IPv6地址，再删除该接口上的VRRP备份组，以避免地址冲突</p> <p>IP地址拥有者的运行优先级始终为255，无需用户配置；IP地址拥有者始终工作在抢占方式</p> <p>路由器在某个备份组中作为IP地址拥有者时，如果在该路由器上执行vrrp ipv6 vrid track priority reduced或vrrp ipv6 vrid track switchover命令，则该配置不会生效。该路由器不再作为IP地址拥有者后，之前的配置才会生效</p>
VRRP关联Track项状态	被监视Track项的状态由Negative变为Positive或Notready后，对应的路由器优先级会自动恢复或故障恢复后的原Master路由器会重新抢占为Master状态

3. 创建备份组，并配置备份组的虚拟IPv6 地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 创建备份组，并配置备份组的虚拟 IPv6 地址，该虚拟 IPv6 地址为链路本地地址。

```
vrrp ipv6 vrid virtual-router-id virtual-ip virtual-address link-local
```

备份组的第一个虚拟 IPv6 地址必须是链路本地地址，并且每个备份组只允许有一个链路本地地址，该地址必须最后一个删除。

4. 配置备份组的相关参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置备份组的虚拟 IPv6 地址，该虚拟 IPv6 地址为全球单播地址。

```
vrrp ipv6 vrid virtual-router-id virtual-ip virtual-address
```

缺省情况下，没有为备份组指定全球单播地址类型的虚拟 IPv6 地址。

- (4) 配置路由器在备份组中的优先级。

```
vrrp ipv6 vrid virtual-router-id priority priority-value
```

缺省情况下，路由器在备份组中的优先级为 100。

- (5) 配置备份组中的路由器工作在抢占方式，并配置抢占延迟时间。

```
vrrp ipv6 vrid virtual-router-id preempt-mode [ delay delay-value ]
```

缺省情况下，备份组中的路由器工作在抢占方式，抢占延迟时间为 0 厘秒。

- (6) 配置监视指定的 Track 项。

```
vrrp ipv6 vrid virtual-router-id track track-entry-number  
{ forwarder-switchover member-ip ipv6-address | priority reduced  
[ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }
```

缺省情况下，未指定被监视的 Track 项。

5. 关闭备份组

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 关闭 IPv6 VRRP 备份组。

```
vrrp ipv6 vrid virtual-router-id shutdown
```

缺省情况下，IPv6 VRRP 备份组处于开启状态。

1.7.5 配置虚拟转发器监视功能

1. 功能简介

在 VRRP 标准协议模式和负载均衡模式均可配置虚拟转发器监视功能，但只有在 VRRP 负载均衡模式下虚拟转发器监视功能才会起作用。

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 Notready 后，路由器中所有虚拟转发器的权重会自动恢复。

2. 配置限制和指导

- 缺省情况下，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。当监视的上行链路出现故障时，配置的权重降低数额需保证 VF Owner 的权重低于失效下限，即权重降低的数额大于 245，其它的虚拟转发器才能接替 VF Owner 成为 AVF。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置虚拟转发器监视指定的 Track 项。

```
vrrp ipv6 vrid virtual-router-id track track-entry-number  
{ forwarder-switchover member-ip ipv6-address | priority reduced  
[ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }  
缺省情况下，未指定虚拟转发器监视的 Track 项。
```

1.7.6 配置IPv6 VRRP报文的相关属性

1. 配置限制和指导

- IPv6 VRRP 备份组中的路由器上配置的 VRRP 通告报文发送间隔可以不同。Master 路由器根据自身配置的报文发送间隔定时发送通告报文，并在通告报文中携带 Master 路由器上配置的发送间隔；Backup 路由器接收到 Master 路由器发送的通告报文后，记录报文中携带的 Master 通告报文发送间隔，如果在 $3 \times \text{发送间隔} + \text{Skew_Time}$ 内未收到 Master 路由器发送的 VRRP 通告报文，则认为 Master 路由器出现故障，重新选举 Master 路由器。
- 网络流量过大可能会导致 Backup 路由器在指定时间内未收到 Master 路由器的 VRRP 通告报文，而发生状态转换。可以通过将 VRRP 通告报文的发送间隔延长的办法来解决该问题。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置备份组中 Master 路由器发送 VRRP 通告报文的发送间隔。

```
vrrp ipv6 vrid virtual-router-id timer advertise adver-interval
```

缺省情况下，备份组中 Master 路由器发送 VRRP 通告报文的发送间隔为 100 厘秒。

建议配置 VRRP 通告报文的发送间隔大于 100 厘秒，否则会对系统的稳定性产生影响。

- (4) 退回系统视图。

```
quit
```

- (5) 配置 IPv6 VRRP 报文的 DSCP 优先级。

```
vrrp ipv6 dscp dscp-value
```

缺省情况下，IPv6 VRRP 报文的 DSCP 优先级为 56。

DSCP 用来体现报文自身的优先等级，决定报文传输的优先程度。

1.7.7 配置IPv6 VRRP Master路由器定时发送ND报文

1. 功能简介

开启本功能后，Master 路由器定时发送 ND 报文用来保证下游设备的 MAC 地址表项能够定时刷新。

2. 配置限制和指导

- 该命令只在 VRRP 标准模式下生效。

- 重复执行本命令修改 ND 报文的发送时间间隔,修改后的时间间隔在下一个发送时间间隔生效。
- 为了防止设备在同一时间发送大量 ND 报文,当设备同时作为多个 IPv6 VRRP 备份组的 Master 路由器时,在这些 IPv6 VRRP 备份组中 Master 路由器会在执行本命令后的 *interval/2* 到 *interval* 时间内随机发送第一个 ND 报文。
- 如果设备上配置了大量的 IPv6 VRRP 备份组,同时又配置了很小的 ND 报文发送时间间隔,那么 ND 报文的实际发送时间间隔可能会远远高于用户配置的时间间隔。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv6 VRRP Master 路由器定时发送 ND 报文。

```
vrrp ipv6 send-nd [ interval interval ]
```

缺省情况下, IPv6 VRRP Master 路由器不会定时发送 ND 报文。

1.7.8 配置IPv6 VRRP成员备份组关联管理备份组功能

1. 功能简介

设备上配置多个 IPv6 VRRP 备份组承担流量转发时,因为每个 IPv6 VRRP 备份组都需要单独维护自己的状态机,所以会产生大量 IPv6 VRRP 通告报文,对网络和 CPU 性能都造成大量负荷。通过将 IPv6 VRRP 备份组分为管理备份组和成员备份组,当成员备份组关联管理备份组后,成员备份组就不再发送 IPv6 VRRP 通告报文进行设备间的主备协商,其设备主备状态与管理备份组保持一致,从而大大减少了 IPv6 VRRP 通告报文对网络带宽和 CPU 处理性能的影响

2. 配置限制和指导

- IPv6 VRRP 管理备份组需要配置路由器在备份组中的优先级、抢占方式及监视功能等功能,保证可以正常选举出 Master 设备,IPv6 VRRP 成员备份组不需要配置上述功能。
- 在 IPv6 VRRP 标准协议模式和负载均衡模式下均可配置成员备份组关联管理备份组功能,但只有在 IPv6 VRRP 标准协议模式下配置才会起作用。
- IPv6 VRRP 备份组无法同时作为管理备份组和成员备份组。
- 如果 IPv6 VRRP 备份组所关联的管理备份组不存在,则该 IPv6 VRRP 备份组始终处于 Inactive 状态。
- 如果 IPv6 VRRP 备份组在关联管理备份组前处于 Inactive 或 Initialize 状态,关联的管理备份组处于除 Inactive 状态的其他状态,则关联之后该 IPv6 VRRP 备份组状态保持不变。
- 由于成员备份组不主动发送 IPv6 VRRP 通告报文,可能导致下游设备上的 MAC 表项不正确,建议同时配置 **vrrp ipv6 send-nd** 命令开启 IPv6 VRRP Master 路由器定时发送 ND 报文。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 IPv6 VRRP 管理备份组。

vrrip ipv6 vrid *virtual-router-id* **name** *name*

缺省情况下，未配置 IPv6 VRRP 管理备份组。

- (4) 退回系统视图。

quit

- (5) 进入接口视图。

interface *interface-type* *interface-number*

- (6) 配置 IPv6 VRRP 成员备份组关联 IPv6 VRRP 管理备份组。

vrrip ipv6 vrid *virtual-router-id* **follow** *name*

缺省情况下，未配置 IPv6 VRRP 成员备份组关联 IPv6 VRRP 管理备份组。

1.7.9 IPv6 VRRP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IPv6 VRRP 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 IPv6 VRRP 统计信息。

表1-2 IPv6 VRRP 显示和维护

操作	命令
显示IPv6 VRRP备份组的状态信息	display vrrp ipv6 [interface <i>interface-type</i> <i>interface-number</i> [vrid <i>virtual-router-id</i>]] [verbose]
显示IPv6 VRRP管理备份组及成员备份组关联信息	display vrrp ipv6 binding [interface <i>interface-type</i> <i>interface-number</i> [vrid <i>virtual-router-id</i>] name <i>name</i>]
显示IPv6 VRRP备份组的统计信息	display vrrp ipv6 statistics [interface <i>interface-type</i> <i>interface-number</i> [vrid <i>virtual-router-id</i>]]
清除IPv6 VRRP备份组的统计信息	reset vrrp ipv6 statistics [interface <i>interface-type</i> <i>interface-number</i> [vrid <i>virtual-router-id</i>]]

1.8 IPv4 VRRP典型配置举例

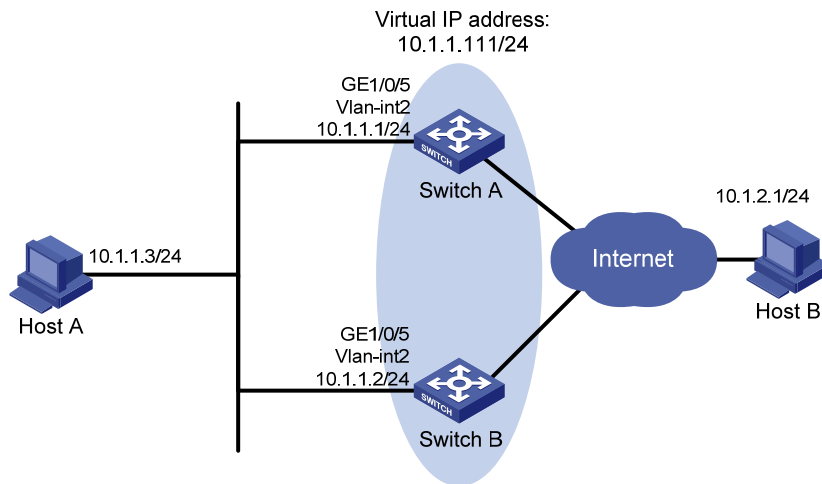
1.8.1 VRRP单备份组配置举例

1. 组网需求

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 10.1.1.111/24；
- 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。

2. 组网图

图1-9 VRRP 单备份组配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 VLAN2。

```
<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 10.1.1.1 255.255.255.0
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.111。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

设置 Switch A 在备份组 1 中的优先级为 110，高于 Switch B 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 priority 110
```

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 5000 厘秒。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

(2) 配置 Switch B

配置 VLAN2。

```
<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 10.1.1.2 255.255.255.0
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.111。


```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
# 设置 Switch B 在备份组 1 中的优先级为 100。
[SwitchB-Vlan-interface2] vrrp vrid 1 priority 100
# 设置 Switch B 工作在抢占方式，抢占延迟时间为 5000 厘秒。
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

4. 验证配置

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。

显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
VRID              : 1                      Adver Timer   : 100
Admin Status     : Up                     State         : Master
Config Pri       : 110                    Running Pri   : 110
Preempt Mode     : Yes                    Delay Time    : 5000
Auth Type        : None
Virtual IP       : 10.1.1.111
Virtual MAC      : 0000-5e00-0101
Master IP        : 10.1.1.1
```

显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
VRID              : 1                      Adver Timer   : 100
Admin Status     : Up                     State         : Backup
Config Pri       : 100                    Running Pri   : 100
Preempt Mode     : Yes                    Delay Time    : 5000
Become Master    : 401ms left
Auth Type        : None
Virtual IP       : 10.1.1.111
Virtual MAC      : 0000-5e00-0101
Master IP        : 10.1.1.1
```

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

Switch A 出现故障后，在 Host A 上仍然可以 ping 通 Host B。通过 **display vrrp verbose** 命令查看 Switch B 上备份组的详细信息。

Switch A 出现故障后，显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
```

```

Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 100
  Admin Status  : Up                     State          : Master
  Config Pri    : 100                    Running Pri    : 100
  Preempt Mode  : Yes                    Delay Time     : 5000
  Auth Type     : None
  Virtual IP    : 10.1.1.111
  Virtual MAC   : 0000-5e00-0101
  Master IP     : 10.1.1.2

```

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

Switch A 故障恢复后，显示 Switch A 上备份组 1 的详细信息。

```

[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 100
  Admin Status  : Up                     State          : Master
  Config Pri    : 110                    Running Pri    : 110
  Preempt Mode  : Yes                    Delay Time     : 5000
  Auth Type     : None
  Virtual IP    : 10.1.1.111
  Virtual MAC   : 0000-5e00-0101
  Master IP     : 10.1.1.1

```

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。

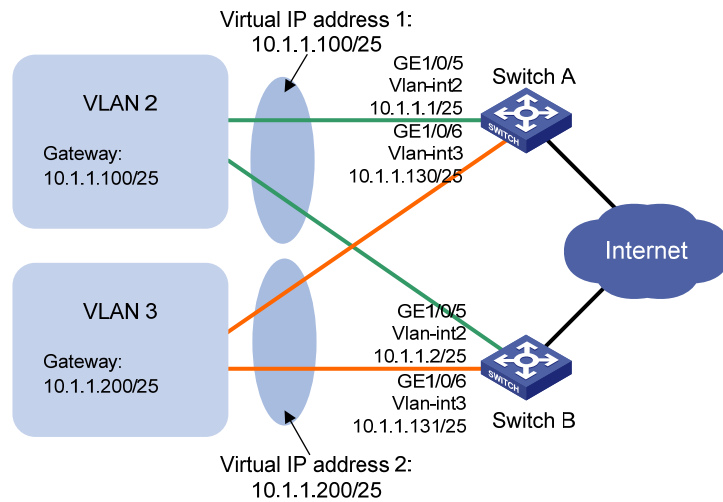
1.8.2 多个VLAN中的VRRP备份组配置举例

1. 组网需求

- VLAN 2 内主机的缺省网关为 10.1.1.100/25；VLAN 3 内主机的缺省网关为 10.1.1.200/25；
- Switch A 和 Switch B 同时属于虚拟 IP 地址为 10.1.1.100/25 的备份组 1 和虚拟 IP 地址为 10.1.1.200/25 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。

2. 组网图

图1-10 多个 VLAN 中的 VRRP 备份组配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 VLAN 2。

```
<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 10.1.1.1 255.255.255.128
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.100。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100
```

设置 Switch A 在备份组 1 中的优先级为 110，高于 Switch B 的优先级 100，以保证在备份组 1 中 Switch A 成为 Master 负责转发流量。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface2] quit
```

配置 VLAN 3。

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.1.1.130 255.255.255.128
```

创建备份组 2，并配置备份组 2 的虚拟 IP 地址为 10.1.1.200。

```
[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200
```

(2) 配置 Switch B

配置 VLAN 2。

```
<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 10.1.1.2 255.255.255.128
# 创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.100。
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100
[SwitchB-Vlan-interface2] quit
# 配置 VLAN 3。
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 10.1.1.131 255.255.255.128
# 创建备份组 2，并配置备份组 2 的虚拟 IP 地址为 10.1.1.200。
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200
# 设置 Switch B 在备份组 2 中的优先级为 110，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。
[SwitchB-Vlan-interface3] vrrp vrid 2 priority 110
```

4. 验证配置

可以通过 **display vrrp verbose** 命令查看配置后的结果。

显示 Switch A 上备份组的详细信息。

```
[SwitchA-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 2

Interface Vlan-interface2
VRID              : 1                      Adver Timer    : 100
Admin Status      : Up                    State           : Master
Config Pri        : 110                   Running Pri     : 110
Preempt Mode      : Yes                   Delay Time      : 0
Auth Type         : None
Virtual IP        : 10.1.1.100
Virtual MAC       : 0000-5e00-0101
Master IP         : 10.1.1.1

Interface Vlan-interface3
VRID              : 2                      Adver Timer    : 100
Admin Status      : Up                    State           : Backup
Config Pri        : 100                   Running Pri     : 100
Preempt Mode      : Yes                   Delay Time      : 0
Become Master     : 203ms left
Auth Type         : None
Virtual IP        : 10.1.1.200
Virtual MAC       : 0000-5e00-0102
Master IP         : 10.1.1.131
```

显示 Switch B 上备份组的详细信息。

```
[SwitchB-Vlan-interface3] display vrrp verbose
```

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 2

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 0
Become Master	: 211ms left		
Auth Type	: None		
Virtual IP	: 10.1.1.100		
Virtual MAC	: 0000-5e00-0101		
Master IP	: 10.1.1.1		

Interface Vlan-interface3

VRID	: 2	Adver Timer	: 100
Admin Status	: Up	State	: Master
Config Pri	: 110	Running Pri	: 110
Preempt Mode	: Yes	Delay Time	: 0
Auth Type	: None		
Virtual IP	: 10.1.1.200		
Virtual MAC	: 0000-5e00-0102		
Master IP	: 10.1.1.131		

以上显示信息表示在备份组 1 中 Switch A 为 Master, Switch B 为 Backup, 缺省网关为 10.1.1.100/25 的主机通过 Switch A 访问 Internet; 备份组 2 中 Switch A 为 Backup, Switch B 为 Master, 缺省网关为 10.1.1.200/25 的主机通过 Switch B 访问 Internet。

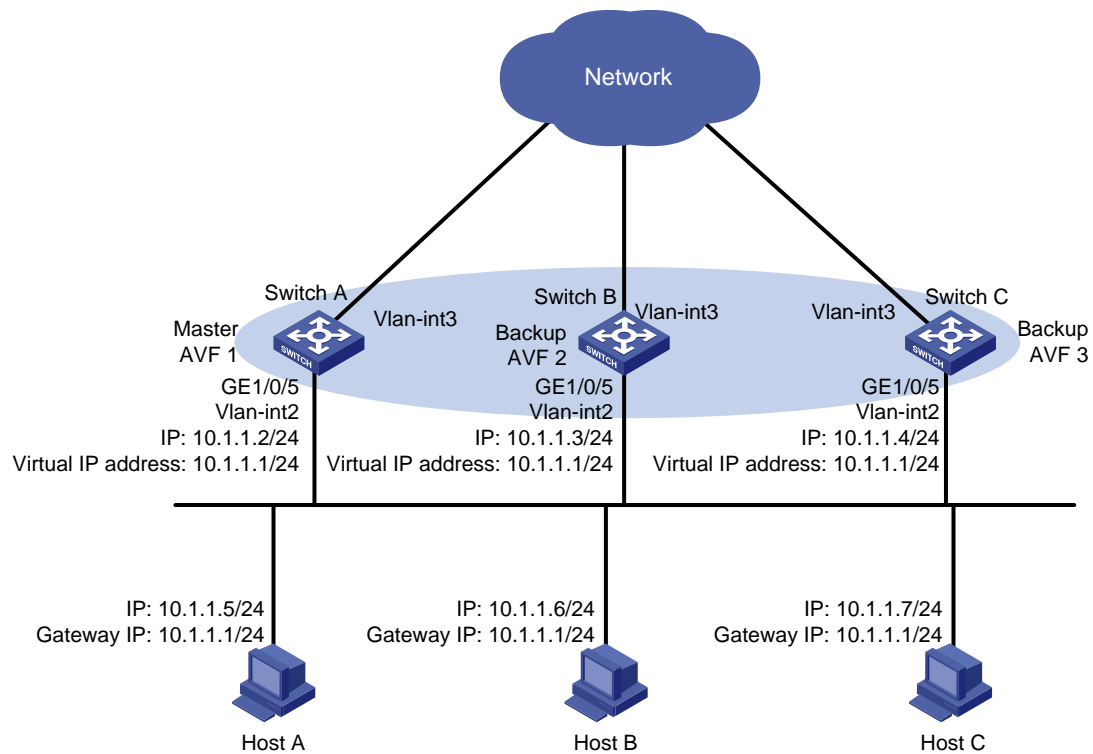
1.8.3 VRRP 负载均衡模式配置举例

1. 组网需求

- 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 网段内主机的缺省网关为 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;
- 备份组 1 工作在负载均衡模式, 通过一个备份组实现负载分担, 充分利用网关资源;
- 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 (VLAN 接口 3) 的状态。当上行接口出现故障时, 降低 Switch A、Switch B 或 Switch C 上虚拟转发器的权重, 以便其它设备接管它的转发任务。

2. 组网图

图1-11 VRRP 负载均衡模式配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 VLAN 2。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
```

配置 VRRP 工作在负载均衡模式。

```
[SwitchA] vrrp mode load-balance
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.1。

```
[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
```

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 priority 120
```

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 5000 厘秒。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
[SwitchA-Vlan-interface2] quit
```

创建和 VLAN 接口 3 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] track 1 interface vlan-interface 3
```

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, 以便其它设备接替 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。

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250
```

(2) 配置 Switch B

配置 VLAN 2。

```
<SwitchB> system-view
```

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/5
```

```
[SwitchB-vlan2] quit
```

配置 VRRP 工作在负载均衡模式。

```
[SwitchB] vrrp mode load-balance
```

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] 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
```

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 priority 110
```

配置 Switch B 工作在抢占方式, 抢占延迟时间为 5000 厘秒。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

```
[SwitchB-Vlan-interface2] quit
```

创建和 VLAN 接口 3 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] track 1 interface vlan-interface 3
```

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, 以便其它设备接替 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。

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250
```

(3) 配置 Switch C

配置 VLAN 2。

```
<SwitchC> system-view
```

```
[SwitchC] vlan 2
```

```
[SwitchC-vlan2] port gigabitethernet 1/0/5
```

```
[SwitchC-vlan2] quit
```

配置 VRRP 工作在负载均衡模式。

```
[SwitchC] vrrp mode load-balance
```

创建备份组 1, 并配置备份组 1 的虚拟 IP 地址为 10.1.1.1。

```
[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
```

配置 Switch C 工作在抢占方式，抢占延迟时间为 5000 厘秒。

```
[SwitchC-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
[SwitchC-Vlan-interface2] quit
```

创建和 VLAN 接口 3 物理状态关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Switch C 的上行接口出现故障。

```
[SwitchC] track 1 interface vlan-interface 3
```

配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Switch C 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，以便其它设备接替 Switch C 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250
```

4. 验证配置

配置完成后，在 Host A 上可以 ping 通外网。通过 **display vrrp verbose** 命令查看配置后的结果。

显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
```

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Master
Config Pri	: 120	Running Pri	: 120
Preempt Mode	: Yes	Delay Time	: 5000
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 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

显示 Switch B 上备份组 1 的详细信息。

[SwitchB-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 110	Running Pri	: 110
Preempt Mode	: Yes	Delay Time	: 5000
Become Master	: 410ms left		
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

显示 Switch C 上备份组 1 的详细信息。

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID            : 1                      Adver Timer   : 100
  Admin Status    : Up                    State          : Backup
  Config Pri      : 100                   Running Pri    : 100
  Preempt Mode    : Yes                    Delay Time     : 5000
  Become Master   : 401ms left
  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，Switch B 和 Switch C 为 Backup。Switch A、Switch B 和 Switch C 上各自存在一个 AVF，并存在作为备份的两个 LVF。

当 Switch A 的上行接口（VLAN 接口 3）出现故障后，通过 **display vrrp verbose** 命令查看 Switch A 上备份组的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID            : 1                      Adver Timer   : 100
```

```

Admin Status      : Up                      State      : Master
Config Pri       : 120                      Running Pri  : 120
Preempt Mode     : Yes                      Delay Time   : 5000
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
```

通过 **display vrrp verbose** 命令查看 Switch C 上备份组的详细信息。

```
[SwitchC-Vlan-interface2] display vrrp verbose
```

IPv4 Virtual Router Information:

```
Running Mode : Load Balance
```

Total number of virtual routers : 1

Interface Vlan-interface2

```

VRID      : 1                      Adver Timer : 100
Admin Status : Up                  State      : Backup
Config Pri : 100                   Running Pri : 100
Preempt Mode : Yes                 Delay Time  : 5000
Become Master : 401ms left
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

```

```

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

```

以上显示信息表示 **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。**Switch C** 成为虚拟 MAC 地址 **000f-e2ff-0011** 对应虚拟转发器的 AVF，接管 **Switch A** 的转发任务。

Timeout Timer 超时后（约 1800 秒后），查看 **Switch C** 上备份组的详细信息。

```
[SwitchC-Vlan-interface2] display vrrp verbose
```

IPv4 Virtual Router Information:

```
Running Mode      : Load Balance
```

Total number of virtual routers : 1

Interface Vlan-interface2

```

VRID              : 1                      Adver Timer   : 100
Admin Status      : Up                    State         : Backup
Config Pri        : 100                   Running Pri    : 100
Preempt Mode      : Yes                   Delay Time     : 5000
Become Master     : 402ms left
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

```

以上显示信息表示,Timeout Timer 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 的报文。

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。

```

[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
VRID              : 1          Adver Timer   : 100
Admin Status     : Up        State          : Master
Config Pri       : 110       Running Pri    : 110
Preempt Mode     : Yes       Delay Time     : 5000
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

```

以上显示信息表示 Switch A 出现故障后,Switch B 的优先级高于 Switch C,将抢占成为 Master,同时删除了虚拟 MAC 地址 000f-e2ff-0011 对应的虚拟转发器。

1.9 IPv6 VRRP典型配置举例

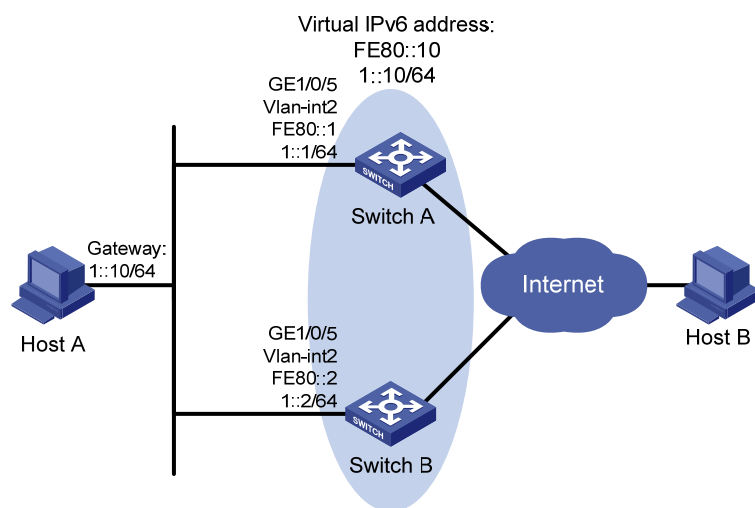
1.9.1 VRRP单备份组配置举例

1. 组网需求

- Host A 需要访问 Internet 上的 Host B；Host A 通过交换机发送的 RA 消息学习到缺省网关地址为 1::10/64；
- 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。

2. 组网图

图1-12 VRRP 单备份组配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 VLAN 2。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

创建备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

配置 Switch A 在备份组 1 中的优先级为 110，高于 Switch B 的优先级 100，以保证 Switch A 成为 Master 负责转发流量。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

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 Router 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 5000 厘秒。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

配置允许发布 RA 消息，以便 Host A 通过 RA 消息学习到缺省网关地址。

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
```

(2) 配置 Switch B

配置 VLAN 2。

```
<SwitchB> system-view
```

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/5
```

```
[SwitchB-vlan2] quit
```

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
```

```
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

创建备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

配置 Switch B 工作在抢占方式，抢占延迟时间为 5000 厘秒。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

配置允许发布 RA 消息，以便 Host A 通过 RA 消息学习到缺省网关地址。

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

4. 验证配置

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp ipv6 verbose** 命令查看配置后的结果。

显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
```

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : FE80::10
1::10

Virtual MAC : 0000-5e00-0201

Master IP : FE80::1

显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
```

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

```

Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 100
  Admin Status  : Up                    State          : Backup
  Config Pri    : 100                   Running Pri    : 100
  Preempt Mode  : Yes                   Delay Time     : 5000
  Become Master : 403ms left
  Auth Type     : None
  Virtual IP    : FE80::10
                  1::10
  Virtual MAC   : 0000-5e00-0201
  Master IP     : FE80::1

```

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

Switch A 出现故障后，在 Host A 上仍然可以 ping 通 Host B。通过 **display vrrp ipv6 verbose** 命令查看 Switch B 上备份组的信息。

Switch A 出现故障后，显示 Switch B 上备份组 1 的详细信息。

```

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1

Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 100
  Admin Status  : Up                    State          : Master
  Config Pri    : 100                   Running Pri    : 100
  Preempt Mode  : Yes                   Delay Time     : 5000
  Auth Type     : None
  Virtual IP    : FE80::10
                  1::10
  Virtual MAC   : 0000-5e00-0201
  Master IP     : FE80::2

```

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

Switch A 故障恢复后，显示 Switch A 上备份组 1 的详细信息。

```

[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1

Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 100
  Admin Status  : Up                    State          : Master
  Config Pri    : 110                   Running Pri    : 110
  Preempt Mode  : Yes                   Delay Time     : 5000
  Auth Type     : None
  Virtual IP    : FE80::10
                  1::10
  Virtual MAC   : 0000-5e00-0201
  Master IP     : FE80::1

```


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。

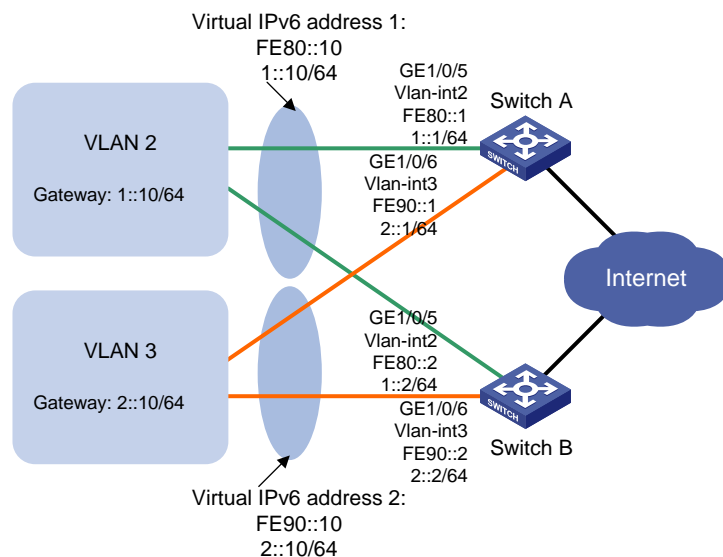
1.9.2 多个VLAN中的VRRP备份组配置举例

1. 组网需求

- Switch A 和 Switch B 同时属于虚拟 IPv6 地址为 1::10/64、FE80::10 的备份组 1 和虚拟 IPv6 地址为 2::10/64、FE90::10 的备份组 2；
- VLAN 2 内主机通过交换机发送的 RA 消息学习到缺省网关地址为 1::10/64；VLAN 3 内主机通过路由器发送的 RA 消息学习到缺省网关地址为 2::10/64；
- 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。

2. 组网图

图1-13 多个 VLAN 中的 VRRP 备份组配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 VLAN 2。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
# 创建备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

```

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
# 设置 Switch A 在备份组 1 中的优先级为 110，高于 Switch B 的优先级 100，以保证在备份组 1
中 Switch A 成为 Master 负责转发流量。
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
# 配置允许发布 RA 消息，以便 VLAN 2 内主机通过 RA 消息学习到缺省网关地址。
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
[SwitchA-Vlan-interface2] quit
# 配置 VLAN 3。
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address fe90::1 link-local
[SwitchA-Vlan-interface3] ipv6 address 2::1 64
# 创建备份组 2，并配置备份组 2 的虚拟 IPv6 地址为 FE90::10 和 2::10。
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
# 配置允许发布 RA 消息，以便 VLAN 3 内主机通过 RA 消息学习到缺省网关地址。
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt

```

(2) 配置 Switch B

```

# 配置 VLAN 2。
<SwitchB> system-view
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
# 创建备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 1::10。
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
# 配置允许发布 RA 消息，以便 VLAN 2 内主机通过 RA 消息学习到缺省网关地址。
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2] quit
# 配置 VLAN 3。
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address fe90::2 link-local
[SwitchB-Vlan-interface3] ipv6 address 2::2 64
# 创建备份组 2，并配置备份组 2 的虚拟 IPv6 地址为 FE90::10 和 2::10。
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
# 设置 Switch B 在备份组 2 中的优先级为 110，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。

```

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 priority 110
```

配置允许发布 RA 消息，以便 VLAN 3 内主机通过 RA 消息学习到缺省网关地址。

```
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
```

4. 验证配置

可以通过 **display vrrp ipv6 verbose** 命令查看配置后的结果。

显示 Switch A 上备份组的详细信息。

```
[SwitchA-Vlan-interface3] display vrrp ipv6 verbose
```

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 2

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Master
Config Pri	: 110	Running Pri	: 110
Preempt Mode	: Yes	Delay Time	: 0
Auth Type	: None		
Virtual IP	: FE80::10		
	1::10		
Virtual MAC	: 0000-5e00-0201		
Master IP	: FE80::1		

Interface Vlan-interface3

VRID	: 2	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 0
Become Master	: 402ms left		
Auth Type	: None		
Virtual IP	: FE90::10		
	2::10		
Virtual MAC	: 0000-5e00-0202		
Master IP	: FE90::2		

显示 Switch B 上备份组的详细信息。

```
[SwitchB-Vlan-interface3] display vrrp ipv6 verbose
```

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 2

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 0
Become Master	: 401ms left		
Auth Type	: None		
Virtual IP	: FE80::10		
	1::10		
Virtual MAC	: 0000-5e00-0201		

Master IP : FE80::1

Interface Vlan-interface3

VRID	: 2	Adver Timer	: 100
Admin Status	: Up	State	: Master
Config Pri	: 110	Running Pri	: 110
Preempt Mode	: Yes	Delay Time	: 0
Auth Type	: None		
Virtual IP	: FE90::10		
	2::10		
Virtual MAC	: 0000-5e00-0202		
Master IP	: FE90::2		

以上显示信息表示在备份组 1 中 Switch A 为 Master，Switch B 为 Backup，缺省网关为 1::10/64 的主机通过 Switch A 访问 Internet；备份组 2 中 Switch A 为 Backup，Switch B 为 Master，缺省网关为 2::10/64 的主机通过 Switch B 访问 Internet。

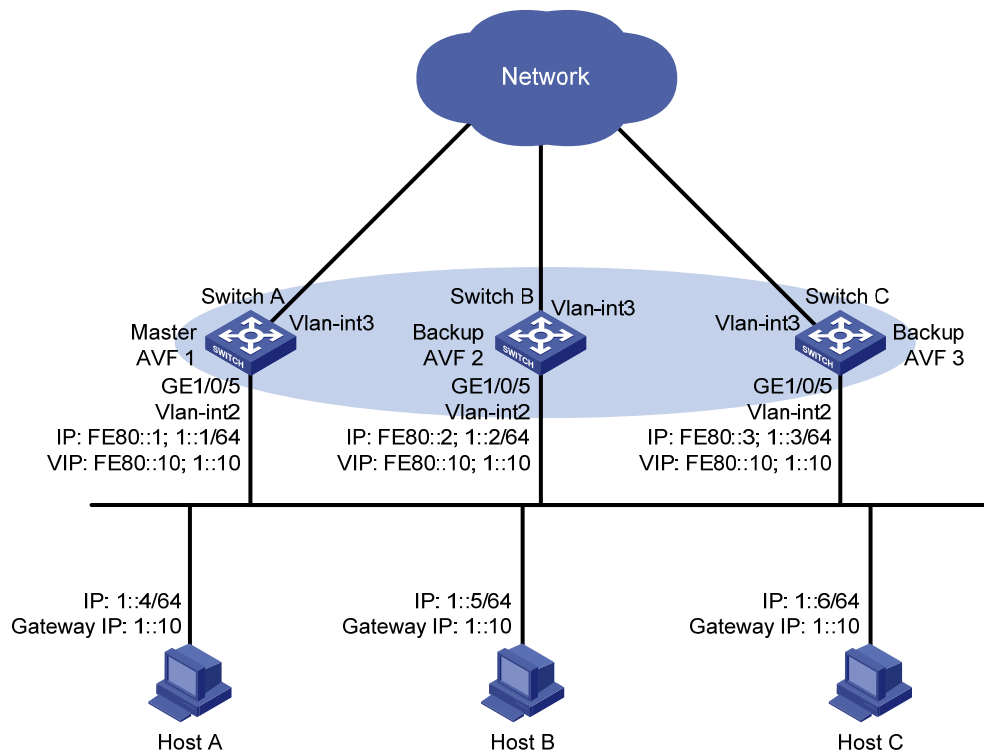
1.9.3 VRRP负载均衡模式配置举例

1. 组网需求

- Switch A、Switch B 和 Switch C 属于虚拟 IPv6 地址为 FE80::10 和 1::10 的备份组 1；
- 1::/64 网段内主机通过交换机发送的 RA 消息学习到缺省网关地址为 1::10，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；
- 备份组 1 工作在负载均衡模式，通过一个备份组实现负载分担，充分利用网关资源；
- 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（VLAN 接口 3）的状态。当上行接口出现故障时，降低 Switch A、Switch B 或 Switch C 上虚拟转发器的权重，以便其它设备接管它的转发任务。

2. 组网图

图1-14 VRRP 负载均衡模式配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 VLAN 2。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
```

配置 VRRP 工作在负载均衡模式。

```
[SwitchA] vrrp ipv6 mode load-balance
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 FE80::10 和 1::10。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

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 ipv6 vrid 1 priority 120
```

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 5000 厘秒。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

配置允许发布 RA 消息，以便 1::/64 网段内主机通过 RA 消息学习到缺省网关地址。

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
```

```
[SwitchA-Vlan-interface2] quit
```

创建和 VLAN 接口 3 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] track 1 interface vlan-interface 3
```

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，以便其它设备接替 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。

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250
```

(2) 配置 Switch B

配置 VLAN 2。

```
<SwitchB> system-view
```

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/5
```

```
[SwitchB-vlan2] quit
```

配置 VRRP 工作在负载均衡模式。

```
[SwitchB] vrrp ipv6 mode load-balance
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 FE80::10 和 1::10。

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
```

```
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

配置 Switch B 在备份组 1 中的优先级为 110，高于 Switch C 的优先级 100，以保证 Switch A 出现故障时，Switch B 成为 Master。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

配置 Switch B 工作在抢占方式，抢占延迟时间为 5000 厘秒。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

配置允许发布 RA 消息，以便 1::/64 网段内主机通过 RA 消息学习到缺省网关地址。

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

```
[SwitchB-Vlan-interface2] quit
```

创建和 VLAN 接口 3 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] track 1 interface vlan-interface 3
```

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，以便其它设备接替 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。

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250
```

(3) 配置 Switch C

配置 VLAN 2。

```

<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/5
[SwitchC-vlan2] quit
# 配置 VRRP 工作在负载均衡模式。
[SwitchC] vrrp ipv6 mode load-balance
# 创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 FE80::10 和 1::10。
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ipv6 address fe80::3 link-local
[SwitchC-Vlan-interface2] ipv6 address 1::3 64
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
# 配置 Switch C 工作在抢占方式，抢占延迟时间为 5000 厘秒。
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
# 配置允许发布 RA 消息，以便 1::/64 网段内主机通过 RA 消息学习到缺省网关地址。
[SwitchC-Vlan-interface2] undo ipv6 nd ra halt
[SwitchC-Vlan-interface2] quit
# 创建和 VLAN 接口 3 物理状态关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Switch C 的上行接口出现故障。
[SwitchC] track 1 interface vlan-interface 3
# 配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Switch C 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，以便其它设备接替 Switch C 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250

```

4. 验证配置

配置完成后，在 Host A 上可以 ping 通外网。通过 **display vrrp ipv6 verbose** 命令查看配置后的结果。

显示 Switch A 上备份组 1 的详细信息。

```

[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode      : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID           : 1                      Adver Timer   : 100
  Admin Status   : Up                    State         : Master
  Config Pri     : 120                   Running Pri    : 120
  Preempt Mode   : Yes                   Delay Time    : 5000
  Auth Type      : None
  Virtual IP     : FE80::10
                  1::10
  Member IP List : FE80::1 (Local, Master)
                  FE80::2 (Backup)
                  FE80::3 (Backup)
Forwarder Information: 3 Forwarders 1 Active

```

```

Config Weight : 255
Running Weight : 255
Forwarder 01
State : Active
Virtual MAC : 000f-e2ff-4011 (Owner)
Owner ID : 0000-5e01-1101
Priority : 255
Active : local
Forwarder 02
State : Listening
Virtual MAC : 000f-e2ff-4012 (Learnt)
Owner ID : 0000-5e01-1103
Priority : 127
Active : FE80::2
Forwarder 03
State : Listening
Virtual MAC : 000f-e2ff-4013 (Learnt)
Owner ID : 0000-5e01-1105
Priority : 127
Active : FE80::3
Forwarder Weight Track Information:
Track Object : 1 State : Positive Weight Reduced : 250

```

显示 Switch B 上备份组 1 的详细信息。

```

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 100
Admin Status : Up State : Backup
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5000
Become Master : 401ms left
Auth Type : None
Virtual IP : FE80::10
1::10
Member IP List : FE80::2 (Local, Backup)
FE80::1 (Master)
FE80::3 (Backup)
Forwarder Information: 3 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
State : Listening
Virtual MAC : 000f-e2ff-4011 (Learnt)
Owner ID : 0000-5e01-1101
Priority : 127
Active : FE80::1

```


Forwarder 02

State : Active
Virtual MAC : 000f-e2ff-4012 (Owner)
Owner ID : 0000-5e01-1103
Priority : 255
Active : local

Forwarder 03

State : Listening
Virtual MAC : 000f-e2ff-4013 (Learnt)
Owner ID : 0000-5e01-1105
Priority : 127
Active : FE80::3

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

显示 Switch C 上备份组 1 的详细信息。

[SwitchC-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 5000
Become Master	: 402ms left		
Auth Type	: None		
Virtual IP	: FE80::10		
	1::10		
Member IP List	: FE80::3 (Local, Backup)		
	FE80::1 (Master)		
	FE80::2 (Backup)		

Forwarder Information: 3 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Listening
Virtual MAC : 000f-e2ff-4011 (Learnt)
Owner ID : 0000-5e01-1101
Priority : 127
Active : FE80::1

Forwarder 02

State : Listening
Virtual MAC : 000f-e2ff-4012 (Learnt)
Owner ID : 0000-5e01-1103
Priority : 127
Active : FE80::2

Forwarder 03

State : Active

```
Virtual MAC      : 000f-e2ff-4013 (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, Switch B 和 Switch C 为 Backup。Switch A、Switch B 和 Switch C 上各自存在一个 AVF, 并存在作为备份的两个 LVF。

当 Switch A 的上行接口 (VLAN 接口 3) 出现故障后, 通过 **display vrrp ipv6 verbose** 命令查看 Switch A 上备份组的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
```

```
Running Mode      : Load Balance
```

Total number of virtual routers : 1

Interface Vlan-interface2

```
VRID              : 1                      Adver Timer   : 100
Admin Status      : Up                    State         : Master
Config Pri        : 120                   Running Pri   : 120
Preempt Mode      : Yes                   Delay Time    : 5000
Auth Type         : None
Virtual IP         : FE80::10
                  : 1::10
Member IP List     : FE80::1 (Local, Master)
                  : FE80::2 (Backup)
                  : FE80::3 (Backup)
```

Forwarder Information: 3 Forwarders 0 Active

```
Config Weight    : 255
```

```
Running Weight   : 5
```

Forwarder 01

```
State           : Initialize
Virtual MAC      : 000f-e2ff-4011 (Owner)
Owner ID         : 0000-5e01-1101
Priority         : 0
Active           : FE80::3
```

Forwarder 02

```
State           : Initialize
Virtual MAC      : 000f-e2ff-4012 (Learnt)
Owner ID         : 0000-5e01-1103
Priority         : 0
Active           : FE80::2
```

Forwarder 03

```
State           : Initialize
Virtual MAC      : 000f-e2ff-4013 (Learnt)
Owner ID         : 0000-5e01-1105
Priority         : 0
Active           : FE80::3
```

Forwarder Weight Track Information:

```
Track Object    : 1          State : Negative  Weight Reduced : 250
```

通过 **display vrrp ipv6 verbose** 命令查看 Switch C 上备份组的详细信息。

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
```

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 5000
Become Master	: 410ms left		
Auth Type	: None		
Virtual IP	: FE80::10 1::10		
Member IP List	: FE80::3 (Local, Backup) FE80::1 (Master) FE80::2 (Backup)		

Forwarder Information: 3 Forwarders 2 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State	: Active
Virtual MAC	: 000f-e2ff-4011 (Take Over)
Owner ID	: 0000-5e01-1101
Priority	: 85
Active	: local

Forwarder 02

State	: Listening
Virtual MAC	: 000f-e2ff-4012 (Learnt)
Owner ID	: 0000-5e01-1103
Priority	: 85
Active	: FE80::2

Forwarder 03

State	: Active
Virtual MAC	: 000f-e2ff-4013 (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 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。Switch C 成为虚拟 MAC 地址 000f-e2ff-4011 对应虚拟转发器的 AVF，接管 Switch A 的转发任务。

Timeout Timer 超时后（约 1800 秒后），查看 Switch C 上备份组的详细信息。

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
```

IPv6 Virtual Router Information:

Running Mode : Load Balance

```

Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 100
  Admin Status  : Up                     State          : Backup
  Config Pri    : 100                    Running Pri    : 100
  Preempt Mode  : Yes                     Delay Time     : 5000
  Become Master : 400ms left
  Auth Type     : None
  Virtual IP    : FE80::10
                  1::10
  Member IP List : FE80::3 (Local, Backup)
                  FE80::1 (Master)
                  FE80::2 (Backup)
Forwarder Information: 2 Forwarders 1 Active
  Config Weight : 255
  Running Weight : 255
Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-4012 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority        : 127
  Active         : FE80::2
Forwarder 03
  State          : Active
  Virtual MAC    : 000f-e2ff-4013 (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, Timeout Timer 超时后, 删除虚拟 MAC 地址 000f-e2ff-4011 对应的虚拟转发器, 不再转发目的 MAC 地址为该 MAC 的报文。

Switch A 出现故障后, 通过 **display vrrp ipv6 verbose** 命令查看 Switch B 上备份组的详细信息。

```

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode      : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 100
  Admin Status  : Up                     State          : Master
  Config Pri    : 110                    Running Pri    : 110
  Preempt Mode  : Yes                     Delay Time     : 5000
  Auth Type     : None
  Virtual IP    : FE80::10
                  1::10
  Member IP List : FE80::2 (Local, Master)
                  FE80::3 (Backup)

```

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 02

State : Active

Virtual MAC : 000f-e2ff-4012 (Owner)

Owner ID : 0000-5e01-1103

Priority : 255

Active : local

Forwarder 03

State : Listening

Virtual MAC : 000f-e2ff-4013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 127

Active : FE80::3

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

以上显示信息表示 Switch A 出现故障后，Switch B 的优先级高于 Switch C，将抢占成为 Master，同时删除了虚拟 MAC 地址 000f-e2ff-4011 对应的虚拟转发器。

1.10 VRRP常见故障处理

1.10.1 出现配置错误的提示

1. 故障现象

在配置过程中出现配置错误的提示，提示内容如下："The virtual router detected a VRRP configuration error."

2. 故障分析

- 可能是备份组内的设备配置不一致造成的，具体包括以下几种情况：
 - 备份组运行的是 VRRPv2 版本时，报文携带的通告报文发送间隔与当前备份组不一致，VRRPv3 版本不受此限制。
 - 报文携带的虚拟 IP 地址个数与当前备份组不一致。
 - 报文携带的虚拟 IP 地址列表与当前备份组不一致。
- 可能是备份组内的设备收到攻击者发送的非法 VRRP 报文，如 IP 地址拥有者收到优先级为 255 的 VRRP 报文。

3. 故障处理

- 对于第一种情况，可以通过修改配置来解决。
- 对于第二种情况，则是有些攻击者有不良企图，应当通过定位和防止攻击来解决。

1.10.2 同一个备份组内出现多个Master路由器

1. 故障现象

同一个备份组内出现多台 Master 路由器。

2. 故障分析

- 若短时间内存在多台 Master 路由器，属于正常情况，无需进行人工干预。
- 若多台 Master 路由器长时间共存，这很有可能是由于 Master 路由器之间收不到 VRRP 报文，或者收到的报文不合法造成的。

3. 故障处理

先在多台 Master 路由器之间执行 ping 操作。如果 ping 不通，则检查网络连接是否正确；如果能 ping 通，则检查 VRRP 的配置是否一致。对于同一个 VRRP 备份组的配置，必须要保证虚拟 IP 地址个数、每个虚拟 IP 地址和认证方式完全一样。如果使用的是 IPv4 VRRP，还需保证 IPv4 VRRP 使用的版本一致。如果是 VRRPv2 版本，还要求 VRRP 通告发送间隔一致。

1.10.3 VRRP的状态频繁转换

1. 故障现象

在运行过程中 VRRP 的状态频繁转换。

2. 故障分析

这种情况一般是由于 VRRP 通告报文发送间隔太短造成的。

3. 故障处理

增加通告报文的发送间隔或者设置抢占延迟都可以解决这种故障。

目 录

1 BFD.....	1-1
1.1 BFD简介.....	1-1
1.1.1 BFD会话的建立与拆除	1-1
1.1.2 单跳检测和多跳检测	1-1
1.1.3 BFD会话的工作方式和检测模式	1-1
1.1.4 BFD支持的应用	1-2
1.1.5 协议规范	1-2
1.2 BFD配置限制和指导.....	1-3
1.3 echo报文方式配置	1-3
1.4 控制报文方式配置.....	1-3
1.4.1 配置限制和指导	1-3
1.4.2 配置单跳检测	1-4
1.4.3 配置多跳检测	1-5
1.5 配置BFD模板.....	1-5
1.6 开启告警功能.....	1-6
1.7 BFD显示和维护.....	1-6

1 BFD

1.1 BFD简介

BFD（Bidirectional Forwarding Detection，双向转发检测）是一个通用的、标准化的、介质无关和协议无关的快速故障检测机制，用于检测 IP 网络中链路的连通状况，保证设备之间能够快速检测到通信故障，以便能够及时采取措施，保证业务持续运行。BFD 可以为各种上层协议（如路由协议）快速检测两台设备间双向转发路径的故障。上层协议通常采用 Hello 报文机制检测故障，所需时间为秒级，而 BFD 可以提供毫秒级检测。

1.1.1 BFD会话的建立与拆除

BFD 本身并没有发现机制，而是靠被服务的上层协议通知来建立会话。上层协议在建立新的邻居关系后，将邻居的参数及检测参数（包括目的地址和源地址等）通告给 BFD；BFD 根据收到的参数建立 BFD 会话。

当网络出现故障时：

- (1) BFD 检测到链路故障后，拆除 BFD 会话，通知上层协议邻居不可达；
- (2) 上层协议中止邻居关系；
- (3) 如果网络中存在备用路径，设备将选择备用路径进行通信。

1.1.2 单跳检测和多跳检测

BFD 可以用来进行单跳和多跳检测：

- 单跳检测：是指对两个直连设备进行 IP 连通性检测，这里所说的“单跳”是 IP 的一跳。
- 多跳检测：BFD 可以检测两个设备间任意路径的链路情况，这些路径可能跨越很多跳。

1.1.3 BFD会话的工作方式和检测模式

BFD 会话通过 echo 报文和控制报文实现。

1. echo报文方式

echo 报文封装在 UDP 报文中传送，其 UDP 目的端口号为 3785。

本端发送 echo 报文建立 BFD 会话，对链路进行检测。对端不建立 BFD 会话，只需把收到的 echo 报文转发回本端。如果在检测时间内没有收到对端转发回的 echo 报文，则认为会话 down。

当 BFD 会话工作于 echo 报文方式时，仅支持单跳检测，并且不受检测模式的控制。

2. 控制报文方式

控制报文封装在 UDP 报文中传送，对于单跳检测其 UDP 目的端口号为 3784，对于多跳检测其 UDP 目的端口号为 4784。

链路两端通过周期性发送控制报文建立 BFD 会话，对链路进行检测。

BFD 会话建立前有两种模式：主动模式和被动模式。

- 主动模式：在建立会话前不管是否收到对端发来的 BFD 控制报文，都会主动发送 BFD 控制报文；
 - 被动模式：在建立会话前不会主动发送 BFD 控制报文，直到收到对端发送来的控制报文。
- 通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。

BFD 会话建立后有两种模式：异步模式和查询模式。

- 异步模式：设备周期性发送 BFD 控制报文，如果在检测时间内没有收到对端发送的 BFD 控制报文，则认为会话 down。
- 查询模式：设备周期性发送 BFD 控制报文，但是对端（缺省为异步模式）会停止周期性发送 BFD 控制报文。如果通信双方都是查询模式，则双方都停止周期性发送 BFD 控制报文。当需要验证连接性的时候，设备会以协商的周期连续发送几个 P 比特位置 1 的 BFD 控制报文。如果在检测时间内没有收到返回的报文，就认为会话 down；如果收到对方回应的 F 比特位置 1 的报文，就认为连通，停止发送报文，等待下一次触发查询。

1.1.4 BFD支持的应用

表1-1 BFD 支持的应用

应用	参见信息
静态路由 OSPF RIP IP快速重路由	“三层技术-IP路由配置指导” S5110V2-SI、S5000V3-EI和S5000E-X系列交换机不支持OSPF S5000V3-EI和S5000E-X系列以太网交换机不支持RIP
IPv6静态路由 OSPFv3	“三层技术-IP路由配置指导” S5110V2-SI、S5000V3-EI和S5000E-X系列交换机不支持OSPFv3
PIM	“IP组播配置指导”
Track	“可靠性配置指导”
以太网链路聚合	“二层技术-以太网交换配置指导”

1.1.5 协议规范

与 BFD 相关的协议规范有：

- RFC 5880: Bidirectional Forwarding Detection (BFD)
- RFC 5881: Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)
- RFC 5882: Generic Application of Bidirectional Forwarding Detection (BFD)
- RFC 5883: Bidirectional Forwarding Detection (BFD) for Multihop Paths
- RFC 7130: Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces

1.2 BFD配置限制和指导

缺省 BFD 运行版本 1，同时兼容版本 0。不能通过命令行配置修改为版本 0，当对端设备运行版本 0 会话时，本端会自动切换到版本 0。

BFD 会话建立后，可以动态协商 BFD 的相关参数（例如最小发送间隔、最小接收间隔、初始模式、报文认证等），两端协议通过发送相应的协商报文后采用新的参数，不影响会话的当前状态。

对于建立在跨成员设备的聚合接口上的 BFD 会话，当负责收发 BFD 报文的主设备异常重启时，从设备接替收发 BFD 报文的工作需要一定的时间，如果 BFD 会话检测时间较短或者会话数量较多，可能会出现 BFD 会话震荡的情况。

1.3 echo报文方式配置

1. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 echo 报文源 IP 地址。请至少选择以下一项进行配置。

- 配置 echo 报文源 IPv4 地址。

```
bfd echo-source-ip ip-address
```

缺省情况下，未配置 echo 报文的源 IPv4 地址。

为了避免对端发送大量的 ICMP 重定向报文造成网络拥塞，建议不要将 echo 报文的源 IPv4 地址配置为属于该设备任何一个接口所在网段。

- 配置 echo 报文源 IPv6 地址。

```
bfd echo-source-ipv6 ipv6-address
```

缺省情况下，未配置 echo 报文的源 IPv6 地址。

echo 报文源 IPv6 地址仅支持全球单播地址。

- (3) （可选）配置 echo 报文方式的 BFD 参数。

- a. 进入接口视图。

```
interface interface-type interface-number
```

- b. 配置接收 echo 报文的最小时间间隔。

```
bfd min-echo-receive-interval interval
```

接收 echo 报文的最小时间间隔为 400 毫秒。

- c. 配置 BFD 检测时间倍数。

```
bfd detect-multiplier interval
```

缺省情况下，BFD 检测时间倍数为 5。

1.4 控制报文方式配置

1.4.1 配置限制和指导

配置被服务的上层协议支持 BFD 功能后，无需执行本配置，设备上会自动创建控制报文方式的 BFD 会话。

BFD 版本 0 不支持以下命令，配置不生效。

- **bfd session init-mode**
- **bfd authentication-mode**
- **bfd demand enable**
- **bfd echo enable**

1.4.2 配置单跳检测

- (1) 进入系统视图。

system-view

- (2) 配置 BFD 会话建立前的运行模式。

bfd session init-mode { active | passive }

缺省情况下，BFD 会话建立前的运行模式为主动模式。

- (3) 进入接口视图。

interface interface-type interface-number

- (4) （可选）配置单跳 BFD 控制报文进行认证的方式。

**bfd authentication-mode { m-md5 | m-sha1 | md5 | sha1 | simple } key-id
{ cipher cipher-string | plain plain-string }**

缺省情况下，单跳 BFD 控制报文不进行认证。

- (5) 配置 BFD 会话为查询模式。

bfd demand enable

缺省情况下，BFD 会话为异步模式。

- (6) （可选）使能 echo 功能。

bfd echo [receive | send] enable

缺省情况下，echo 功能处于关闭状态。

使能 echo 功能并且会话 up 后，设备周期性发送 echo 报文检测链路连通性，同时降低控制报文的接收速率。

- (7) 配置发送单跳 BFD 控制报文的最小时间间隔。

bfd min-transmit-interval interval

发送单跳 BFD 控制报文的最小时间间隔为 400 毫秒。

- (8) 配置接收单跳 BFD 控制报文的最小时间间隔。

bfd min-receive-interval interval

接收单跳 BFD 控制报文的最小时间间隔为 400 毫秒。

- (9) 配置单跳检测的 BFD 检测时间倍数。

bfd detect-multiplier interval

缺省情况下，单跳检测的 BFD 检测时间倍数为 5。

- (10) （可选）创建一个检测本接口状态的 BFD 会话。

**bfd detect-interface source-ip ip-address [discriminator local
local-value remote remote-value]**

缺省情况下，不存在检测本接口状态的 BFD 会话。

本功能实现了接口状态与 BFD 会话状态的快速联动。当检测到链路故障时，将接口链路层协议状态置为“DOWN(BFD)”，从而帮助依赖接口链路层协议状态的应用快速收敛。

1.4.3 配置多跳检测

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 BFD 会话建立前的运行模式。

```
bfd session init-mode { active | passive }
```

缺省情况下，BFD 会话建立前的运行模式为主动模式。

- (3) （可选）配置多跳 BFD 控制报文进行认证的方式。

```
bfd multi-hop authentication-mode { m-md5 | m-sha1 | md5 | sha1 | simple }  
key-id { cipher cipher-string | plain plain-string }
```

缺省情况下，多跳 BFD 控制报文不进行认证。

- (4) 配置多跳 BFD 控制报文的端口号。

```
bfd multi-hop destination-port port-number
```

缺省情况下，多跳 BFD 控制报文的端口号为 4784。

- (5) 配置多跳检测的 BFD 检测时间倍数。

```
bfd multi-hop detect-multiplier value
```

缺省情况下，多跳检测的 BFD 检测时间倍数为 5。

- (6) 配置接收多跳 BFD 控制报文的最小时间间隔。

```
bfd multi-hop min-receive-interval interval
```

接收多跳 BFD 控制报文的最小时间间隔为 400 毫秒。

- (7) 配置发送多跳 BFD 控制报文的最小时间间隔。

```
bfd multi-hop min-transmit-interval interval
```

发送多跳 BFD 控制报文的最小时间间隔为 400 毫秒。

1.5 配置BFD模板

1. 功能简介

对于未指定出接口的会话，无法通过会话出接口配置 BFD 会话参数。使用 BFD 全局多跳可以配置，但是缺乏灵活性。通过 BFD 模板可以对参数进行灵活配置，LSP 以及 PW 的 BFD 检测关联到 BFD 模板即可指定会话参数。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 BFD 模板，并进入 BFD 模板视图。

```
bfd template template-name
```

- (3) （可选）配置 BFD 控制报文进行认证的方式。

```
bfd authentication-mode { m-md5 | m-sha1 | md5 | sha1 | simple } key-id  
{ cipher cipher-string | plain plain-string }
```

缺省情况下，BFD 控制报文不进行认证。

BFD 版本 0 不支持本命令，配置不生效。

- (4) 配置 BFD 检测时间倍数。

```
bfd detect-multiplier value
```

缺省情况下，BFD 检测时间倍数为 5。

- (5) 配置接收 BFD 控制报文的最小时间间隔。

```
bfd min-receive-interval interval
```

接收单跳 BFD 控制报文的最小时间间隔为 400 毫秒。

- (6) 配置发送 BFD 控制报文的最小时间间隔。

```
bfd min-transmit-interval interval
```

发送单跳 BFD 控制报文的最小时间间隔为 400 毫秒。

1.6 开启告警功能

1. 功能简介

开启 BFD 模块的告警功能后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。（有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。）

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 BFD 的告警功能。

```
snmp-agent trap enable bfd
```

缺省情况下，BFD 的告警功能处于开启状态。

1.7 BFD显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 BFD 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 BFD 会话的统计信息。

表1-2 BFD 显示和维护

操作	命令
显示BFD会话信息	display bfd session [discriminator value verbose]
清除BFD会话统计信息	reset bfd session statistics

目 录

1 Track	1-1
1.1 Track简介	1-1
1.1.1 联动功能实现机制	1-1
1.1.2 与Track模块实现联动功能的监测模块	1-2
1.1.3 与Track模块实现联动功能的应用模块	1-2
1.2 Track配置限制和指导	1-2
1.3 联动功能应用举例	1-2
1.4 Track配置任务简介	1-3
1.5 配置Track与监测模块联动	1-3
1.5.1 配置Track与NQA联动	1-3
1.5.2 配置Track与BFD联动	1-4
1.5.3 配置Track与CFD联动	1-4
1.5.4 配置Track与接口管理联动	1-5
1.5.5 配置Track与路由管理联动	1-5
1.5.6 配置Track与LLDP联动	1-6
1.6 配置Track与应用模块联动	1-6
1.6.1 Track与应用模块联动配置准备	1-6
1.6.2 配置Track与VRRP联动	1-6
1.6.3 配置Track与静态路由联动	1-7
1.6.4 配置Track与策略路由联动	1-8
1.6.5 配置Track与Smart Link联动	1-10
1.6.6 配置Track与EAA联动	1-11
1.6.7 配置Track与ERPS联动	1-11
1.7 Track显示和维护	1-12
1.8 Track典型配置举例	1-12
1.8.1 VRRP、Track与NQA联动配置举例（Master监视上行链路）	1-12
1.8.2 VRRP、Track与BFD联动配置举例（Backup监视Master）	1-16
1.8.3 VRRP、Track与BFD联动配置举例（Master监视上行链路）	1-19
1.8.4 静态路由、Track与NQA联动配置举例	1-22
1.8.5 静态路由、Track与BFD联动配置举例	1-27
1.8.6 VRRP、Track与接口管理联动配置举例（Master监视上行接口）	1-30
1.8.7 静态路由、Track与LLDP联动配置举例	1-33
1.8.8 Smart Link、Track和CFD联动配置举例	1-37

1 Track

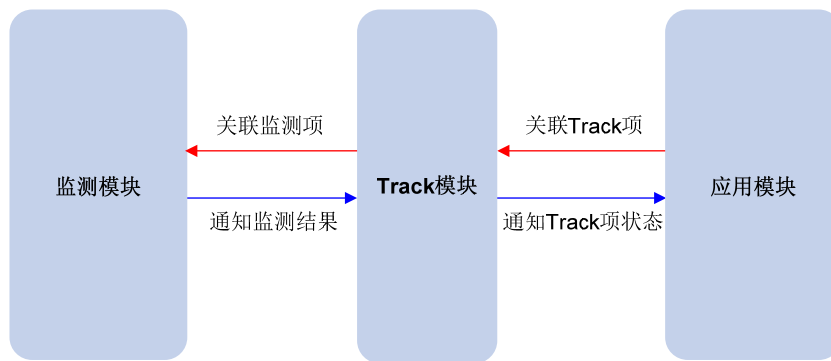
1.1 Track简介

Track 用于在监测模块、Track 模块和应用模块之间建立关联，来实现这些模块之间的联合动作。联动功能在应用模块和监测模块之间增加了 Track 模块，通过 Track 模块屏蔽不同监测模块的差异，将监测结果以统一的形式通知给应用模块，从而简化应用模块的处理。

1.1.1 联动功能实现机制

如 图 1-1 所示，联动功能利用监测模块对链路状态、网络性能等进行监测，并通过Track模块将监测结果及时通知给应用模块，以便应用模块进行相应的处理。例如，在NQA、Track和静态路由之间建立联动，利用NQA监测静态路由的下一跳地址是否可达。NQA监测到下一跳不可达时，通过Track通知静态路由模块该监测结果，以便静态路由模块将该条路由置为无效，确保报文不再通过该静态路由转发。

图1-1 联动功能实现示意图



1. Track模块与监测模块联动

Track 模块通过 Track 项与监测模块建立关联。Track 项定义了 Positive、Negative 和 NotReady 三种状态。监测模块负责对接口状态、链路状态等进行监测，并将监测结果通知给 Track 模块；Track 模块根据监测结果改变 Track 项的状态。

- 如果监测结果为监测对象工作正常（如接口处于 up 状态、网络可达），则对应 Track 项的状态为 Positive。
- 如果监测结果为监测对象出现异常（如接口处于 down 状态、网络不可达），则对应 Track 项的状态为 Negative。
- 如果监测结果无效（如 NQA 作为监测模块时，与 Track 项关联的 NQA 测试组不存在），则对应 Track 项的状态为 NotReady。

2. Track模块与应用模块联动

应用模块通过引用 Track 项与 Track 模块建立关联。Track 项的状态改变后，通知应用模块；应用模块根据 Track 项的状态，及时进行相应的处理，从而避免通信的中断或服务质量的降低。

1.1.2 与Track模块实现联动功能的监测模块

目前，可以与 Track 模块实现联动功能的监测模块包括：

- NQA（Network Quality Analyzer，网络质量分析）
- BFD（Bidirectional Forwarding Detection，双向转发检测）
- CFD（Connectivity Fault Detection，连通错误检测）
- 接口管理
- 路由管理
- LLDP（Link Layer Discovery Protocol，链路层发现协议）

1.1.3 与Track模块实现联动功能的应用模块

目前，可以与 Track 模块实现联动功能的应用模块包括：

- VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）
- 静态路由
- 策略路由
- Smart Link
- EAA
- ERPS

1.2 Track配置限制和指导

在某些情况下，Track 项状态发生变化后，如果立即通知应用模块，则可能会由于路由无法及时恢复等原因，导致通信中断。例如，VRRP 备份组中 Master 路由器通过 Track 监视上行接口的状态。上行接口出现故障时，Track 通知 Master 路由器降低优先级，使得 Backup 路由器抢占成为新的 Master，负责转发报文。当上行接口恢复时，如果 Track 立即通知原来的 Master 路由器恢复优先级，该路由器将立即承担转发任务。此时该路由器可能尚未恢复上行的路由，从而导致报文转发失败。在这种情况下，用户可以配置 Track 项状态发生变化时，延迟一定的时间通知应用模块。

1.3 联动功能应用举例

下面以 NQA、Track 和静态路由联动为例，说明联动功能的工作原理。

用户在设备上配置了一条静态路由，下一跳地址为 192.168.0.88。如果 192.168.0.88 可达，则报文可以通过该静态路由转发，该静态路由有效；如果 192.168.0.88 不可达，则通过该静态路由转发报文会导致报文转发失败，此时，需要将该静态路由置为无效。通过在 NQA、Track 模块和静态路由之间建立联动，可以实现实时监测下一跳的可达性，以便及时判断静态路由是否有效。

在此例中联动功能的配置方法及其工作原理为：

- (1) 创建 NQA 测试组，通过 NQA 测试组监测目的地址 192.168.0.88 是否可达。
- (2) 创建和 NQA 测试组关联的 Track 项。192.168.0.88 可达时，NQA 会将监测结果通知给 Track 模块，Track 模块将该 Track 项的状态变为 Positive；192.168.0.88 不可达时，NQA 将监测结果通知给 Track 模块，Track 模块将该 Track 项的状态变为 Negative。

- (3) 配置这条静态路由和 Track 项关联。如果 Track 模块通知静态路由 Track 项的状态为 Positive，则静态路由模块将这条路由置为有效；如果 Track 模块通知静态路由 Track 项的状态为 Negative，则静态路由模块将这条路由置为无效。

1.4 Track配置任务简介

为了实现联动功能，需要在 Track 与监测模块、Track 与应用模块之间分别建立联动关系。Track 配置任务如下：

- (1) 配置 Track 与监控模块联动。
- [配置Track与NQA联动](#)
 - [配置Track与BFD联动](#)
 - [配置Track与CFD联动](#)
 - [配置Track与接口管理联动](#)
 - [配置Track与路由管理联动](#)
 - [配置Track与LLDP联动](#)
- (2) 配置 Track 与应用模块联动。
- [配置Track与VRRP联动](#)
 - [配置Track与静态路由联动](#)
 - [配置Track与策略路由联动](#)
 - [配置Track与Smart Link联动](#)
 - [配置Track与EAA联动](#)
 - [配置Track与ERPS联动](#)

1.5 配置Track与监测模块联动

1.5.1 配置Track与NQA联动

1. 功能简介

NQA 测试组周期性地探测某个目的地址是否可达、是否可以与某个目的服务器建立 TCP 连接等。如果在 Track 项和 NQA 测试组之间建立了关联，则当连续探测失败的次数达到指定的阈值时，NQA 将通知 Track 模块监测对象出现异常，Track 模块将与 NQA 测试组关联的 Track 项的状态置为 Negative；否则，NQA 通知 Track 模块监测对象正常工作，Track 模块将 Track 项的状态置为 Positive。NQA 的详细介绍，请参见“网络管理和监控配置指导”中的“NQA”。

2. 配置限制和指导

配置 Track 项时，引用的 NQA 测试组或联动项可以不存在，此时该 Track 项的状态为 NotReady。

3. 配置步骤

- (1) 进入系统视图。
- system-view**
- (2) 创建与 NQA 测试组中指定联动项关联的 Track 项，并指定 Track 项状态变化时通知应用模块的延迟时间。

```
track track-entry-number nqa entry admin-name operation-tag reaction
item-number [ delay { negative negative-time | positive positive-time }
* ]
```

1.5.2 配置Track与BFD联动

1. 功能简介

如果在 Track 项和 BFD 会话之间建立了关联，则当 BFD 判断出对端不可达时，BFD 会通知 Track 模块将与 BFD 会话关联的 Track 项的状态置为 Negative；否则，通知 Track 模块将 Track 项的状态置为 Positive。

BFD 会话支持两种工作方式：Echo 报文方式和控制报文方式。Track 项只能与 Echo 报文方式的 BFD 会话建立关联，不能与控制报文方式的 BFD 会话建立联动。BFD 的详细介绍，请参见“可靠性配置指导”中的“BFD”。

2. 配置限制和指导

配置 Track 与 BFD 联动时，VRRP 备份组的虚拟 IP 地址不能作为 BFD 会话探测的本地地址和远端地址。

3. 配置准备

配置 Track 与 BFD 联动前，需要配置 BFD echo 报文的源地址，配置方法请参见“可靠性配置指导”中的“BFD”。

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建和 BFD 会话关联的 Track 项，并指定 Track 项状态变化时通知应用模块的延迟时间。

```
track track-entry-number bfd echo interface interface-type
interface-number remote ip remote-ip-address local ip local-ip-address
[ delay { negative negative-time | positive positive-time } * ]
```

1.5.3 配置Track与CFD联动

1. 功能简介

如果在 Track 项和 CFD 连续性检测功能之间建立了关联，则当 CFD 判断出对端不可达时，CFD 会通知 Track 模块将与 CFD 连续性检测功能关联的 Track 项的状态置为 Negative；否则，通知 Track 模块将 Track 项的状态置为 Positive。CFD 的详细介绍，请参见“可靠性配置指导”中的“CFD”。

2. 配置准备

配置 Track 与 CFD 连续性检测功能联动前，需要开启 CFD 服务并创建 MEP，配置方法请参见“可靠性配置指导”中的“CFD”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建和会话关联的 Track 项，并指定 Track 项状态变化时通知应用模块的延迟时间。

```
track track-entry-number cfd cc service-instance instance-id mep
mep-id [ delay { negative negative-time | positive positive-time } * ]
```

1.5.4 配置Track与接口管理联动

1. 功能简介

接口管理用来监视接口的链路状态和网络层协议状态。如果在 Track 项和接口之间建立了关联，则当接口的链路状态或网络层协议状态为 up 时，接口管理通知 Track 模块将与接口关联的 Track 项的状态置为 Positive；接口的链路状态或网络层协议状态为 down 时，接口管理通知 Track 模块将 Track 项的状态为 Negative。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建和接口管理关联的 Track 项。请至少选择其中一项进行配置。

- 监视接口的链路状态，并指定 Track 项状态变化时通知应用模块的延迟时间。

```
track track-entry-number interface interface-type interface-number
[ delay { negative negative-time | positive positive-time } * ]
```

- 监视接口的物理状态，并指定 Track 项状态变化时通知应用模块的延迟时间。

```
track track-entry-number interface interface-type interface-number
physical [ delay { negative negative-time | positive positive-time }
* ]
```

- 监视接口的网络层协议状态，并指定 Track 项状态变化时通知应用模块的延迟时间。

```
track track-entry-number interface interface-type interface-number
protocol { ipv4 | ipv6 } [ delay { negative negative-time | positive
positive-time } * ]
```

1.5.5 配置Track与路由管理联动

1. 功能简介

如果在 Track 项和路由管理之间建立了关联，当对应的路由条目在路由表中存在时，路由管理通知 Track 模块将与之关联的 Track 项状态设置为 Positive；当对应的路由条目在路由表中被删除时，路由管理将通知 Track 模块将与之关联的 Track 项状态设置为 Negative。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建与路由管理关联的 Track 项，并指定 Track 项状态变化时通知应用模块的延迟时间。

```
track track-entry-number ip route ip-address { mask-length | mask }
reachability [ delay { negative negative-time | positive positive-time }
* ]
```

1.5.6 配置Track与LLDP联动

1. 功能简介

如果在 Track 项和接口的 LLDP 邻居之间建立了关联，当接口下存在 LLDP 邻居时，Track 项的状态为 Positive；接口下不存在 LLDP 邻居时，Track 项的状态为 Negative。LLDP 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“LLDP”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建与接口的 LLDP 邻居状态关联的 Track 项，并指定 Track 项状态变化时通知应用模块的延迟时间。

```
track track-entry-number lldp neighbor interface interface-type  
interface-number [ delay { negative negative-time | positive  
positive-time } * ]
```

1.6 配置Track与应用模块联动

1.6.1 Track与应用模块联动配置准备

用户配置 Track 和应用模块联动时，需保证联动的 Track 项已被创建，否则应用模块可能会获取到错误的 Track 项状态信息。

1.6.2 配置Track与VRRP联动

1. 功能简介

VRRP 工作在标准协议模式和负载均衡模式时，通过在 Track 模块和 VRRP 备份组之间建立联动，可以实现：

- 根据上行链路的状态，改变路由器的优先级。当路由器的上行链路出现故障时，备份组无法感知上行链路的故障，如果该路由器为 Master，将会导致局域网内的主机无法访问外部网络。通过联动功能，可以解决该问题。利用监测模块监视路由器上行链路的状态，并在监测模块、Track 模块和 VRRP 备份组之间建立联动，当上行链路出现故障时，通知将 Track 项状态变为 Negative，并将路由器的优先级降低指定的数额。从而，使得备份组内其它路由器的优先级高于这个路由器的优先级，成为 Master 路由器，保证局域网内主机与外部网络的通信不会中断。
- 在 Backup 路由器上监视 Master 路由器的状态。当 Master 路由器出现故障时，工作在切换模式的 Backup 路由器能够迅速成为 Master 路由器，以保证通信不会中断。

VRRP 工作在负载均衡模式时，通过在 Track 模块和 VRRP 虚拟转发器之间建立联动，还可以实现：

- 根据上行链路的状态，改变虚拟转发器的优先级。当 AVF（Active Virtual Forwarder，动态虚拟转发器）的上行链路出现故障时，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。
- 在 LVF（Listening Virtual Forwarder，监听虚拟转发器）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。

VRRP 配置的详细介绍，请参见“可靠性配置指导”中的“VRRP”。

2. 配置限制和指导

接口 IP 地址与虚拟 IP 地址相同的路由器称为 IP 地址拥有者。路由器在某个备份组中作为 IP 地址拥有者时，如果在该路由器上配置该备份组监视指定的接口或 Track 项，则该配置不会生效。该路由器不再作为 IP 地址拥有者后，之前的配置才会生效。

被监视 Track 项的状态由 **Negative** 变为 **Positive** 或 **NotReady** 后，对应的路由器优先级或虚拟转发器优先级会自动恢复。

3. 配置Track与VRRP备份组联动

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 VRRP 备份组监视指定的 Track 项。

```
vrrp [ ipv6 ] vrid virtual-router-id track track-entry-number  
{ forwarder-switchover member-ip ip-address | priority reduced  
[ priority-reduced ] switchover | weight reduced [ weight-reduced ] }
```

缺省情况下，未指定 VRRP 备份组监视的 Track 项。

VRRP 工作在标准协议模式和负载均衡模式时，均支持本配置。

4. 配置Track与VRRP虚拟转发器联动

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置虚拟转发器监视指定的 Track 项。

```
vrrp [ ipv6 ] vrid virtual-router-id track track-entry-number  
{ forwarder-switchover member-ip ip-address | priority reduced  
[ priority-reduced ] switchover | weight reduced [ weight-reduced ] }
```

缺省情况下，未配置虚拟转发器的监视功能。

在 VRRP 标准协议模式和负载均衡模式下均可进行本配置，但只有在 VRRP 负载模式下本配置才会起作用。

1.6.3 配置Track与静态路由联动

1. 功能简介

静态路由是一种特殊的路由，由管理员手工配置。配置静态路由后，去往指定目的地的报文将按照管理员指定的路径进行转发。静态路由配置的详细介绍，请参见“三层技术-IP 路由配置指导”中的“静态路由”。

静态路由的缺点在于：不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化时，可能会导致静态路由不可达，网络通信中断。

为了防止这种情况发生，可以配置其它路由和静态路由形成备份关系。静态路由可达时，根据静态路由转发报文，其它路由处于备份状态；静态路由不可达时，根据备份路由转发报文，从而避免通信中断，提高了网络可靠性。

通过在 **Track** 模块和静态路由之间建立联动，可以实现静态路由可达性的实时判断。

如果在配置静态路由时只指定了下一跳而未指定出接口，可以通过联动功能，利用监测模块监视静态路由下一跳的可达性，并根据 **Track** 项的状态来判断静态路由的可达性：

- 当 **Track** 项状态为 **Positive** 时，静态路由的下一跳可达，配置的静态路由将生效；
- 当 **Track** 项状态为 **Negative** 时，静态路由的下一跳不可达，配置的静态路由无效；
- 当 **Track** 项状态为 **NotReady** 时，无法判断静态路由的下一跳是否可达，此时配置的静态路由生效。

2. 配置限制和指导

在静态路由进行迭代时，**Track** 项监测的应该是静态路由迭代后最终的下一跳地址，而不是配置中指定的下一跳地址。否则，可能导致错误地将有效路由判断为无效路由。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置通过 **Track** 与静态路由联动，检测静态路由下一跳是否可达。

```
ip route-static { dest-address { mask-length | mask } | group group-name }  
{ interface-type interface-number [ next-hop-address ]  
[ backup-interface interface-type interface-number [ backup-nexthop  
backup-nexthop-address ] [ permanent ] | bfd { control-packet |  
echo-packet } | permanent | track track-entry-number ] |  
next-hop-address [ recursive-lookup host-route ] [ bfd control-packet  
bfd-source ip-address | permanent | track track-entry-number ] }  
[ preference preference ] [ tag tag-value ] [ description text ]
```

缺省情况下，未配置 **Track** 与静态路由联动。

1.6.4 配置Track与策略路由联动

1. 功能简介

策略路由是一种依据用户指定的策略灵活选路的机制，满足策略的报文将执行指定的操作，以指导报文转发。策略路由配置的详细介绍，请参见“三层技术-IP 路由配置指导”中的“策略路由”。

策略路由无法判断对报文执行的操作的可用性。当执行的操作不可用时，策略路由仍然对报文执行该操作，可能会导致报文转发失败。例如，策略路由中配置满足一定条件的报文，需要通过指定的出接口转发。当该出接口所在的链路出现故障时，策略路由无法感知链路故障，仍然通过该接口转发报文，导致报文转发失败。

通过联动功能，可以解决上述问题，增强了策略路由应用的灵活性，以及策略路由对网络环境的动态感知能力。配置策略路由执行的操作与 **Track** 项关联，利用监测模块监视链路的状态，通过 **Track** 项的状态来动态地决定策略路由操作的可用性：

- Track 项状态为 **Positive** 时，表示链路正常工作，与该 Track 项关联的策略路由操作生效，可以指导转发；
- Track 项状态为 **Negative** 时，表示链路出现故障，与该 Track 项关联的策略路由操作无效，转发时忽略该配置项；
- Track 项状态为 **NotReady** 时，与该 Track 项关联的策略路由操作生效，可以指导转发。

目前，支持与 Track 项关联的策略路由操作包括：

- 设置报文的下一跳

2. 配置准备

配置 Track 与策略路由联动前，需要先创建策略或一个策略节点，并配置匹配规则。

3. 配置Track与IPv4 策略路由联动

- (1) 进入系统视图。

```
system-view
```

- (2) 创建策略或一个策略节点，并进入该策略视图。

```
policy-based-route policy-name [ deny | permit ] node node-number
```

- (3) 设置匹配规则。

- 设置 ACL 匹配规则。

```
if-match acl { acl-number | name acl-name }
```

缺省情况下，未设置 ACL 匹配规则。

策略路由不支持匹配二层信息的 ACL 匹配规则。

设置 ACL 匹配规则时，对于 ACL 规则的 **permit/deny** 动作以及 **time-range** 指定的规则生效时间段等的处理机制不再生效。

- (4) 配置指导报文转发类动作。请至少选择其中一项进行配置。

- 设置报文的下一跳，并与 Track 项关联。

```
apply next-hop { ip-address [ direct ] [ track  
track-entry-number ] }<1-n>
```

缺省情况下，未设置报文转发的下一跳。

4. 配置Track与IPv6 策略路由联动

- (1) 进入系统视图。

```
system-view
```

- (2) 创建策略或一个策略节点，并进入该策略视图。

```
ipv6 policy-based-route policy-name [ deny | permit ] node node-number
```

- (3) 设置匹配规则。

- 设置 ACL 匹配规则。

```
if-match acl { ipv6-acl-number | name ipv6-acl-name }
```

缺省情况下，未设置 ACL 匹配规则。

IPv6 策略路由不支持匹配二层信息的 ACL 匹配规则。

设置 ACL 匹配规则时，对于 ACL 规则的 **permit/deny** 动作以及 **time-range** 指定的规则生效时间段等的处理机制不再生效。

(4) 配置指导报文转发类动作。请至少选择其中一项进行配置。

- 设置报文的下一跳，并与 Track 项关联。

```
apply next-hop { ipv6-address [ direct ] [ track track-entry-number ] }  
&<1-n>
```

缺省情况下，未设置报文转发的下一跳。

1.6.5 配置Track与Smart Link联动

1. 功能简介

上行链路上的中间传输设备或传输链路发生故障（如光纤链路发生单通、错纤、丢包等故障）以及故障排除时，Smart Link 本身无法感知到这个变化。Smart Link 组的成员端口需要通过 Track 项与专门的链路检测协议联动来检测端口的链路状态，当链路检测协议检测到故障发生或故障恢复时就通知 Smart Link 进行链路切换。

用户可以配置 Smart Link 组的成员端口与 Track 项关联，使该端口通过 Track 项与 CFD 的连续性检测功能进行联动来监测该端口的上行链路状态。

Track 模块根据监测模块的监测结果改变 Track 项的状态，并将 Track 项状态通知给 Smart Link 组；Smart Link 组根据 Track 项状态进行相应处理：

- 如果 Track 项的状态为 **Positive**，说明该端口的上行链路正常，Smart Link 组不进行链路切换；
- 如果 Track 项的状态为 **Negative**，说明该端口的上行链路出现故障，Smart Link 组根据抢占模式和该端口的成员角色判断是否需要链路切换；
- 如果 Track 项的状态为 **NotReady**，说明 Track 关联监测模块的配置尚未生效，该端口维持原有转发状态不变。

关于 Smart Link 的详细介绍，请参见“可靠性配置指导”中的“Smart Link”。

2. 配置限制和指导

Smart Link 组的成员端口联动的 Track 项，必须是和 CFD 连续性检测功能关联的 Track 项。S5110V2-SI、S5000V3-EI 和 S5000E-X 系列交换机暂不支持本特性。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入二层以太网或二层聚合接口视图。

```
interface interface-type interface-number
```

(3) 配置 Smart Link 组的成员端口与 Track 项联动。

```
port smart-link group group-id track track-entry-number
```

缺省情况下，Smart Link 组的成员端口未与 Track 项联动。

1.6.6 配置Track与EAA联动

1. 功能简介

配置 Track 与 EAA 联动后，当关联的 Track 项状态由 Positive 变为 Negative 或者 Negative 变为 Positive 时，触发监控策略执行；如果关联多个 Track 项，则最后一个处于 Positive（Negative）状态的 Track 项变为 Negative（Positive）时，触发监控策略执行。

如果配置了抑制时间，触发策略的同时开始计时，定时器超时前，收到状态从 Positive（Negative）变为 Negative（Positive）的消息，直接丢弃，不会处理。直到定时器超时后，收到状态从 Positive（Negative）变为 Negative（Positive）的消息才处理，再一次触发策略执行。

EAA 的详细介绍，请参见“网络管理和监控”中的“EAA”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 CLI 监控策略并进入 CLI 监控策略视图。

```
rtm cli-policy policy-name
```

- (3) 配置 Track 监控事件。

```
event track track-entry-number-list state { negative | positive }  
[ suppress-time suppress-time ]
```

缺省情况下，未配置 Track 监控事件。

1.6.7 配置Track与ERPS联动

1. 功能简介

当链路中的中间传输设备或传输链路发生故障（如光纤链路发生单通、错纤、丢包等故障）以及故障排除时，ERPS 本身无法感知到这个变化。ERPS 环的成员端口需要通过专门的链路检测协议来检测端口的链路状态，当链路检测协议检测到故障发生或故障恢复时就通知 ERPS 进行链路倒换。

ERPS 环实例的成员端口通过 Track 项与链路检测协议进行联动，目前仅支持与 CFD（Connectivity Fault Detection，连通错误检测）的连续性检测功能联动。当端口与 CFD 连续性检测功能联动时，CFD 按照检测 VLAN 和检测端口来通知故障检测事件，只有当端口所在 ERPS 环实例的控制 VLAN 与 CFD 监控的 VLAN 一致时，才响应此事件。

Track 模块根据监测模块的监测结果改变 Track 项的状态，并将 Track 项状态通知给 ERPS 环；ERPS 环根据 Track 项状态进行相应处理：

- 如果 Track 项的状态为 Positive，说明该端口的上行链路正常，ERPS 环不进行链路切换；
- 如果 Track 项的状态为 Negative，说明该端口的上行链路出现故障，ERPS 环进行链路切换；
- 如果 Track 项的状态为 NotReady，说明 Track 关联监测模块的配置尚未生效，该端口维持原有转发状态不变。

关于 ERPS 的详细介绍，请参见“可靠性配置指导”中的“ERPS”。

2. 配置限制和指导

在配置端口与 Track 项联动之前，必须保证该端口已加入相应的 ERPS 环实例。

3. 配置步骤

- (1) 进入系统视图。
`system-view`
- (2) 进入二层以太网或二层聚合接口视图。
`interface interface-type interface-number`
- (3) 配置成员端口的 Track 联动。
`port erps ring ring-id instance instance-id track track-entry-index`
缺省情况下，未配置 ERPS 成员端口与 Track 机制联动。

1.7 Track显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 Track 的运行情况，通过查看显示信息验证配置的效果。

表1-1 Track 显示和维护

操作	命令
显示Track项的信息	<code>display track { track-entry-number all [negative positive] } [brief]</code>

1.8 Track典型配置举例

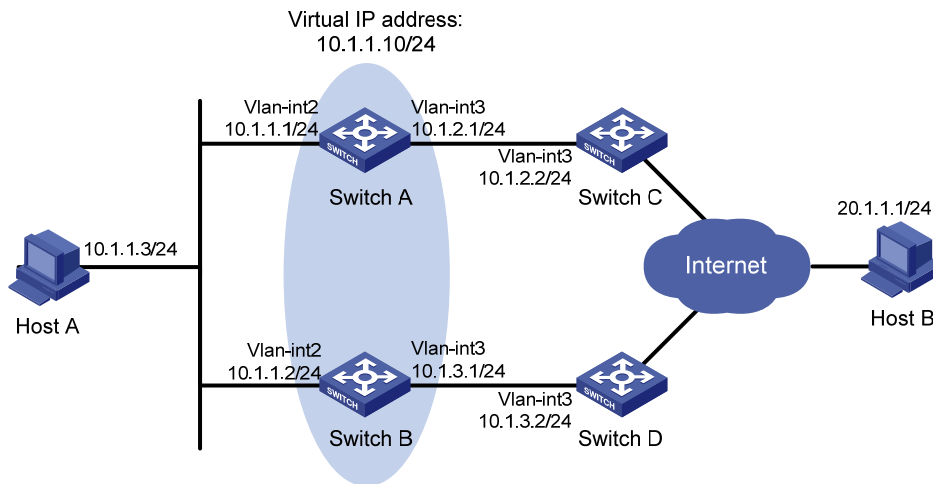
1.8.1 VRRP、Track与NQA联动配置举例（Master监视上行链路）

1. 组网需求

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 10.1.1.10/24；
- Switch A 和 Switch B 属于虚拟 IP 地址为 10.1.1.10 的备份组 1；
- 当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当通过 NQA 监测到 Switch A 上行链路不通时，Host A 发送给 Host B 的报文通过 Switch B 转发。

2. 组网图

图1-2 VRRP、Track 与 NQA 联动配置组网图



3. 配置步骤

- (1) 按照 图 1-2 创建VLAN，在VLAN中加入对应的端口，并配置各VLAN接口的IP地址，具体配置过程略。

- (2) 在 Switch A 上配置 NQA 测试组

```
<SwitchA> system-view
# 创建管理员名为 admin、操作标签为 test 的 NQA 测试组。
[SwitchA] nga entry admin test
# 配置测试类型为 ICMP-echo。
[SwitchA-nga-admin-test] type icmp-echo
# 配置目的地址为 10.1.2.2。
[SwitchA-nga-admin-test-icmp-echo] destination ip 10.1.2.2
# 测试频率为 100ms。
[SwitchA-nga-admin-test-icmp-echo] frequency 100
# 配置联动项 1（连续失败 5 次触发联动）。
[SwitchA-nga-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchA-nga-admin-test-icmp-echo] quit
# 启动探测。
[SwitchA] nga schedule admin test start-time now lifetime forever
```

- (3) 在 Switch A 上配置 Track 项

```
# 配置 Track 项 1，关联 NQA 测试组（管理员为 admin，操作标签为 test）的联动项 1。
[SwitchA] track 1 nga entry admin test reaction 1
```

- (4) 在 Switch A 上配置 VRRP

```
# 在 VLAN 接口 2 下，配置 VRRP 适用版本为 VRRPv2。
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp version 2
# 创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.10。
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
# 设置 Switch A 在备份组 1 中的优先级为 110。
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
# 设置备份组的认证方式为 simple，认证字为 hello。
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple plain hello
# 设置 Master 发送 VRRP 报文的间隔时间为 500 厘秒。
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 500
# 设置 Switch A 工作在抢占方式，抢占延迟时间为 5000 厘秒。
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
# 设置监视 Track 项。
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 30
```

(5) 在 Switch B 上配置 VRRP

```
# 在 VLAN 接口 2 下，配置 VRRP 适用版本为 VRRPv2。
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp version 2
# 创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.10。
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
# 设置备份组的认证方式为 simple，认证字为 hello。
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple plain hello
# 设置 Master 发送 VRRP 报文的间隔时间为 500 厘秒。
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 500
# 设置 Switch B 工作在抢占方式，抢占延迟时间为 5000 厘秒。
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

4. 验证配置

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp** 命令查看配置后的结果。

显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
VRID              : 1                Adver Timer   : 500
Admin Status     : Up               State         : Master
Config Pri       : 110              Running Pri   : 110
Preempt Mode     : Yes              Delay Time    : 5000
Auth Type        : Simple           Key           : *****
Virtual IP       : 10.1.1.10
Virtual MAC      : 0000-5e00-0101
Master IP        : 10.1.1.1
VRRP Track Information:
Track Object     : 1                State : Positive      Pri Reduced : 30
```

显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
```

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 500
Admin Status	: Up	State	: Backup
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 5000
Become Master	: 2200ms left		
Auth Type	: Simple	Key	: *****
Virtual IP	: 10.1.1.10		
Master IP	: 10.1.1.1		

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

Switch A 与 Switch C 不通时，在 Host A 上仍然可以 ping 通 Host B。通过 **display vrrp** 命令查看备份组的信息。

Switch A 与 Switch C 不通时，显示 Switch A 上备份组 1 的详细信息。

[SwitchA-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 500
Admin Status	: Up	State	: Backup
Config Pri	: 110	Running Pri	: 80
Preempt Mode	: Yes	Delay Time	: 5000
Become Master	: 2200ms left		
Auth Type	: Simple	Key	: *****
Virtual IP	: 10.1.1.10		
Master IP	: 10.1.1.2		

VRRP Track Information:

Track Object	: 1	State	: Negative	Pri Reduced	: 30
--------------	-----	-------	------------	-------------	------

Switch A 与 Switch C 不通时，显示 Switch B 上备份组 1 的详细信息。

[SwitchB-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 500
Admin Status	: Up	State	: Master
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 5000
Auth Type	: Simple	Key	: *****
Virtual IP	: 10.1.1.10		
Virtual MAC	: 0000-5e00-0101		
Master IP	: 10.1.1.2		

以上显示信息表示 Switch A 与 Switch C 不通时, Switch A 的优先级降低为 80, 成为 Backup, Switch B 成为 Master, Host A 发送给 Host B 的报文通过 Switch B 转发。

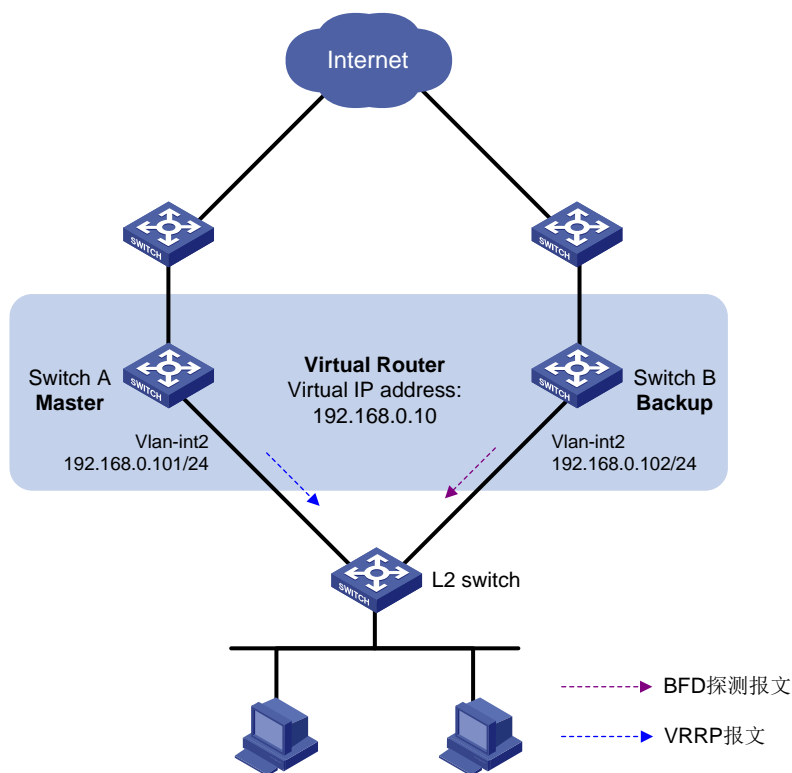
1.8.2 VRRP、Track与BFD联动配置举例（Backup监视Master）

1. 组网需求

- Switch A 和 Switch B 属于虚拟 IP 地址为 192.168.0.10 的备份组 1；
- 局域网内的主机上设置缺省网关为 192.168.0.10，当 Switch A 正常工作时，局域网内的主机通过 Switch A 访问外部网络；Switch A 出现故障时，Switch B 接替其工作，局域网内的主机通过 Switch B 访问外部网络；
- Master 出现故障时，Backup 若只依赖于 VRRP 通告报文的超时时间来判断是否应该抢占，切换时间一般在 3 秒~4 秒之间，无法达到秒级以下的切换速度；如果 Backup 通过 BFD 检测 Master 的运行状态，则能够在毫秒级的时间内发现 Master 的故障，立即抢占成为 Master，加快切换速度。

2. 组网图

图1-3 VRRP、Track 与 BFD 联动（Backup 监视 Master）配置组网图



3. 配置步骤

(1) 按照 图 1-3 创建VLAN，在VLAN中加入对应的端口，并配置各VLAN接口的IP地址，具体配置过程略。

(2) 在 Switch A 上配置 VRRP

```
<SwitchA> system-view
```

```
[SwitchA] interface vlan-interface 2
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 192.168.0.10，Switch A 在备份组 1 中的优先级为 110。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

```
[SwitchA-Vlan-interface2] return
```

(3) 在 Switch B 上配置 BFD 功能

配置 BFD echo 报文的源地址为 10.10.10.10。

```
<SwitchB> system-view
```

```
[SwitchB] bfd echo-source-ip 10.10.10.10
```

(4) 在 Switch B 上创建和 BFD 会话关联的 Track 项

创建和 BFD 会话关联的 Track 项 1，检测 Switch A 是否可达。

```
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 192.168.0.101 local ip 192.168.0.102
```

(5) 在 Switch B 上配置 VRRP

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 192.168.0.10，备份组 1 监视 Track 项 1 的状态，当 Track 项状态为 Negative 时，Switch B 快速从 Backup 切换为 Master 状态。

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

```
[SwitchB-Vlan-interface2] vrrp vrid 1 track 1 switchover
```

```
[SwitchB-Vlan-interface2] return
```

4. 验证配置

显示 Switch A 上备份组的详细信息。

```
<SwitchA> display vrrp verbose
```

IPv4 Virtual Router Information:

```
Running Mode      : Standard
```

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Master
Config Pri	: 110	Running Pri	: 110
Preempt Mode	: Yes	Delay Time	: 0
Auth Type	: None		
Virtual IP	: 192.168.0.10		
Virtual MAC	: 0000-5e00-0101		
Master IP	: 192.168.0.101		

显示 Switch B 上备份组的详细信息。

```
<SwitchB> display vrrp verbose
```

IPv4 Virtual Router Information:

```
Running Mode      : Standard
```

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 100	Running Pri	: 100


```

Preempt Mode      : Yes          Delay Time   : 0
Become Master    : 2200ms left
Auth Type        : None
Virtual IP       : 192.168.0.10
Master IP        : 192.168.0.101
VRRP Track Information:
Track Object      : 1            State : Positive      Switchover

```

显示 Switch B 上 Track 项的信息。

```

<SwitchB> display track 1
Track ID: 1
State: Positive
Duration: 0 days 0 hours 0 minutes 32 seconds
Notification delay: Positive 0, Negative 0 (in seconds)
Tracked object:
  BFD session mode: Echo
  Outgoing interface: Vlan-interface2
  VPN instance name: --
  Remote IP: 192.168.0.101
  Local IP: 192.168.0.102

```

以上显示信息表示 Track 项状态为 Positive 时，Switch A 为 Master 路由器，Switch B 为 Backup 路由器。

打开 Switch B 的 VRRP 状态调试信息开关和 BFD 事件通知调试信息开关。

```

<SwitchB> terminal debugging
<SwitchB> terminal monitor
<SwitchB> debugging vrrp fsm
<SwitchB> debugging bfd ntfy

```

Switch A 出现故障时，Switch B 上输出如下调试信息。

```

*Dec 17 14:44:34:142 2008 SwitchB BFD/7/DEBUG: Notify application:TRACK State:DOWN
*Dec 17 14:44:34:144 2008 SwitchB VRRP4/7/FSM:
  IPv4 Vlan-interface2 | Virtual Router 1 : Backup --> Master  reason: The status of the tracked
object changed

```

显示 Switch B 上备份组的详细信息。

```

<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID            : 1          Adver Timer   : 100
  Admin Status    : Up        State          : Master
  Config Pri      : 100       Running Pri    : 100
  Preempt Mode    : Yes       Delay Time     : 0
  Auth Type       : None
  Virtual IP      : 192.168.0.10
  Virtual MAC     : 0000-5e00-0101
  Master IP       : 192.168.0.102
VRRP Track Information:

```

Track Object : 1 State : Negative Switchover

以上调试信息表示，BFD 探测到 Switch A 出现故障后，立即由 Track 通知 VRRP 模块将 Switch B 的状态切换为 Master，不再等待 VRRP 通告报文的超时时间，从而保证 Backup 路由器能够快速切换为 Master。

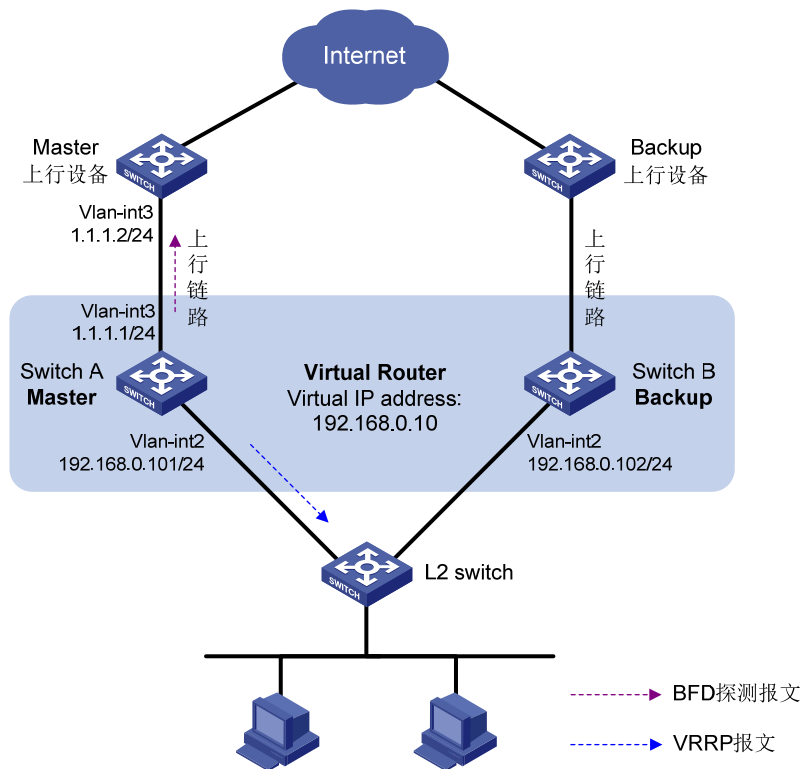
1.8.3 VRRP、Track与BFD联动配置举例（Master监视上行链路）

1. 组网需求

- Switch A 和 Switch B 属于虚拟 IP 地址为 192.168.0.10 的备份组 1；
- 局域网内的主机上设置缺省网关为 192.168.0.10；
- Switch A 正常工作时，局域网内的主机通过 Switch A 访问外部网络；Switch A 通过 BFD 检测到上行链路不通时，降低自己在备份组中的优先级，以便 Switch B 抢占成为 Master，保证局域网内的主机通过 Switch B 正常通信。

2. 组网图

图1-4 VRRP、Track 与 BFD 联动（Master 监视上行链路）配置组网图



3. 配置步骤

- (1) 按照 图 1-4 创建VLAN，在VLAN中加入对应的端口，并配置各VLAN接口的IP地址，具体配置过程略。

- (2) 在 Switch A 上配置 BFD 功能

配置 BFD echo 报文的源地址为 10.10.10.10。

```
<SwitchA> system-view
```

- ```
[SwitchA] bfd echo-source-ip 10.10.10.10
```
- (3) 在 Switch A 上创建和 BFD 会话关联的 Track 项
- # 创建和 BFD 会话关联的 Track 项 1，检测 IP 地址为 1.1.1.2 的上行设备是否可达。
- ```
[SwitchA] track 1 bfd echo interface vlan-interface 3 remote ip 1.1.1.2 local ip 1.1.1.1
```
- (4) 在 Switch A 上配置 VRRP
- # 创建备份组 1，配置备份组 1 的虚拟 IP 地址为 192.168.0.10；Switch A 在备份组 1 中的优先级为 110；配置备份组 1 监视 Track 项 1 的状态，当 Track 项状态为 Negative 时，Switch A 的优先级降低 20。
- ```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 20
[SwitchA-Vlan-interface2] return
```
- (5) 在 Switch B 上配置 VRRP
- # 创建备份组 1，配置备份组 1 的虚拟 IP 地址为 192.168.0.10。
- ```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
[SwitchB-Vlan-interface2] return
```

4. 验证配置

显示 Switch A 上备份组的详细信息。

```
<SwitchA> display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
VRID              : 1                Adver Timer   : 100
Admin Status     : Up                State         : Master
Config Pri       : 110              Running Pri    : 110
Preempt Mode     : Yes              Delay Time    : 0
Auth Type        : None
Virtual IP       : 192.168.0.10
Virtual MAC      : 0000-5e00-0101
Master IP        : 192.168.0.101
VRRP Track Information:
Track Object     : 1                State : Positive      Pri Reduced : 20
```

显示 Switch A 上 Track 项 1 的信息。

```
<SwitchA> display track 1
Track ID: 1
State: Positive
Duration: 0 days 0 hours 0 minutes 32 seconds
Notification delay: Positive 0, Negative 0 (in seconds)
Tracked object:
BFD session mode: Echo
Outgoing interface: Vlan-interface2
```

```
VPN instance name: --
Remote IP: 1.1.1.2
Local IP: 1.1.1.1
```

显示 Switch B 上备份组的详细信息。

```
<SwitchB> display vrrp verbose
```

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 0
Become Master	: 2200ms left		
Auth Type	: None		
Virtual IP	: 192.168.0.10		
Master IP	: 192.168.0.101		

以上显示信息表示 Track 项 1 的状态为 Positive 时, Switch A 为 Master 路由器, Switch B 为 Backup 路由器。

当 Switch A 监视的上行链路出现故障时, Track 项 1 的状态变为 Negative。

```
<SwitchA> display track 1
```

Track ID: 1

State: Negative

Duration: 0 days 0 hours 0 minutes 32 seconds

Notification delay: Positive 0, Negative 0 (in seconds)

Tracked object:

BFD session mode: Echo

Outgoing interface: Vlan-interface2

VPN instance name: --

Remote IP: 1.1.1.2

Local IP: 1.1.1.1

查看 Switch A 上备份组的详细信息。

```
<SwitchA> display vrrp verbose
```

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Backup
Config Pri	: 110	Running Pri	: 90
Preempt Mode	: Yes	Delay Time	: 0
Become Master	: 2200ms left		
Auth Type	: None		
Virtual IP	: 192.168.0.10		
Master IP	: 192.168.0.102		

VRRP Track Information:

Track Object	: 1	State	: Negative	Pri Reduced	: 20
--------------	-----	-------	------------	-------------	------

显示 Switch B 上备份组的详细信息。

```
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID            : 1                Adver Timer   : 100
  Admin Status    : Up              State         : Master
  Config Pri      : 100             Running Pri    : 100
  Preempt Mode    : Yes             Delay Time    : 0
  Auth Type       : None
  Virtual IP      : 192.168.0.10
  Virtual MAC     : 0000-5e00-0101
  Master IP       : 192.168.0.102
```

以上显示信息表示 Switch A 通过 BFD 检测到上行链路不通时，将自己的优先级降低为 90，从而保证 Switch B 抢占成为 Master。

1.8.4 静态路由、Track与NQA联动配置举例

1. 组网需求

Switch A、Switch B、Switch C 和 Switch D 连接了 20.1.1.0/24 和 30.1.1.0/24 两个网段，在交换机上配置静态路由以实现两个网段的互通，并配置路由备份以提高网络的可靠性。

Switch A 作为 20.1.1.0/24 网段内主机的缺省网关，在 Switch A 上存在两条到达 30.1.1.0/24 网段的静态路由，下一跳分别为 Switch B 和 Switch C。这两条静态路由形成备份，其中：

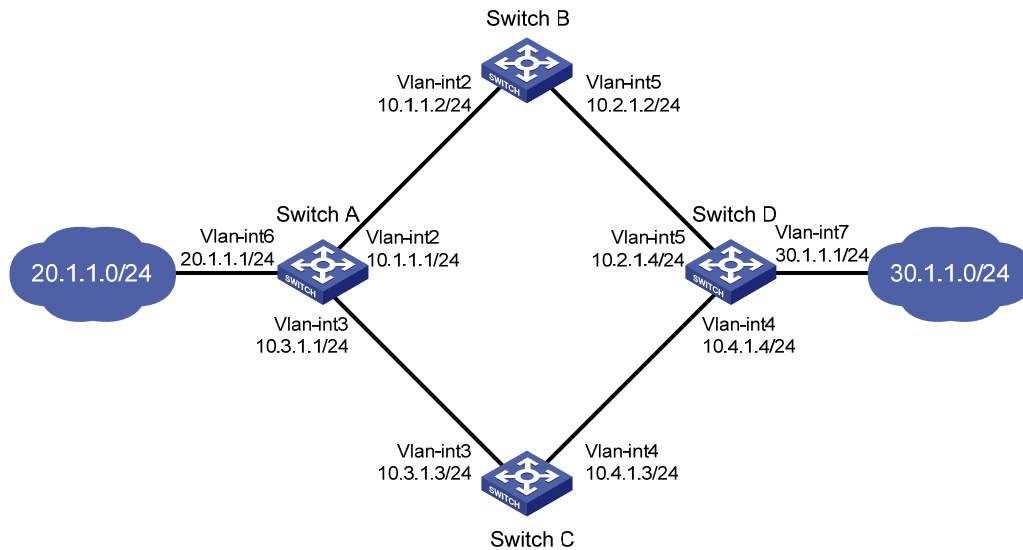
- 下一跳为 Switch B 的静态路由优先级高，作为主路由。该路由可达时，Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路由作为备份路由。
- 在 Switch A 上通过静态路由、Track 与 NQA 联动，实时判断主路由是否可达。当主路由不可达时，备份路由生效，Switch A 通过 Switch C 将报文转发到 30.1.1.0/24 网段。

同样地，Switch D 作为 30.1.1.0/24 网段内主机的缺省网关，在 Switch D 上存在两条到达 20.1.1.0/24 网段的静态路由，下一跳分别为 Switch B 和 Switch C。这两条静态路由形成备份，其中：

- 下一跳为 Switch B 的静态路由优先级高，作为主路由。该路由可达时，Switch D 通过 Switch B 将报文转发到 20.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路由作为备份路由。
- 在 Switch D 上通过静态路由、Track 与 NQA 联动，实时判断主路由是否可达。当主路由不可达时，备份路由生效，Switch D 通过 Switch C 将报文转发到 20.1.1.0/24 网段。

2. 组网图

图1-5 静态路由、Track 与 NQA 联动配置组网图



3. 配置步骤

- (1) 按照 图 1-5 创建VLAN，在VLAN中加入对应的端口，并配置各VLAN接口的IP地址，具体配置过程略。

- (2) 配置 Switch A

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.2，优先级为缺省值 60，该路由与 Track 项 1 关联。

```
<SwitchA> system-view
```

```
[SwitchA] ip route-static 30.1.1.0 24 10.1.1.2 track 1
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3，优先级为 80。

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

配置到达 10.2.1.4 的静态路由：下一跳地址为 10.1.1.2。

```
[SwitchA] ip route-static 10.2.1.4 24 10.1.1.2
```

创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[SwitchA] nqa entry admin test
```

配置测试类型为 ICMP-echo。

```
[SwitchA-nqa-admin-test] type icmp-echo
```

配置测试的目的地址为 10.2.1.4，下一跳地址为 10.1.1.2，以便通过 NQA 检测 Switch A—Switch B—Switch D 这条路径的连通性。

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
```

```
[SwitchA-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.2
```

配置测试频率为 100ms。

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

配置联动项 1（连续失败 5 次触发联动）。

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail  
threshold-type consecutive 5 action-type trigger-only
```

```
[SwitchA-nqa-admin-test-icmp-echo] quit
```

启动探测。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

配置 Track 项 1，关联 NQA 测试组（管理员为 admin，操作标签为 test）的联动项 1。

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

(3) 配置 Switch B

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.4。

```
<SwitchB> system-view
```

```
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.1。

```
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```

(4) 配置 Switch C

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.4。

```
<SwitchC> system-view
```

```
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.1。

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

(5) 配置 Switch D

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2，优先级为缺省值 60，该路由与 Track 项 1 关联。

```
<SwitchD> system-view
```

```
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2 track 1
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3，优先级为 80。

```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

配置到达 10.1.1.1 的静态路由：下一跳地址为 10.2.1.2。

```
[SwitchD] ip route-static 10.1.1.1 24 10.2.1.2
```

创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[SwitchD] nqa entry admin test
```

配置测试类型为 ICMP-echo。

```
[SwitchD-nqa-admin-test] type icmp-echo
```

配置测试的目的地址为 10.1.1.1，下一跳地址为 10.2.1.2，以便通过 NQA 检测 Switch D—Switch B—Switch A 这条路径的连通性。

```
[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

```
[SwitchD-nqa-admin-test-icmp-echo] next-hop ip 10.2.1.2
```

配置测试频率为 100ms。

```
[SwitchD-nqa-admin-test-icmp-echo] frequency 100
```

配置联动项 1（连续失败 5 次触发联动）。

```
[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail  
threshold-type consecutive 5 action-type trigger-only
```

```
[SwitchD-nqa-admin-test-icmp-echo] quit
```

启动探测。

```
[SwitchD] nqa schedule admin test start-time now lifetime forever
```

配置 Track 项 1，关联 NQA 测试组（管理员为 admin，操作标签为 test）的联动项 1。

```
[SwitchD] track 1 nqa entry admin test reaction 1
```

4. 验证配置

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
```

Track ID: 1

State: Positive

Duration: 0 days 0 hours 0 minutes 32 seconds

Notification delay: Positive 0, Negative 0 (in seconds)

Tracked object:

NQA entry: admin test

Reaction: 1

Remote IP/URL: --

Local IP: --

Interface: --

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table
```

Destinations : 10 Routes : 10

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan2
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.0/24	Static	60	0	10.1.1.2	Vlan2
10.3.1.0/24	Direct	0	0	10.3.1.1	Vlan3
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan6
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	Static	60	0	10.1.1.2	Vlan2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表示,NQA 测试的结果为主路由可达(Track 项状态为 Positive),Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。

在 Switch B 上删除 VLAN 接口 2 的 IP 地址。

```
<SwitchB> system-view
```

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] undo ip address
```

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
```

Track ID: 1

State: Negative

Duration: 0 days 0 hours 0 minutes 32 seconds

Notification delay: Positive 0, Negative 0 (in seconds)

Tracked object:

NQA entry: admin test

Reaction: 1

Remote IP/URL: --

Local IP: --

Interface: --

显示 Switch A 的路由表。

[SwitchA] display ip routing-table

Destinations : 10 Routes : 10

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan2
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.0/24	Static	60	0	10.1.1.2	Vlan2
10.3.1.0/24	Direct	0	0	10.3.1.1	Vlan3
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan6
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	Static	80	0	10.3.1.3	Vlan3
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表示，NQA 测试的结果为主路由不可达（Track 项状态为 Negative），则备份路由生效，Switch A 通过 Switch C 将报文转发到 30.1.1.0/24 网段。

主路由出现故障后，20.1.1.0/24 网段内的主机仍然可以与 30.1.1.0/24 网段内的主机通信。

[SwitchA] ping -a 20.1.1.1 30.1.1.1

Ping 30.1.1.1: 56 data bytes, press CTRL_C to break

Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms

Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms

Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms

Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms

Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---

5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss

round-trip min/avg/max/std-dev = 1/1/2/1 ms

Switch D 上的显示信息与 Switch A 类似。主路由出现故障后，30.1.1.0/24 网段内的主机仍然可以与 20.1.1.0/24 网段内的主机通信。

[SwitchB] ping -a 30.1.1.1 20.1.1.1

Ping 20.1.1.1: 56 data bytes, press CTRL_C to break

Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms

Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms

Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms

Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms

Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---

5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss

round-trip min/avg/max/std-dev = 1/1/2/1 ms

1.8.5 静态路由、Track与BFD联动配置举例

1. 组网需求

Switch A、Switch B 和 Switch C 连接了 20.1.1.0/24 和 30.1.1.0/24 两个网段，在交换机上配置静态路由以实现两个网段的互通，并配置路由备份以提高网络的可靠性。

Switch A 作为 20.1.1.0/24 网段内主机的缺省网关，在 Switch A 上存在两条到达 30.1.1.0/24 网段的静态路由，下一跳分别为 Switch B 和 Switch C。这两条静态路由形成备份，其中：

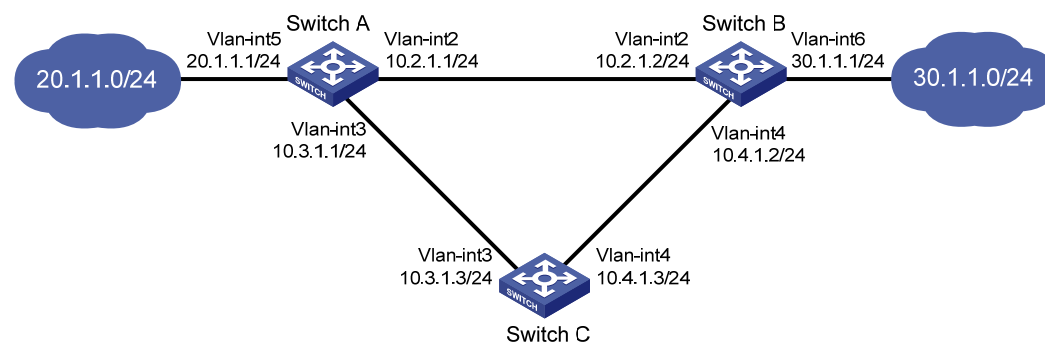
- 下一跳为 Switch B 的静态路由优先级高，作为主路由。该路由可达时，Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路由作为备份路由。
- 在 Switch A 上通过静态路由、Track 与 BFD 联动，实时判断主路由是否可达。当主路由不可达时，BFD 能够快速检测到路由故障，使得备份路由生效，Switch A 通过 Switch C 和 Switch B 将报文转发到 30.1.1.0/24 网段。

同样地，Switch B 作为 30.1.1.0/24 网段内主机的缺省网关，在 Switch B 上存在两条到达 20.1.1.0/24 网段的静态路由，下一跳分别为 Switch A 和 Switch C。这两条静态路由形成备份，其中：

- 下一跳为 Switch A 的静态路由优先级高，作为主路由。该路由可达时，Switch B 通过 Switch A 将报文转发到 20.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路由作为备份路由。
- 在 Switch B 上通过静态路由、Track 与 BFD 联动，实时判断主路由是否可达。当主路由不可达时，BFD 能够快速检测到路由故障，使得备份路由生效，Switch B 通过 Switch C 和 Switch A 将报文转发到 20.1.1.0/24 网段。

2. 组网图

图1-6 静态路由、Track 与 BFD 联动配置组网图



3. 配置步骤

(1) 按照 图 1-6 创建VLAN，在VLAN中加入对应的端口，并配置各VLAN接口的IP地址，具体配置过程略。

(2) 配置 Switch A

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2，优先级为缺省值 60，该路由与 Track 项 1 关联。

```
<SwitchA> system-view
```

```
[SwitchA] ip route-static 30.1.1.0 24 10.2.1.2 track 1
# 配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3，优先级为 80。
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
# 配置 BFD echo 报文的源地址为 10.10.10.10。
[SwitchA] bfd echo-source-ip 10.10.10.10
# 创建和 BFD 会话关联的 Track 项 1，检测 Switch A 是否可以与静态路由的下一跳 Switch B 互通。
[SwitchA] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.2 local ip 10.2.1.1
```

(3) 配置 Switch B

```
# 配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.1，优先级为缺省值 60，该路由与 Track 项 1 关联。
<SwitchB> system-view
[SwitchB] ip route-static 20.1.1.0 24 10.2.1.1 track 1
# 配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3，优先级为 80。
[SwitchB] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
# 配置 BFD echo 报文的源地址为 1.1.1.1。
[SwitchB] bfd echo-source-ip 1.1.1.1
# 创建和 BFD 会话关联的 Track 项 1，检测 Switch B 是否可以与静态路由的下一跳 Switch A 互通。
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.1 local ip 10.2.1.2
```

(4) 配置 Switch C

```
# 配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.2。
<SwitchC> system-view
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.2
# 配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.1。
[SwitchB] ip route-static 20.1.1.0 24 10.3.1.1
```

4. 验证配置

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 10.2.1.2
    Local IP: 10.2.1.1
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table
```

Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan2
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	Direct	0	0	10.3.1.1	Vlan3
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan5
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	Static	60	0	10.2.1.2	Vlan2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表示，BFD 检测的结果为下一跳地址 10.2.1.2 可达（Track 项状态为 Positive），主路由生效，Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。

在 Switch B 上删除 VLAN 接口 2 的 IP 地址。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] undo ip address
```

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 10.2.1.2
    Local IP: 10.2.1.1
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table
```

Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan2
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	Direct	0	0	10.3.1.1	Vlan3
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan5
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	Static	80	0	10.3.1.3	Vlan3
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表示，BFD 检测的结果为下一跳地址 10.2.1.2 不可达（Track 项状态为 Negative），备份路由生效，Switch A 通过 Switch C 和 Switch B 将报文转发到 30.1.1.0/24 网段。

主路由出现故障后，20.1.1.0/24 网段内的主机仍然可以与 30.1.1.0/24 网段内的主机通信。

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56 data bytes, press CTRL_C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

Switch B 上的显示信息与 Switch A 类似。主路由出现故障后，30.1.1.0/24 网段内的主机仍然可以与 20.1.1.0/24 网段内的主机通信。

```
[SwitchB] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56 data bytes, press CTRL_C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

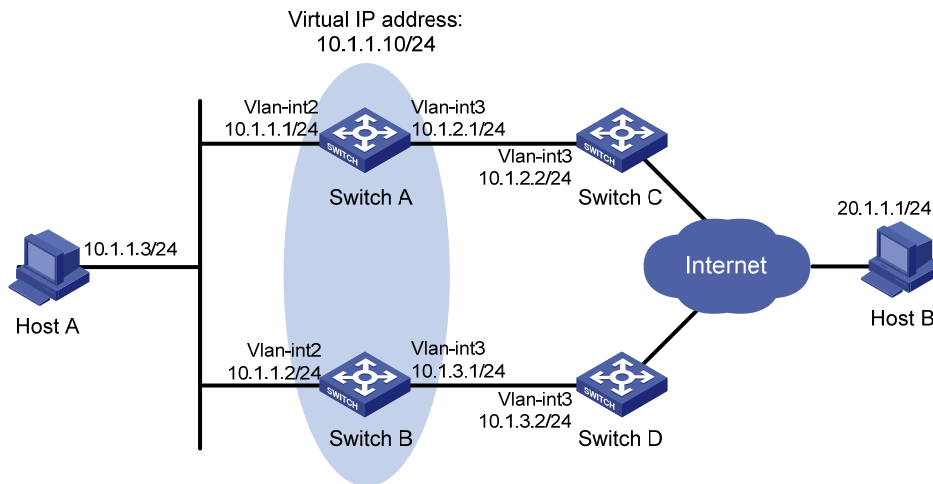
1.8.6 VRRP、Track与接口管理联动配置举例（Master监视上行接口）

1. 组网需求

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 10.1.1.10/24；
- Switch A 和 Switch B 属于虚拟 IP 地址为 10.1.1.10 的备份组 1；
- 当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当通过接口管理监测到 Switch A 连接上行链路的 VLAN 接口 3 出现故障时，Host A 发送给 Host B 的报文通过 Switch B 转发。

2. 组网图

图1-7 VRRP、Track 与接口管理联动配置组网图



3. 配置步骤

- (1) 按照 图 1-7 创建VLAN，在VLAN中加入对应的端口，并配置各VLAN接口的IP地址，具体配置过程略。

- (2) 在 Switch A 上配置 Track 项

创建 Track 项 1，与上行接口 VLAN 接口 3 的链路状态关联。

```
[SwitchA] track 1 interface vlan-interface 3
```

- (3) 在 Switch A 上配置 VRRP

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.10。

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

设置 Switch A 在备份组 1 中的优先级为 110。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

设置监视 Track 项。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 30
```

- (4) 在 Switch B 上配置 VRRP

```
<SwitchB> system-view
```

```
[SwitchB] interface vlan-interface 2
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.10。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

4. 验证配置

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp** 命令查看配置后的结果。

显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
```

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

```

Interface Vlan-interface2
  VRID          : 1                Adver Timer   : 100
  Admin Status  : Up               State        : Master
  Config Pri    : 110              Running Pri   : 110
  Preempt Mode  : Yes              Delay Time    : 0
  Auth Type     : None
  Virtual IP    : 10.1.1.10
  Virtual MAC   : 0000-5e00-0101
  Master IP     : 10.1.1.1
VRRP Track Information:
  Track Object   : 1                State : Positive      Pri Reduced : 30

```

显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
```

```
IPv4 Virtual Router Information:
```

```
Running Mode      : Standard
```

```
Total number of virtual routers : 1
```

```

Interface Vlan-interface2
  VRID          : 1                Adver Timer   : 100
  Admin Status  : Up               State        : Backup
  Config Pri    : 100              Running Pri   : 100
  Preempt Mode  : Yes              Delay Time    : 0
  Become Master : 2200ms left
  Auth Type     : None
  Virtual IP    : 10.1.1.10
  Master IP     : 10.1.1.1

```

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

在 Switch A 上关闭 VLAN 接口 3。

```
[SwitchA-Vlan-interface2] interface vlan-interface 3
```

```
[SwitchA-Vlan-interface3] shutdown
```

关闭 Switch A 的上行接口后，在 Host A 上仍然可以 ping 通 Host B。通过 **display vrrp** 命令查看备份组的信息。

关闭 Switch A 的上行接口后，显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface3] display vrrp verbose
```

```
IPv4 Virtual Router Information:
```

```
Running Mode      : Standard
```

```
Total number of virtual routers : 1
```

```

Interface Vlan-interface2
  VRID          : 1                Adver Timer   : 100
  Admin Status  : Up               State        : Backup
  Config Pri    : 110              Running Pri   : 80
  Preempt Mode  : Yes              Delay Time    : 0
  Become Master : 2200ms left
  Auth Type     : None
  Virtual IP    : 10.1.1.10
  Master IP     : 10.1.1.2

```

```
VRRP Track Information:
```

Track Object : 1 State : Negative Pri Reduced : 30

关闭 Switch A 的上行接口后，显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
```

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID	: 1	Adver Timer	: 100
Admin Status	: Up	State	: Master
Config Pri	: 100	Running Pri	: 100
Preempt Mode	: Yes	Delay Time	: 0
Auth Type	: None		
Virtual IP	: 10.1.1.10		
Virtual MAC	: 0000-5e00-0101		
Master IP	: 10.1.1.2		

以上显示信息表示关闭 Switch A 的上行接口后，Switch A 的优先级降低为 80，成为 Backup，Switch B 成为 Master，Host A 发送给 Host B 的报文通过 Switch B 转发。

1.8.7 静态路由、Track与LLDP联动配置举例

1. 组网需求

Device A、Device B 和 Device C 连接了 20.1.1.0/24 和 30.1.1.0/24 两个网段，在交换机上配置静态路由以实现两个网段的互通，并配置路由备份以提高网络的可靠性。

Device A 作为 20.1.1.0/24 网段内主机的缺省网关，在 Device A 上存在两条到达 30.1.1.0/24 网段的静态路由，下一跳分别为 Device B 和 Device C。这两条静态路由形成备份，其中：

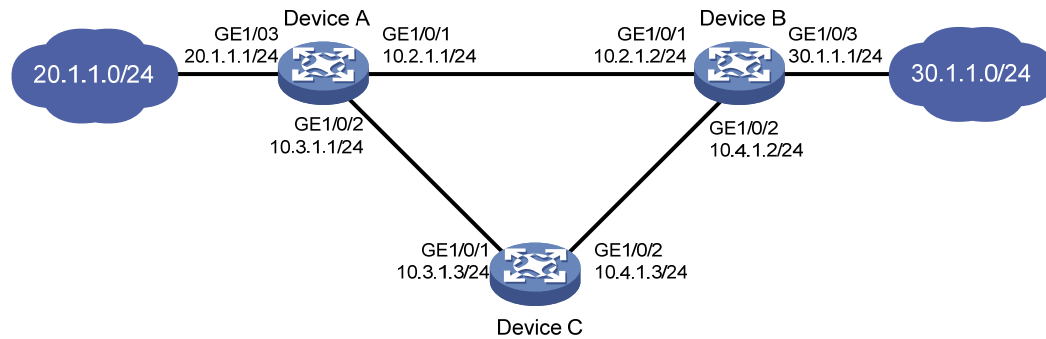
- 下一跳为 Device B 的静态路由优先级高，作为主路由。该路由可达时，Device A 通过 Device B 将报文转发到 30.1.1.0/24 网段。
- 下一跳为 Device C 的静态路由作为备份路由。
- 在 Device A 上通过静态路由、Track 与 LLDP 联动，实时判断主路由是否可达。当主路由不可达时，LLDP 能够检测到路由故障，使得备份路由生效，Device A 通过 Device C 和 Device B 将报文转发到 30.1.1.0/24 网段。

同样地，Device B 作为 30.1.1.0/24 网段内主机的缺省网关，在 Device B 上存在两条到达 20.1.1.0/24 网段的静态路由，下一跳分别为 Device A 和 Device C。这两条静态路由形成备份，其中：

- 下一跳为 Device A 的静态路由优先级高，作为主路由。该路由可达时，Device B 通过 Device A 将报文转发到 20.1.1.0/24 网段。
- 下一跳为 Device C 的静态路由作为备份路由。
- 在 Device B 上通过静态路由、Track 与 LLDP 联动，实时判断主路由是否可达。当主路由不可达时，LLDP 能够检测到路由故障，使得备份路由生效，Device B 通过 Device C 和 Device A 将报文转发到 20.1.1.0/24 网段。

2. 组网图

图1-8 静态路由、Track 与 LLDP 联动配置组网图



3. 配置步骤

(1) 按照 图 1-8 配置各接口的IP地址，具体配置过程略。

(2) 配置 Device A

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2，优先级为缺省值 60，该路由与 Track 项 1 关联。

```
<DeviceA> system-view
[DeviceA] ip route-static 30.1.1.0 24 10.2.1.2 track 1
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3，优先级为 80。

```
[DeviceA] ip route-static 20.1.1.0 24 10.3.1.3 preference 80
```

全局开启 LLDP 功能。

```
[DeviceA] lldp global enable
```

在接口 GigabitEthernet1/0/1 上开启 LLDP 功能（此步骤可省略，LLDP 功能在接口上缺省开启）。

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] lldp enable
```

创建和 LLDP 邻居关联的 Track 项 1，检测 Device A 是否可以与静态路由的下一跳 Device B 互通。

```
[DeviceA] track 1 lldp neighbor interface gigabitethernet 1/0/1
```

(3) 配置 Device B

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.1，优先级为缺省值 60，该路由与 Track 项 1 关联。

```
<DeviceB> system-view
[DeviceB] ip route-static 20.1.1.0 24 10.2.1.1 track 1
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3，优先级为 80。

```
[DeviceB] ip route-static 30.1.1.0 24 10.4.1.3 preference 80
```

全局开启 LLDP 功能。

```
[DeviceB] lldp global enable
```

在接口 GigabitEthernet1/0/1 上开启 LLDP 功能（此步骤可省略，LLDP 功能在接口上缺省开启）。

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] lldp enable
```

创建和 LLDP 邻居关联的 Track 项 1，检测 Device B 是否可以与静态路由的下一跳 Device A 互通。

```
[DeviceB] track 1 lldp neighbor interface gigabitethernet 1/0/1
```

(4) 配置 Device C

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.2。

```
<DeviceC> system-view
```

```
[DeviceC] ip route-static 30.1.1.0 24 10.4.1.2
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.1。

```
[DeviceC] ip route-static 20.1.1.0 24 10.3.1.1
```

4. 验证配置

显示 Device A 上 Track 项的信息。

```
[DeviceA] display track all
```

Track ID: 1

State: Positive

Duration: 0 days 0 hours 0 minutes 32 seconds

Notification delay: Positive 0, Negative 0 (in seconds)

Tracked object:

LLDP interface: GigabitEthernet1/0/1

显示 Device A 的路由表。

```
[DeviceA] display ip routing-table
```

Destinations : 9

Routes : 9

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.2.1.0/24	Direct	0	0	10.2.1.1	GE1/0/1
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	Direct	0	0	10.3.1.1	GE1/0/2
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	GE1/0/3
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	Static	60	0	10.2.1.2	GE1/0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表示，LLDP 检测的结果为下一跳地址 10.2.1.2 可达（Track 项状态为 Positive），主路由生效，Device A 通过 Device B 将报文转发到 30.1.1.0/24 网段。

在 Device B 上关闭接口 GigabitEthernet1/0/1 的 LLDP 功能。

```
<DeviceB> system-view
```

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] undo lldp enable
```

显示 Device A 上 Track 项的信息。

```
[DeviceA] display track all
```

Track ID: 1

State: Negative

Duration: 0 days 0 hours 0 minutes 32 seconds

Notification delay: Positive 0, Negative 0 (in seconds)

```
Tracked object:
  LLDP interface: GigabitEthernet1/0/1
```

显示 Device A 的路由表。

```
[DeviceA] display ip routing-table
```

```
Destinations : 9          Routes : 9
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.2.1.0/24	Direct	0	0	10.2.1.1	GE1/0/1
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	Direct	0	0	10.3.1.1	GE1/0/2
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	GE1/0/3
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	Static	80	0	10.3.1.3	GE1/0/2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表示，LLDP 检测的结果为下一跳地址 10.2.1.2 不可达（Track 项状态为 Negative），备份路由生效，Device A 通过 Device C 和 Device B 将报文转发到 30.1.1.0/24 网段。

主路由出现故障后，20.1.1.0/24 网段内的主机仍然可以与 30.1.1.0/24 网段内的主机通信。

```
[DeviceA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56 data bytes, press CTRL_C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

Device B 上的显示信息与 Device A 类似。主路由出现故障后，30.1.1.0/24 网段内的主机仍然可以与 20.1.1.0/24 网段内的主机通信。

```
[DeviceB] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56 data bytes, press CTRL_C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

1.8.8 Smart Link、Track和CFD联动配置举例

具体配置举例请参见“可靠性配置指导”中的“Smart Link”。