H3C S5500-HI 系列以太网交换机

可靠性配置指导

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W102-20131220
产品版本：Release 52xx 系列

前 言

H3C S5500-HI 系列以太网交换机配置指导共分为十一本手册，介绍了 S5500-HI 系列以太网交换机 Release52xx 系列软件版本各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《可靠性配置指导》主要介绍了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

新增及修改特性说明

本手册对应 S5500-HI 系列以太网交换机的 Release52xx 系列软件版本，各版本间特性差异如下：

- Release5206 与 Release5203 版本相比，无新增、修改特性。
- Release5203 与Release5101 版本相比，新增、修改了部分特性，具体请参见 表 1。

表1 Release5203 与 Release5101 版本间特性差异

配置指导	新增及修改特性
可靠性概述	无
以太网OAM	无
CFD	无
DLDP	修改特性：配置DLDP报文的认证方式及密码命令行修改
RRPP	无
Smart Link	无
Monitor Link	无

配置指导	新增及修改特性
VRRP	新增特性： • 支持在三层聚合接口上配置 VRRP • 配置 VRRP 报文的 DSCP 优先级 修改特性：配置VRRP报文的认证方式及认证字命令行修改
双机热备	无
BFD	无
Track	无

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。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*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 | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、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。

5. 端口编号示例约定

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。

产品配套资料

H3C S5500-HI 系列以太网交换机的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	产品彩页	帮助您了解产品的主要规格参数及亮点
	技术白皮书	帮助您了解产品和特性功能，对于特色及复杂技术从细节上进行介绍
硬件介绍及安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	H3C 设备防雷安装指导手册	帮助您了解防雷接地设计和工程安装方法，以保证交换机具有良好的抗雷击性能
	快速安装指南	指导您对设备进行初始安装，通常针对最常用的情况，减少您的检索时间
	安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装

大类	资料名称	内容介绍
	风扇安装手册	帮助您了解产品支持的可插拔风扇模块的外观、功能、规格、安装及拆卸方法
	电源手册	帮助您了解产品支持的可插拔电源模块的外观、功能、规格、安装及拆卸方法
	RPS电源用户手册	帮助您了解产品支持的RPS电源的外观、功能、规格
	H3C低端系列以太网交换机RPS电源选购指南	帮助您了解各种RPS电源适用的交换机产品型号及RPS电源配套电缆的相关规格
	接口模块扩展卡用户手册	帮助您了解该接口模块扩展卡的外观、规格、安装及拆卸方法
	H3C低端系列以太网交换机可插拔模块手册	帮助您了解产品支持的可插拔模块类型、外观和规格
	H3C可插拔SFP[SFP+][XFP]模块安装指南	帮助您掌握SFP/SFP+/XFP模块的正确安装方法，避免因操作不当而造成器件损坏
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	故障处理手册	指导您快速定位并处理软件故障
	版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

010-62982107

网址：http://www.h3c.com.cn

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 可靠性概述

随着网络的快速普及和应用的日益深入，各种增值业务（如 IPTV、视频会议等）得到了广泛部署，网络中断可能影响大量业务、造成重大损失。因此，作为业务承载主体的基础网络，其可靠性日益成为受关注的焦点。

在实际网络中，总避免不了各种非技术因素造成的网络故障和服务中断。因此，提高系统容错能力、提高故障恢复速度、降低故障对业务的影响，是提高系统可靠性的有效途径。

1.1 可靠性需求

可靠性需求根据其目标和实现方法的不同可分为三个级别，各级别的目标和实现方法如表 1-1 所示。

表1-1 可靠性需求的级别

级别	目标	实现方法
1	减少系统的软、硬件故障	• 硬件：简化电路设计、提高生产工艺、进行可靠性试验等 • 软件：软件可靠性设计、软件可靠性测试等
2	即使发生故障，系统功能也不受影响	设备和链路的冗余设计、部署倒换策略、提高倒换成功率
3	尽管发生故障导致功能受损，但系统能够快速恢复	提供故障检测、诊断、隔离和恢复技术

在上述三个级别的可靠性需求中，第 1 级别需求的满足应在网络设备的设计和生产过程中予以考虑；第 2 级别需求的满足应在设计网络架构时予以考虑；第 3 级别需求则应在网络部署过程中，根据网络架构和业务特点采用相应的可靠性技术来予以满足。

1.2 可靠性度量

通常，我们使用 MTBF（Mean Time Between Failures，平均故障间隔时间）和 MTTR（Mean Time to Repair，平均修复时间）这两个技术指标来评价系统的可靠性。

1. MTBF

MTBF 是指一个系统无故障运行的平均时间，通常以小时为单位。MTBF 越多，可靠性也就越高。

2. MTTR

MTTR 是指一个系统从故障发生到恢复所需的平均时间，广义的 MTTR 还涉及备件管理、客户服务等，是设备维护的一项重要指标。

MTTR 的计算公式为：MTTR=故障检测时间+硬件更换时间+系统初始化时间+链路恢复时间+路由覆盖时间+转发恢复时间。公式中各项的值越小，MTTR 也就越少，可靠性也就越高。

1.3 可靠性技术

通过前面的介绍可知，提高 MTBF 或降低 MTTR 都可以提高网络的可靠性。在实际网络中，各种因素造成的故障难以避免，因此能够让网络从故障中快速恢复的技术就显得非常重要。本节介绍的各种可靠性技术将主要从降低 MTTR 的角度，为满足第 2、3 级别的可靠性需求来提供技术手段。

可靠性技术的种类繁多，我们根据其解决网络故障的侧重不同，将其大致分为故障检测技术和保护倒换技术两大类。

1.3.1 故障检测技术

故障检测技术侧重于网络的故障检测和诊断。CFD、DLDP、以太网OAM都属于链路层的故障检测技术；BFD是一种通用的故障检测技术，可用于各层面的故障检测；NQA用于对网络质量进行诊断和评估；Monitor Link和Track通过故障检测的联动机制来与其它可靠性技术进行配合。对这些技术的进一步介绍如 表 1-2 所示。

表1-2 故障检测技术

名称	简介	详细介绍
CFD	全称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，是一种二层链路上基于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、确认故障并定位故障	可靠性配置指导/CFD
DLDP	全称Device Link Detection Protocol（设备链路检测协议），用于监控光纤或铜质双绞线的链路状态。当发现单向链路后，会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生	可靠性配置指导/DLDP
以太网OAM	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。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	可靠性配置指导/以太网OAM
BFD	全称Bidirectional Forwarding Detection（双向转发检测），是一个通用的、标准化的、介质无关、协议无关的快速故障检测机制，用于快速检测、监控网络中链路或IP路由的转发连通状况	可靠性配置指导/BFD
NQA	全称Network Quality Analyzer（网络质量分析），通过发送测试报文，对网络性能、网络提供的服务及服务质量进行分析，并为用户提供网络性能和服务质量的参数，如时延抖动、TCP连接时延、FTP连接时延和文件传输速率等	网络管理和监控配置指导/NQA
Monitor Link	一种端口联动方案，主要用于配合二层拓扑协议的组网应用。它通过监控设备的上行端口，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备份链路的切换	可靠性配置指导/Monitor Link
Track	用于实现联动功能。联动功能由应用模块、Track模块和监测模块三部分组成，它通过建立联动项来实现不同模块间的联动，即由监测模块通过Track模块触发应用模块来执行某种操作。监测模块负责对链路状态、网络性能等进行探测，并通过Track模块将探测结果通知给应用模块；应用模块感知到网络状态变化后，及时进行相应处理，从而避免通信的中断或服务质量的降低	可靠性配置指导/Track

1.3.2 保护倒换技术

保护倒换技术侧重于网络的故障恢复，主要通过对硬件、链路、路由信息和业务信息等进行冗余备份以及故障时的快速切换，从而保证网络业务的连续性。对各种保护倒换技术的具体介绍如 表 1-3 所示。

表1-3 保护倒换技术

名称	简介	详细介绍
以太网链路聚合	简称链路聚合，它通过将多条以太网物理链路捆绑在一起成为一条逻辑链路，实现了增加链路带宽的目的，而这些捆绑在一起的链路通过相互间的动态备份，可以有效地提高链路的可靠性	二层技术-以太网交换配置指导/以太网链路聚合
Smart Link	实现了双上行组网主备链路的冗余备份，并在主用链路发生故障后使流量能够迅速切换到备用链路上，具备较高的收敛速度	可靠性配置指导/Smart Link
MSTP	全称Multiple Spanning Tree Protocol（多生成树协议），是一种二层管理协议，它通过选择性地阻塞网络中的冗余链路来消除二层环路，同时还具备链路备份的功能	二层技术-以太网交换配置指导/生成树
RRPP	全称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。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路，具备较高的收敛速度	可靠性配置指导/RRPP
FRR	全称Fast ReRoute（快速重路由），是一种实现网络局部保护的技术。它通过为主路由或路径建立备份路由或路径，当主路由或路径出现故障时能够迅速切换到备份路由或路径，从而减少网络故障引起的数据丢失。支持该技术的协议有RIP、OSPF、IS-IS、静态路由和RSVP-TE等	三层技术-IP路由配置指导、MPLS配置指导/相关协议内容
GR	全称Graceful Restart（平滑重启），是一种保证转发业务在设备进行IP/MPLS转发协议（如BGP、IS-IS、OSPF、IPv6 BGP、IPv6 IS-IS、OSPFv3、LDP和RSVP-TE等）重启或主备倒换时不中断的技术。它需要周边设备的配合来完成路由等信息的备份与恢复	三层技术-IP路由配置指导、MPLS配置指导/相关协议内容
NSR	全称Nonstop Routing（不间断路由），是一种保证数据传输在设备进行主备倒换时不中断的技术，设备形成IRF后支持该功能。它通过将IP等转发信息从Master设备备份到Slave设备，从而在设备进行主备倒换时，无需周边设备配合即可完成上述信息的备份与恢复。支持该技术的协议只有IS-IS	三层技术-IP路由配置指导/IS-IS
双机热备	通过两台设备之间的业务备份，当其中一台设备发生故障时，利用VRRP或动态路由机制将业务流量切换到备份设备，由于该设备已备份有故障设备的业务信息，业务数据便可从该设备上通过，从而在很大程度上避免了网络业务的中断	可靠性配置指导/双机热备
VRRP	全称Virtual Router Redundancy Protocol（虚拟路由器冗余协议），是一种容错协议，在具有组播或广播能力的局域网（如以太网）中，使设备出现故障时仍能提供缺省链路，有效地避免了单一链路发生故障后出现网络中断的问题	可靠性配置指导/VRRP

从前面的介绍可知，可靠性技术的种类繁多，面对越来越复杂的网络环境，要想依靠单一的技术来解决所有的可靠性问题几乎无法实现。因此，需要在对网络环境和用户需求进行细致分析的基础上，综合运用各种可靠性技术来提高网络的可靠性。此外，在建网之初还应充分考虑组网的可靠性，譬

如：根据业务现状或业务预测，边缘层的节点在接入时应采用冗余备份机制，分别与汇聚层的节点相连；核心层的各节点之间尽量采用全连接的方式，等等。

总之，提高网络可靠性是一个系统工程，需要网络设计和管理者在网络的设计、建设与维护过程中加以全面考虑。

目 录

1 以太网OAM配置

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

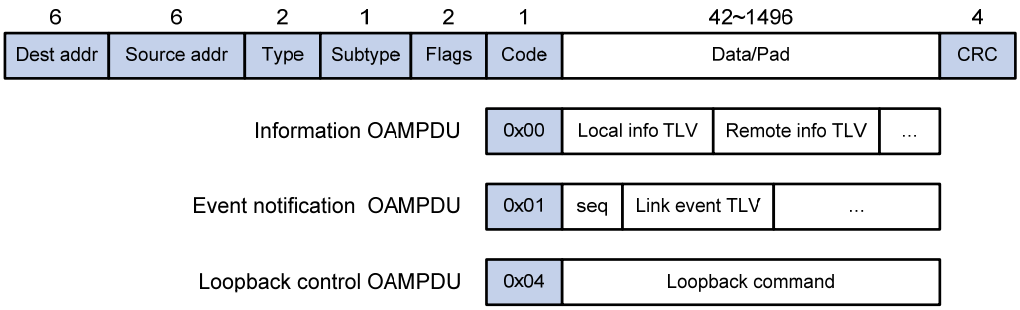
以太网 OAM 的主要功能包括：

- 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 Units，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。

图1-1 常见的 OAMPDU 报文



如 图 1-1 所示，是几种常见OAMPDU的报文格式，各重要字段的含义如 表 1-1 所示。

表1-1 OAMPDU 重要字段含义

字段	含义
Dest addr	以太网OAM报文目的MAC地址，为慢协议组播地址：0x0180-C200-0002。由于慢协议报文不能被网桥转发，因此以太网OAM报文也不能被转发
Source addr	以太网OAM报文源MAC地址，为发送端的桥MAC地址，是一个单播MAC地址

字段	含义
Type	以太网OAM报文的协议类型，为0x8809
Subtype	以太网OAM报文的协议子类型，为0x03
Flags	Flag域，包含了以太网OAM实体的状态信息
Code	OAMPDU报文的类型

说明

我们称使能了以太网 OAM 功能的端口为“以太网 OAM 实体”，简称“OAM 实体”。

图 1-1 中几类OAMPDU报文的作用如 表 1-2 所示。

表1-2 各类 OAMPDU 报文的作用

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，该报文中带有使能或去使能环回功能的信息，根据该信息开启或关闭远端环回功能

1.1.3 以太网OAM工作流程

以太网 OAM 功能建立在以太网 OAM 连接的基础上，下面对以太网 OAM 的工作流程进行简要介绍。

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 实体收到对端的配置参数后，决定是否建立 OAM 连接。当两端 OAM 实体对 Loopback 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，在这两种模式下设备的处理能力如 表 1-3 所示。

表1-3 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

处理能力	主动模式	被动模式
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，但需要对端为主动模式	可以

说明

- 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 实体只能等待对端 OAM 实体的连接请求。
- 都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。

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对端 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 1-4 所示）时，将向其对端发送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状况。

表1-4 一般链路事件

事件类型	描述
错误信号事件（Errored Symbol Event）	单位时间内的错误信号数量超过定义的阈值
错误帧事件（Errored Frame Event）	单位时间内的错误帧数量超过定义的阈值
错误帧周期事件（Errored Frame Period Event）	指定帧数N为周期，在收到N个帧的周期内错误帧数超过定义的阈值
错误帧秒数事件（Errored Frame Seconds Event）	指定M秒数下有错误帧的秒数超过了定义的阈值

说明

- 错误帧周期事件的检测周期将被系统转换为某端口在该周期内能发送 64 字节帧的最大帧数（不含帧间隙和前导码），即以最大帧数作为周期，其计算公式为：最大帧数 = 接口带宽（bps）× 错误帧周期事件的检测周期（ms）÷（64 × 8 × 1000）。
- 错误帧秒：如果在某一秒内发生了错误帧，则将该秒称为错误帧秒。

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）通知给对端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 1-5 所示。

表1-5 紧急链路事件

事件类型	描述	OAMPDU 发送频率
链路故障（Link Fault）	对端链路信号丢失	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

说明

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

- 支持接收携带以上三种类型紧急链路事件的 Information OAMPDU。
- 仅千兆光口支持发送携带链路故障事件的 Information OAMPDU。
- 仅支持在设备重启或端口被 shutdown 时发送携带致命故障事件的 Information OAMPDU，但 IRF 物理端口不支持发送该报文。有关 IRF 物理端口的详细介绍，请参见“IRF 配置指导”中的“IRF”。
- 不支持发送携带紧急事件的 Information OAMPDU。

4. 远端环回

远端环回是指主动模式下的 OAM 实体向对端（远端）发送除 OAMPDU 以外的所有其它报文时，对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配置任务简介

表1-6 以太网 OAM 配置任务简介

配置任务		说明	详细配置
配置以太网OAM基本功能		必选	1.3
配置以太网OAM连接检测定时器		可选	1.4
配置一般链路事件的检测参数	配置错误信号事件的检测参数	可选	1.5.1
	配置错误帧事件检测参数	可选	1.5.2
	配置错误帧周期事件检测参数	可选	1.5.3
	配置错误帧秒数事件检测参数	可选	1.5.4
配置以太网OAM远端环回功能	使能以太网OAM远端环回功能	可选	1.6.1
	拒绝对端发起的以太网OAM远端环回	可选	1.6.2

1.3 配置以太网OAM基本功能

以太网 OAM 的连接模式分为主动和被动模式，当使能了以太网 OAM 功能之后，以太网端口开始使用预设的连接模式与其对端端口建立以太网 OAM 连接。

表1-7 配置以太网 OAM 基本功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置以太网OAM的连接模式	**oam mode** { **active** | **passive** }	可选 缺省情况下，以太网OAM的连接模式为主动模式
使能以太网OAM功能	**oam enable**	必选 缺省情况下，以太网端口的以太网OAM功能处于关闭状态

注意

在使能了以太网 OAM 功能的端口上不能改变以太网 OAM 的连接模式。如需改变连接模式，请先关闭该端口上的以太网 OAM 功能。

1.4 配置以太网OAM连接检测定时器

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对端 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。

表1-8 配置以太网 OAM 连接检测定时器

操作	命令	说明
进入系统视图	**system-view**	-
配置以太网OAM握手报文的发送间隔	**oam timer hello** *interval*	可选 缺省情况下，以太网OAM握手报文的发送间隔为1000毫秒
配置以太网OAM连接的超时时间	**oam timer keepalive** *interval*	可选 缺省情况下，以太网OAM连接的超时时间为5000毫秒

注意

由于以太网 OAM 连接超时后，本端 OAM 实体将老化与对端 OAM 实体的连接关系，使 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（建议配置为其五倍或以上），否则会导致以太网 OAM 连接的不稳定。

1.5 配置一般链路事件的检测参数

说明

当以太网 OAM 连接建立后，本节中所配置的各事件检测周期和阈值将会在所有以太网端口上自动有效。

1.5.1 配置错误信号事件的检测参数

在错误信号事件的检测周期内，如果某以太网端口上所发生的错误信号数大于或等于错误信号事件的检测阈值，则将在该端口上产生一个错误信号事件。

表1-9 配置错误信号事件的检测参数

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置错误信号事件的检测周期	**oam errored-symbol period** *period-value*	可选 缺省情况下，错误信号事件的检测周期为1秒
配置错误信号事件的检测阈值	**oam errored-symbol threshold** *threshold-value*	可选 缺省情况下，错误信号事件的检测阈值为1

1.5.2 配置错误帧事件的检测参数

在错误帧事件的检测周期内，如果某以太网端口上所发生的错误帧数大于或等于错误帧事件的检测阈值，则将在该端口上产生一个错误帧事件。

表1-10 配置错误帧事件的检测参数

操作	命令	说明
进入系统视图	**system-view**	-
配置错误帧事件的检测周期	**oam errored-frame period** *period-value*	可选 缺省情况下，错误帧事件的检测周期为1秒
配置错误帧事件的检测阈值	**oam errored-frame threshold** *threshold-value*	可选 缺省情况下，错误帧事件的检测阈值为1

1.5.3 配置错误帧周期事件的检测参数

在错误帧周期事件的检测周期内，如果某以太网端口上所发生的错误帧数大于或等于错误帧周期事件的检测阈值，则将在该端口上产生一个错误帧周期事件。

表1-11 配置错误帧周期事件的检测参数

操作	命令	说明
进入系统视图	**system-view**	-
配置错误帧周期事件的检测周期	**oam errored-frame-period period** *period-value*	可选 缺省情况下，错误帧周期事件的检测周期为1000毫秒
配置错误帧周期事件的检测阈值	**oam errored-frame-period threshold** *threshold-value*	可选 缺省情况下，错误帧周期事件的检测阈值为1

1.5.4 配置错误帧秒数事件的检测参数

在错误帧秒数事件的检测周期内，如果某以太网端口上所发生的错误帧秒数大于或等于错误帧秒数事件的检测阈值，则将在该端口上产生一个错误帧秒数事件。

表1-12 配置错误帧秒数事件的检测参数

操作	命令	说明
进入系统视图	**system-view**	-
配置错误帧秒数事件的检测周期	**oam errored-frame-seconds period** *period-value*	可选 缺省情况下，错误帧秒数事件的检测周期为60秒
配置错误帧秒数事件的检测阈值	**oam errored-frame-seconds threshold** *threshold-value*	可选 缺省情况下，错误帧秒数事件的检测阈值为1

注意

错误帧秒数事件检测的阈值不要大于设定的周期值，否则不会发生错误帧秒数事件。

1.6 配置以太网OAM远端环回功能

1.6.1 使能以太网OAM远端环回功能

在本端端口上使能了以太网 OAM 远端环回功能之后，该端口将向对端端口发送 Loopback Control OAMPDU，使对端进入 OAM 环回状态。然后，用户可以从本端向对端发送测试报文，并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。

用户可以在用户视图或系统视图下使能指定端口的以太网 OAM 远端环回功能，也可以在端口视图下使能当前端口的以太网 OAM 远端环回功能，三者的配置效果相同。

1. 在用户视图下使能以太网OAM远端环回功能

表1-13 在用户视图下使能以太网 OAM 远端环回功能

操作	命令	说明
使能指定端口的以太网OAM远端环回功能	**oam loopback interface** *interface-type interface-number*	必选 缺省情况下，端口上的以太网OAM远端环回功能处于关闭状态

2. 在系统视图下使能以太网OAM远端环回功能

表1-14 在系统视图下使能以太网 OAM 远端环回功能

操作	命令	说明
进入系统视图	**system-view**	-
使能指定端口的以太网OAM远端环回功能	**oam loopback interface** *interface-type interface-number*	必选 缺省情况下，端口上的以太网OAM远端环回功能处于关闭状态

3. 在端口视图下使能以太网OAM远端环回功能

表1-15 在端口视图下使能以太网 OAM 远端环回功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
使能当前端口的以太网OAM远端环回功能	**oam loopback**	必选 缺省情况下，端口上的以太网OAM远端环回功能处于关闭状态

注意

由于远端环回功能将使正常业务受到影响，因此请慎重使用。

说明

- 只有当端口上的以太网 OAM 连接已建立完成，且以太网 OAM 的连接模式为主动模式时，才能在该端口上使能以太网 OAM 远端环回功能。
- 只有本端和对端端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。
- 远端环回功能需要远端硬件的支持，如果远端硬件不支持，会提示用户。
- 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，端口将自动执行一次先关闭再开启的操作。导致端口退出远端环回的原因有：使用 **undo oam enable** 命令关闭以太网 OAM 功能、使用 **undo oam loopback interface** 或 **undo oam loopback** 命令关闭以太网 OAM 远端环回功能或 OAM 连接超时等。
- 由于远端环回功能主要用于测单条链路，所以聚合成员端口和业务环回成员端口并不支持该功能；此外，处于远端环回过程中的端口也不能加入聚合组或业务环回组。有关聚合组和业务环回组的详细介绍，请分别参见“二层技术-以太网交换配置指导”中的“以太网链路聚合”和“业务环回组”。
- 如果在远端环回过程中开启了内部环回测试功能，远端环回将终止。有关环回测试功能的详细介绍，请参见“二层技术-以太网交换配置指导”中的“以太网端口”。

1.6.2 拒绝对端发起的以太网OAM远端环回

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，用户可以通过本配置使本端端口不受对端发来的 Loopback Control OAMPDU 的控制，从而拒绝其发起的以太网 OAM 远端环回。

表1-16 拒绝对端发起的以太网 OAM 远端环回

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
拒绝对端发起的以太网OAM远端环回	**oam loopback reject-request**	必选 缺省情况下，端口不拒绝对端发起的以太网OAM远端环回

1.7 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1-17 以太网 OAM 显示和维护

操作	命令
查看以太网OAM的全局配置信息	**display oam configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看以太网OAM的紧急链路事件统计信息	**display oam critical-event** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看以太网OAM的一般链路事件统计信息	**display oam link-event** { **local | remote** } [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看以太网OAM连接的信息	**display oam** { **local | remote** } [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除以太网OAM的报文和一般链路事件统计信息	**reset oam** [**interface** *interface-type interface-number*]

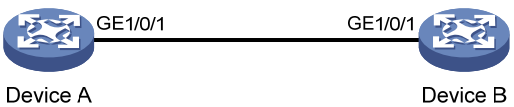
1.8 以太网OAM典型配置举例

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，来检测 Device A 与 Device B 之间的链路性能。

2. 组网图

图1-2 以太网 OAM 典型配置组网图



3. 配置步骤

(1) 配置 Device A

在端口 GigabitEthernet1/0/1 上配置以太网 OAM 的连接模式为被动模式，并使能以太网 OAM 功能。

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

配置错误帧事件的检测周期为 20 秒，检测阈值为 10。

```
[DeviceA] oam errored-frame period 20
[DeviceA] oam errored-frame threshold 10
```

(2) 配置 Device B

在端口 GigabitEthernet1/0/1 上配置以太网 OAM 的连接模式为主动模式，并使能以太网 OAM 功能。

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

(3) 检验配置效果

通过使用 **display oam configuration** 命令可以查看以太网 OAM 的配置信息，例如：

查看 Device A 上以太网 OAM 的配置信息。

```
[DeviceA] display oam configuration
Configuration of the link event window/threshold :
------------------------------------------------------------------------------
Errored-symbol Event period(in seconds)          :     1
Errored-symbol Event threshold                   :     1
Errored-frame Event period(in seconds)           :     20
Errored-frame Event threshold                    :     10
Errored-frame-period Event period(in ms)         :     1000
Errored-frame-period Event threshold             :     1
Errored-frame-seconds Event period(in seconds)   :     60
Errored-frame-seconds Event threshold            :     1

Configuration of the timer :
------------------------------------------------------------------------------
Hello timer(in ms)                               :     1000
Keepalive timer(in ms)                           :     5000
```

以上显示信息表明：除错误帧事件的检测周期为 20 秒、检测阈值为 10 以外，其余参数都为缺省值。

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

查看 Device A 所有端口上以太网 OAM 的紧急链路事件统计信息。

```
[DeviceA] display oam critical-event
Port        : GigabitEthernet1/0/1
Link Status : Up
Event statistic :
------------------------------------------------------------------------------
```

```
Link Fault    :0    Dying Gasp    : 0    Critical Event    : 0
```

以上显示信息表明：Device A 与 Device B 之间的链路上尚未发生过任何紧急链路事件。

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

查看 Device B 所有端口上以太网 OAM 的一般链路事件的远端统计信息。

```
[DeviceB] display oam link-event remote
Port :GigabitEthernet1/0/1
Link Status :Up
OAMRemoteErrFrameEvent : (ms = milliseconds)
--------------------------------------------------------------------------
Event Time Stamp          : 5789        Errored Frame Window   : 200(100ms)
Errored Frame Threshold   : 10          Errored Frame          : 13
Error Running Total       : 350         Event Running Total    : 17
```

以上显示信息表明：从 Device A 开始运行时起，总共发生了 350 次错误，其中错误帧事件有 17 次，链路性能并不稳定。

目 录

1 CFD配置

1.1 CFD简介

CFD 是 Connectivity Fault Detection（连通错误检测）的简称，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。它是一种二层链路上基于 VLAN 的端到端 OAM（Operations, 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，确认故障并确定故障发生的位置。

1.1.1 CFD基本概念

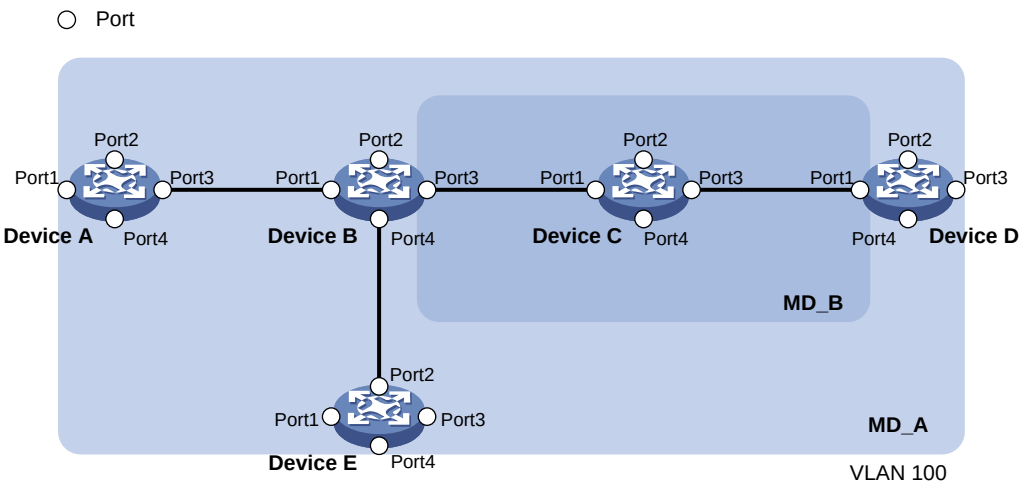
1. MD

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。

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

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。

一个 MA 服务于一个 VLAN，MA 中的 MP 所发送的报文都带有该 VLAN 的标签，同时 MA 中的 MP 可以接收由本 MA 中其它 MP 发来的报文。MA 的级别等于其所属 MD 的级别。

3. MP

MP（Maintenance Point，维护点）配置在端口上，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）两种：

(1) MEP

MEP 确定了 MA 的边界，它以“MEP ID”来标识。

MEP 所属的 MA 确定了该 MEP 发出的报文所属的 VLAN；MEP 的级别等于其所属 MD 的级别，MEP 发出的报文的级别等于该 MEP 的级别。MEP 的级别决定了其所能处理的报文的级别：当 MEP 收到高于自己级别的报文时不会进行处理，而是将其按原有路径转发；而当 MEP 收到小于等于自己级别的报文时才会进行处理。

说明

上述描述是指同一 VLAN 内的报文处理方式，不同 VLAN 内的报文之间是相互隔离的，不会相互影响。

MEP 具有方向性，分为内向 MEP 和外向 MEP 两种：内向 MEP 通过除其所在的端口以外的所有端口向外发送 CFD 协议报文，即在其所属 MA 所服务的 VLAN 中进行广播；而外向 MEP 则直接通过其所在的端口向外发送 CFD 协议报文。

(2) MIP

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 可以配合 MEP 完成类似于 ping 和 tracert 的功能。当 MIP 收到不等于自己级别的报文时不会进行处理，而是将其按原有路径转发；只有当 MIP 收到等于自己级别的报文时才会进行处理。

MIP所属的MA确定了该MEP所能接收的报文所属的VLAN；MIP的级别由其创建规则和所属MD的级别共同确定。MIP由系统按照以下规则在端口上自动创建：如果端口上尚不存在MIP，就按照级别由低到高依次检查每个MD中的MA，在各级别的检查中都按照如 图 1-2 所示的流程来确定是否在本级别创建MIP。

图1-2 MIP 的创建流程

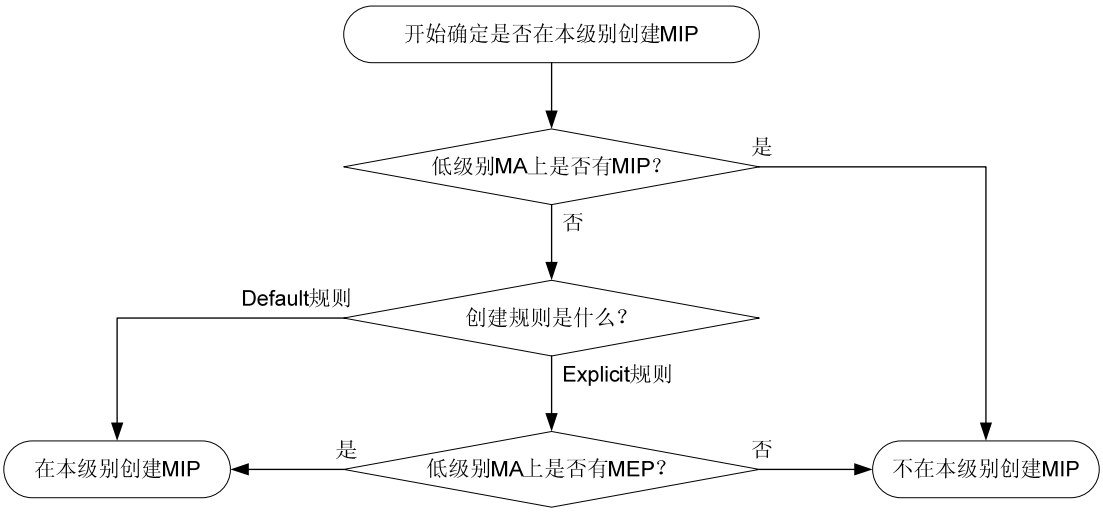
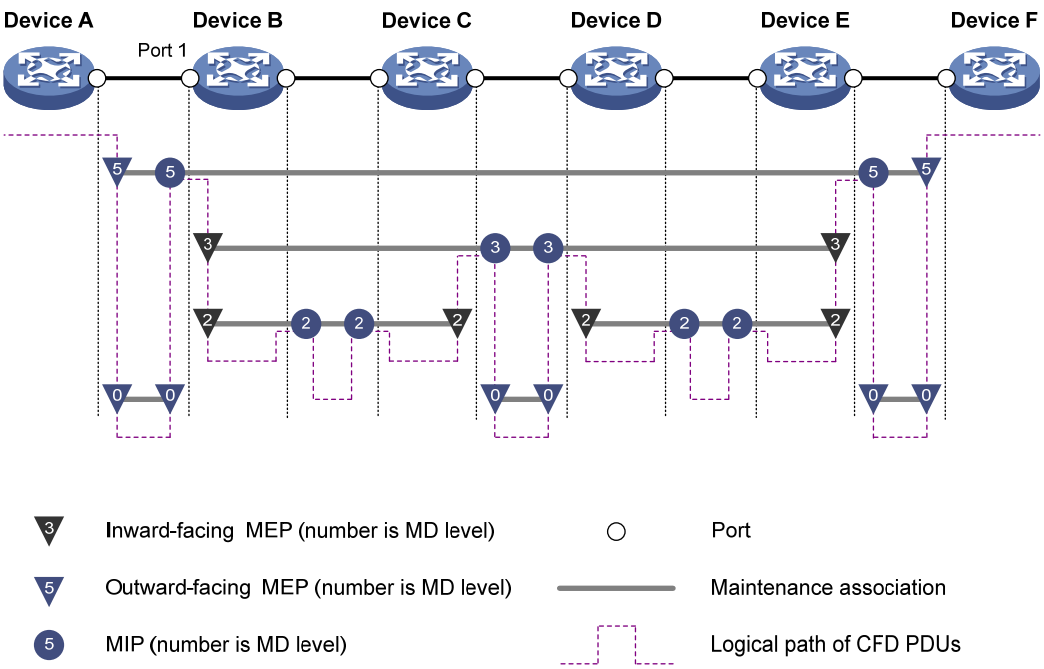


图 1-3 所示为CFD的一种分级配置方式，图中共有 0、2、3、5 四个级别的MD，标识号较大的MD的级别高、控制范围广；标识号较小的MD的级别低、控制范围小。在Device A～Device F的各端口上配置了MP，譬如Device B的Port 1 上配置有：级别为 5 的MIP、级别为 3 的内向MEP、级别为 2 的内向MEP和级别为 0 的外向MEP。

图1-3 CFD 的分级配置



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 列表中除其本身以外的所有远端 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，包括：

- 连续性检测功能
- 环回功能
- 链路跟踪功能
- 告警抑制功能
- 单向丢包测试功能
- 帧时延测试功能
- 比特错误测试功能

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 报文和 LBR 报文都是单播报文。

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 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，分为单向时延测试和双向时延测试两种：

(1)　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。

(2)　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。

1.1.3 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配置任务简介

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 在不同设备上的名称相同。
- 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 中的同一 MA 在不同设备上的名称相同。
- 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 的边界端口上应规划 MEP，非边界设备或端口上可规划 MIP。

在完成网络规划之后，请进行下列配置。

表1-1 CFD 配置任务简介

配置任务			说明	详细配置
CFD基础配置	使能CFD功能		必选	1.3.1
	配置CFD版本		可选	1.3.2
	配置服务实例	配置有MD名称的服务实例	二者必选其一	1.3.3 1.
		配置无MD名称的服务实例		1.3.3 2.
	配置MEP		必选	1.3.4
	配置MIP的创建规则		必选	1.3.5
配置CFD各项功能	配置连续性检测功能		必选	1.4.2
	配置环回功能		可选	1.4.3
	配置链路跟踪功能		可选	1.4.4
	配置告警抑制功能		可选	1.4.5
	配置单向丢包测试功能		可选	1.4.6
	配置单向时延测试功能		可选	1.4.7
	配置双向时延测试功能		可选	1.4.8
	配置比特错误测试功能		可选	1.4.9

说明

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基础配置

1.3.1 使能CFD功能

在进行 CFD 的其它配置任务之前，请先使能 CFD 功能。

表1-2 使能 CFD 功能

操作	命令	说明
进入系统视图	**system-view**	-
使能CFD功能	**cfd enable**	必选 缺省情况下，CFD功能处于关闭状态

1.3.2 配置CFD版本

CFD 协议有三种版本：IEEE 802.1ag draft5.2 版本、IEEE 802.1ag draft5.2 过渡版本和 IEEE 802.1ag 标准版本。同一 MD 中的设备所采用的 CFD 版本应保持一致，否则这些设备之间的 CFD 协议报文将无法互通。

表1-3 配置 CFD 版本

操作	命令	说明
进入系统视图	**system-view**	-
配置CFD采用的协议版本	**cfd version** { **draft5** | **draft5-plus** | **standard** }	必选 缺省情况下，CFD采用的协议版本为IEEE 802.1ag标准版本

注意

当设备上存在 MD（包括通过 **cfd md** 命令创建的或通过 **cfd service-instance maid format** 命令自动生成的 MD）时，不允许在标准版本与 draft5.2 版本或 draft5.2 过渡版本之间进行切换，但允许在 draft5.2 版本与 draft5.2 过渡版本之间进行切换；当设备上不存在 MD 时则无此限制。

1.3.3 配置服务实例

在配置 MEP 和 MIP 之前，必须首先配置服务实例（Service Instance）。一个服务实例用一个整数表示，代表了一个 MD 中的一个 MA。MD 和 MA 确定了服务实例内的 MP 所处理的报文的级别属性和 VLAN 属性。

服务实例可分为有 MD 名称的服务实例和无 MD 名称的服务实例两种，前者在 CFD 协议的任何版本下都有效，而后者只在 CFD 协议的 IEEE 802.1ag 标准版本下有效。用户可根据实际情况创建其中的一种。

1. 配置有MD名称的服务实例

在创建有 MD 名称的服务实例之前，必须先为该服务实例创建 MD 和 MA。

请严格按照下列顺序依次创建 MD、MA 和有 MD 名称的服务实例。

表1-4 配置有 MD 名称的服务实例

操作	命令	说明
进入系统视图	**system-view**	-
创建MD	**cfd md** *md-name* **level** *level-value*	必选 缺省情况下，不存在MD
创建MA	**cfd ma** *ma-name* **md** *md-name* **vlan** *vlan-id*	必选 缺省情况下，不存在MA
创建有MD名称的服务实例	**cfd service-instance** *instance-id* **md** *md-name* **ma** *ma-name*	必选 缺省情况下，不存在服务实例

2. 配置无MD名称的服务实例

在创建无 MD 名称的服务实例时，系统会自动为该服务实例创建 MA 和 MD。

表1-5 配置无 MD 名称的服务实例

操作	命令	说明
进入系统视图	**system-view**	-
创建无MD名称的服务实例	**cfd service-instance** *instance-id* **maid format** { **icc-based** *ma-name* | **string** *ma-name* } **level** *level-value* **vlan** *vlan-id*	必选 缺省情况下，不存在服务实例

1.3.4 配置MEP

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。

在创建 MEP 前必须先配置 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。

表1-6 配置 MEP

操作	命令	说明
进入系统视图	**system-view**	-
配置MEP列表	**cfd meplist** *mep-list* **service-instance** *instance-id*	必选 缺省情况下，不存在MEP列表
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
创建MEP	**cfd mep** *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }	必选 缺省情况下，端口上不存在MEP
使能MEP	**cfd mep service-instance** *instance-id* **mep** *mep-id* **enable**	必选 缺省情况下，MEP处于关闭状态

注意

创建的 MEP 必须已包含在对应服务实例的 MEP 列表中，否则不能创建成功。

1.3.5 配置MIP的创建规则

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、1DM、DMM、TST 等）。请根据网络规划配置 MIP 的创建规则。

表1-7 配置 MIP 的创建规则

操作	命令	说明
进入系统视图	**system-view**	-
配置MIP的创建规则	**cfd mip-rule** { **default** | **explicit** } **service-instance** *instance-id*	必选 缺省情况下，没有配置MIP的创建规则，也不存在MIP

注意

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：

- 使能或关闭 CFD 功能
- 创建或删除端口上的 MEP
- 端口的 VLAN 属性发生变化
- MIP 的创建规则发生变化

1.4 配置CFD各项功能

1.4.1 配置准备

在配置 CFD 各项功能之前，需完成以下配置任务：

- CFD 基础配置

1.4.2 配置连续性检测功能

在配置其它各项 CFD 功能之前，必须先配置连续性检测功能。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。

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 1-8 所示。

表1-8 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

请通过以下操作来配置连续性检测功能。

表1-9 配置连续性检测功能

操作	命令	说明
进入系统视图	**system-view**	-
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*	可选 缺省情况下，MEP发送的CCM报文中时间间隔域的值为4
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能MEP的CCM报文发送功能	**cfd cc service-instance** *instance-id* **mep** *mep-id* **enable**	必选 缺省情况下，MEP的CCM报文发送功能处于关闭状态

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。
- 对于 S5500-28SC-HI 和 S5500-52SC-HI 交换机，Interval 域的有效取值范围为 4～7，当配置该参数取值为 1～3 时，会有告警提示且实际配置不生效。

1.4.3 配置环回功能

通过配置环回功能，可以检查链路状况，从而实现链路连通性的验证。

表1-10 配置环回功能

操作	命令	说明
启用环回功能检查链路状况	**cfd loopback service-instance** *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**number** *number*]	必选 缺省情况下，环回功能未启用 本命令可在任意视图下执行 本系列交换机上配置了外向维护端点时，不支持**target-mep**参数

1.4.4 配置链路跟踪功能

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。
- 自动发送链路跟踪报文：使能本功能后，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。

表1-11 配置链路跟踪功能

操作	命令	说明
查找源MEP到目标MEP的路径	**cfd linktrace service-instance** *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**ttl** *ttl-value*] [**hw-only**]	必选 本命令可在任意视图下执行 本系列交换机上配置了外向维护端点时，不支持**target-mep**参数
进入系统视图	**system-view**	-
使能自动发送链路跟踪报文功能	**cfd linktrace auto-detection** [**size** *size-value*]	必选 缺省情况下，自动发送链路跟踪报文功能处于关闭状态

1.4.5 配置告警抑制功能

通过配置告警抑制功能可以减少 MEP 故障告警的数量。

表1-12 配置告警抑制功能

操作	命令	说明
进入系统视图	**system-view**	-
使能告警抑制功能	**cfd ais enable**	必选 缺省情况下，告警抑制功能处于关闭状态
配置AIS报文的发送级别	**cfd ais level** *level-value* **service-instance** *instance-id*	必选 缺省情况下，没有配置AIS报文的发送级别
配置AIS报文的发送周期	**cfd ais period** *period-value* **service-instance** *instance-id*	可选 缺省情况下，AIS报文的发送周期为1秒

注意

- 如果没有配置 AIS 报文的发送级别，则该维护实例中的 MEP 将无法发送 AIS 报文，且 AIS 报文发送级别必须高于本 MEP 所在 MD 的级别。
- 接收 AIS 报文的 MEP 也只有使能了告警抑制功能并配置了正确的 AIS 报文发送级别才能抑制故障告警，并继续向更高级别的 MD 发送 AIS 报文。如果只使能了告警抑制功能，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，而不会再发送 AIS 报文。

1.4.6 配置单向丢包测试功能

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。

表1-13 配置单向丢包测试功能

操作	命令	说明
进入系统视图	**system-view**	-
启用单向丢包测试功能	**cfd slm service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	必选 缺省情况下，单向丢包测试功能未启用 本系列交换机上配置了外向维护端点时，不支持**target-mep**参数

注意

单向丢包测试功能只能在 CFD 协议的 IEEE 802.1ag 标准版本下起作用。

1.4.7 配置单向时延测试功能

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。

表1-14 配置单向时延测试功能

操作	命令	说明
进入系统视图	**system-view**	-
启用单向时延测试功能	**cfd dm one-way service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	必选 缺省情况下，单向时延测试功能未启用 本系列交换机上配置了外向维护端点时，不支持**target-mep**参数

注意

- 单向时延测试功能只能在 CFD 协议的 IEEE 802.1ag 标准版本下起作用。
- 测试时要求源 MEP 和目标 MEP 的时钟同步，用于单向时延变化测量时两端时钟可以不同步。
- 测试结果需在目标 MEP 上通过 **display cfd dm one-way history** 命令来查看。

1.4.8 配置双向时延测试功能

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。

表1-15 配置双向时延测试功能

操作	命令	说明
进入系统视图	**system-view**	-
启用双向时延测试功能	**cfd dm two-way service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	必选 缺省情况下，双向时延测试功能未启用 本系列交换机上配置了外向维护端点时，不支持**target-mep**参数

注意

双向时延测试功能只能在 CFD 协议的 IEEE 802.1ag 标准版本下起作用。

1.4.9 配置比特错误测试功能

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。

表1-16 配置比特错误测试功能

操作	命令	说明
进入系统视图	**system-view**	-
启用比特错误测试功能	**cfd 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**]]	必选 缺省情况下，比特错误测试功能未启用 本系列交换机上配置了外向维护端点时，不支持**target-mep**参数

注意

- 比特错误测试功能只能在 CFD 协议的 IEEE 802.1ag 标准版本下起作用。
- 测试结果需在目标 MEP 上通过 **display cfd tst** 命令来查看。

1.5 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1-17 CFD 显示和维护

操作	命令
显示CFD和AIS的使能状态	**display cfd status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示CFD采用的协议版本	**display cfd version** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MD的配置信息	**display cfd md** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MA的配置信息	**display cfd ma** [[*ma-name*] **md** { *md-name* | **level** *level-value* }] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示服务实例的配置信息	**display cfd service-instance** [*instance-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示服务实例内的MEP列表	**display cfd meplist** [**service-instance** *instance-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
显示MP的信息	**display cfd mp** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MEP的属性和运行信息	**display cfd mep** *mep-id* **service-instance** *instance-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MEP上获得的LTR报文信息	**display cfd linktrace-reply** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示远端MEP的信息	**display cfd remote-mep service-instance** *instance-id* **mep** *mep-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示自动发送LTM报文所收到的LTR报文的内容	**display cfd linktrace-reply auto-detection** [**size** *size-value*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MEP上AIS的配置和动态信息	**display cfd ais** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MEP上单向时延的测试结果	**display cfd dm one-way history** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MEP上比特错误的测试结果	**display cfd tst** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除MEP上单向时延的测试结果	**reset cfd dm one-way history** [**service-instance** *instance-id* [**mep** *mep-id*]]
清除MEP上比特错误的测试结果	**reset cfd tst** [**service-instance** *instance-id* [**mep** *mep-id*]]

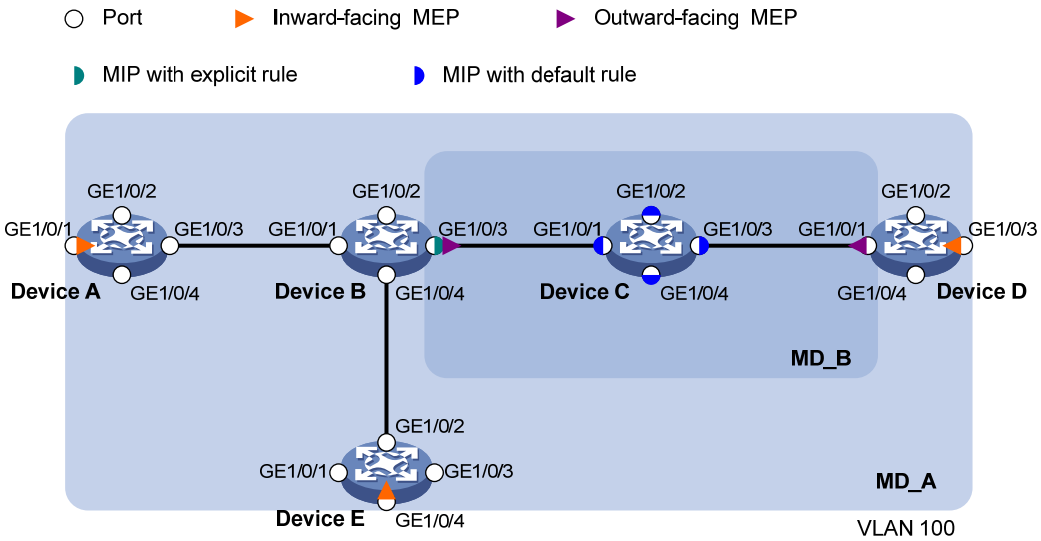
1.6 CFD典型配置举例

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-FC00-6511、0010-FC00-6512、0010-FC00-6513、0010-FC00-6514 和 0010-FC00-6515。
- 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的检测。

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) 使能 CFD 功能

在 Device A 上使能 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，在 MD_A 中创建服务于 VLAN 100 的 MA MA_A，并为 MD_A 和 MA_A 创建服务实例 1。

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

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，在 MD_A 中创建服务于 VLAN 100 的 MA MA_A，并为 MD_A 和 MA_A 创建服务实例 1；再创建级别为 3 的 MD MD_B，在 MD_B 中创建服务于 VLAN 100 的 MA MA_B，并为 MD_B 和 MA_B 创建服务实例 2。

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

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，在 MD_B 中创建服务于 VLAN 100 的 MA MA_B，并为 MD_B 和 MA_B 创建服务实例 2。

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

(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 上创建并使能服务实例 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] cfd mep service-instance 1 mep 1001 enable
[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 上创建并使能服务实例 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] cfd mep service-instance 2 mep 2001 enable
[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 上创建并使能服务实例 2 内的外向 MEP 4001，然后在端口 GigabitEthernet1/0/3 上创建并使能服务实例 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] cfd mep service-instance 2 mep 4001 enable
[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] cfd mep service-instance 1 mep 4002 enable
[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 上创建并使能服务实例 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] cfd mep service-instance 1 mep 5001 enable
[DeviceE-GigabitEthernet1/0/4] quit
```

(5) 配置 MIP 的创建规则

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 上使能服务实例 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 上使能服务实例 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 上使能服务实例 2 内 MEP 4001 的 CCM 报文发送功能，并在端口 GigabitEthernet1/0/3 上使能服务实例 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 上使能服务实例 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 上使能告警抑制功能，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
```

4. 检验配置效果

(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 0010-FC00-6515 with the sequence number start from 1001-43404:
Reply from 0010-FC00-6515: sequence number=1001-43404 time=5ms
Reply from 0010-FC00-6515: sequence number=1001-43405 time=5ms
Reply from 0010-FC00-6515: sequence number=1001-43406 time=5ms
Reply from 0010-FC00-6515: sequence number=1001-43407 time=5ms
Reply from 0010-FC00-6515: sequence number=1001-43408 time=5ms
Send: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-FC00-6515            63      0010-FC00-6512   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-FC00-6514
Far-end frame loss: 10    Near-end frame loss: 20
Reply from 0010-FC00-6514
Far-end frame loss: 40    Near-end frame loss: 40
Reply from 0010-FC00-6514
Far-end frame loss: 0     Near-end frame loss: 10
Reply from 0010-FC00-6514
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%    Near-end frame loss rate: 32%
Send 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。譬如：

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
Info: 5 1DMs process is done, 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
Send 1DM total number: 0
Received 1DM 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。譬如：

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-FC00-6514: 10ms
Reply from 0010-FC00-6514: 9ms
```

```
Reply from 0010-FC00-6514: 11ms
Reply from 0010-FC00-6514: 5ms
Reply from 0010-FC00-6514: 5ms
Average: 8ms
Send DMMs: 5       Received: 5        Lost: 0

Frame delay variation: 5ms  4ms  6ms  0ms  0ms
Average: 3ms
```

(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。譬如：

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
Info: TST process is done. 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
Send TST total number: 0
Received TST total number: 5
Received from 0010-FC00-6511, sequence number 1: Bit True
Received from 0010-FC00-6511, sequence number 2: Bit True
Received from 0010-FC00-6511, sequence number 3: Bit True
Received from 0010-FC00-6511, sequence number 4: Bit True
Received from 0010-FC00-6511, sequence number 5: Bit True
```

目 录

1 DLDP配置

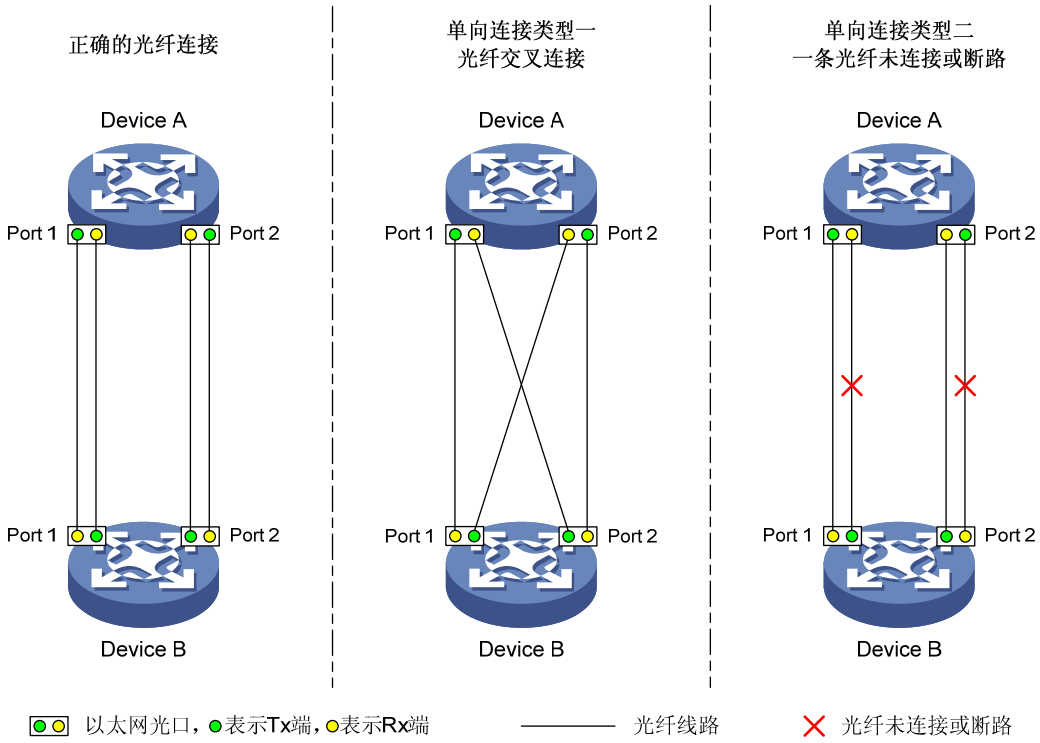
1.1 DLDP简介

1.1.1 DLDP产生背景

在实际组网中，有时会出现一种特殊的现象——单向链路（即单通）。所谓单向链路是指本端设备可以通过链路层收到对端设备发送的报文，但对端设备不能收到本端设备的报文。单向链路会引起一系列问题，比如生成树拓扑中存在环路等。

以光纤连接为例，单向链路可分为两种类型：一种是光纤交叉相连，另一种是一条光纤未连接或一条光纤断路。如 图 1-1 所示，是正确的光纤连接与上述两种类型单向连接的对比示意。

图1-1 正确与错误的光纤连接对比



DLDP（Device Link Detection Protocol，设备链路检测协议）可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生。

DLDP 是链路层协议，它与物理层协议协同工作来监控设备的链路状态。物理层的自动协商机制进行物理信号和故障的检测；DLDP 进行对端设备的识别、单向链路的识别和关闭不可达端口等工作。二者协同工作，可以检测和关闭物理和逻辑的单向连接。如果链路两端在物理层都能独立正常工作，DLDP 会在链路层检测这些链路是否正确连接、两端是否可以正确的交互报文。这种检测不能通过物理层的自动协商机制实现。

1.1.2 DLDP工作原理

1. DLDP协议状态

DLDP协议的状态类型如 表 1-1 所示。

表1-1 DLDP 协议状态

状态	说明
Initial（初始）	DLDP协议未使能时的初始化状态
Inactive（非活动）	DLDP协议已使能且链路down时所处的状态
Active（活动）	DLDP协议已使能且链路up，或者清空邻居表项后所处的状态
Advertisement（通告）	所有邻居双向连通（two way）或者处于Active状态超过5秒后进入的状态，这是一种没有发现单向链路时的比较稳定的状态
Probe（探测）	收到一个未知邻居的报文后进入的状态，此时将发送探测报文检测链路是否为单向链路。该状态启动Probe发送定时器，为每个需要探测的邻居启动一个Echo等待定时器
Disable（单通）	DLDP协议检测到单向链路，或在加强模式下邻居消失时的状态。此时端口不再接收和发送除DLDPDU以外的报文
DelayDown（延迟down）	当DLDP状态处于Active状态、Advertisement状态或Probe状态时，如果收到端口down事件，不会立即删除邻居、进入Inactive状态，而是先进入临时的DelayDown状态 在该状态下，DLDP邻居信息仍然被保留，同时启动DelayDown定时器

2. DLDP协议中的定时器

DLDP协议工作过程中需要使用到的定时器如 表 1-2 所示。

表1-2 DLDP 协议中的定时器

定时器	说明
Active发送定时器	发送带有RSY标记的Advertisement报文的时间间隔（缺省为1秒）：即在Active状态下每秒发送1个带RSY标记的Advertisement报文，最多会发送5个报文
Advertisement发送定时器	发送普通Advertisement报文的时间间隔（缺省为5秒）
Probe发送定时器	发送Probe报文的时间间隔（固定为1秒）：即在Probe状态下每秒发送一次、每次发送1个Probe报文，最多会发送10个报文
Echo等待定时器	在DLDP切换到Probe状态或启动加强探测时启用Echo等待定时器（超时时间为10秒）。若该定时器超时后仍未收到来自邻居应答本端的Echo报文，则将本端的状态置为单通，并将状态机转到Disable状态，发送Disable报文，并根据用户配置的DLDP Down模式，提示用户手动或者自动关闭本端口，同时删除该邻居表项
邻居老化定时器	每个新邻居加入时都要建立邻居表项，并启用相应的邻居老化定时器，当收到邻居报文时刷新相应的邻居表项和邻居老化定时器： • 在普通模式下，若该定时器超时后仍未收到邻居发来的报文，则发送带有 RSY 标记的 Advertisement 报文，同时删除该邻居表项 • 在加强模式下，若该定时器超时后仍未收到邻居发来的报文，则启用加强定时器 邻居老化定时器的超时时间是Advertisement定时器的3倍

定时器	说明
加强定时器	在加强模式下，若邻居老化定时器超时后仍未收到邻居发来的报文，则对该邻居启用加强定时器（超时时间为1秒）。在该定时器启用之后，每秒向邻居发送1个Probe报文，会连续发送8次
DelayDown定时器	当DLDP处于Active、Advertisement或Probe状态时，如果收到端口down事件，不会立即删除邻居并进入Inactive状态，而是先进入DelayDown状态并启动DelayDown定时器（此时仍保留DLDP邻居信息，且只响应端口up事件）： • 若该定时器超时后仍未收到端口 up 事件，则删除 DLDP 邻居信息并进入 Inactive 状态 • 若该定时器超时前收到了端口 up 事件，则返回到原来的 DLDP 状态
恢复探测定时器	恢复探测定时器的时间间隔为2秒：即处于Disable状态下的端口每2秒发送1个RecoverProbe报文，用于检测单向链路是否恢复

3. DLDP协议工作模式

DLDP 协议有如下两种工作模式：

- 普通模式：在该模式下，一旦有邻居老化定时器超时，只是在删除该邻居表项的同时发送一个带 RSY 标记的 Advertisement 报文。
- 加强模式：在该模式下，一旦有邻居老化定时器超时，则启动加强定时器，每 1 秒发送 1 个 Probe 报文（连续发送 8 个）用于主动探测该邻居，如果 Echo 等待定时器超时仍未收到来自邻居的 Echo 报文，则进入 Disable 状态。

DLDP协议的工作模式与邻居表项老化之间的对应关系如 表 1-3 所示。

表1-3 DLDP 协议工作模式与邻居表项老化关系表

DLDP 协议工作模式	邻居老化后是否主动探测该邻居的存在	邻居老化定时器超时后是否立即删除该邻居表项	邻居老化定时器超时后是否启用加强定时器
普通模式	否	是	否
加强模式	是	否	是（加强定时器超时后开始发送Probe报文）

DLDP协议的工作模式与其可识别的单向链路类型之间的对应关系如 表 1-4 所示。

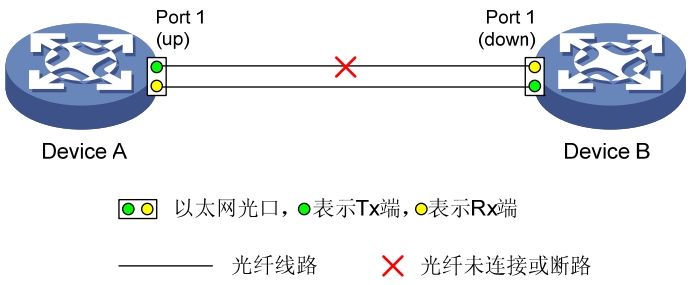
表1-4 单向链路类型与 DLDP 协议工作模式关系表

单向链路类型	光纤是否可能出现此种情况	铜质双绞线是否可能出现此种情况	DLDP 协议工作在哪种模式下可识别
交叉连接	是	否	在普通模式和加强模式下均可识别
某一方向线路未连接或断路	是	是	在普通模式下不可识别，在加强模式下可识别。此时，Rx端有信号的端口将处于Disable状态，而Rx端没有信号的端口将处于Inactive状态

加强模式的目的在于检测网络黑洞，防止出现一端up而另一端down的情况。有些设备在端口配置为强制速率和强制全双工模式时，会出现如 图 1-2 所示的情况（以光纤连接为例）：当DLDP协议未使能时，尽管Device B的端口虽已down掉，但由于普通的链路层协议无法检测出来，因此Device A

的端口还处于up状态；而当DLDP协议已使能并工作在加强模式下时，Device A的端口在邻居老化定时器超时后会进行主动探测，如果在Echo等待定时器超时仍未收到Device B的端口返回的Echo报文，Device A的端口就将进入Disable状态。此时由于Device B的端口的物理状态为down，因此其DLDP状态为Inactive。

图1-2 加强模式应用场景示意图



4. DLDP认证方式

为了防止网络攻击和恶意探测，用户可以在端口上配置 DLDP 报文认证方式，分为下列三种：

- 不认证方式：发送 DLDP 报文一方将认证字字段置为全 0，认证类型字段置为 0；接收 DLDP 报文一方要将报文中的认证字和认证类型同本端配置进行比较，如果不一致，则丢弃报文。
- 简单认证方式：发送 DLDP 报文一方将认证字字段置为用户配置的密码，认证类型字段置为 1；接收 DLDP 报文一方要将报文中的认证字和认证类型同本端配置进行比较，如果不一致，则丢弃报文。
- MD5 认证方式：发送 DLDP 报文一方将认证字字段置为用户配置的密码采用 MD5 算法加密后的摘要，认证类型字段置为 2；接收 DLDP 报文一方要将报文中的认证字和认证类型分别与本端配置的密码用 MD5 算法加密后的摘要以及本端的认证类型进行比较，如果不一致，则丢弃报文。

5. DLDP工作过程

(1) 如果使能了DLDP的端口链路状态为up，DLDP会向对端发送DLDP报文，同时分析处理对端设备发送过来的DLDP报文。如 表 1-5 所示，DLDP在不同状态下发送的报文类型不同。

表1-5 不同 DLDP 状态下发送的报文类型

DLDP 状态	发送的报文类型
Active	带有RSY标记的Advertisement报文
Advertisement	普通Advertisement报文
Probe	Probe报文
Disable	发送一个Disable报文，随后发送RecoverProbe报文

说明

当从其它 DLDP 状态(不包括 Inactive 和 Disable)迁移到 Initial 状态时，DLDP 将发送 Flush 报文。

(2) DLDP 会对收到的报文进行如下分析和处理：

- 在认证方式下，对报文进行认证。如果报文通不过认证，丢弃该报文。
- 报文中的通告时间间隔如果和本设备的不一致，丢弃该报文。
- 对DLDP报文进行相应的处理，具体处理方式如 表 1-6 所示。

表1-6 DLDP 对收到报文的处理方式

收到的报文类型	处理方式
带RSY标记的Advertisement报文	取出报文中的邻居信息后，判断邻居表中是否有该邻居的表项： • 如果没有，则为该邻居建立表项、启动该表项的老化定时器，并将 DLDP 状态切换到 Probe 状态 • 如果有，则刷新该表项的老化定时器，并将 DLDP 状态切换到 Probe 状态
普通Advertisement报文	取出报文中的邻居信息后，判断邻居表中是否有该邻居的表项： • 如果没有，则为该邻居建立表项、启动该表项的老化定时器，并将 DLDP 状态切换到 Probe 状态 • 如果有，则刷新该表项的老化定时器
Flush报文	判断本端口是否处于Disable状态： • 如果是，则不需进行任何处理 • 如果不是，且邻居表中有该邻居的表项，则删除该表项
Probe报文	取出报文中的邻居信息后，判断邻居表中是否有该邻居的表项： • 如果没有，则为该邻居建立表项，将 DLDP 状态切换到 Probe 状态，并向对端回复 Echo 报文 • 如果有，则刷新该表项的老化定时器，并向对端回复 Echo 报文
Echo报文	取出报文中的邻居信息后，判断邻居表中是否有该邻居的表项： • 如果没有，则为该邻居建立表项、启动该表项的老化定时器，并将 DLDP 状态切换到 Probe 状态 • 如果有，则检查报文中携带的邻居信息是否与本机相同：若不同则丢弃该报文；否则将该邻居标记为双向连通，如果所有邻居的状态都是双向连通，则将 DLDP 状态由 Probe 切换到 Advertisement，同时将 Echo 定时器置为无效
Disable报文	判断本端口是否处于Disable状态： • 如果是，则不需进行任何处理 • 如果不是，则先将对应邻居的状态置为单通，再判断各邻居的状态：若所有邻居的状态都为单通，则本端口进入 Disable 状态；若存在状态未知的邻居，则待其状态确定后再进行处理；若存在处于双通状态的邻居，则删除所有处于单通状态的邻居
RecoverProbe报文	判断本端口是否处于Disable或Advertisement状态： • 如果都不是，则不需进行任何处理 • 如果是其中之一，则回应 RecoverEcho 报文
RecoverEcho报文	判断本端口是否处于Disable状态： • 如果不是，则不需进行任何处理 • 如果是，则检查该报文中携带的邻居信息是否与本端口的相同，若相同则本端口转换为 Active 状态

收到的报文类型	处理方式
LinkDown报文	判断本端口是否工作在加强模式下： • 如果不是，则不需进行任何处理 • 如果是，且本端口尚未处于 Disable 状态，则先将对应邻居的状态置为单通，再判断各邻居的状态：若所有邻居的状态都为单通，则本端口进入 Disable 状态；若存在状态未知的邻居，则待其状态确定后再进行处理；若存在处于双通状态的邻居，则删除所有处于单通状态的邻居

(3) 如果 DLDP 没有收到邻居的 Echo 应答报文，会做如下处理：

表1-7 未收到邻居 Echo 应答报文时的处理过程

未收到邻居 Echo 报文	处理过程
普通模式下，Echo等待定时器超时还未收到	先将对应邻居的状态置为单通，再判断各邻居的状态： • 如果所有邻居的状态都为单通，则删除全部邻居，将 DLDP 状态切换到 Disable，输出日志和跟踪信息，向邻居发送 Disable 报文，并根据用户配置的 DLDP Down 模式手动或自动关闭本端端口 • 如果存在状态未知的邻居，则待其状态确定后再进行处理 • 如果存在处于双通状态的邻居，则删除所有处于单通状态的邻居
加强模式下，由于加强探测启动的Echo定时器超时还未收到	

6. 链路自动恢复机制

如果端口的关闭模式被设置为系统自动关闭，当 DLDP 检测到单向链路时，把端口的状态设置为 DLDP Down，处于此状态的端口不会转发业务报文，也不能收发除 DLDPDU 之外的任何协议报文。

处于 DLDP Down 状态端口能在链路恢复之时，从 DLDP Down 状态中恢复。DLDP Down 状态下的端口仍然会周期性的发送链路恢复探测报文（RecoverProbe 报文），一旦收到正确的恢复回应报文（RecoverEcho 报文），则说明单向链路已经变为双向链路，DLDP 将此端口重新 up。其具体过程如下：

处于 DLDP Down 状态的端口向外每 2 秒发送一次 RecoverProbe 报文。报文中只携带本端口的信息。对端如果收到该报文，则以 RecoverEcho 报文作为应答。一旦本端收到 RecoverEcho 报文，检查 RecoverEcho 报文中携带的邻居信息是否和本端口信息相同。如果相同，则认为本端口和该邻居之间已经恢复双向连通，则端口从 Disable 状态迁移到 Active 状态，开始重新建立邻居关系。

链路恢复报文只在处于 DLDP Down 状态的端口上发送和处理。如果端口被用户使用 **shutdown** 命令手工关闭，则自动恢复机制不能生效。

7. DLDP邻居状态

DLDP邻居的状态有三种，如 表 1-8 所示。

表1-8 DLDP 邻居状态

状态类型	说明
未知状态	刚建立这个邻居，目前正在对邻居进行探测，还没有收到邻居回应时的邻居状态。该状态只在探测（Probe）过程中存在，探测结束后就转为双通或者单通
双通状态	收到邻居回应后的邻居状态，表示目前处于正常的双向连通状态，该状态可以长期稳定存在
单通状态	检测到单通链路时的邻居状态，此时会将该邻居删除

1.2 DLDP配置任务简介

表1-9 DLDP 配置任务简介

配置任务	说明	详细配置
配置端口的双工模式和速率	必选	1.3
使能DLDP功能	必选	1.4
配置DLDP的工作模式	可选	1.5
配置发送Advertisement报文的时间间隔	可选	1.6
配置DelayDown定时器的超时时间	可选	1.7
配置发现单向链路后端口的关闭模式	可选	1.8
配置DLDP报文的认证方式	可选	1.9
重置DLDP的状态	可选	1.10

注意

- 为确保 DLDP 能够正常工作，要保证两端设备的 DLDP 功能都处于使能状态，且发送 Advertisement 报文的时间间隔、DLDP 报文的认证方式及口令都相同。
- DLDP 不会处理任何 LACP（Link Aggregation Control Protocol，链路聚合控制协议）事件，DLDP 会将端口聚合组中的每条链路都视为独立的链路进行处理。
- 请确保两端设备上运行的 DLDP 版本一致，否则 DLDP 的运行可能出现问题。

1.3 配置端口的双工模式和速率

为了使 DLDP 能够正常工作，需要将两端端口的双工模式都配置为全双工模式，速率都配置为相同的强制速率。

说明

有关 **duplex** 和 **speed** 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“以太网端口”。

1.4 使能DLDP功能

要启用 DLDP 功能，必须先全局使能 DLDP 功能，再在端口上使能 DLDP 功能。

表1-10 使能 DLDP 功能

操作		命令	说明
进入系统视图		**system-view**	-
全局使能DLDP功能		**dldp enable**	必选 缺省情况下，全局的DLDP功能处于关闭状态
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 二层以太网端口视图下的配置只对当前端口生效，端口组视图下的配置对当前端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
使能端口的DLDP功能		**dldp enable**	必选 缺省情况下，端口上的DLDP功能处于关闭状态

说明

- 只能在以太网端口（包括光口和电口）上使能 DLDP 功能。
- DLDP 功能只有在物理链路连通后才会起作用，因此在使能 DLDP 之前，请连接好光纤或铜质双绞线。

1.5 配置DLDP的工作模式

DLDP 的工作模式分为普通模式和加强模式两种：在普通模式下，DLDP 协议在老化邻居表项时不会主动探测邻居是否存在；而在加强模式下，DLDP 协议在老化邻居表项时会主动探测邻居是否存在。

表1-11 配置 DLDP 的工作模式

操作	命令	说明
进入系统视图	**system-view**	-
配置DLDP的工作模式	**dldp work-mode** { **enhance** | **normal** }	可选 缺省情况下，DLDP的工作模式为普通模式

1.6 配置发送Advertisement报文的时间间隔

通过合理调整发送 Advertisement 报文的时间间隔，可使 DLDP 在不同的网络环境下都能够及时发现单向链路。通常情况下，发送 Advertisement 报文的时间间隔应小于 STP 收敛时间的三分之一：若此间隔太长，可能导致在 DLDP 关闭单向链路前出现 STP 环路，由于设备需较长时间才能发现单向链路，因此会造成较多错误流量的转发；若此间隔太短，则会增加网络的流量。建议采用缺省值。

表1-12 配置发送 Advertisement 报文的时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
配置发送Advertisement报文的时间间隔	**dldp interval** *time*	可选 缺省情况下，发送Advertisement报文的时间间隔为5秒

说明

- 本配置将应用于所有使能了 DLDP 功能的端口上。
- 请确保通过光纤/铜质双绞线连接的两台设备上发送 Advertisement 报文的时间间隔相同，否则 DLDP 将不能正常工作。

1.7 配置DelayDown定时器的超时时间

有些端口在 Tx 端发生故障时会引起 Rx 端光信号的抖动（表现为该端口 down 后随即又 up），为避免在这种情况下直接进入 Inactive 状态而清除了邻居信息，因此先进入 DelayDown 状态，同时启动 DelayDown 定时器，待该定时器超时后再进入 Inactive 状态。如果在 DelayDown 定时器超时之前端口 up 了，则返回之前的 DLDP 状态。

表1-13 配置 DelayDown 定时器的超时时间

操作	命令	说明
进入系统视图	**system-view**	-
配置DelayDown定时器的超时时间	**dldp delaydown-timer** *time*	可选 缺省情况下，DelayDown定时器的超时时间为1秒

说明

本配置将应用于所有使能了 DLDP 功能的端口上。

1.8 配置发现单向链路后端口的关闭模式

当 DLDP 检测到单向链路时，可以采用两种方式关闭单通的端口：

- 手动模式：其目的是为了避免网络性能差时，DLDP 协议检测到单通就立即自动关闭端口，从而造成业务报文不能收发，是针对这种误判较多的情形所采取的一种折中方案。它仅依靠 DLDP 协议检测单向链路，端口的关闭由网络管理员手动完成。在该模式下，当 DLDP 检测到单通时，DLDP 状态机只输出 Log 和 Trap 信息，建议此时用户使用 **shutdown** 命令手工关闭此端口，然后 DLDP 状态机才会迁移到 Disable 状态。

- 自动模式：在该模式下，当 DLDP 协议检测到单通时，除了 DLDP 状态机迁移到 Disable 状态并输出 Log 和 Trap 信息外，还会自动将端口的状态设置为 DLDP Down。

表1-14 配置发现单向链路后端口的关闭模式

操作	命令	说明
进入系统视图	**system-view**	-
配置发现单向链路后端口的关闭模式	**dldp unidirectional-shutdown** { **auto** | **manual** }	可选 缺省情况下，发现单向链路后端口的关闭模式为自动模式

说明

- 如果欲在端口上配置 OAM 远端环回，建议先将发现单向链路后端口的关闭模式配置为手动模式，否则 DLDP 收到了由本端口发出的报文后会认为出现单向链路而自动关闭端口，从而导致 OAM 远端环回失效。
- 当设备业务量较大或 CPU 利用率较高时，可能会出现 DLDP 误报的情况。此时建议将发现单向链路后端口的关闭模式配置为手动模式，以减小由于 DLDP 误报而造成的影响。

1.9 配置DLDP报文的认证方式

通过配置适当的 DLDP 报文的认证方式，可以防止网络攻击和恶意探测。DLDP 报文的认证方式可分为三种：不认证、简单认证和 MD5 认证。

表1-15 配置 DLDP 报文的认证方式

操作	命令	说明
进入系统视图	**system-view**	-
配置当前设备与邻居设备端口间的DLDP认证方式	**dldp authentication-mode** { **none** | { **md5** | **simple** } *password* }	必选 缺省情况下，当前设备与邻居设备端口间的DLDP认证方式为**none**，即不认证

注意

请确保两台设备间相连端口上配置的 DLDP 认证方式和密码相同，否则 DLDP 将不能正常工作。

1.10 重置DLDP的状态

DLDP 协议发现单向链路后，端口进入 Disable 状态。此时需要根据用户选择的端口关闭模式，提示用户关闭端口或自动将端口的状态设为 DLDP Down。如果用户需要该端口重新探测，可以通过下列方式重置端口的 DLDP 状态：

- 对于使用 **shutdown** 命令手工关闭的端口，用户需要手动输入 **undo shutdown** 命令来恢复对端口的探测。
- 对于系统自动设置为 DLDP Down 的端口，用户可以等待 DLDP 通过链路自动恢复机制，发现邻居恢复双通后启用端口；也可以使用 **dldp reset** 命令来手工恢复，从而使处于 DLDP Down 状态下的端口重新进行单向链路的检测。

恢复后的端口状态与端口的物理状态有关：如果端口的物理状态为 down，则端口的 DLDP 状态变为 Inactive；如果端口的物理状态为 up，则端口的 DLDP 状态变为 Active。

重置 DLDP 的状态可以在全局进行或在端口上进行：

1. 全局重置DLDP的状态

在系统视图下全局重置 DLDP 的状态，将对设备上所有端口的 DLDP 状态进行重置。

表1-16 全局重置 DLDP 的状态

操作	命令	说明
进入系统视图	**system-view**	-
全局重置DLDP的状态	**dldp reset**	必选

2. 在端口上重置DLDP的状态

在端口上重置 DLDP 的状态，只能对当前端口或端口组中所有端口的 DLDP 状态进行重置。

表1-17 在端口上重置 DLDP 的状态

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 二层以太网端口视图下的配置只对当前端口生效，端口组视图下的配置对当前端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
重置DLDP的状态		**dldp reset**	必选

1.11 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1-18 DLDP 显示和维护

操作	命令
显示端口的DLDP配置信息	**display dldp** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口的DLDP报文统计信息	**display dldp statistics** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
清除端口的DLDP报文统计信息	**reset dldp statistics** [*interface-type interface-number*]

1.12 DLDP典型配置举例

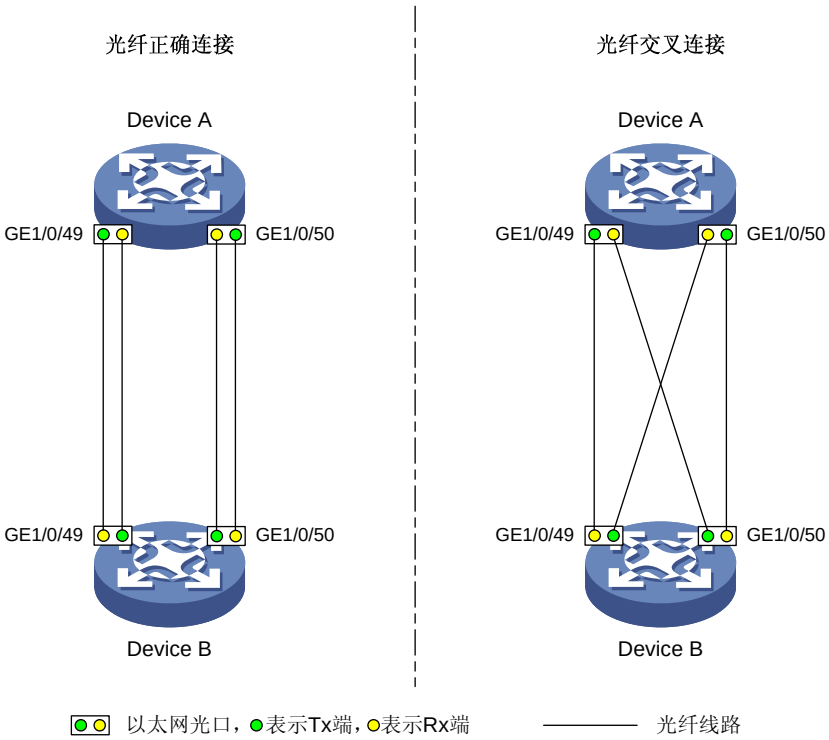
1.12.1 自动关闭单向链路配置举例

1. 组网需求

- Device A 和 Device B 各自的端口 Gigabitethernet1/0/49 和 Gigabitethernet1/0/50 之间分别通过一对光纤进行连接。
- 要求通过配置，使 DLDP 检测到单向链路故障后自动关闭故障端口，并在网络管理员排除故障后，故障端口能够自动恢复。

2. 组网图

图1-3 自动关闭单向链路配置组网图



3. 配置步骤

(1) 配置 Device A

全局使能 DLDP 功能。

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

在端口 GigabitEthernet1/0/49 上配置双工模式为全双工、端口速率为 1000Mbps，并使能 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/49
[DeviceA-GigabitEthernet1/0/49] duplex full
[DeviceA-GigabitEthernet1/0/49] speed 1000
[DeviceA-GigabitEthernet1/0/49] dldp enable
[DeviceA-GigabitEthernet1/0/49] quit
```

在端口 GigabitEthernet1/0/50 上配置双工模式为全双工、端口速率为 1000Mbps，并使能 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] duplex full
[DeviceA-GigabitEthernet1/0/50] speed 1000
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit
```

配置 DLDP 的工作模式为加强模式。

```
[DeviceA] dldp work-mode enhance
```

配置发现单向链路后端口的关闭模式为自动模式。

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

(2) 配置 Device B

全局使能 DLDP 功能。

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

在端口 GigabitEthernet1/0/49 上配置双工模式为全双工、端口速率为 1000Mbps，并使能 DLDP 功能。

```
[DeviceB] interface gigabitethernet 1/0/49
[DeviceB-GigabitEthernet1/0/49] duplex full
[DeviceB-GigabitEthernet1/0/49] speed 1000
[DeviceB-GigabitEthernet1/0/49] dldp enable
[DeviceB-GigabitEthernet1/0/49] quit
```

在端口 GigabitEthernet1/0/50 上配置双工模式为全双工、端口速率为 1000Mbps，并使能 DLDP 功能。

```
[DeviceB] interface gigabitethernet 1/0/50
[DeviceB-GigabitEthernet1/0/50] duplex full
[DeviceB-GigabitEthernet1/0/50] speed 1000
[DeviceB-GigabitEthernet1/0/50] dldp enable
[DeviceB-GigabitEthernet1/0/50] quit
```

配置 DLDP 的工作模式为加强模式。

```
[DeviceB] dldp work-mode enhance
```

配置发现单向链路后端口的关闭模式为自动模式。

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

(3) 检验配置效果

配置完成后，通过使用 **display dldp** 命令可以查看端口上的 DLDP 配置信息。例如：

查看 Device A 所有使能了 DLDP 的端口上的 DLDP 配置信息。

```
[DeviceA] display dldp
 DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : enhance
```

```
 DLDP authentication-mode : none
 DLDP unidirectional-shutdown : auto
 DLDP delaydown-timer : 1s
 The number of enabled ports is 2.

Interface GigabitEthernet1/0/49
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 59
         Neighbor state : two way
         Neighbor aged time : 11

Interface GigabitEthernet1/0/50
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 60
         Neighbor state : two way
         Neighbor aged time : 12
```

以上信息表明，端口 GigabitEthernet1/0/49 和 GigabitEthernet1/0/50 上的 DLDP 状态机均处于 Advertisement 状态，说明这两个端口所在的链路均处于双通状态。

在 Device A 上打开系统信息监视功能，并分别打开 Log 和 Trap 信息的显示功能。

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging
<DeviceA> terminal trapping
```

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

```
<DeviceA>
#Jan 12 17:36:18:798 2012 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1.1<hh3cDLDPUnidirectionalPort> : DLDP detects a unidirectional
link in port 17825792.

%Jan 12 17:36:18:799 2012 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status is
DOWN.
%Jan 12 17:36:18:799 2012 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO: -Slot=1; DLDP detects a
unidirectional link on port GigabitEthernet1/0/49. The transceiver has malfunction in the
Tx direction or cross-connected links exist between the local device and its neighbor. The
shutdown mode is AUTO. DLDP shuts down the port.
#Jan 12 17:36:20:189 2012 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1.1<hh3cDLDPUnidirectionalPort> : DLDP detects a unidirectional
link in port 17825793.

%Jan 12 17:36:20:189 2012 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status is
DOWN.
%Jan 12 17:36:20:190 2012 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO: -Slot=1; DLDP detects a
unidirectional link on port GigabitEthernet1/0/50. The transceiver has malfunction in the
```

```
Tx direction or cross-connected links exist between the local device and its neighbor. The shutdown mode is AUTO. DLDP shuts down the port.

%Jan 12 16:54:56:040 2012 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO_ENHANCE: -Slot=1; In enhanced DLDP mode, port GigabitEthernet1/0/49 cannot detect its aged-out neighbor. The transceiver has malfunction in the Tx direction or cross-connected links exist between the local device and its neighbor. The shutdown mode is AUTO. DLDP shuts down the port.
```

以上信息表明，端口 GigabitEthernet1/0/49 和 GigabitEthernet1/0/50 的链路状态均已变为 down；DLDP 在这两个端口上都检测到了单向链路，并自动关闭了这两个端口。

经过网络管理员排查，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，网络管理员将这两对光纤重新进行了正确连接，然后在 Device A 上看到如下 Log 信息：

```
<DeviceA>
%Jan 12 17:47:33:869 2012 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status is UP.
%Jan 12 17:47:35:894 2012 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status is UP.
```

以上信息表明，端口 GigabitEthernet1/0/49 和 GigabitEthernet1/0/50 的链路状态均已重新变为 up。

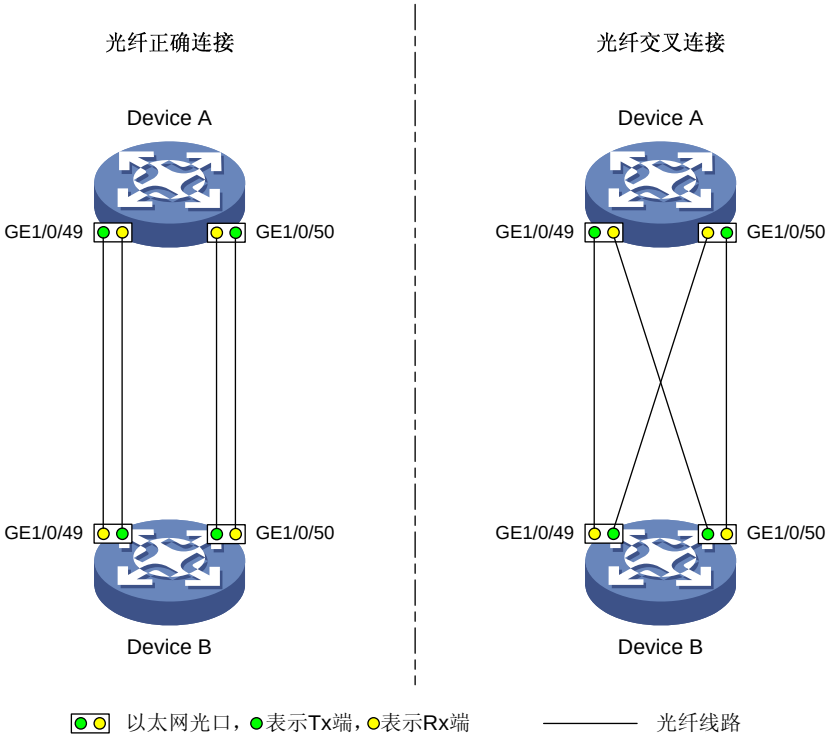
1.12.2 手动关闭单向链路配置举例

1. 组网需求

- Device A 和 Device B 各自的端口 Gigabitethernet1/0/49 和 Gigabitethernet1/0/50 之间分别通过一对光纤进行连接。
- 要求通过配置，使 DLDP 检测到单向链路故障后，提示网络管理员手工关闭故障端口。

2. 组网图

图1-4 手动关闭单向链路配置组网图



3. 配置步骤

(1) 配置 Device A

全局使能 DLDP 功能。

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

在端口 GigabitEthernet1/0/49 上配置双工模式为全双工、端口速率为 1000Mbps，并使能 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/49
[DeviceA-GigabitEthernet1/0/49] duplex full
[DeviceA-GigabitEthernet1/0/49] speed 1000
[DeviceA-GigabitEthernet1/0/49] dldp enable
[DeviceA-GigabitEthernet1/0/49] quit
```

在端口 GigabitEthernet1/0/50 上配置双工模式为全双工、端口速率为 1000Mbps，并使能 DLDP 功能。

```
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] duplex full
[DeviceA-GigabitEthernet1/0/50] speed 1000
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit
```

配置 DLDP 的工作模式为加强模式。

```
[DeviceA] dldp work-mode enhance
```

配置发现单向链路后端口的关闭模式为手动模式。

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

(2) 配置 Device B

全局使能 DLDP 功能。

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

在端口 GigabitEthernet1/0/49 上配置双工模式为全双工、端口速率为 1000Mbps，并使能 DLDP 功能。

```
[DeviceB] interface gigabitethernet 1/0/49
[DeviceB-GigabitEthernet1/0/49] duplex full
[DeviceB-GigabitEthernet1/0/49] speed 1000
[DeviceB-GigabitEthernet1/0/49] dldp enable
[DeviceB-GigabitEthernet1/0/49] quit
```

在端口 GigabitEthernet1/0/50 上配置双工模式为全双工、端口速率为 1000Mbps，并使能 DLDP 功能。

```
[DeviceB] interface gigabitethernet 1/0/50
[DeviceB-GigabitEthernet1/0/50] duplex full
[DeviceB-GigabitEthernet1/0/50] speed 1000
[DeviceB-GigabitEthernet1/0/50] dldp enable
[DeviceB-GigabitEthernet1/0/50] quit
```

配置 DLDP 的工作模式为加强模式。

```
[DeviceB] dldp work-mode enhance
```

配置发现单向链路后端口的关闭模式为手动模式。

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

(3) 检验配置效果

配置完成后，通过使用 **display dldp** 命令可以查看端口上的 DLDP 配置信息。例如：

查看 Device A 所有使能了 DLDP 的端口上的 DLDP 配置信息。

```
[DeviceA] display dldp
 DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : enhance
 DLDP authentication-mode : none
 DLDP unidirectional-shutdown : manual
 DLDP delaydown-timer : 1s
 The number of enabled ports is 2.

Interface GigabitEthernet1/0/49
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 59
         Neighbor state : two way
         Neighbor aged time : 11
```

```
Interface GigabitEthernet1/0/50
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 60
         Neighbor state : two way
         Neighbor aged time : 12
```

以上信息表明，端口 GigabitEthernet1/0/49 和 GigabitEthernet1/0/50 上的 DLDP 状态机均处于 Advertisement 状态，说明这两个端口所在的链路均处于双通状态。

在 Device A 上打开系统信息监视功能，并分别打开 Log 和 Trap 信息的显示功能。

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging
<DeviceA> terminal trapping
```

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

```
<DeviceA>
#Jan 12 18:10:38:481 2012 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1.1<hh3cDLDPUnidirectionalPort> : DLDP detects a unidirectional
link in port 17825792.

%Jan 12 18:10:38:481 2012 DeviceA DLDP/3/DLDP_UNIDIRECTION_MANUAL: -Slot=1; DLDP detects a
unidirectional link on port GigabitEthernet1/0/49. The transceiver has malfunction in the
Tx direction or cross-connected links exist between the local device and its neighbor. The
shutdown mode is MANUAL. The port needs to be shut down by the user.
#Jan 12 18:10:38:618 2012 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1.1<hh3cDLDPUnidirectionalPort> : DLDP detects a unidirectional
link in port 17825793.

%Jan 12 18:10:38:618 2012 DeviceA DLDP/3/DLDP_UNIDIRECTION_MANUAL: -Slot=1; DLDP detects a
unidirectional link on port GigabitEthernet1/0/50. The transceiver has malfunction in the
Tx direction or cross-connected links exist between the local device and its neighbor. The
shutdown mode is MANUAL. The port needs to be shut down by the user.
```

以上信息表明，DLDP 在端口 GigabitEthernet1/0/49 和 GigabitEthernet1/0/50 上都检测到了单向链路，并提示用户手工关闭故障端口。

经过网络管理员排查，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，网络管理员将故障端口手工关闭：

在 Device A 上分别关闭端口 GigabitEthernet1/0/49 和 GigabitEthernet1/0/50，并看到如下 Log 信息：

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/49
[DeviceA-GigabitEthernet1/0/49] shutdown
%Jan 12 18:16:12:044 2012 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status is
DOWN.
[DeviceA-GigabitEthernet1/0/49] quit
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] shutdown
```

```
%Jan 12 18:18:03:583 2012 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status is DOWN.
```

以上信息表明，端口 GigabitEthernet1/0/49 和 GigabitEthernet1/0/50 的链路状态均已变为 down。

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，网络管理员将已排除故障的端口重新打开：

在 Device A 上分别打开端口 GigabitEthernet1/0/50 和 GigabitEthernet1/0/49，并看到如下 Log 信息：

```
[DeviceA-GigabitEthernet1/0/50] undo shutdown
[DeviceA-GigabitEthernet1/0/50]
%Jan 12 18:22:11:698 2012 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status is UP.
[DeviceA-GigabitEthernet1/0/50] quit
[DeviceA] interface gigabitethernet 1/0/49
[DeviceA-GigabitEthernet1/0/49] undo shutdown
[DeviceA-GigabitEthernet1/0/49]
%Jan 12 18:22:46:065 2012 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status is UP.
```

以上信息表明，端口 GigabitEthernet1/0/49 和 GigabitEthernet1/0/50 的链路状态均已重新变为 up。

1.13 常见配置错误举例

1.13.1 DLDP检测不出单向链路

1. 故障现象

Device A 和 Device B 通过两对光纤相连，并在这两台设备上都使能了 DLDP；假设 Device A 与 Device B 间出现了光纤交叉连接的情况，但 DLDP 并未检测出链路单通，且四个端口均处于 Advertisement 状态。

2. 故障分析

如下两个原因均会导致上述情况的出现：

- Device A 和 Device B 上配置的发送 Advertisement 报文的时间间隔不一致。
- Device A 和 Device B 上配置的 DLDP 报文认证方式或认证口令不一致。

3. 故障排除

在 Device A 和 Device B 上配置相同的发送 Advertisement 报文的时间间隔、DLDP 报文的认证方式及口令。

目 录

1 RRPP配置

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。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路，具备较高的收敛速度。

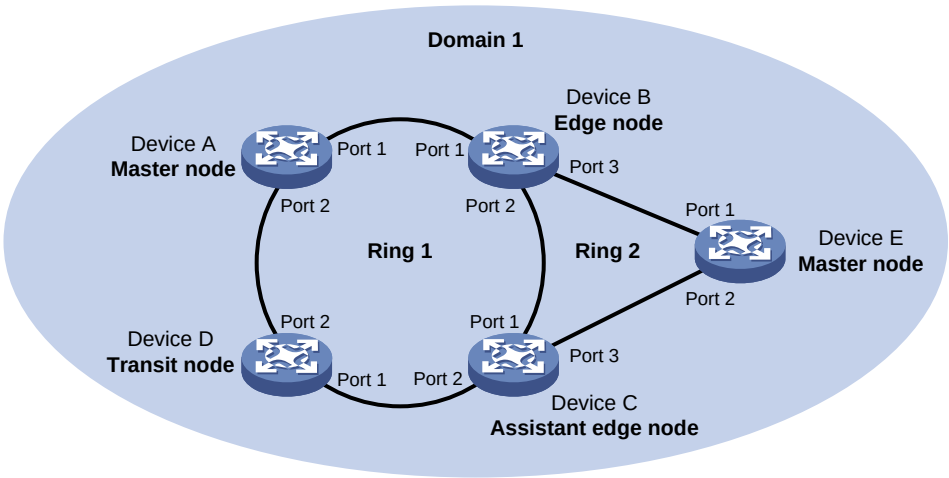
1.1.1 RRPP产生背景

城域网和企业网大多采用环网来构建以提供高可靠性，但环上任意一个节点发生故障都会影响业务。环网采用的技术一般是 RPR 或以太网环。RPR 需要专用硬件，因此成本较高。而以太网环技术日趋成熟且成本低廉，城域网和企业网采用以太网环的趋势越来越明显。

目前，解决二层网络环路问题的技术有 RSTP/PVST/MSTP 和 RRPP。RSTP/PVST/MSTP 应用比较成熟，但收敛时间在秒级。RRPP 是专门应用于以太网环的链路层协议，具有比 RSTP/PVST/MSTP 更快的收敛速度。并且 RRPP 的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。

1.1.2 RRPP基本概念

图1-1 RRPP 组网示意图



1. RRPP域

具有相同的域 ID 和控制 VLAN，并且相互连通的设备构成一个 RRPP 域。一个 RRPP 域具有 RRPP 主环、子环、控制 VLAN、主节点、传输节点、主端口和副端口、公共端口和边缘端口等要素。

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网络拓扑称为一个 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 域可以包含一个或多个 RRPP 环，但只能有一个主环，其它均为子环。

RRPP 环的状态有以下两种：

- 健康状态：整个环网物理链路是连通的；
- 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和数据VLAN

控制 VLAN 和数据 VLAN 是相对而言的：

(1) 控制 VLAN

控制 VLAN 用来传递 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，系统将自动把比主控制 VLAN 的 VLAN ID 值大 1 的 VLAN 作为子控制 VLAN。

同一个 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。

(2) 数据 VLAN

与控制 VLAN 相对，数据 VLAN 用来传输数据报文。数据 VLAN 中既可包含 RRPP 端口，也可包含非 RRPP 端口。

4. 节点

RRPP 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：

- 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，它在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. 主端口和副端口

主节点和传输节点各自有两个端口接入 RRPP 环，其中一个为主端口，另一个为副端口。端口的角色由用户的配置来决定。

(1) 主节点的主端口和副端口在功能上有所区别：

- 主节点的主端口用来发送探测环路的报文，副端口用来接收该报文。
- 当 RRPP 环处于健康状态时，主节点的副端口在逻辑上阻塞数据 VLAN，只允许控制 VLAN 的报文通过；当 RRPP 环处于断裂状态时，主节点的副端口将解除数据 VLAN 的阻塞状态，转发数据 VLAN 的报文。

(2) 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。

6. 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。

端口的角色由用户的配置决定。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。

7. RRPP环组

RRPP环组是为减少Edge-Hello报文（关于此报文的介绍请参见“1.1.3 RRPP协议报文”）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。

1.1.3 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	由主节点发起，对网络进行环路完整性检测
Fast-Hello	由主节点发起，对网络进行环路完整性快速检测
Link-Down	由传输节点、边缘节点或者辅助边缘节点发起，在这些节点的自身链路down时通知主节点环路消失
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更新各自MAC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更新各自MAC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

报文类型	说明
Edge-Hello	由边缘节点发起，对边缘节点与辅助边缘节点之间的主环链路进行检测
Fast-Edge-Hello	由边缘节点发起，对边缘节点与辅助边缘节点之间的主环链路进行快速检测
Major-Fault	由辅助边缘节点发起，在边缘节点和辅助边缘节点之间主环链路不连通时通知边缘节点主环链路故障

说明

子环的协议报文在主环中被当作数据报文传送，而主环的协议报文则只能在主环中传送。

1.1.4 RRPP定时器

RRPP 在检测以太网环的链路状况时，主节点根据 Hello 定时器从主端口发送 Hello 报文，根据 Fail 定时器判断副端口是否收到 Hello 报文。

- Hello 定时器：规定了主节点从主端口发送 Hello 报文的周期。
- 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。
- Fast-Hello 定时器：规定了主节点从主端口发送 Fast-Hello 报文的周期。
- Fast-Fail 定时器：规定了主节点从主端口发出 Fast-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 Fast-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。

说明

- 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 Hello 定时器和 Fail 定时器的值，以保证环网上各节点定时器的值是一致的。
- 在同一 RRPP 域中，传输节点不会通过收到的 Fast-Hello 报文来学习主节点上 Fast-Hello 定时器和 Fast-Fail 定时器的值。

1.1.5 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。

主节点周期性地从其主端口发送 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定时器超时前收到 Hello 报文，主节点将保持副端口的阻塞状态。如果环路是断裂的，主节点的副端口在定时器超时前无法收到 Hello 报文，主节点将解除数据 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 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 报文后立刻解除数据 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 表项和 ARP/ND 表项。各节点更新表项后，数据流则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。这段时间对于数据 VLAN 来说，网络有可能形成一个临时的环路，从而产生广播风暴。

为了防止产生临时环路，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. 负载分担机制

在同一个环网中，可能同时存在多个 VLAN 的数据流量，RRPP 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。

通过在同一个环网上配置多个 RRPP 域，不同 RRPP 域发送不同 VLAN（称为保护 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 1-6 所示，Domain 1 和Domain 2 都配置Ring 1 为主环，两个RRPP域所保护的VLAN不同。Device A为Domain 1 中Ring 1 的主节点；Device B为Domain 2 中Ring 1 的主节点。通过配置，可以实现不同VLAN分别阻塞不同的链路，从而实现单环的负载分担。

6. 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（若配置更多子环或多个域负载分担的情况，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。

7. 快速检测机制

RRPP 的快速收敛依赖于传输节点能够快速检测到链路故障，并立即发出通知。而在 RRPP 的实际运用中，环网中的某些设备并不支持 RRPP 协议，由于无法感知到这些设备之间的链路故障，RRPP 只能通过超时机制进行链路切换，但这将导致流量中断时间过长，不能达到用户毫秒级切换的需要。

RRPP 快速检测机制可以解决上述问题。在配置了快速检测功能之后，当 RRPP 在检测以太网环的链路状况时：

- 主节点会以 Fast-Hello 定时器周期性地从主端口发送 Fast-Hello 报文：在 Fast-Fail 定时器超时前，若其副端口收到了该报文，就认为环路处于健康状态；否则，认为环路处于断裂状态。
- 边缘节点会以最高精度定时器周期性地从公共端口发送 Fast-Edge-Hello 报文：在三倍于最高精度定时器值的时间间隔内，若辅助边缘节点没有收到该报文，就认为子环在主环上的传输通道处于断裂状态。

如 图 1-2 所示，当在Ring 1 的主节点Device A上使能了RRPP域 1 的快速检测功能后，Device A将周期性地发送Fast-Hello报文，并根据在Fast-Fail时间内是否收到Fast-Hello报文来判断环路状态，从而实现链路状态的快速检测。

说明

- 最高精度定时器就是设备所能提供的周期最短的定时器。
- 要实现快速检测功能，要求 RRPP 环的主节点、边缘节点和辅助边缘节点都支持快速检测机制。

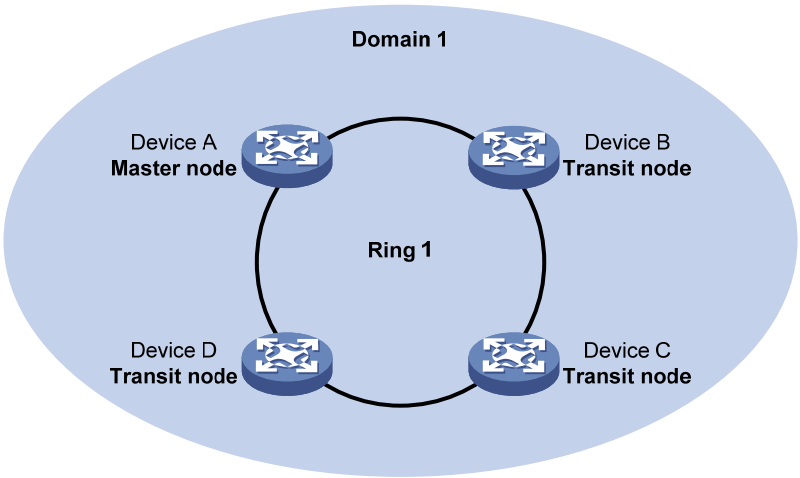
1.1.6 RRPP典型组网

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

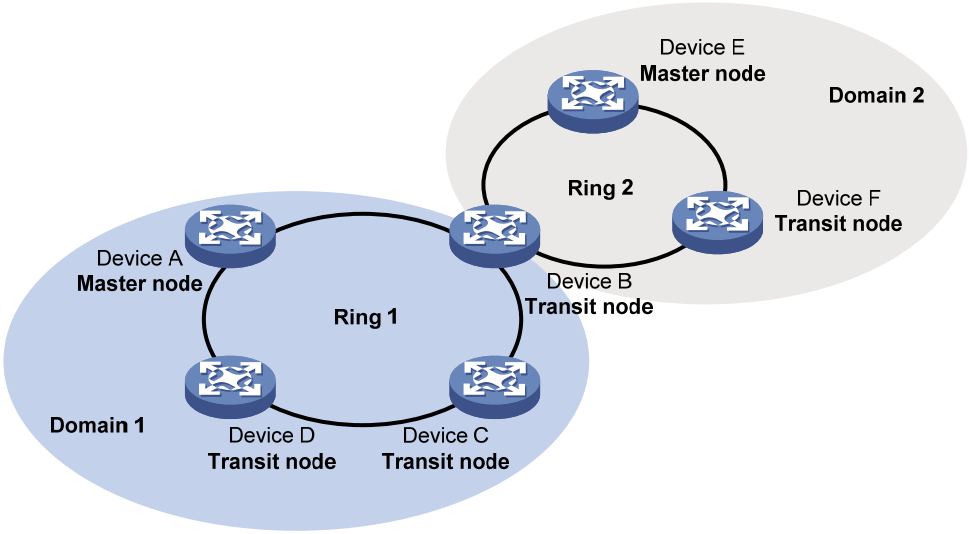
图1-2 单环示意图



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。

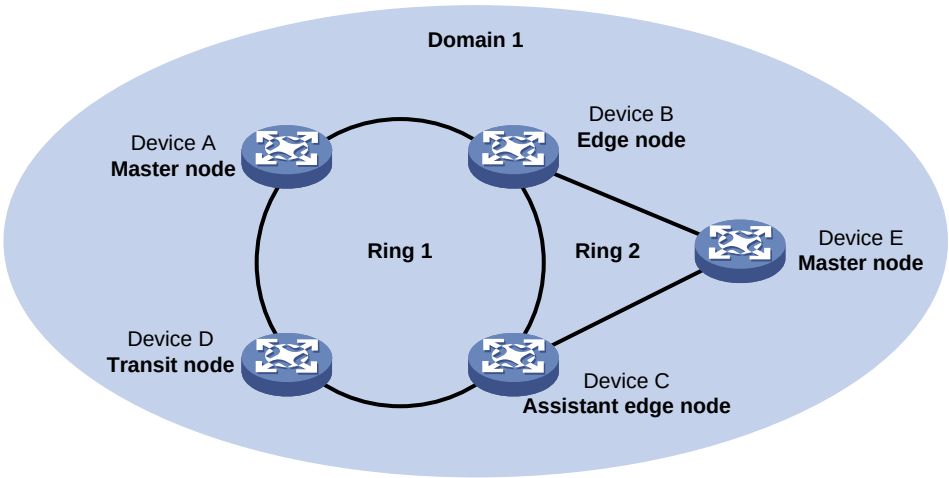
图1-3 相切环示意图



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。

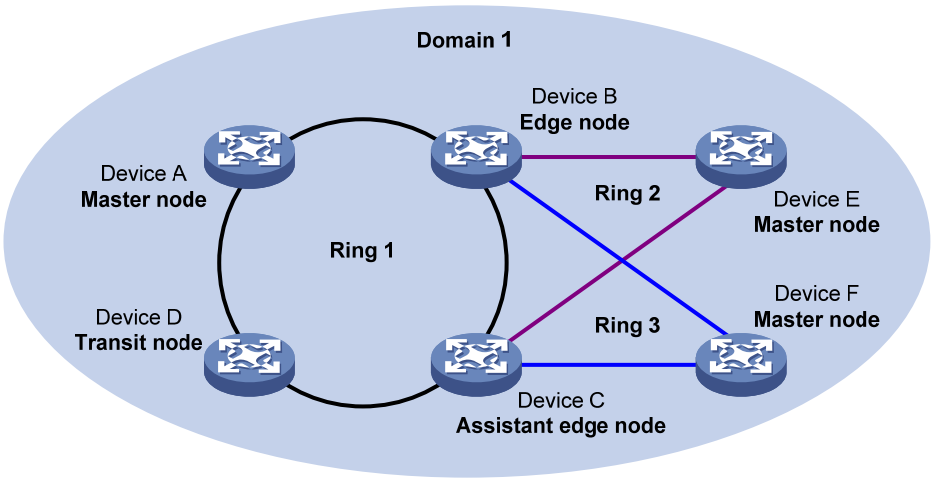
图1-4 相交环示意图



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

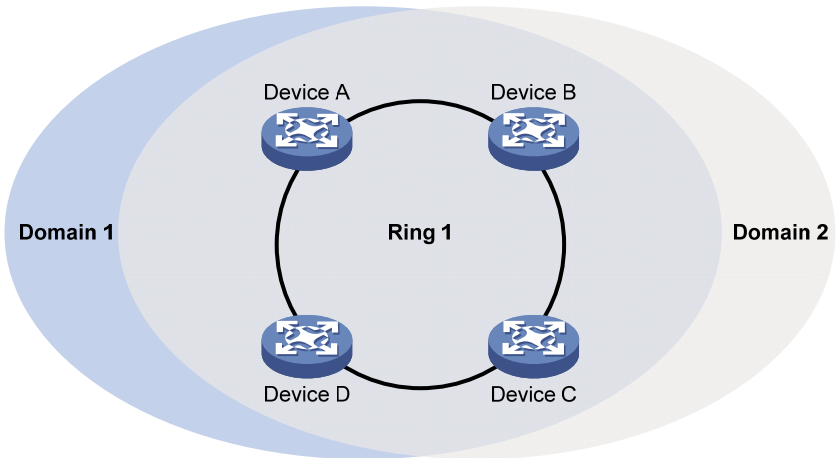


5. 单环负载分担组网

在单环网络拓扑中，可以通过配置多域实现链路的负载分担。

如 图 1-6 所示，Domain 1 和Domain 2 都配置Ring 1 为主环，两个域所保护的VLAN不同。Device A为Domain 1 中Ring 1 的主节点；Device B为Domain 2 中Ring 1 的主节点。通过配置，可以实现不同VLAN分别阻塞不同的链路，从而实现单环的负载分担。

图1-6 单环负载分担组网示意图

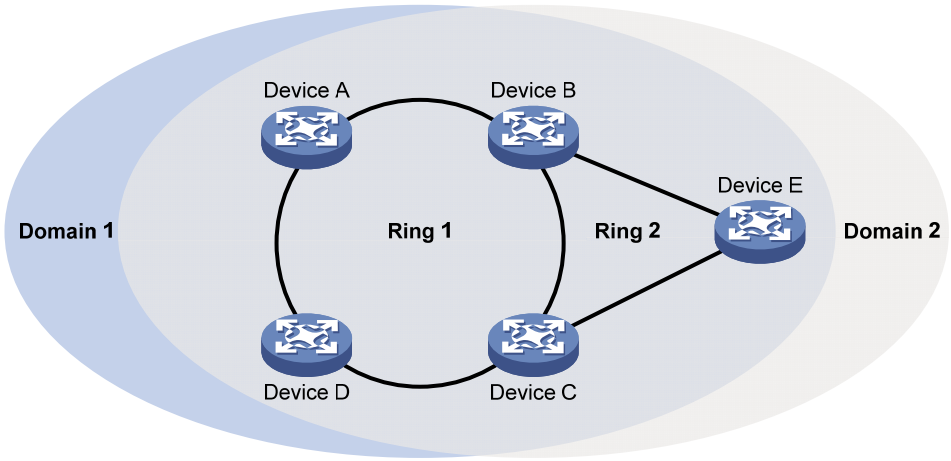


6. 相交环负载分担组网

在相交环网络拓扑中，也可以通过配置多域实现链路的负载分担。

如 图 1-7 所示，Domain 1 和Domain 2 都配置Ring 1 和Ring 2 分别为其主环和子环，两个域所保护的VLAN不同。Device A为Domain 1 中Ring 1 的主节点；Device D为Domain 2 中Ring 1 的主节点；Device E分别为Domain 1 和Domain 2 中子环Ring 2 的主节点，但阻塞的端口不同。通过配置，可以实现不同VLAN的流量分别在子环和主环通过不同的链路，从而实现相交环的负载分担。

图1-7 相交环负载分担组网示意图



1.1.7 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配置任务简介

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 和数据 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。

表1-2 RRPP 配置任务简介

配置任务		说明	详细配置
创建RRPP域		必选 请在RRPP域内的所有节点上配置	1.3
配置控制VLAN		必选 请在RRPP域内的所有节点上配置	1.4
配置保护VLAN		必选 请在RRPP域内的所有节点上配置	1.5
配置RRPP环	配置RRPP端口	必选 请在RRPP域内的所有节点上配置	1.6.1
	配置RRPP节点	必选 请在RRPP域内的所有节点上配置	1.6.2
激活RRPP域		必选 请在RRPP域内的所有节点上配置	1.7
配置RRPP定时器		可选 请在RRPP域内的主节点上配置	1.8

配置任务		说明	详细配置
配置RRPP快速检测	使能快速检测功能	可选 请在RRPP域内的主节点、边缘节点和辅助边缘节点上配置	1.9.1
	配置快速检测定时器	可选 请在RRPP域内的主节点上配置	1.9.2
配置RRPP环组		可选 请在RRPP域内的边缘节点和辅助边缘节点上配置	1.10

注意

- 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。
- 配置 RRPP 之前，需先搭建好以太网环形拓扑的组网环境。

1.3 创建RRPP域

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。

请在欲指定为 RRPP 节点的设备上进行如下配置。

表1-3 创建 RRPP 域

操作	命令	说明
进入系统视图	**system-view**	-
创建RRPP域，并进入RRPP域视图	**rrpp domain** *domain-id*	必选

1.4 配置控制VLAN

配置 RRPP 环之前必须先配置控制 VLAN，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。

请在 RRPP 域内的所有节点上进行如下配置。

表1-4 配置控制 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入RRPP域视图	**rrpp domain** *domain-id*	-
配置RRPP域的控制VLAN	**control-vlan** *vlan-id*	必选

说明

- 请勿将接入 RRPP 环的端口的缺省 VLAN 配置为控制 VLAN，而且控制 VLAN 内不能运行 QinQ（802.1Q in 802.1Q）和 VLAN 映射功能，否则 RRPP 协议报文将无法正常收发。
- 配置 RRPP 环之前允许用户删除或修改已配置好的控制 VLAN，但配置 RRPP 环之后便不再允许。控制 VLAN 只能通过 **undo control-vlan** 命令删除，而不能通过 **undo vlan** 命令删除。
- 如果要在一台未配置 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。

1.5 配置保护VLAN

配置 RRPP 环之前必须先配置保护 VLAN，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。

由于保护 VLAN 的配置是通过引用 MSTI（Multiple Spanning Tree Instance，多生成树实例）来实现的，因此在配置保护 VLAN 之前，应先配置好 MSTI 与所要保护的 VLAN 之间的映射关系（在 PVST 模式下，系统会自动将 VLAN 与 MSTI 进行映射）。有关 MSTI 和 PVST 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”。

请在 RRPP 域内的所有节点上进行如下配置。

表1-5 配置保护 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入MST域视图	**stp region-configuration**	在PVST模式下无需执行本操作
配置VLAN与MSTI的映射关系	**instance** *instance-id* **vlan** *vlan-list*	二者可选其一 缺省情况下，所有VLAN都映射到CIST（即MSTI 0）上 在PVST模式下无需执行本操作
	vlan-mapping modulo *modulo*	
激活MST域的配置	**active region-configuration**	必选 在PVST模式下无需执行本操作
显示当前生效的MST域配置信息	**display stp region-configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display**命令可以在任意视图执行 通过本操作可以查看MSTI所映射的VLAN
退回系统视图	**quit**	在PVST模式下无需执行本操作
进入RRPP域视图	**rrpp domain** *domain-id*	-
配置RRPP域的保护VLAN	**protected-vlan reference-instance** *instance-id-list*	必选 缺省情况下，RRPP域不保护任何VLAN

说明

- 在配置负载分担时，不同 RRPP 域的保护 VLAN 必须不同。
- 有关 **stp region-configuration**、**instance**、**vlan-mapping modulo**、**active region-configuration** 和 **display stp region-configuration** 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”。

1.6 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。

说明

- RRPP 端口的端口类型只能是二层以太网端口或二层聚合接口，但当上述端口是二层聚合组、业务环回组或 Smart Link 组的成员端口时除外。
- 当把二层聚合接口配置为 RRPP 端口后，仍可添加或删除对应聚合组中的成员端口。

1.6.1 配置RRPP端口

请在各节点欲接入 RRPP 环的端口上进行如下配置。

表1-6 配置 RRPP 端口

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	-
配置端口的链路类型为Trunk类型	**port link-type trunk**	必选 缺省情况下，端口的链路类型为Access类型
配置Trunk端口允许保护VLAN的报文通过	**port trunk permit vlan** { *vlan-id-list* | **all** }	必选 缺省情况下，Trunk端口只允许VLAN 1的报文通过
关闭生成树协议	**undo stp enable**	必选 缺省情况下，端口上的生成树协议处于开启状态
配置端口信认报文的802.1p优先级	**qos trust dot1p**	必选 缺省情况下，信任模式为信任接收端口的优先级。

说明

- 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。
- 有关 **port link-type trunk** 和 **port trunk permit vlan** 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”。
- 有关 **undo stp enable** 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”。
- 必须配置 RRPP 端口信认报文的 802.1p 优先级，以确保端口对 RRPP 协议报文的处理优先于数据报文。有关 **qos trust dot1p** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“优先级映射配置命令”。
- 不建议在 RRPP 端口上启用 OAM 远端环回功能，否则可能引起短时间的广播风暴。
- 接入 RRPP 环的端口不能配置为镜像组的目的端口。
- 建议在 RRPP 端口上不要配置端口的物理连接状态 up/down 抑制时间，以提高 RRPP 的拓扑变化收敛速度，具体请参见“二层技术-以太网交换命令参考/以太网端口”中的 **undo link-delay** 命令。

1.6.2 配置RRPP节点

说明

如果一台设备处于同一 RRPP 域的多个 RRPP 环上，则只能有一个主环，且该设备在其它子环上的节点角色只能是边缘节点或辅助边缘节点。

1. 配置主节点

请在欲配置为主节点的设备上进行如下配置。

表1-7 配置主节点

操作	命令	说明
进入系统视图	**system-view**	-
进入RRPP域视图	**rrpp domain** *domain-id*	-
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*	必选

2. 配置传输节点

请在欲配置为传输节点的设备上进行如下配置。

表1-8 配置传输节点

操作	命令	说明
进入系统视图	**system-view**	-
进入RRPP域视图	**rrpp domain** *domain-id*	-
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*	必选

3. 配置边缘节点

在配置边缘节点时，必须先配置主环再配置子环。

请在欲配置为边缘节点的设备上进行如下配置。

表1-9 配置边缘节点

操作	命令	说明
进入系统视图	**system-view**	-
进入RRPP域视图	**rrpp domain** *domain-id*	-
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*	必选
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*]	必选

4. 配置辅助边缘节点

在配置辅助边缘节点时，必须先配置主环再配置子环。

请在欲配置为辅助边缘节点的设备上进行如下配置。

表1-10 配置辅助边缘节点

操作	命令	说明
进入系统视图	**system-view**	-
进入RRPP域视图	**rrpp domain** *domain-id*	-
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*	必选
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*]	必选

1.7 激活RRPP域

只有当 RRPP 协议和 RRPP 环都使能之后，当前设备的 RRPP 域才能被激活。

请在 RRPP 域内的所有节点上进行如下配置。

表1-11 激活 RRPP 域

操作	命令	说明
进入系统视图	**system-view**	-
使能RRPP协议	**rrpp enable**	必选 缺省情况下，RRPP协议处于关闭状态
进入RRPP域视图	**rrpp domain** *domain-id*	-
使能RRPP环	**ring** *ring-id* **enable**	必选 缺省情况下，RRPP环处于关闭状态

注意

为避免子环的 Hello 报文在主环上形成环路，在子环的主节点上使能子环之前，请先在主环的主节点上使能主环。在边缘节点和辅助边缘节点上，需对主环和子环分别进行操作：

- 使能子环前必须先使能主环；
- 关闭主环前必须先关闭其所在 RRPP 域内的所有子环。

1.8 配置RRPP定时器

请在 RRPP 域内的主节点上进行如下配置。

表1-12 配置 RRPP 定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入RRPP域视图	**rrpp domain** *domain-id*	-
配置Hello和Fail定时器	**timer hello-timer** *hello-value* **fail-timer** *fail-value*	必选 缺省情况下，Hello定时器的值为1秒，Fail定时器的值为3秒

注意

- 配置时，应确保 Fail 定时器的值不小于 Hello 定时器取值的 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 定时器取值之差大于子环主节点上 Hello 定时器取值的 2 倍。

1.9 配置RRPP快速检测

说明

本系列交换机中 S5500-28SC-HI 和 S5500-52SC-HI 不支持 RRPP 快速检测功能。

1.9.1 使能快速检测功能

请在 RRPP 域内的主节点、边缘节点和辅助边缘节点上进行如下配置。

表1-13 使能快速检测功能

操作	命令	说明
进入系统视图	**system-view**	-
进入RRPP域视图	**rrpp domain** *domain-id*	-
使能RRPP域的快速检测功能	**fast-detection enable**	必选 缺省情况下，RRPP域的快速检测功能处于关闭状态

注意

- 在 RRPP 子环的主节点上配置快速检测功能时，需保证该环的边缘节点和辅助边缘节点也都支持快速检测功能，否则不建议配置此功能。
- 请按照先边缘节点、后辅助边缘节点的顺序来配置快速检测功能，否则辅助边缘节点可能会因收不到 Fast-Edge-Hello 报文而误认为主环故障。

1.9.2 配置快速检测定时器

请在 RRPP 域内的主节点上进行如下配置。

表1-14 配置 RRPP 快速检测

操作	命令	说明
进入系统视图	**system-view**	-
进入RRPP域视图	**rrpp domain** *domain-id*	-
配置Fast-Fail定时器	**timer fast-fail-timer** *fast-fail-value*	可选 缺省情况下，Fast-Fail定时器的值为600毫秒
配置Fast-Hello定时器	**timer fast-hello-timer** *fast-hello-value*	可选 缺省情况下，Fast-Hello定时器的值为200毫秒

注意

- 配置时，应确保 Fast-Fail 定时器的值不小于 Fast-Hello 定时器取值的 3 倍。
- 在双归属环组网中，为避免主环故障时出现临时环路，应确保子环主节点上 Fast-Fail 定时器的值不小于最高定时器精度值的 6 倍，且子环主节点与主环主节点上的 Fast-Fail 定时器取值之差大于子环主节点上 Fast-Hello 定时器取值的 2 倍。

1.10 配置RRPP环组

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。环组应分别配置在边缘节点和辅助边缘节点上，且只能配置在这两种节点上。

请在 RRPP 域内的边缘节点和辅助边缘节点上进行如下配置。

表1-15 配置 RRPP 环组

操作	命令	说明
进入系统视图	**system-view**	-
创建RRPP环组，并进入RRPP环组视图	**rrpp ring-group** *ring-group-id*	必选
将子环加入RRPP环组	**domain** *domain-id* **ring** *ring-id-list*	必选

说明

- 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。

1.11 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1-16 RRPP 显示和维护

操作	命令
显示RRPP的摘要信息	**display rrpp brief** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示RRPP环组的配置信息	**display rrpp ring-group** [*ring-group-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示RRPP的详细信息	**display rrpp verbose domain** *domain-id* [**ring** *ring-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示RRPP报文的统计信息	**display rrpp statistics domain** *domain-id* [**ring** *ring-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除RRPP报文的统计信息	**reset rrpp statistics domain** *domain-id* [**ring** *ring-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.12 RRPP典型配置举例

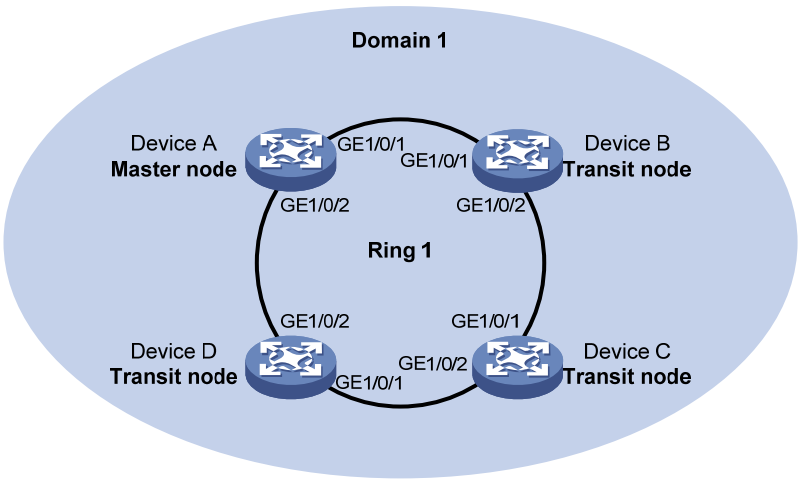
1.12.1 单环配置举例

1. 组网需求

- Device A～Device D构成RRPP域1，该域的控制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1-8 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[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，并使能该环。

```
[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
```

使能 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[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，并使能该环。

```
[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
```

使能 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。

(5) 检验配置效果

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

1.12.2 相交环配置举例

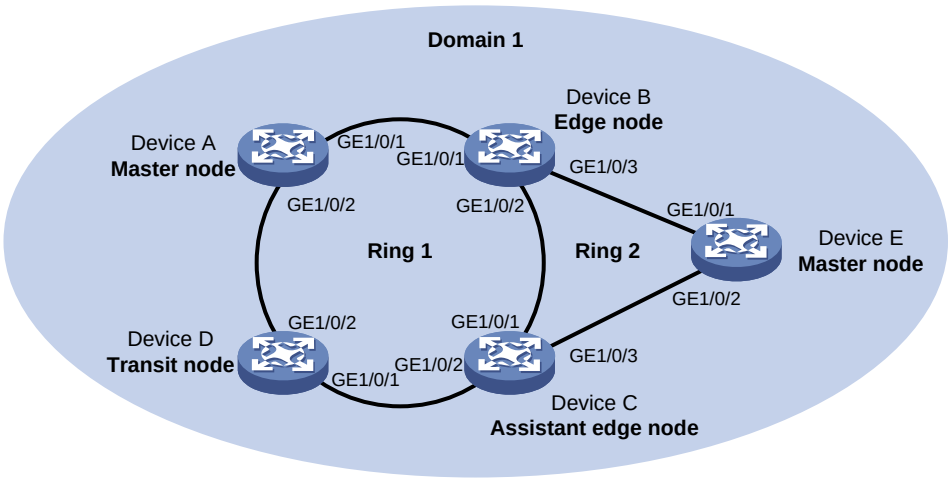
1. 组网需求

- 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1-9 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
```

```
[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，并使能该环。

```
[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
```

使能 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[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] undo link-delay
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[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，并使能该环。

```
[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，并使能该环。

```
[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 2 enable
[DeviceB-rrpp-domain1] quit
```

使能 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[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] undo link-delay
[DeviceC-GigabitEthernet1/0/3] undo stp enable
```

```
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[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，并使能该环。

```
[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，并使能该环。

```
[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
```

使能 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[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，并使能该环。

```
[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
```

使能 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[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，并使能该环。

```
[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
```

使能 RRPP 协议。

```
[DeviceE] rrpp enable
```

(6) 检验配置效果

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

1.12.3 双边双归属环配置举例

1. 组网需求

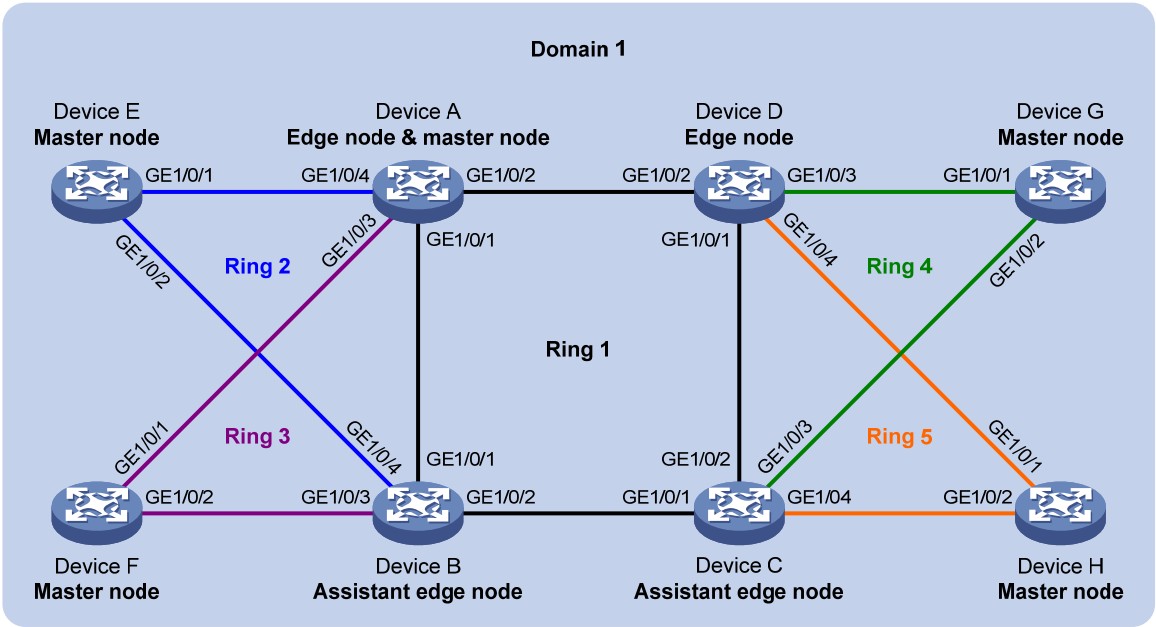
- Device A～Device H 构成 RRPP 域 1，该域的控制 VLAN 为 VLAN 4092，保护 VLAN 为 VLAN 1～30。
- Device A～Device D 构成主环 Ring 1；Device A、Device B 和 Device E 构成子环 Ring 2；Device A、Device B 和 Device F 构成子环 Ring 3；Device C、Device D 和 Device G 构成子环 Ring 4；Device C、Device D 和 Device H 构成子环 Ring 5。
- Device A、Device E、Device F、Device G 和 Device H 分别是 Ring 1～Ring 5 的主节点，其各自的 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别为主、副端口。
- Device A 同时也是其所在子环的边缘节点，GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 为边缘端口；Device D 是主环的传输节点及其所在子环的边缘节点，GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 为边缘端口；Device B 和 Device C 都是主环的传输节点及其所在子环的辅助边缘节点，其各自的 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 都为边缘端口。

注意

请对主节点的主、副端口进行合理规划，以免由于副端口阻塞数据 VLAN 而影响其它协议的正常应用。

2. 组网图

图1-10 双边双归属环配置组网图



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～GigabitEthernet1/0/4 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo link-delay
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] qos trust dot1p
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] undo link-delay
[DeviceA-GigabitEthernet1/0/4] undo stp enable
[DeviceA-GigabitEthernet1/0/4] qos trust dot1p
[DeviceA-GigabitEthernet1/0/4] port link-type trunk
[DeviceA-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/4] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 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，并使能该环。

```
[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
```

配置本设备为子环 Ring 2 的边缘节点，边缘端口为 GigabitEthernet1/0/4，并使能该环。

```
[DeviceA-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceA-rrpp-domain1] ring 2 enable
```

配置本设备为子环 Ring 3 的边缘节点，边缘端口为 GigabitEthernet1/0/3，并使能该环。

```
[DeviceA-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceA-rrpp-domain1] ring 3 enable
[DeviceA-rrpp-domain1] quit
```

使能 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～GigabitEthernet1/0/4 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
```

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[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] undo link-delay
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo link-delay
[DeviceB-GigabitEthernet1/0/4] undo stp enable
[DeviceB-GigabitEthernet1/0/4] qos trust dot1p
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/4] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 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，并使能该环。

```
[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 的辅助边缘节点，边缘端口为 GigabitEthernet1/0/4，并使能该环。

```
[DeviceB-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceB-rrpp-domain1] ring 2 enable
```

配置本设备为子环 Ring 3 的辅助边缘节点，边缘端口为 GigabitEthernet1/0/3，并使能该环。

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

使能 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～GigabitEthernet1/0/4 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[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] undo link-delay
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/3] quit
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] undo link-delay
[DeviceC-GigabitEthernet1/0/4] undo stp enable
[DeviceC-GigabitEthernet1/0/4] qos trust dot1p
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/4] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 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，并使能该环。

```
[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 4 的辅助边缘节点，边缘端口为 GigabitEthernet1/0/3，并使能该环。
```
[DeviceC-rrpp-domain1] ring 4 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 4 enable
```
配置本设备为子环 Ring 5 的辅助边缘节点，边缘端口为 GigabitEthernet1/0/4，并使能该环。
```
[DeviceC-rrpp-domain1] ring 5 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 5 enable
[DeviceC-rrpp-domain1] quit
```
使能 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～GigabitEthernet1/0/4 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[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] undo link-delay
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] qos trust dot1p
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/3] quit
[DeviceD] interface gigabitethernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] undo link-delay
[DeviceD-GigabitEthernet1/0/4] undo stp enable
[DeviceD-GigabitEthernet1/0/4] qos trust dot1p
[DeviceD-GigabitEthernet1/0/4] port link-type trunk
```

```
[DeviceD-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/4] quit
```

创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 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，并使能该环。

```
[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
```

配置本设备为子环 Ring 4 的边缘节点，边缘端口为 GigabitEthernet1/0/3，并使能该环。

```
[DeviceD-rrpp-domain1] ring 4 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceD-rrpp-domain1] ring 4 enable
```

配置本设备为子环 Ring 5 的边缘节点，边缘端口为 GigabitEthernet1/0/4，并使能该环。

```
[DeviceD-rrpp-domain1] ring 5 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceD-rrpp-domain1] ring 5 enable
[DeviceD-rrpp-domain1] quit
```

使能 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[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，并使能该环。

```
[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
```

使能 RRPP 协议。

```
[DeviceE] rrpp 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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] qos trust dot1p
[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 RRPP 域 1，将 VLAN 4092 配置为该域的控制 VLAN，并将 MSTI 1 所映射的 VLAN 配置为该域的保护 VLAN。

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

配置本设备为子环 Ring 3 的主节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceF] rrpp enable
```

(7) 配置 Device G

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

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

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1～30 通过。

```
[DeviceG] interface gigabitethernet 1/0/1
[DeviceG-GigabitEthernet1/0/1] undo link-delay
[DeviceG-GigabitEthernet1/0/1] undo stp enable
[DeviceG-GigabitEthernet1/0/1] qos trust dot1p
[DeviceG-GigabitEthernet1/0/1] port link-type trunk
[DeviceG-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceG-GigabitEthernet1/0/1] quit
[DeviceG] interface gigabitethernet 1/0/2
[DeviceG-GigabitEthernet1/0/2] undo link-delay
[DeviceG-GigabitEthernet1/0/2] undo stp enable
[DeviceG-GigabitEthernet1/0/2] qos trust dot1p
[DeviceG-GigabitEthernet1/0/2] port link-type trunk
[DeviceG-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceG-GigabitEthernet1/0/2] quit
```

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

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

配置本设备为子环 Ring 4 的主节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[DeviceG-rrpp-domain1] ring 4 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceG-rrpp-domain1] ring 4 enable
[DeviceG-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceG] rrpp enable
```

(8) 配置 Device H

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

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

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1～30 通过。

```
[DeviceH] interface gigabitethernet 1/0/1
[DeviceH-GigabitEthernet1/0/1] undo link-delay
[DeviceH-GigabitEthernet1/0/1] undo stp enable
[DeviceH-GigabitEthernet1/0/1] qos trust dot1p
[DeviceH-GigabitEthernet1/0/1] port link-type trunk
[DeviceH-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceH-GigabitEthernet1/0/1] quit
[DeviceH] interface gigabitethernet 1/0/2
[DeviceH-GigabitEthernet1/0/2] undo link-delay
[DeviceH-GigabitEthernet1/0/2] undo stp enable
[DeviceH-GigabitEthernet1/0/2] qos trust dot1p
[DeviceH-GigabitEthernet1/0/2] port link-type trunk
[DeviceH-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceH-GigabitEthernet1/0/2] quit
```

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

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

配置本设备为子环 Ring 5 的主节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[DeviceH-rrpp-domain1] ring 5 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceH-rrpp-domain1] ring 5 enable
[DeviceH-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceH] rrpp enable
```

(9) 检验配置效果

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

1.12.4 相交环负载分担配置举例

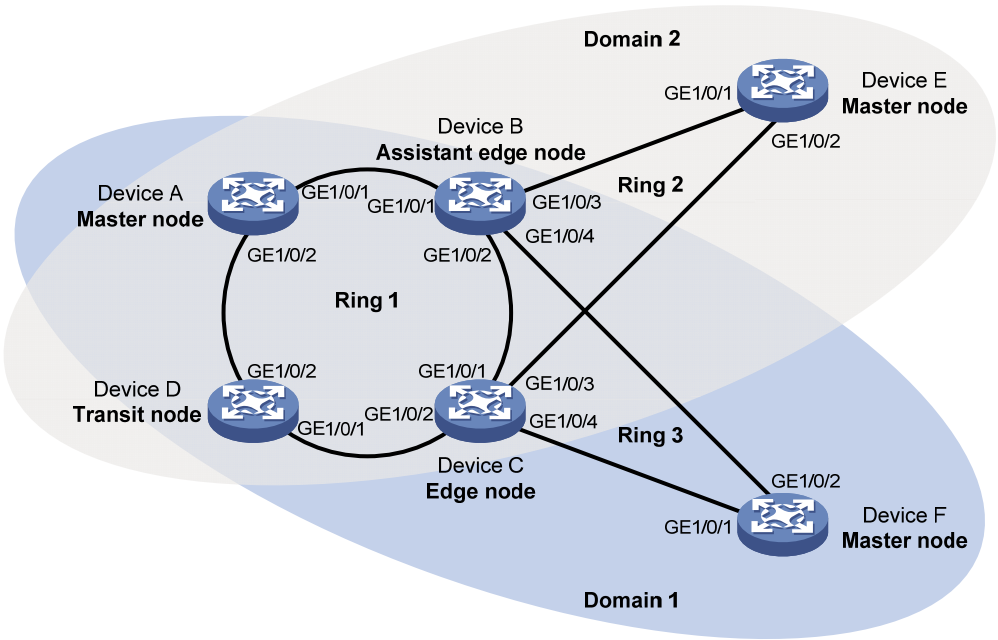
1. 组网需求

- Device A、Device B、Device C、Device D 和 Device F 构成 RRPP 域 1，该域的控制 VLAN 为 VLAN 100。在该域中，Device A 和 Device D 分别为主环 Ring 1 的主节点和传输节点，Device F、Device C 和 Device B 分别为子环 Ring 3 的主节点、边缘节点和辅助边缘节点。

- Device A、Device B、Device C、Device D 和 Device E 构成 RRPP 域 2，该域的控制 VLAN 为 VLAN 105。在该域中，Device A 和 Device D 分别为主环 Ring 1 的主节点和传输节点，Device E、Device C 和 Device B 分别为子环 Ring 2 的主节点、边缘节点和辅助边缘节点。
- RRPP 域 1 的保护 VLAN 为 VLAN 1，RRPP 域 2 的保护 VLAN 为 VLAN 2。由此可以按照 VLAN 在主环上实现负载分担。
- 由于子环 Ring 2 和 Ring 3 的边缘节点和辅助边缘节点的配置相同，且其对应的主环链路也相同，因此可将子环 Ring 2 和 Ring 3 加入环组，以减少 Edge-Hello 报文的收发数量。

2. 组网图

图1-11 相交环负载分担配置组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 1 和 2，将 VLAN 1 和 2 分别映射到 MSTI 1 和 2 上，并激活 MST 域的配置。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 2
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1
[DeviceA-mst-region] instance 2 vlan 2
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1 和 2 通过。

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

```
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 2
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 2
[DeviceA-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 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 100
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

在 RRPP 域 1 内配置本设备为主环 Ring 1 的主节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[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
```

创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTI 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceA] rrpp domain 2
[DeviceA-rrpp-domain2] control-vlan 105
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
```

在 RRPP 域 2 内配置本设备为主环 Ring 1 的主节点，主端口为 GigabitEthernet1/0/2，副端口为 GigabitEthernet1/0/1，并使能该环。

```
[DeviceA-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceA] rrpp enable
```

(2) 配置 Device B

创建 VLAN 1 和 2，将 VLAN 1 和 2 分别映射到 MSTI 1 和 2 上，并激活 MST 域的配置。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 2
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1
[DeviceB-mst-region] instance 2 vlan 2
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1 和 2 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo link-delay
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 2
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 2
[DeviceB-GigabitEthernet1/0/2] quit
```

在端口 GigabitEthernet1/0/3 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 2 通过。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo link-delay
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/3] quit
```

在端口 GigabitEthernet1/0/4 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1 通过。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo link-delay
[DeviceB-GigabitEthernet1/0/4] undo stp enable
[DeviceB-GigabitEthernet1/0/4] qos trust dot1p
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/4] quit
```

创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 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 100
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

在 RRPP 域 1 内配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[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
```

在 RRPP 域 1 内配置本设备为子环 Ring 3 的辅助边缘节点，边缘端口为 GigabitEthernet1/0/4，并使能该环。

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTI 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceB] rrpp domain 2
[DeviceB-rrpp-domain2] control-vlan 105
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

在 RRPP 域 2 内配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[DeviceB-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain2] ring 1 enable
```

在 RRPP 域 2 内配置本设备为子环 Ring 2 的辅助边缘节点，边缘端口为 GigabitEthernet1/0/3，并使能该环。

```
[DeviceB-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain2] ring 2 enable
[DeviceB-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceB] rrpp enable
```

(3) 配置 Device C

创建 VLAN 1 和 2，将 VLAN 1 和 2 分别映射到 MSTI 1 和 2 上，并激活 MST 域的配置。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 2
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1
[DeviceC-mst-region] instance 2 vlan 2
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1 和 2 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo link-delay
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 2
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo link-delay
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
```

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

在端口 GigabitEthernet1/0/3 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口，禁止 VLAN 1 通过、允许 VLAN 2 通过，并配置其缺省 VLAN 为 VLAN 2。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo link-delay
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/3] port trunk pvid vlan 2
[DeviceC-GigabitEthernet1/0/3] quit
```

在端口 GigabitEthernet1/0/4 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1 通过。

```
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] undo link-delay
[DeviceC-GigabitEthernet1/0/4] undo stp enable
[DeviceC-GigabitEthernet1/0/4] qos trust dot1p
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/4] quit
```

创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 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 100
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

在 RRPP 域 1 内配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[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
```

在 RRPP 域 1 内配置本设备为子环 Ring 3 的边缘节点，边缘端口为 GigabitEthernet1/0/4，并使能该环。

```
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 3 enable
[DeviceC-rrpp-domain1] quit
```

创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTI 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceC] rrpp domain 2
[DeviceC-rrpp-domain2] control-vlan 105
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

在 RRPP 域 2 内配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain2] ring 1 enable
```

在 RRPP 域 2 内配置本设备为子环 Ring 2 的边缘节点，边缘端口为 GigabitEthernet1/0/3，并使能该环。

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain2] ring 2 enable
[DeviceC-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceC] rrpp enable
```

(4) 配置 Device D

创建 VLAN 1 和 2，将 VLAN 1 和 2 分别映射到 MSTI 1 和 2 上，并激活 MST 域的配置。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 2
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1
[DeviceD-mst-region] instance 2 vlan 2
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1 和 2 通过。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo link-delay
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 2
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo link-delay
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 2
[DeviceD-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 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 100
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

在 RRPP 域 1 内配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[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
```

创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTI 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceD] rrpp domain 2
[DeviceD-rrpp-domain2] control-vlan 105
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

在 RRPP 域 2 内配置本设备为主环 Ring 1 的传输节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceD] rrpp enable
```

(5) 配置 Device E

创建 VLAN 2，将 VLAN 2 映射到 MSTI 2 上，并激活 MST 域的配置。

```
<DeviceE> system-view
[DeviceE] vlan 2
[DeviceE-vlan2] quit
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 2 vlan 2
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，将端口配置为 Trunk 端口，禁止 VLAN 1 通过、允许 VLAN 2 通过，并配置其缺省 VLAN 为 VLAN 2。

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo link-delay
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceE-GigabitEthernet1/0/1] port trunk pvid vlan 2
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo link-delay
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceE-GigabitEthernet1/0/2] port trunk pvid vlan 2
[DeviceE-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTI 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceE] rrpp domain 2
[DeviceE-rrpp-domain2] control-vlan 105
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2
```

在 RRPP 域 2 内配置本设备为子环 Ring 2 的主节点，主端口为 GigabitEthernet1/0/2，副端口为 GigabitEthernet1/0/1，并使能该环。

```
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 1
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceE] rrpp enable
```

(6) 配置 Device F

创建 VLAN 1，将 VLAN 1 映射到 MSTI 1 上，并激活 MST 域的配置。

```
<DeviceF> system-view
[DeviceF] vlan 1
[DeviceF-vlan1] quit
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 1
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，将端口配置为 Trunk 端口且允许 VLAN 1 通过。

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo link-delay
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] qos trust dot1p
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/1] quit
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] undo link-delay
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] qos trust dot1p
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/2] quit
```

创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 VLAN，并将 MSTI 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[DeviceF] rrpp domain 1
[DeviceF-rrpp-domain1] control-vlan 100
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

在 RRPP 域 1 内配置本设备为子环 Ring 3 的主节点，主端口为 GigabitEthernet1/0/1，副端口为 GigabitEthernet1/0/2，并使能该环。

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

```
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceF] rrpp enable
```

(7) 完成以上配置后，在 Device B 和 Device C 上分别配置 RRPP 环组

在 Device B 上创建 RRPP 环组 1，并为其配置子环。

```
[DeviceB] rrpp ring-group 1
[DeviceB-rrpp-ring-group1] domain 2 ring 2
[DeviceB-rrpp-ring-group1] domain 1 ring 3
```

在 Device C 上创建 RRPP 环组 1，并为其配置子环。

```
[DeviceC] rrpp ring-group 1
[DeviceC-rrpp-ring-group1] domain 2 ring 2
[DeviceC-rrpp-ring-group1] domain 1 ring 3
```

(8) 检验配置效果

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

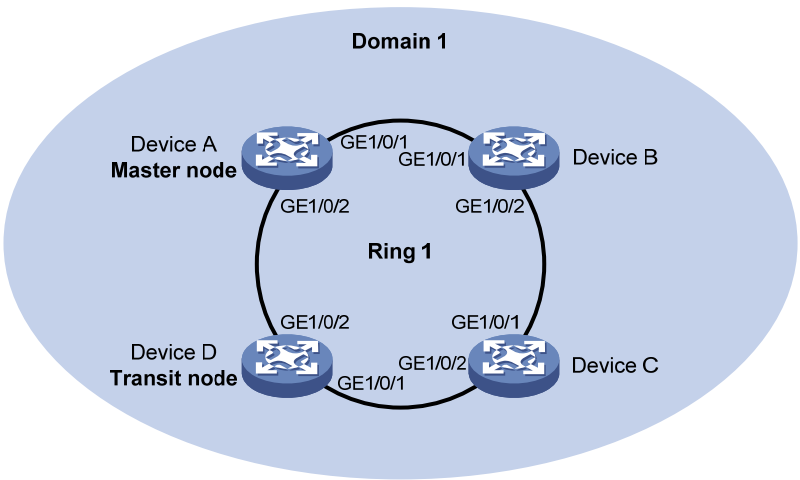
1.12.5 快速检测配置举例

1. 组网需求

- Device A～Device D 构成 RRPP 域 1，该域的控制 VLAN 为 VLAN 4092，保护 VLAN 为 VLAN 1～30。
- Device A 为主节点，支持 RRPP 快速检测功能；Device D 为传输节点；Device B 和 Device C 则为不支持 RRPP 协议的设备。
- 由于 Device B 和 Device C 都不支持 RRPP 协议，它们之间的链路出现故障时无法及时通知主节点，因此要求通过配置 RRPP 快速检测功能，使 Device B 和 Device C 之间的链路出现故障后环网也能够快速切换。

2. 组网图

图1-12 快速检测配置组网图



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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[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，并使能该环。

```
[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
```

使能快速检测功能，并配置 Fast-Fail 定时器和 Fast-Hello 定时器的值分别为 300 毫秒和 100 毫秒。请注意在配置时，确保 Fast-Fail 定时器的值不小于 Fast-Hello 定时器取值的 3 倍，否则将无法配置成功。

```
[DeviceA-rrpp-domain1] fast-detection enable
[DeviceA-rrpp-domain1] timer fast-hello-timer 100
[DeviceA-rrpp-domain1] timer fast-fail-timer 300
[DeviceA-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceA] rrpp enable
```

(2) 配置 Device B

创建 VLAN 4092 和 4093。

```
<DeviceB> system-view
[DeviceB] vlan 4092 to 4093
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1～30、4092 和 4093 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo link-delay
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30 4092 4093
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30 4092 4093
```

(3) 配置 Device C

创建 VLAN 4092 和 4093。

```
<DeviceC> system-view
[DeviceC] vlan 4092 to 4093
```

分别在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，并将端口配置为 Trunk 端口且允许 VLAN 1～30、4092 和 4093 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo link-delay
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30 4092 4093
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo link-delay
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30 4092 4093
```

(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 上取消物理连接状态 up/down 抑制时间配置，关闭生成树协议，配置端口信任报文的 802.1p 优先级，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] undo link-delay
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[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] undo link-delay
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[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，并使能该环。

```
[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
```

使能 RRPP 协议。

```
[DeviceD] rrpp enable
```

(5) 检验配置效果

配置完成后，用户可以使用 **display** 命令查看 Device A 和 Device D 上 RRPP 的配置和运行情况。

1.13 常见配置错误举例

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

3. 故障排除

- 使用 **display rrpp brief** 命令查看各个节点是否都配置并使能了 RRPP 协议。如果没有则使用 **rrpp enable** 和 **ring enable** 命令使能 RRPP 协议和 RRPP 环。
- 使用 **display rrpp brief** 命令查看各节点的域 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** 命令查看各个节点各个环的端口链路状态。
- 在各个节点上使用 **debugging rrpp** 命令查看端口是否有 Hello 报文的接收或发送，如果没有则说明有报文丢失。

目 录

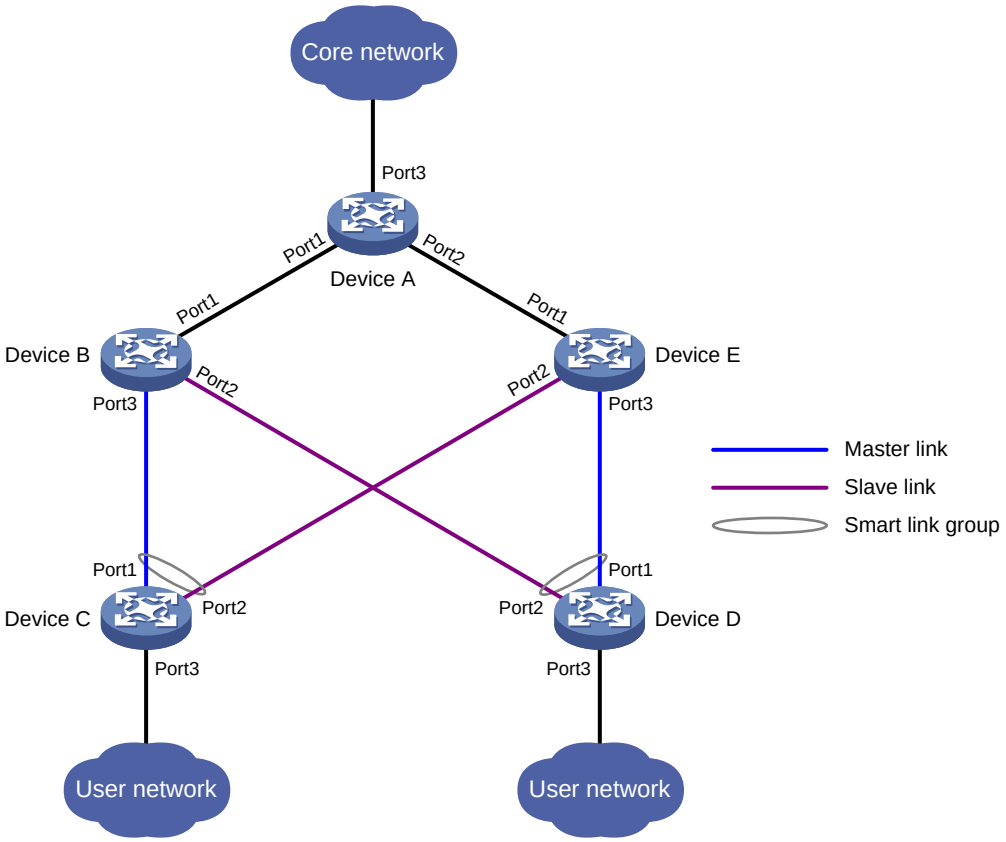
1 Smart Link配置

1.1 Smart Link简介

1.1.1 Smart Link产生背景

当下游设备连接到上游设备时，使用单上行方式容易出现单点故障，造成业务中断。因此通常采用双上行方式，即将一台下游设备同时连接到两台上游设备，以最大限度地避免单点故障，提高网络可靠性，如 图 1-1 所示。

图1-1 Smart Link 应用场景示意图



双上行组网虽然能提高网络可靠性，但又引入了环路问题。通常可通过 STP（Spanning Tree Protocol，生成树协议）或 RRPP（Rapid Ring Protection Protocol，快速环网保护协议）来消除环路，但 STP 在收敛速度上只能达到秒级，不适用于对收敛时间有很高要求的用户，而 RRPP 尽管在收敛速度上能达到要求，但组网配置的复杂度较高，主要适用于较复杂的环形组网。

说明

有关 STP 和 RRPP 的详细介绍，请分别参见“二层技术-以太网交换配置指导”中的“生成树”和“可靠性配置指导”中的“RRPP”。

为了满足用户对链路快速收敛的要求，同时又能简化配置，我们针对双上行组网提出了 Smart Link 解决方案，实现了主备链路的冗余备份，并在主用链路发生故障后使流量能够迅速切换到备用链路上，因此具备较高的收敛速度。Smart Link 的主要特点如下：

- 专用于双上行组网。
- 收敛速度快（达到亚秒级）。
- 配置简单，便于用户操作。

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端口，其中一个为主端口，另一个为从端口。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和Device D各自的端口Port1 和Port2 分别组成了一个Smart Link组，其中Port1 处于转发状态，而Port2 处于待命状态。

2. 主端口/从端口

主端口和从端口是 Smart Link 组中的两个端口角色。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。但是，主端口并不一直处于转发状态，而从端口也并不一直处于待命状态。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各自的端口Port1 为主端口，Port2 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，原有的转发表项将不适用于新的拓扑网络，需要网络中的所有设备进行 MAC 地址转发表项和 ARP/ND 表项的更新。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 是 Smart Link 组控制其转发状态的用户数据 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内广播发送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. 链路备份机制

在 图 1-1 所示的组网中，Device C的端口Port1 所在的链路是主链路，Port2 所在的链路是从链路。正常情况下，Port1 处于转发状态，Port2 处于待命状态。当主链路出现故障时，Port1 将自动阻塞并切换到待命状态，Port2 将切换到转发状态。

说明

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. 网络拓扑变更机制

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，需要提供一种 MAC 地址转发表项和 ARP/ND 表项的更新机制。目前更新机制有以下两种：

- 自动通过流量刷新 MAC 地址转发表项和 ARP/ND 表项。此方式适用于与不支持 Smart Link 功能的设备（包括其他厂商设备）对接的情况，需要有上行流量触发。
- 由 Smart Link 设备从新的链路上发送 Flush 报文。此方式需要上行的设备都能够识别 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. 角色抢占机制

在 图 1-1 所示的组网中，Device C的端口Port1 所在的链路是主链路，Port2 所在的链路是从链路。当主链路出现故障时，Port1 将自动阻塞并切换到待命状态，Port2 则从待命状态切换到转发状态。当主链路恢复后：

- 在非角色抢占模式下，Port1 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。
- 在角色抢占模式下，Port2 将自动阻塞并切换到待命状态，而 Port1 则切换回转发状态。

4. 负载分担机制

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），且该端口在不同 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。

1.1.4 Smart Link联动机制

1. 端口检测联动机制

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。

说明

有关 Monitor Link 的详细介绍和配置，请参见“可靠性配置指导”中的“Monitor Link”。

2. 链路检测联动机制

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 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。

当端口与 CFD（Connectivity Fault Detection，连通错误检测）的 CC（Continuity Check，连续性检测）机制联动时，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 CC 事件。

说明

有关 CFD CC 机制的详细介绍和配置，请参见“可靠性配置指导”中的“CFD”。

1.2 Smart Link配置任务简介

表1-1 Smart Link 配置任务简介

配置任务		说明	详细配置
配置Smart Link设备	配置Smart Link组的保护VLAN	必选	1.3.2
	配置Smart Link组的成员端口	必选	1.3.3
	配置抢占功能	可选	1.3.4
	使能发送Flush报文功能	可选	1.3.5
	配置与CFD CC机制联动	可选	1.3.6
配置相关设备	使能接收Flush报文功能	必选	1.4.2

说明

- Smart Link设备是指支持Smart Link功能、且配置了Smart Link组和从指定控制VLAN发送Flush报文功能的设备，如 图 1-1 中的Device C和Device D。
- 相关设备是指支持Smart Link功能、在实际应用中为配合Smart Link设备而需使能从指定控制VLAN接收Flush报文功能的设备，如 图 1-1 中的Device A、Device B和Device E。

1.3 配置Smart Link设备

1.3.1 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）：

- 需先手工关闭该端口，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；
- 需先关闭该端口的生成树协议和 RRPP 功能，并确保该端口不是聚合成员端口或业务环回组成员端口。

注意

在关闭生成树协议之后到 Smart Link 开始工作之前，网络中可能会形成环路。

1.3.2 配置Smart Link组的保护VLAN

由于保护 VLAN 的配置是通过引用 MSTI 来实现的，因此在配置保护 VLAN 之前，应先配置好 MSTI 与所要保护的 VLAN 之间的映射关系（在 PVST 模式下，系统会自动将 VLAN 与 MSTI 进行映射）。有关 MSTI 和 PVST 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”。

表1-2 配置 Smart Link 组的保护 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入MST域视图	**stp region-configuration**	在PVST模式下无需执行本操作
配置VLAN映射表	**instance** *instance-id* **vlan** *vlan-list*	二者可选其一 缺省情况下，所有VLAN都映射到CIST（即MSTI 0）上 在PVST模式下无需执行本操作
	vlan-mapping modulo *modulo*	
激活MST域的配置	**active region-configuration**	必选 在PVST模式下无需执行本操作
显示当前生效的MST域配置信息	**display stp region-configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display**命令可以在任意视图执行 通过本操作可以查看MSTI所映射的VLAN
退回系统视图	**quit**	在PVST模式下无需执行本操作
创建Smart Link组，并进入Smart Link组视图	**smart-link group** *group-id*	-
配置Smart Link组的保护VLAN	**protected-vlan reference-instance** *instance-id-list*	必选 缺省情况下，Smart Link组不保护任何VLAN

说明

有关 **stp region-configuration**、**instance**、**vlan-mapping modulo**、**active region-configuration** 和 **display stp region-configuration** 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”。

1.3.3 配置Smart Link组的成员端口

可在 Smart Link 组视图或端口视图下配置 Smart Link 组的成员端口，各视图下的配置效果相同。

1. Smart Link组视图下的配置

表1-3 Smart Link 组视图下配置 Smart Link 组的成员端口

操作	命令	说明
进入系统视图	**system-view**	-
进入Smart Link组视图	**smart-link group** *group-id*	-
配置Smart Link组的成员端口	**port** *interface-type interface-number* { **master** | **slave** }	必选

2. 端口视图下的配置

表1-4 端口视图下配置 Smart Link 组的成员端口

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	-
配置Smart Link组的成员端口	**port smart-link group** *group-id* { **master** | **slave** }	必选

1.3.4 配置Smart Link抢占功能

表1-5 配置 Smart Link 抢占功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Smart Link组视图	**smart-link group** *group-id*	-
配置抢占模式为角色抢占模式	**preemption mode role**	必选 缺省情况下，设备工作在非抢占模式
配置抢占延时	**preemption delay** *delay-time*	可选 缺省情况下，抢占延时为1秒

注意

抢占延时在配置抢占模式为角色抢占模式之后才会生效。

1.3.5 使能发送Flush报文功能

表1-6 使能发送 Flush 报文功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Smart Link组视图	**smart-link group** *group-id*	-
使能发送Flush报文的功能	**flush enable** [**control-vlan** *vlan-id*]	可选 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

注意

- 需要为不同的 Smart Link 组配置不同的控制 VLAN。
- 用户需要配置保证控制 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。

1.3.6 配置端口与CFD CC机制联动

表1-7 配置 Smart Link 设备

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置Smart Link组的成员端口与CFD CC机制联动	**port smart-link group** *group-id* **track cfd cc**	可选 缺省情况下，Smart Link组的端口与CFD CC机制未联动

注意

在配置 Smart Link 组的成员端口与 CFD CC 机制联动时，该端口所在 Smart Link 组的控制 VLAN 必须与 CFD CC 的检测 VLAN 相一致。

1.4 配置相关设备

1.4.1 配置准备

配置相关设备时，建议在其与 Smart Link 组的成员端口直接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。

1.4.2 使能接收Flush报文功能

并非需要在相关设备的所有端口上都使能从指定控制 VLAN 接收 Flush 报文功能，只有那些处于从 Smart Link 设备到其目的设备主、从链路上的端口才需进行此配置。

表1-8 使能接收 Flush 报文功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	-
使能接收Flush报文的功能	**smart-link flush enable** [**control-vlan** *vlan-id-list*]	必选 缺省情况下，接收Flush报文的功能处于关闭状态

注意

- 相关设备的所有控制 VLAN 上都应使能接收 Flush 报文的功能。
- 如果不配置处理 Flush 报文的控制 VLAN，设备将对收到的 Flush 报文不做处理直接转发。
- 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，若二者不相同，相关设备将对接收到的 Flush 报文不做处理直接转发。
- 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。
- 用户需要配置保证控制 VLAN 存在，且使能接收 Flush 报文功能的端口允许控制 VLAN 的报文通过。

1.5 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1-9 Smart Link 显示和维护

操作	命令
查看Smart Link组的信息	**display smart-link group** { *group-id* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
查看设备收到的Flush报文信息	**display smart-link flush** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除Flush报文的统计信息	**reset smart-link statistics**

1.6 Smart Link典型配置举例

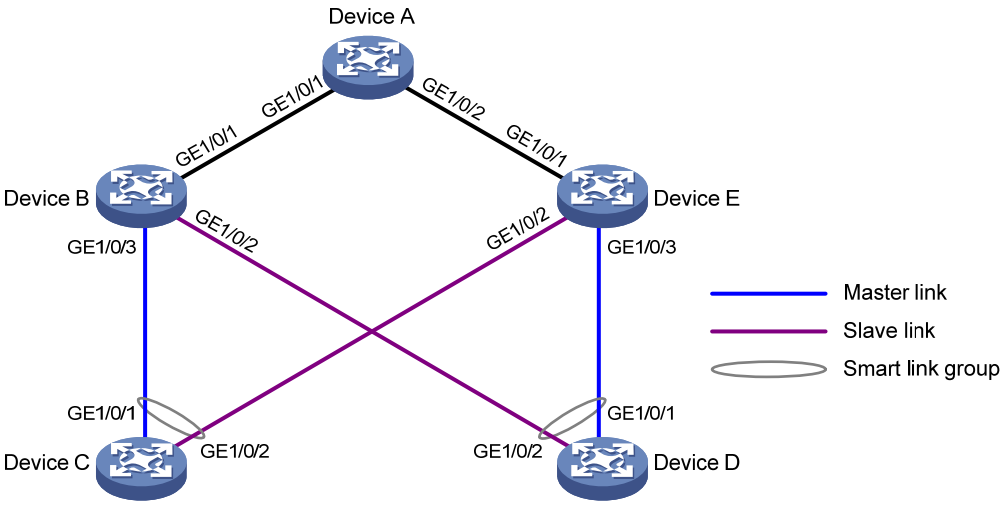
1.6.1 单Smart Link组配置举例

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 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
```

在 Smart Link 组 1 中使能发送 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 master
[DeviceD-smlk-group1] port gigabitethernet 1/0/2 slave
```

在 Smart Link 组 1 中使能发送 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，在该端口上使能接收 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，使能接收 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，使能接收 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，在该端口上使能接收 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，使能接收 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，使能接收 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，在这些端口上使能接收 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
```

(6) 检验配置效果

通过使用 **display smart-link group** 命令可以查看设备上 Smart Link 组的信息：

查看 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
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  ACTVIE   5           16:37:20 2012/01/12

 GigabitEthernet1/0/2      SLAVE   STANDBY  1           17:45:20 2012/01/12
```

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：

查看 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             : 16:25:21 2012/01/12
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

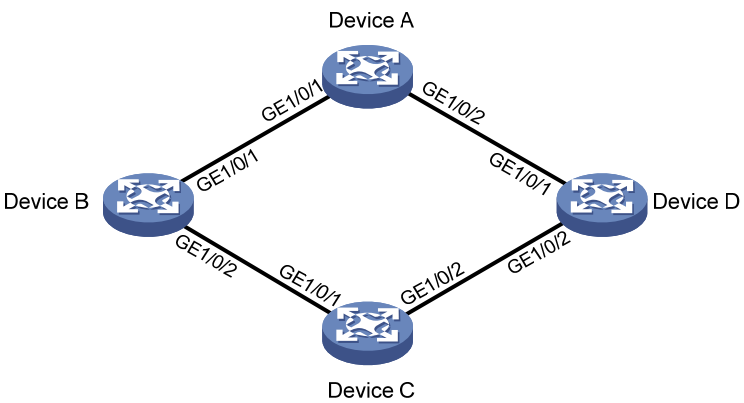
1.6.2 多Smart Link组负载分担配置举例

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 MSTI2 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 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
```

在 Smart Link 组 1 中配置抢占模式为角色抢占模式；使能发送 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 master
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 slave
```

在 Smart Link 组 2 中配置抢占模式为角色抢占模式；使能发送 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，在该端口上使能接收 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，使能接收 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，在该端口上使能接收 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，使能接收 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，在这些端口上使能接收 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
```

(5) 检验配置效果

通过使用 **display smart-link group** 命令可以查看设备上 Smart Link 组的信息：

查看 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
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  ACTVIE   5           16:37:20 2012/01/12

 GigabitEthernet1/0/2      SLAVE   STANDBY  1           17:45:20 2012/01/12


 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
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/2      MASTER  ACTVIE   5           16:37:20 2012/01/12

 GigabitEthernet1/0/1      SLAVE   STANDBY  1           17:45:20 2012/01/12
```

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：

查看 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 2012/01/12
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

1.6.3 Smart Link与CFD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 的维护域MD；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 Smart Link 与 CFD CC 机制的联动，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。

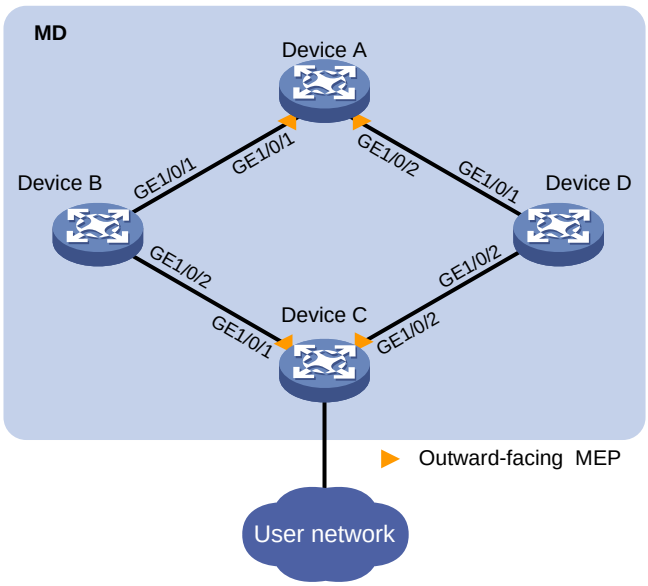
说明

有关 CFD 的详细介绍和配置，请参见“可靠性配置指导”中的“CFD”。

---

2. 组网图

图1-4 Smart Link 与 CFD 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，在这些端口上使能接收 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
```

使能 CFD 功能，并创建级别为 5 的维护域 MD。

```
[DeviceA] cfd enable
[DeviceA] cfd md MD level 5
```

在 MD 中创建服务于 VLAN 10 的维护集 MA_A，并为 MD 和 MA_A 创建服务实例 1。

```
[DeviceA] cfd ma MA_A md MD vlan 10
[DeviceA] cfd service-instance 1 md MD ma MA_A
```

在服务实例 1 内配置维护端点列表，在端口 GigabitEthernet1/0/1 上创建并使能服务实例 1 内的外向维护端点 1002，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 1002 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

在 MD 中创建服务于 VLAN 110 的维护集 MA_B，并为 MD 和 MA_B 创建服务实例 2。

```
[DeviceA] cfd ma MA_B md MD vlan 110
[DeviceA] cfd service-instance 2 md MD ma MA_B
```

在服务实例 2 内配置维护端点列表，在端口 GigabitEthernet1/0/2 上创建并使能服务实例 2 内的外向维护端点 2002，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 2002 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2002 enable
[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，在该端口上使能接收 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，使能接收 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 master
```

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
```
在Smart Link组1中配置抢占模式为角色抢占模式；使能发送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 master
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 slave
```
在Smart Link组2中配置抢占模式为角色抢占模式；使能发送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
```
使能 CFD 功能，并创建级别为 5 的维护域 MD。
```
[DeviceC] cfd enable
[DeviceC] cfd md MD level 5
```
在 MD 中创建服务于 VLAN 10 的维护集 MA_A，并为 MD 和 MA_A 创建服务实例 1。
```
[DeviceC] cfd ma MA_A md MD vlan 10
[DeviceC] cfd service-instance 1 md MD ma MA_A
```
在服务实例 1 内配置维护端点列表，在端口 GigabitEthernet1/0/1 上创建并使能服务实例 1 内的外向维护端点 1001，并使能其 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 mep service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] quit
```
在 MD 中创建服务于 VLAN 110 的维护集 MA_B，并为 MD 和 MA_B 创建服务实例 2。
```
[DeviceC] cfd ma MA_B md MD vlan 110
[DeviceC] cfd service-instance 2 md MD ma MA_B
```
在服务实例 2 内配置维护端点列表，在端口 GigabitEthernet1/0/2 上创建并使能服务实例 2 内的外向维护端点 2001，并使能其 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 mep service-instance 2 mep 2001 enable
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceC-GigabitEthernet1/0/2] quit
```
配置 Smart Link 组 1 的主端口 GigabitEthernet1/0/1 与 CFD CC 机制联动，并重新开启该端口。
```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track cfd cc
```

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

配置 Smart Link 组 2 的主端口 GigabitEthernet1/0/2 与 CFD CC 机制联动，并重新开启该端口。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port smart-link group 2 track cfd cc
[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，在该端口上使能接收 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，使能接收 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
```

(5) 检验配置效果

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：

查看 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
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  DOWN     5           16:37:20 2012/01/12

 GigabitEthernet1/0/2      SLAVE   ACTVIE   3           17:45:20 2012/01/12


 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
--------------------------------------------------------------------------------
GigabitEthernet1/0/2      MASTER  ACTVIE   5           16:37:20 2012/01/12

GigabitEthernet1/0/1      SLAVE   STANDBY  1           17:45:20 2012/01/12
```

有此可见，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。

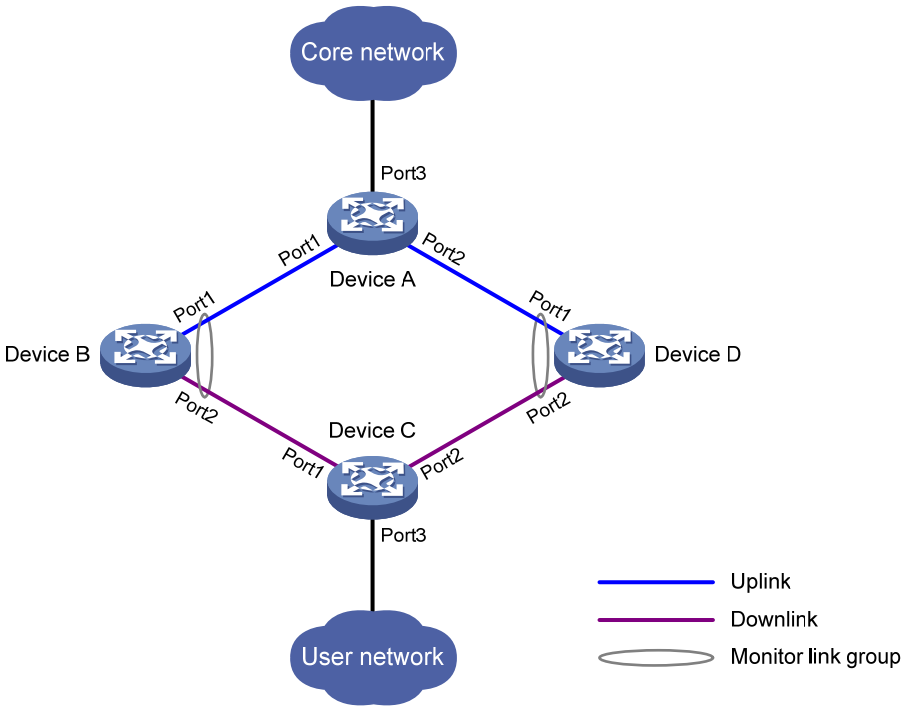
目 录

1 Monitor Link配置

1.1 Monitor Link简介

Monitor Link是一种端口联动方案，主要用于配合二层拓扑协议的组网应用。它通过监控设备的上行端口，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拓扑协议进行链路的切换，如 图 1-1 所示。

图1-1 Monitor Link 应用场景示意图



1.1.1 Monitor Link概念介绍

1. Monitor Link组

Monitor Link 组也叫监控链路组，每个组由上行端口和下行端口共同组成。一个 Monitor Link 组可以有多个上行端口或下行端口，但一个端口只能属于一个 Monitor Link 组。

如 图 1-1 所示，Device B和Device D各自的端口Port1 和Port2 分别组成了一个Monitor Link组，其中Port1 为上行端口，Port2 为下行端口。

2. 上行端口/下行端口

上行端口和下行端口是 Monitor Link 组中的两个端口角色：

- 上行端口又称为 Uplink 端口，是 Monitor Link 组中被监控的端口，Monitor Link 组的状态与之保持联动。当 Monitor Link 组中没有上行端口或所有上行端口都 down 时，Monitor Link 组就处于 down 状态；而只要有一个上行端口 up，Monitor Link 组就处于 up 状态。

- 下行端口又称为 Downlink 端口，是 Monitor Link 组中的监控端口，其状态与 Monitor Link 组的状态保持联动。当 Monitor Link 组的 up/down 状态发生改变时，下行端口的状态就会发生相应的改变，从而与 Monitor Link 组的状态保持一致。

3. 上行链路/下行链路

我们把上行端口所在的链路称为上行链路（Uplink），下行端口所在的链路称为下行链路（Downlink）。

1.1.2 Monitor Link运行机制

每个 Monitor Link 组独立进行上行端口的监控和下行端口的联动。当 Monitor Link 组中没有上行端口或所有上行端口都 down 时，Monitor Link 组就处于 down 状态，并将强制使其所有下行端口的状态都变为 down；而只要有一个上行端口由 down 变为 up，Monitor Link 组的状态就恢复为 up，并使其所有下行端口的状态都恢复为 up。

注意

建议用户不要通过端口开关命令来干预 Monitor Link 组中下行端口的状态。

1.2 配置Monitor Link

1.2.1 配置准备

如果欲配置某端口为 Monitor Link 组的成员端口（上行端口或下行端口），需确保该端口不是聚合成员端口或业务环回组成员端口。

1.2.2 创建Monitor Link组

表1-1 创建 Monitor Link 组

操作	命令	说明
进入系统视图	**system-view**	-
创建Monitor Link组，并进入Monitor Link组视图	**monitor-link group** *group-id*	必选

1.2.3 配置Monitor Link组的成员端口

可在 Monitor Link 组视图或端口视图下配置 Monitor Link 组的成员端口，各视图下的配置效果相同。

1. Monitor Link组视图下的配置

表1-2 Monitor Link 组视图下配置 Monitor Link 组的成员端口

操作	命令	说明
进入系统视图	**system-view**	-
进入Monitor Link组视图	**monitor-link group** *group-id*	-

操作	命令	说明
配置Monitor Link组的成员端口	**port** *interface-type interface-number* { **uplink** | **downlink** }	必选

2. 端口视图下的配置

表1-3 端口视图下配置 Monitor Link 组的成员端口

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口或二层聚合接口视图	**interface** *interface-type interface-number*	-
配置Monitor Link组的成员端口	**port monitor-link group** *group-id* { **uplink** | **downlink** }	必选

说明

- Monitor Link 组的成员端口可以是二层以太网端口或二层聚合接口。
- 一个端口只能属于一个 Monitor Link 组。
- 建议先配置 Monitor Link 的上行端口，以避免下行端口出现不必要的 down/up 状态变化。

1.3 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1-4 Monitor Link 显示和维护

操作	命令
查看Monitor Link组的信息	**display monitor-link group** { *group-id* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.4 Monitor Link典型配置举例

1. 组网需求

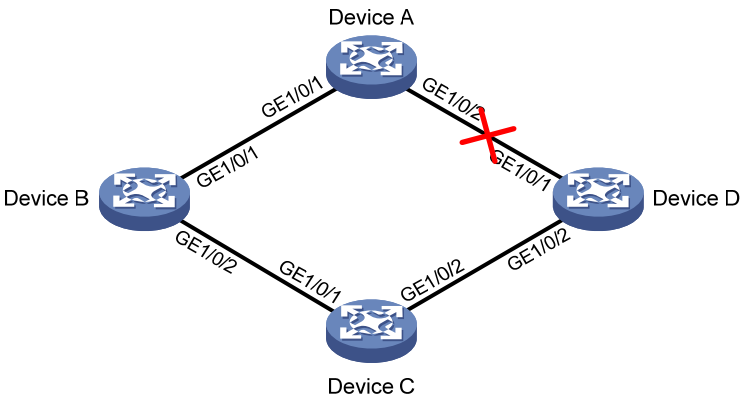
- 在 图 1-2 所示的组网中，Device C为Smart Link设备，Device A、Device B和Device D为相关设备。Device C上VLAN 1～30 的流量通过Smart Link组双上行到Device A。
- 通过配置，在 Device C 上实现双上行链路的灵活备份，并且当 Device A 与 Device B（或 Device D）之间出现链路故障时，Device C 能够感知到这个故障并完成其上行链路的切换。

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
```

在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 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] 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] 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，副端口为 GigabitEthernet1/0/2。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
```
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
```
(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
```
将端口 GigabitEthernet1/0/1 配置为 Trunk 端口且允许 VLAN 1～30 通过，并在该端口上使能接收 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
```
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，并使能接收 Flush 报文的功能。
```
[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
[DeviceB-GigabitEthernet1/0/2] quit
```
创建 Monitor Link 组 1，并配置该组的上行端口为 GigabitEthernet1/0/1，下行端口为 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
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口且允许 VLAN 1～30 通过，并在该端口上使能接收 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
```

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，并使能接收 Flush 报文的功能。

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

创建 Monitor Link 组 1，并配置该组的上行端口为 GigabitEthernet1/0/1，下行端口为 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
```

(5) 检验配置效果

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：

查看 Device B 上 Monitor Link 组 1 的信息。

```
[DeviceB] display monitor-link group 1
 Monitor link group 1 information:
 Group status: UP
 Last-up-time: 16:37:20 2012/1/12
 Last-down-time: 16:35:26 2012/1/12
 Member                    Role     Status
 ----------------------------------------
 GigabitEthernet1/0/1      UPLINK   UP
 GigabitEthernet1/0/2      DOWNLINK UP
```

查看 Device D 上 Monitor Link 组 1 的信息。

```
[DeviceD] display monitor-link group 1
 Monitor link group 1 information:
 Group status: DOWN
 Last-up-time: 16:35:27 2012/1/12
 Last-down-time: 16:37:19 2012/1/12
```

```
Member                    Role     Status
----------------------------------------
GigabitEthernet1/0/1      UPLINK   DOWN
GigabitEthernet1/0/2      DOWNLINK DOWN
```

目 录

1 VRRP配置

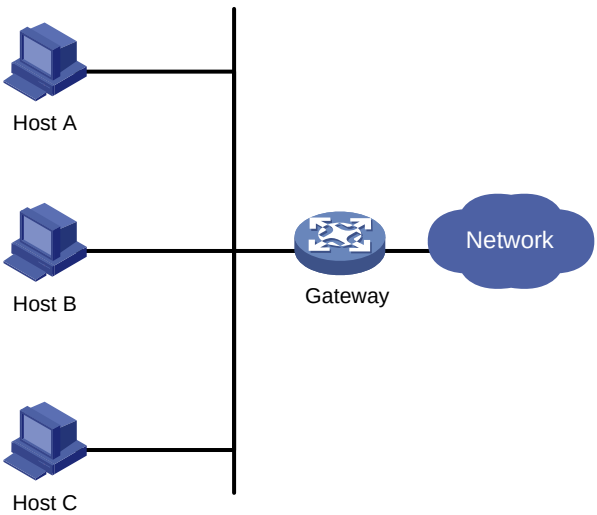
说明

- 本章所指的路由器代表了一般意义下的路由器，以及运行了路由协议的三层交换机。为提高可读性，在手册的描述中将不另行说明。
- 除特殊说明外，VRRP 中对于接口的配置，目前只能在三层以太网端口、VLAN 接口、三层聚合接口上进行。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。
- 加入聚合组的接口上不能配置 VRRP。

1.1 VRRP简介

如 图 1-1 所示，通常，同一网段内的所有主机上都存在一条相同的、以网关为下一跳的缺省路由。主机发往其他网段的报文将通过缺省路由发往网关，再由网关进行转发，从而实现主机与外部网络的通信。当网关发生故障时，本网段内所有以网关为缺省路由的主机将无法与外部网络通信。

图1-1 局域网组网方案



缺省路由为用户的配置操作提供了方便，但是对缺省网关设备提出了很高的稳定性要求。增加出口网关是提高系统可靠性的常见方法，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）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，由 VRRP 的选举机制决定哪台路由器承担转发任务，局域网内的主机只需将虚拟路由器配置为缺省网关。

VRRP 是一种容错协议，在提高可靠性的同时，简化了主机的配置。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台路由器出现故障时仍然提供高可靠的缺省链路，有效避免单一链路发生故障后网络中断的问题，而无需修改动态路由协议、路由发现协议等配置信息。

设备支持两种模式的 VRRP：

- 标准协议模式：基于RFC实现的VRRPv2 和VRRPv3。其中，VRRPv2 基于IPv4，VRRPv3 基于IPv6。VRRPv2 和VRRPv3 在功能实现上并没有区别，只是应用的网络环境不同，详细介绍请参见“1.2 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“1.3 VRRP负载均衡模式”。

1.2 VRRP标准协议模式

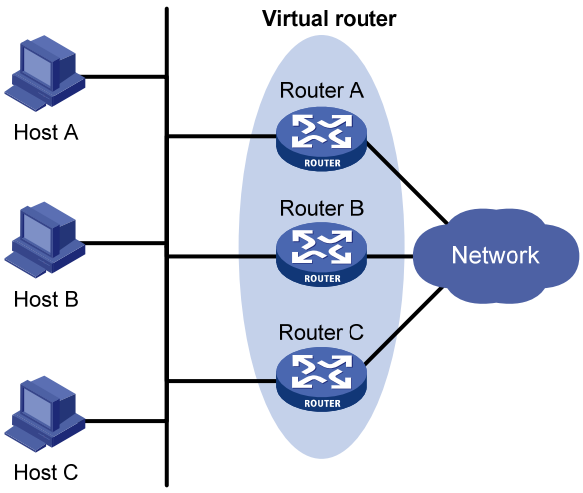
1.2.1 VRRP备份组简介

VRRP 将局域网内的一组路由器划分在一起，称为一个备份组。备份组由一个 Master 路由器和多个 Backup 路由器组成，功能上相当于一台虚拟路由器。

VRRP 备份组具有以下特点：

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

图1-2 VRRP 组网示意图



如 图 1-2 所示，Router A、Router B和Router C组成一个虚拟路由器。此虚拟路由器有自己的IP地址。局域网内的主机将虚拟路由器设置为缺省网关。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。

说明

- 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，只允许配置一个 IP 地址拥有者。
- 路由器在备份组中的状态可以为 Master、Backup 和 Initialize。

1. 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。

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

3. 备份组中路由器的认证方式

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

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

在一个安全的网络中，用户也可以不设置认证方式。

1.2.2 VRRP定时器

VRRP 定时器分为两种：VRRP 通告报文间隔时间定时器和 VRRP 抢占延迟时间定时器。

1. VRRP通告报文时间间隔定时器

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。

用户可以通过设置 VRRP 定时器来调整 Master 路由器发送 VRRP 通告报文的时间间隔。如果 Backup 路由器在等待了 3 个间隔时间后，依然没有收到 VRRP 通告报文，则认为自己是 Master 路由器，并对外发送 VRRP 通告报文，重新进行 Master 路由器的选举。

2. VRRP抢占延迟时间定时器

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），Backup 路由器接收到优先级低于本地优先级的通告报文后，不会立即抢占成为 Master，而是等待一定时间——抢占延迟时间后，才会对外发送 VRRP 通告报文取代原来的 Master 路由器。

1.2.3 VRRP报文格式

Master 路由器以组播的方式定时发送 VRRP 报文通告它的存在。这些报文可以用来检测虚拟路由器的各种参数，还可以用于 Master 路由器的选举。

VRRP报文封装在IP报文中，协议号为 112。VRRPv2 的报文格式如 图 1-3 所示，VRRPv3 的报文格式如 图 1-4 所示。

图1-3 VRRPv2 的报文格式

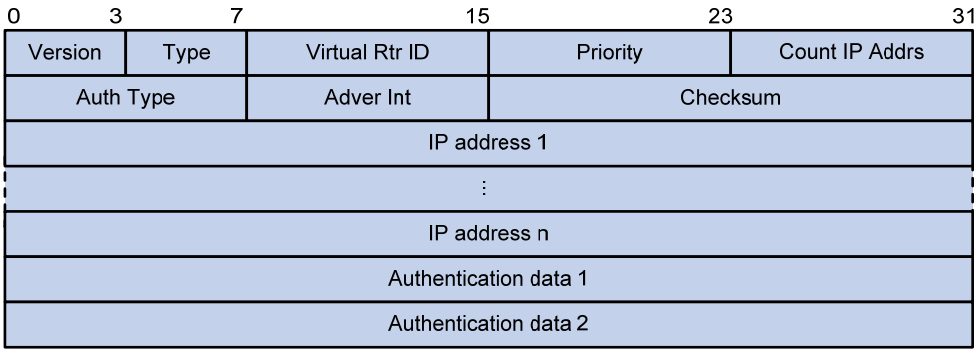
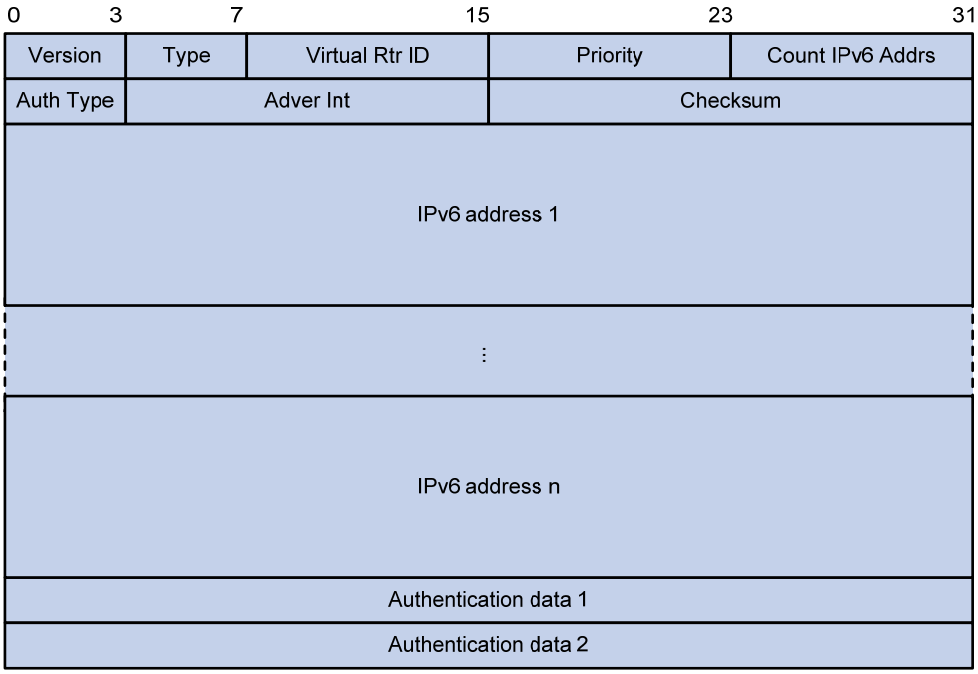


图1-4 VRRPv3 的报文格式



各字段解释如下：

- Version：协议版本号。VRRPv2 对应的版本号为 2；VRRPv3 对应的版本号为 3。
- Type：VRRP 报文的类型。VRRPv2 和 VRRPv3 报文只有一种类型，即 VRRP 通告报文（Advertisement），该字段取值为 1。
- Virtual Rtr ID（VRID）：虚拟路由器号（即备份组号），取值范围 1～255。
- Priority：路由器在备份组中的优先级，取值范围 0～255，数值越大表明优先级越高。
- Count IP Addrs/Count IPv6 Addrs：备份组虚拟 IP 地址的个数。1 个备份组可对应多个虚拟 IP 地址。
- Auth Type：认证类型。该值为 0 表示无认证，为 1 表示简单字符认证，为 2 表示 MD5 认证。VRRPv3 不支持 MD5 认证。
- Adver Int：发送通告报文的时间间隔。VRRPv2 中单位为秒，缺省为 1 秒；VRRPv3 中单位为厘秒，缺省为 100 厘秒。
- Checksum：16 位校验和，用于检测 VRRP 报文中的数据破坏情况。
- IP Address/IPv6 Address：备份组虚拟 IP 地址表项。所包含的地址数定义在 Count IP Addrs/Count IPv6 Addrs 字段。
- Authentication Data：认证字，目前只用于简单字符认证，对于其它认证方式一律填 0。

1.2.4 VRRP工作过程

VRRP 的工作过程如下：

(1) 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。优先级高的路由器成为 Master 路由器；优先级低的成为 Backup 路由器。Master 路由器定期发送 VRRP 通告报文，通知备份组内的其他路由器自己工作正常；Backup 路由器则启动定时器等待通告报文的到来。

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

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

(4) 如果 Backup 路由器的定时器超时后仍未收到 Master 路由器发送来的 VRRP 通告报文，则认为 Master 路由器已经无法正常工作，此时 Backup 路由器会认为自己是 Master 路由器，并对外发送 VRRP 通告报文。备份组内的路由器根据优先级选举出 Master 路由器，承担报文的转发功能。

说明

- 由于路由器上备份组的配置不一致、网络故障等原因造成备份组中存在多个 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: 优先级高的路由器成为 Master; 优先级低的成为 Backup; 如果优先级相同，则 IP 地址大的成为 Master。
- Backup 路由器接收到 VRRP 通告报文后，只会将自己的优先级与通告报文中的优先级进行比较，不会比较 IP 地址。只有自己的优先级大于通告报文中的优先级时，才会抢占成为 Master。

1.2.5 VRRP监视功能

说明

配置 VRRP 监视功能时，需要配置备份组中的路由器工作在抢占方式，以保证只有优先级最高的路由器才能成为 Master、承担转发任务。

1. 监视指定接口功能

VRRP 的监视接口功能更好地扩充了备份功能：不仅能在备份组中某路由器的接口出现故障时提供备份功能，还能在路由器的其它接口（如连接上行链路的接口）不可用时提供备份功能。

路由器连接上行链路的接口出现故障时，备份组无法感知上行链路接口的故障，如果该路由器此时处于 Master 状态，将会导致局域网内的主机无法访问外部网络。通过监视指定接口的功能，可以解决该问题。当连接上行链路的接口处于 Down 或 Removed 状态时，路由器主动降低自己的优先级，使得备份组内其它路由器的优先级高于这个路由器，以便优先级最高的路由器成为 Master，承担转发任务。

2. 监视Track项功能

通过 VRRP 监视 Track 项功能，可以实现：

- 根据上行链路的状态，改变路由器的优先级。当上行链路出现故障，局域网内的主机无法通过路由器访问外部网络时，被监视 Track 项的状态为 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。

说明

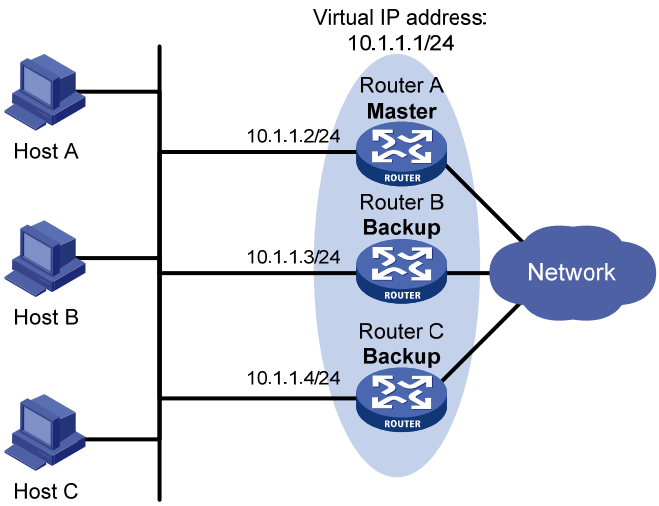
Track 项的详细介绍，请参见“可靠性配置指导”中的“Track”。

1.2.6 VRRP应用（以基于IPv4 的VRRP为例）

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，才会从其他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 1-5 中所示。

图1-5 主备备份 VRRP



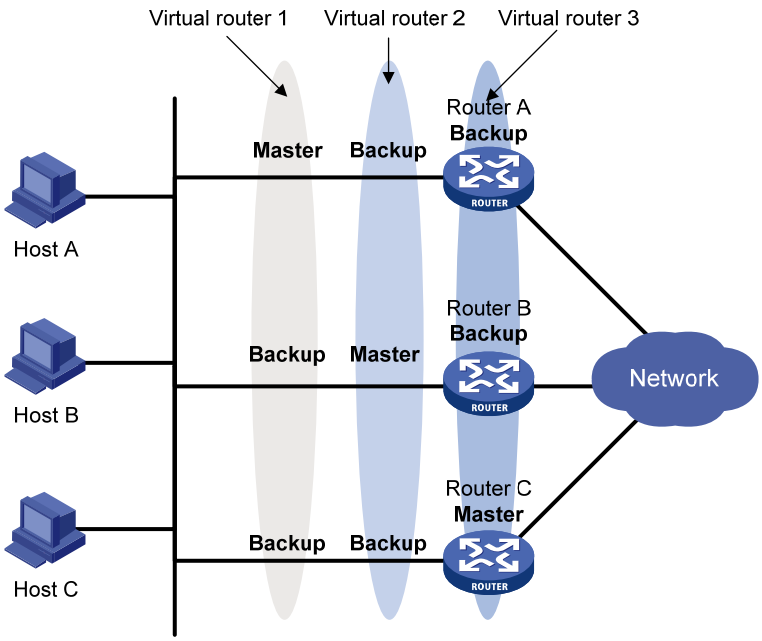
初始情况下，Router A 为 Master 路由器并承担转发任务，Router B 和 Router C 是 Backup 路由器且都处于就绪监听状态。如果 Router A 发生故障，则备份组内处于 Backup 状态的 Router B 和 Router C 路由器将根据优先级选出一个新的 Master 路由器，这个新 Master 路由器继续向网络内的主机提供路由服务。

2. 负载分担

在路由器的一个接口上可以创建多个备份组，使得该路由器可以在一个备份组中作为 Master 路由器，在其他的备份组中作为 Backup 路由器。

负载分担方式是指多台路由器同时承担业务，因此负载分担方式需要两个或者两个以上的备份组，每个备份组都包括一个Master路由器和若干个Backup路由器，各备份组的Master路由器各不相同，如 图 1-6 中所示。

图1-6 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 1-6 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、2 和 3。在配置优先级时，需要确保三个备份组中各路由器的 VRRP 优先级形成交叉对应。

1.3 VRRP负载均衡模式

1.3.1 VRRP负载均衡模式概述

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

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

VRRP 负载均衡模式中，只需创建一个备份组，就可以实现备份组中多个路由器之间的负载分担，避免了 VRRP 备份组中 Backup 路由器始终处于空闲状态、网络资源利用率不高的问题。

说明

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，详见下面的介绍。

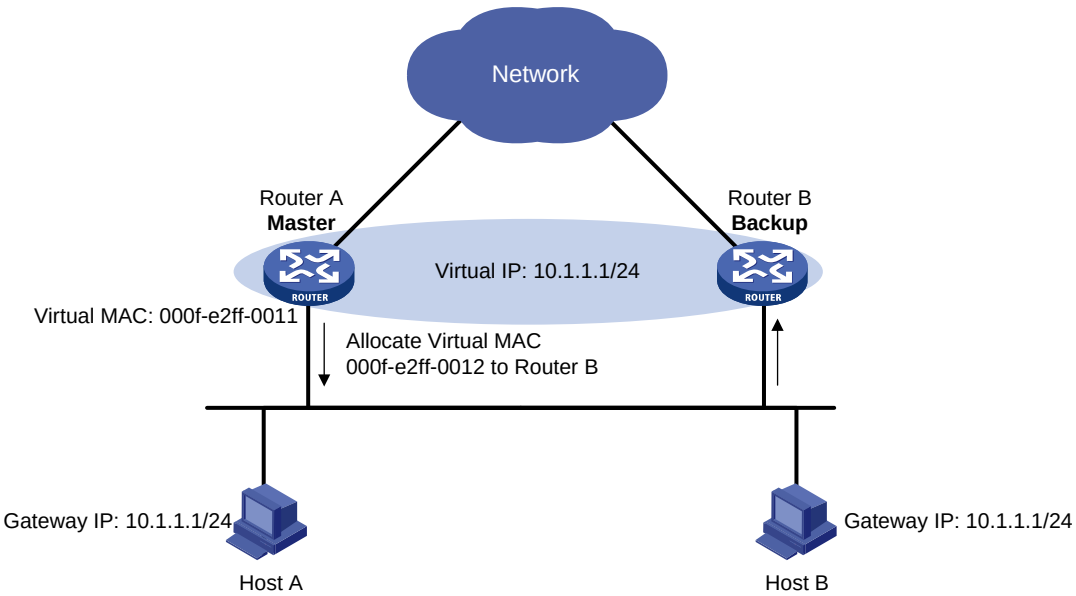
1.3.2 虚拟MAC地址的分配

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，从而实现流量在多个路由器之间分担。备份组中的 Backup 路由器不会应答主机的 ARP/ND 请求。

以 IPv4 网络为例，VRRP 负载均衡模式的具体工作过程为：

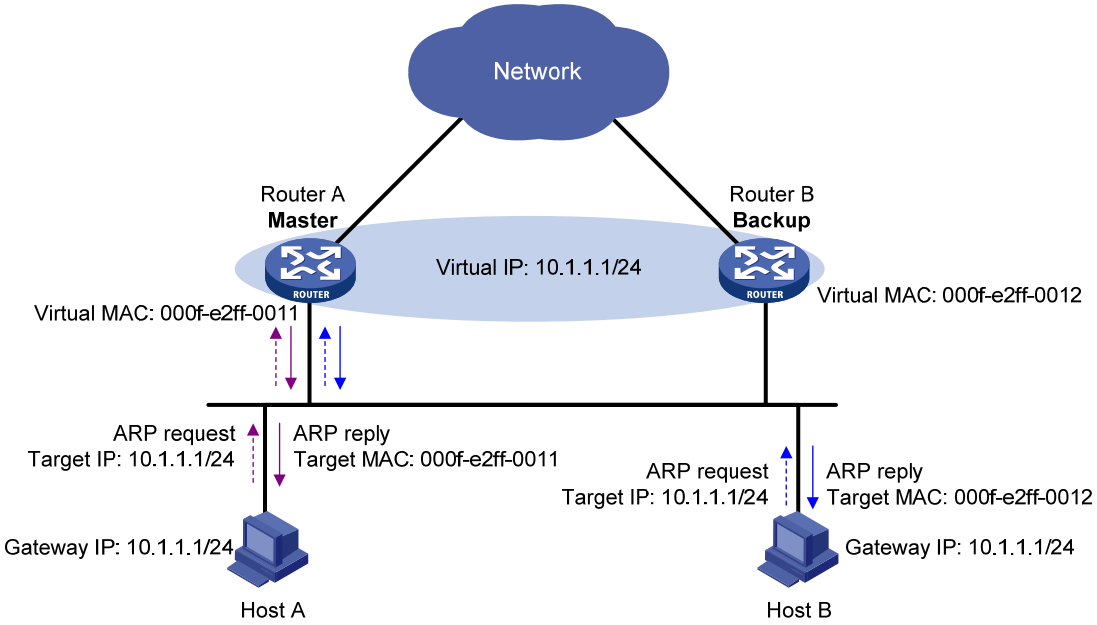
(1) Master为备份组中的路由器（包括Master自身）分配虚拟MAC地址。如 图 1-7 所示，虚拟IP地址为 10.1.1.1/24 的备份组中，Router A作为Master，Router B作为Backup。Router A为自己分配的虚拟MAC地址为 000f-e2ff-0011，为Router B分配的虚拟MAC地址为 000f-e2ff-0012。

图1-7 Master 分配虚拟 MAC 地址



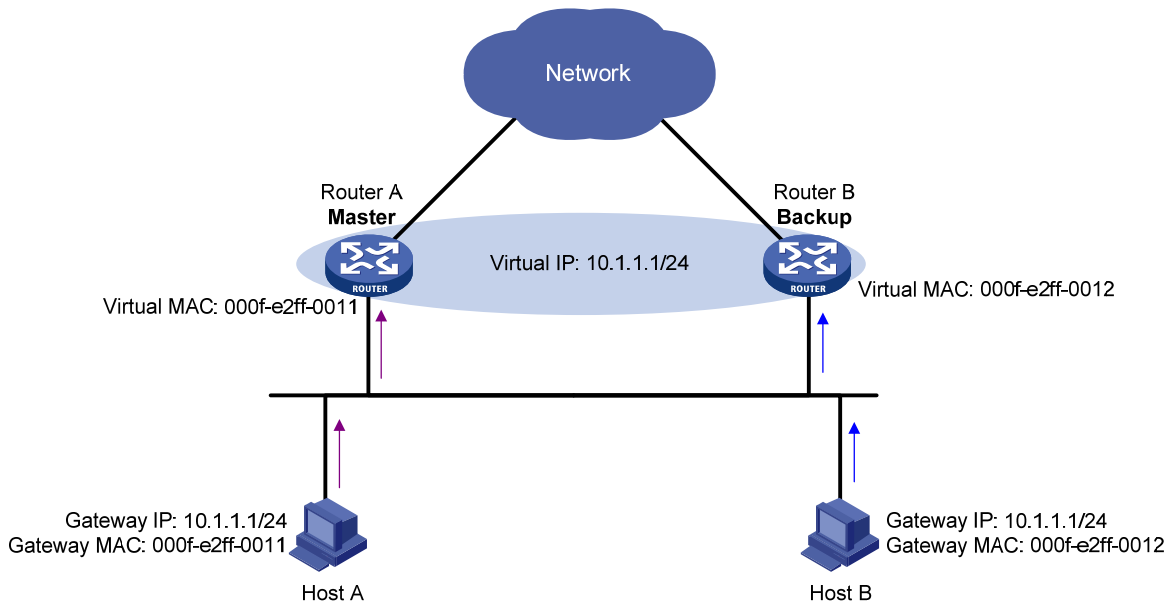
(2) Master接收到主机发送的目标IP地址为虚拟IP地址的ARP请求后，根据负载均衡算法使用不同的虚拟MAC地址应答主机的ARP请求。如 图 1-8 所示，Host A发送ARP请求获取网关 10.1.1.1 对应的MAC地址时，Master（即Router A）使用Router A的虚拟MAC地址应答该请求；Host B发送ARP请求获取网关 10.1.1.1 对应的MAC地址时，Master使用Router B的虚拟MAC地址应答该请求。

图1-8 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 1-9 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1-9 主机通过不同路由器转发流量



1.3.3 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 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) 该路由器将虚拟转发器的信息通告给备份组内其他的路由器。

(3) 备份组内的路由器接收到虚拟转发器信息后，在本地创建该虚拟 MAC 地址对应的虚拟转发器。

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

2. 虚拟转发器的权重和优先级

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

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

设备根据虚拟转发器的权重计算虚拟转发器的优先级：

- 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。

图1-10 虚拟转发器

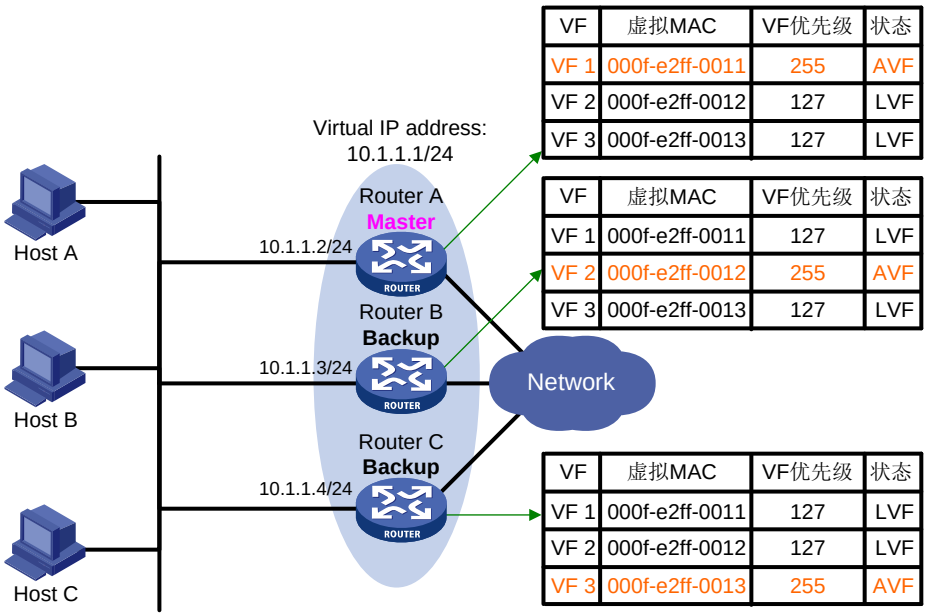


图 1-10 举例说明了备份组中每个路由器上的虚拟转发器信息及其备份关系。Master路由器Router A为自己、Router B、Router C分配的虚拟MAC地址分别为 000f-e2ff-0011、000f-e2ff-0012 和000f-e2ff-0013。虚拟MAC地址对应的虚拟转发器分别为VF 1、VF 2 和VF 3。在Router A、Router B和Router C上都创建了这三个虚拟转发器，并形成备份关系。例如，Router A、Router B和Router C上的VF 1 互相备份：

- Router A 为 VF 1 的 VF Owner，Router A 上 VF 1 的虚拟转发器优先级为最高值 255。因此，Router A 上的 VF 1 作为 AVF，负责转发目的 MAC 地址为虚拟 MAC 地址 000f-e2ff-0011 的流量。
- Router B 和 Router C 上 VF 1 的虚拟转发器优先级为：权重 255/（本地 AVF 数目 1＋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。

说明

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

---

4. 虚拟转发器的定时器

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

- Redirect Timer：VF 重定向定时器。该定时器超时前，Master 路由器还会采用该 VF 对应的虚拟 MAC 地址应答主机的 ARP/ND 请求；该定时器超时后，Master 路由器不再采用该 VF

对应的虚拟 MAC 地址应答主机的 ARP/ND 请求。如果 VF Owner 在 Redirect Timer 超时前恢复，则 VF Owner 可以迅速参与流量的负载分担。

- Timeout Timer：VF 生存定时器，即 AVF 接替 VF Owner 工作的期限。该定时器超时前，备份组中的路由器上都保留该 VF，AVF 负责转发目的 MAC 地址为该 VF 对应虚拟 MAC 地址的报文；该定时器超时后，备份组中的路由器上都删除该 VF，不再转发目的 MAC 地址为该 VF 对应虚拟 MAC 地址的报文。

5. 虚拟转发器监视功能

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

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

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

1.3.4 VRRP负载均衡模式的报文

VRRP 标准协议模式中只定义了一种报文——VRRP 通告报文，且只有 Master 路由器周期性发送该报文，Backup 路由器不会发送 VRRP 通告报文。

为了实现负载均衡，VRRP 负载均衡模式中定义了四种报文：

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

说明

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

1.4 配置基于IPv4的VRRP

1.4.1 基于IPv4 的VRRP配置任务简介

在备份组内的每个路由器上都需进行配置，才能形成一个备份组。

表1-1 VRRP 配置任务简介

配置任务	说明	详细配置
配置VRRP的工作模式	可选	1.4.2
配置虚拟IP地址对应的MAC地址的类型	可选 本配置在VRRP负载均衡模式下不生效	1.4.3
创建备份组并配置虚拟IP地址	必选	1.4.4
配置备份组优先级、抢占方式及监视功能	可选	1.4.5
配置虚拟转发器监视功能	可选 本配置仅在VRRP负载均衡模式下生效	1.4.6
配置VRRP报文的相关属性	可选	1.4.7
开启VRRP的Trap功能	可选	1.4.8

1.4.2 配置VRRP的工作模式

VRRP 具有两种工作模式：

- 标准协议模式：VRRP 备份组中只有 Master 路由器负责转发报文。
- 负载均衡模式：VRRP 备份组中所有存在 AVF 的路由器（可以是 Master，也可以是 Backup）都可以转发报文，实现负载均衡。

配置 VRRP 的工作模式后，路由器上所有的 VRRP 备份组都工作在该模式。

表1-2 配置 VRRP 的工作模式

操作	命令	说明
进入系统视图	**system-view**	-
配置VRRP工作在标准协议模式	**undo vrrp mode**	二者选择其一 缺省情况下，VRRP工作在标准协议模式
配置VRRP工作在负载均衡模式	**vrrp mode load-balance**	

1.4.3 配置虚拟IP地址对应的MAC地址的类型

配置虚拟 IP 地址对应的 MAC 地址的类型后，Master 路由器将根据配置的 MAC 地址类型，选择发送报文的源 MAC 地址，并采用指定类型的 MAC 地址应答主机的 ARP 请求，以便内部网络的主机学习到 IP 地址和 MAC 地址的对应关系。

虚拟 IP 地址对应的 MAC 地址类型有两种：

- 虚拟 MAC 地址：缺省情况下，创建备份组后，会自动生成与之对应的虚拟 MAC 地址，虚拟 IP 地址与此虚拟 MAC 地址对应。如果采用这种对应关系，Master 路由器改变时，内部网络的主机不需要更新 IP 地址与 MAC 地址的绑定。
- 接口的实际 MAC 地址：当备份组中存在 IP 地址拥有者时，如果配置虚拟 IP 地址和虚拟 MAC 地址对应，会造成一个 IP 地址对应两个 MAC 地址。因此用户可以配置备份组虚拟 IP 地址和接口的实际 MAC 地址对应，主机发送的报文将按照实际 MAC 地址转发给 IP 地址拥有者。

表1-3 配置虚拟 IP 地址对应的 MAC 地址的类型

操作	命令	说明
进入系统视图	**system-view**	-
配置虚拟IP地址对应的MAC地址的类型	**vrrp method { real-mac | virtual-mac }**	可选 缺省情况下，采用虚拟MAC地址和虚拟IP地址对应

说明

- 本配置在负载均衡模式下不会生效。无论如何配置虚拟 IP 地址对应的 MAC 地址的类型，在负载均衡模式下，始终是虚拟 IP 地址与虚拟 MAC 地址对应。
- 本配置需要在备份组创建之前就进行设定。如果路由器上已经创建了备份组，则不允许修改虚拟 IP 地址对应的 MAC 地址的类型。
- 如果一台设备的多个接口上创建了相同编号的备份组，且这些备份组的 VRRP 通告报文都需要通过 QinQ 网络发送，则建议采用接口的实际 MAC 地址与虚拟 IP 地址对应，否则可能会导致网络不通。

1.4.4 创建备份组并配置虚拟IP地址

创建 VRRP 备份组的同时，需要配置备份组的虚拟 IP 地址。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。

为备份组指定第一个虚拟 IP 地址时，VRRP 备份组就会自动生成。以后用户再给这个备份组指定虚拟 IP 地址时，VRRP 备份组仅将这个 IP 地址添加到它的备份组虚拟 IP 地址列表中。

说明

建议不要在 Super VLAN 对应的 VLAN 接口下创建 VRRP 备份组，以免对网络性能造成影响。

1. 配置准备

在接口上创建备份组并配置虚拟 IP 地址之前，需要配置接口的 IP 地址，并且保证随后配置的虚拟 IP 地址与接口的 IP 地址在同一网段。

2. 创建备份组并配置虚拟IP地址

表1-4 创建备份组并配置虚拟 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
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*	必选 缺省情况下，没有创建备份组

说明

- 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。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”。
- 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 **network** 命令在该接口上使能 OSPF。**network** 命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“OSPF”。
- VRRP 工作在负载均衡模式时，虚拟 IP 地址不能与 VRRP 备份组中路由器的接口 IP 地址相同，即负载均衡模式的 VRRP 备份组中不能存在 IP 地址拥有者。
- 备份组中所有虚拟 IP 地址都被删除后，该备份组也将同时被删除掉，并且该备份组的所有配置都不再有效。
- 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 IP 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。
- 配置的虚拟 IP 地址和接口 IP 地址在同一网段，且为合法的主机地址时，备份组才能够正常工作；否则，如果配置的虚拟 IP 地址和接口 IP 地址不在同一网段，或为接口 IP 地址所在网段的网络地址或网络广播地址，虽然可以配置成功，但是备份组会始终处于 Initialize 状态，此状态下 VRRP 不起作用。

1.4.5 配置备份组优先级、抢占方式及监视功能

1. 配置准备

在配置备份组优先级、抢占方式及监视功能之前，需要先在接口上创建备份组并配置虚拟 IP 地址。

2. 配置过程

通过优先级、抢占方式和监视指定接口或 Track 项的配置，可以决定备份组中哪个路由器作为 Master 路由器。下面这些配置是可选的，可以根据实际需要进行配置。

表1-5 配置备份组优先级、抢占方式及监视功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置路由器在备份组中的优先级	**vrrp vrid** *virtual-router-id* **priority** *priority-value*	可选 缺省情况下，路由器在备份组中的优先级为100
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** [**timer delay** *delay-value*]	可选 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秒
配置监视指定接口	**vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]	可选 缺省情况下，没有指定被监视的接口
配置监视指定的Track项	**vrrp vrid** *virtual-router-id* **track** *track-entry-number* [**reduced** *priority-reduced* | **switchover**]	可选 缺省情况下，没有指定被监视的Track项

说明

- 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。
- 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。
- 被监视接口的状态由 Down 或 Removed 变为 Up 后，对应路由器的优先级数会自动恢复。
- 被监视 Track 项的状态由 Negative 变为 Positive 或 Invalid 后，对应的路由器优先级会自动恢复。

1.4.6 配置虚拟转发器监视功能

1. 配置准备

在配置虚拟转发器监视功能之前，需要先在接口上创建备份组并配置虚拟 IP 地址。

2. 配置过程

VRRP 工作在负载均衡模式时，如果配置虚拟转发器监视 Track 项并指定权重降低数额，则当 Track 项状态为 Negative 时，路由器上所有虚拟转发器的权重都将降低指定的数额；被监视的 Track 项状态由 Negative 变为 Positive 或 Invalid 后，路由器中所有虚拟转发器的权重会自动恢复。如果配置 LVF 通过 Track 功能监视 AVF 的状态，则当 Track 项状态为 Negative 时，LVF 会马上切换为 AVF，从而避免流量长时间中断。

表1-6 配置虚拟转发器监视功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
配置虚拟转发器监视指定的Track项，并指定权重降低的数额	**vrrp vrid** *virtual-router-id* **weight track** *track-entry-number* [**reduced** *weight-reduced*]	二者至少选择其一 缺省情况下，没有配置虚拟转发器的监视功能
配置LVF通过Track功能监视AVF的状态	**vrrp vrid** *virtual-router-id* **track** *track-entry-number* **forwarder-switchover member-ip** *ip-address*	

说明

- 在 VRRP 标准协议模式和负载均衡模式下均可配置虚拟转发器监视功能，但只有在 VRRP 负载模式下虚拟转发器监视功能才会起作用。
- 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，因此只有配置的权重降低数额能够保证监视的上行链路出现故障时 VF Owner 的权重低于失效下限，即权重降低的数额大于 245，其他的虚拟转发器才能接替 VF Owner 成为 AVF。

1.4.7 配置VRRP报文的相关属性

1. 配置准备

在配置 VRRP 报文的相关属性之前，需要先在接口上创建备份组并配置虚拟 IP 地址。

2. 配置过程

表1-7 配置 VRRP 报文的相关属性

操作	命令	说明
进入系统视图	**system-view**	-
配置VRRP报文的DSCP优先级	**vrrp dscp** *dscp-value*	可选 缺省情况下，VRRP报文的DSCP优先级为48
进入接口视图	**interface** *interface-type interface-number*	-
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**] *key*	可选 缺省情况下，不进行认证
配置备份组中Master路由器发送VRRP通告报文的时间间隔	**vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval*	可选 缺省情况下，备份组中Master路由器发送VRRP通告报文的时间间隔为1秒

操作	命令	说明
禁止检查VRRP报文的TTL域	**vrrp un-check ttl**	可选 缺省情况下，检查VRRP报文的TTL域 进行此配置之前，不需要创建备份组

说明

- 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；加入同一备份组的成员需要设置相同的认证方式和认证字。
- 网络流量过大可能会导致 Backup 路由器在指定时间内没有收到 Master 的 VRRP 通告报文，而发生状态转换。可以通过将 VRRP 通告报文的发送时间间隔延长的办法来解决该问题。
- 备份组中不同路由器上配置的 VRRP 通告报文发送时间间隔不同，也可能会导致 Backup 路由器在指定时间内没有收到 Master 的 VRRP 通告报文，而发生状态转换。可以通过修改路由器上的 VRRP 通告报文发送时间间隔、使得备份组中所有路由器上该值相同的方法来解决此问题。

1.4.8 开启VRRP的Trap功能

开启 VRRP 模块的 Trap 功能后，该模块会生成级别为 errors 的 Trap 报文，用于报告该模块的重要事件。生成的 Trap 报文将被发送到设备的信息中心，通过设置信息中心的参数，最终决定 Trap 报文的输出规则（即是否允许输出以及输出方向）。（有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。）

表1-8 开启 VRRP 的 Trap 功能

操作	命令	说明
进入系统视图	**system-view**	-
开启VRRP模块的Trap功能	**snmp-agent trap enable vrrp [authfailure | newmaster]**	可选 缺省情况下，VRRP模块的Trap功能处于开启状态

说明

snmp-agent trap enable vrrp 命令的详细介绍请参见“网络管理和监控命令参考/SNMP”中的 **snmp-agent trap enable** 命令。

1.4.9 基于IPv4 的VRRP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示基于 IPv4 的 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** 命令可以清除基于 IPv4 的 VRRP 统计信息。

表1-9 VRRP 显示和维护

操作	命令
显示VRRP备份组的状态信息	**display vrrp** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示VRRP备份组的统计信息	**display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除VRRP备份组的统计信息	**reset vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

1.5 配置基于IPv6的VRRP

1.5.1 基于IPv6 的VRRP配置任务简介

在备份组内的每个路由器上都需进行配置，才能形成一个备份组。

表1-10 VRRP 配置任务简介

配置任务	说明	详细配置
配置VRRP的工作模式	可选	1.4.2
配置虚拟IPv6地址对应的MAC地址的类型	可选 本配置在VRRP负载均衡模式下不生效	1.5.2
创建VRRP备份组并配置虚拟IPv6地址	必选	1.5.3
配置备份组优先级、抢占方式及监视功能	可选	1.5.4
配置虚拟转发器监视功能	可选 本配置仅在VRRP负载均衡模式下生效	1.5.5
配置VRRP报文的相关属性	可选	1.5.6

1.5.2 配置虚拟IPv6 地址对应的MAC地址的类型

配置虚拟 IPv6 地址对应的 MAC 地址的类型后，Master 路由器将根据配置的 MAC 地址类型，选择发送报文的源 MAC 地址，并采用指定类型的 MAC 地址应答主机的 ND 请求，以便内部网络的主机学习到 IPv6 地址和 MAC 地址的对应关系。

虚拟 IPv6 地址对应的 MAC 地址类型有两种：

- 虚拟 MAC 地址：缺省情况下，创建备份组后，会自动生成与之对应的虚拟 MAC 地址，虚拟 IPv6 地址与此虚拟 MAC 地址对应。如果采用这种对应关系，Master 路由器改变时，内部网络的主机不需要更新 IPv6 地址与 MAC 地址的绑定。
- 接口的实际 MAC 地址：当备份组中存在 IP 地址拥有者时，如果配置虚拟 IPv6 地址和虚拟 MAC 地址对应，会造成一个 IPv6 地址对应两个 MAC 地址。因此用户可以配置备份组虚拟 IPv6 地址和实际 MAC 地址对应，主机发送的报文将按照实际 MAC 地址转发给 IP 地址拥有者。

表1-11 配置虚拟 IPv6 地址对应的 MAC 地址的类型

操作	命令	说明
进入系统视图	**system-view**	-
配置虚拟IPv6地址对应的MAC地址的类型	**vrrp ipv6 method** { **real-mac** | **virtual-mac** }	可选 缺省情况下，采用备份组的虚拟MAC地址和虚拟IPv6地址对应

说明

- 本配置在负载均衡模式下不会生效，无论如何配置虚拟 IPv6 地址对应的 MAC 地址的类型，在负载均衡模式下，始终是虚拟 IPv6 地址与虚拟 MAC 地址对应。
- 本配置需要在备份组创建之前就进行设定。如果路由器上已经创建了备份组，则不允许修改虚拟 IPv6 地址对应的 MAC 地址的类型。

1.5.3 创建备份组并配置虚拟IPv6 地址

创建 VRRP 备份组的同时，需要配置备份组的虚拟 IPv6 地址。可以为一个备份组配置多个虚拟 IPv6 地址。

为备份组指定第一个虚拟 IPv6 地址时，VRRP 备份组就会自动生成。以后用户再给这个备份组指定虚拟 IPv6 地址时，VRRP 备份组仅仅将这个 IPv6 地址添加到它的备份组虚拟 IPv6 地址列表中。

说明

建议不要在 Super VLAN 对应的 VLAN 接口下创建 VRRP 备份组，以免对网络性能造成影响。

1. 配置准备

在接口上创建备份组并配置虚拟 IPv6 地址之前，需要配置接口的 IPv6 地址，并且保证随后配置的虚拟 IPv6 地址与接口的 IPv6 地址在同一网段。

2. 创建备份组并配置虚拟IPv6 地址

表1-12 创建备份组并配置虚拟 IPv6 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
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**	必选 缺省情况下，没有创建备份组 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

操作	命令	说明
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*	可选 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

说明

- 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** 命令在该接口上使能 OSPFv3 协议。**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”。
- 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。
- 备份组中所有虚拟 IPv6 地址都被删除后，该备份组也将同时被删除掉，并且该备份组的所有配置都不再有效。
- 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。

1.5.4 配置备份组优先级、抢占方式及监视功能

1. 配置准备

在配置备份组优先级、抢占方式及监视功能之前，需要先在接口上创建备份组并配置虚拟 IPv6 地址。

2. 配置过程

通过优先级、抢占方式和监视指定接口或Track项的配置，可以决定备份组中哪个路由器作为Master路由器。下面这些配置是可选的，可以根据实际需要进行配置。

表1-13 配置备份组优先级、抢占方式及监视指定接口

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置路由器在备份组中的优先级	**vrrp ipv6 vrid** *virtual-router-id* **priority** *priority-value*	可选 缺省情况下，路由器在备份组中的优先级为100
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** [**timer delay** *delay-value*]	可选 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秒
配置监视指定接口	**vrrp ipv6 vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]	可选 缺省情况下，没有指定被监视的接口

操作	命令	说明
配置监视指定的Track项	**vrrp ipv6 vrid** *virtual-router-id* **track** *track-entry-number* [**reduced** *priority-reduced* | **switchover**]	可选 缺省情况下，没有指定被监视的Track项

说明

- 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。
- 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。
- 被监视接口的状态由 Down 或 Removed 变为 Up 后，对应路由器的优先级数会自动恢复。
- 被监视 Track 项的状态由 Negative 变为 Positive 或 Invalid 后，对应的路由器优先级会自动恢复。

1.5.5 配置虚拟转发器监视功能

1. 配置准备

在配置虚拟转发器监视功能之前，需要先在接口上创建备份组并配置虚拟 IPv6 地址。

2. 配置过程

VRRP 工作在负载均衡模式时，如果配置虚拟转发器监视 Track 项并指定权重降低的数额，则当 Track 项状态为 Negative 时，路由器上所有虚拟转发器的权重都将降低指定的数额；被监视的 Track 项状态由 Negative 变为 Positive 或 Invalid 后，路由器中所有虚拟转发器的权重会自动恢复。如果配置 LVF 通过 Track 功能监视 AVF 的状态，则当 Track 项状态为 Negative 时，LVF 会马上切换为 AVF，从而避免流量长时间中断。

表1-14 配置虚拟转发器监视功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置虚拟转发器监视指定的Track项，并指定权重降低的数额	**vrrp ipv6 vrid** *virtual-router-id* **weight track** *track-entry-number* [**reduced** *weight-reduced*]	二者至少选择其一 缺省情况下，没有配置虚拟转发器的监视功能
配置LVF通过Track功能监视AVF的状态	**vrrp ipv6 vrid** *virtual-router-id* **track** *track-entry-number* **forwarder-switchover member-ip** *ipv6-address*	

说明

- 在 VRRP 标准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 负载模式下虚拟转发器监视功能才会起作用。
- 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，因此只有配置的权重降低数额能够保证监视的上行链路出现故障时 VF Owner 的权重低于失效下限，即权重降低的数额大于 245，其他的虚拟转发器才能接替 VF Owner 成为 AVF。

1.5.6 配置VRRP报文的相关属性

1. 配置准备

在配置 VRRP 报文的相关属性之前，需要先在接口上创建备份组并配置虚拟 IPv6 地址。

2. 配置过程

表1-15 配置 VRRP 报文的相关属性

操作	命令	说明
进入系统视图	**system-view**	-
配置VRRP报文的DSCP优先级	**vrrp ipv6 dscp** *dscp-value*	可选 缺省情况下，VRRP报文的DSCP优先级为56
进入接口视图	**interface** *interface-type interface-number*	-
配置备份组发送和接收VRRP报文的认证方式和认证字	**vrrp ipv6 vrid** *virtual-router-id* **authentication-mode simple** [**cipher**] *key*	可选 缺省情况下，不进行认证
配置备份组中Master路由器发送VRRP通告报文的时间间隔	**vrrp ipv6 vrid** *virtual-router-id* **timer advertise** *adver-interval*	可选 缺省情况下，备份组中Master路由器发送VRRP通告报文的时间间隔为100厘秒

说明

- 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；加入同一备份组的成员需要设置相同的认证方式和认证字。
- 网络流量过大可能会导致 Backup 路由器在指定时间内没有收到 Master 的 VRRP 通告报文，而发生状态转换。可以通过将 VRRP 通告报文的发送时间间隔延长的办法来解决该问题。
- 备份组中不同路由器上配置的 VRRP 通告报文发送时间间隔不同，也可能会导致 Backup 路由器在指定时间内没有收到 Master 的 VRRP 通告报文，而发生状态转换。可以通过修改路由器上的 VRRP 通告报文发送时间间隔、使得备份组中所有路由器上该值相同的方法来解决此问题。

1.5.7 基于IPv6 的VRRP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示基于 IPv6 的 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** 命令可以清除基于 IPv6 的 VRRP 统计信息。

表1-16 VRRP 显示和维护

操作	命令
显示VRRP备份组的状态信息	**display vrrp ipv6** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示VRRP备份组的统计信息	**display vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除VRRP备份组的统计信息	**reset vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

1.6 基于IPv4的VRRP典型配置举例

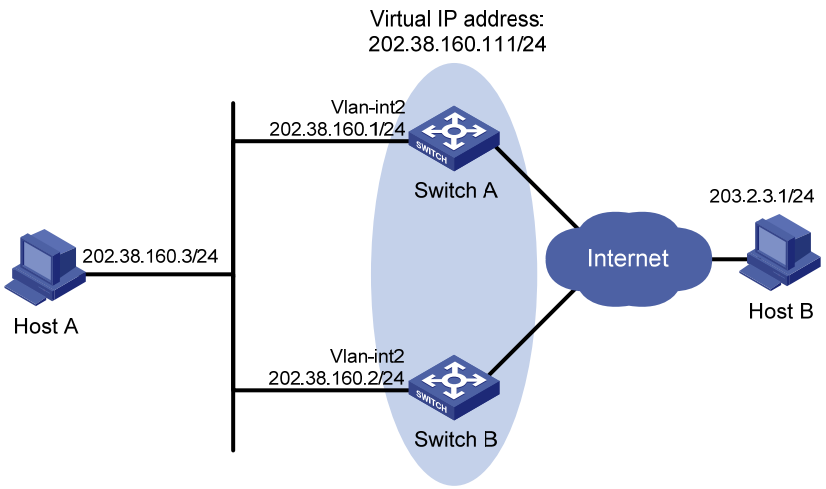
1.6.1 VRRP单备份组配置举例

1. 组网需求

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 202.38.160.111/24；
- Switch A 和 Switch B 属于虚拟 IP 地址为 202.38.160.111/24 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 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1-11 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 202.38.160.1 255.255.255.0
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 202.38.160.111。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

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 5 秒。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

(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 202.38.160.2 255.255.255.0
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 202.38.160.111。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

设置 Switch B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

(3) 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp verbose** 命令查看配置后的结果。

显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer   : 1
     Admin Status   : Up             State         : Master
     Config Pri     : 110            Running Pri   : 110
     Preempt Mode   : Yes            Delay Time    : 5
     Auth Type      : None
```

```
    Virtual IP      : 202.38.160.111
    Virtual MAC     : 0000-5e00-0101
    Master IP       : 202.38.160.1
```

显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
    Run Mode        : Standard
    Run Method      : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
    VRID            : 1               Adver Timer   : 1
    Admin Status    : Up              State         : Backup
    Config Pri      : 100             Running Pri   : 100
    Preempt Mode    : Yes             Delay Time    : 5
    Become Master   : 4200ms left
    Auth Type       : None
    Virtual IP      : 202.38.160.111
    Master IP       : 202.38.160.1
```

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

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 Standby Information:
    Run Mode        : Standard
    Run Method      : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
    VRID            : 1               Adver Timer   : 1
    Admin Status    : Up              State         : Master
    Config Pri      : 100             Running Pri   : 100
    Preempt Mode    : Yes             Delay Time    : 5
    Auth Type       : None
    Virtual IP      : 202.38.160.111
    Virtual MAC     : 0000-5e00-0101
    Master IP       : 202.38.160.2
```

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

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 Standby Information:
    Run Mode        : Standard
    Run Method      : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
```

```
VRID            : 1                 Adver Timer   : 1
Admin Status    : Up                State         : Master
Config Pri      : 110               Running Pri   : 110
Preempt Mode    : Yes               Delay Time    : 5
Auth Type       : None
Virtual IP      : 202.38.160.111
Virtual MAC     : 0000-5e00-0101
Master IP       : 202.38.160.1
```

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。

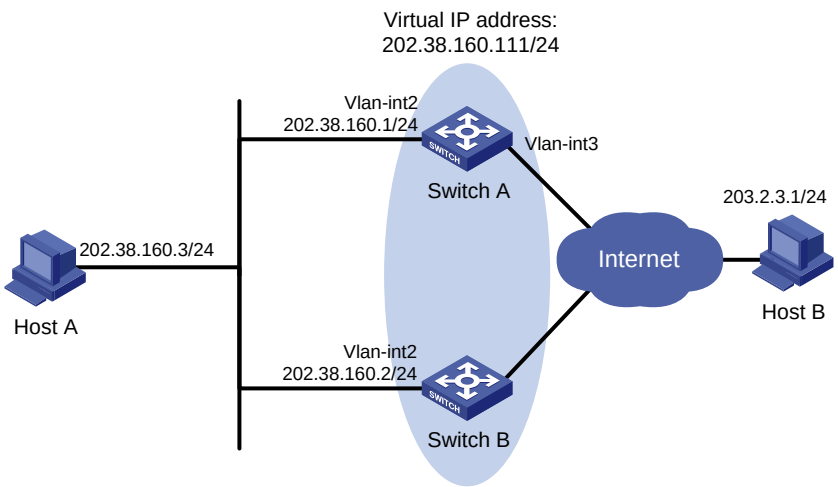
1.6.2 VRRP监视接口配置举例

1. 组网需求

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 202.38.160.111/24；
- Switch A 和 Switch B 属于虚拟 IP 地址为 202.38.160.111/24 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 Switch A 连接 Internet 的 VLAN 接口 3 不可用时，Host A 发送给 Host B 的报文通过 Switch B 转发；
- 为了防止非法用户构造报文攻击备份组，通过简单字符认证方法验证备份组 1 中的 VRRP 报文，认证字为 hello。

2. 组网图

图1-12 VRRP 监视接口配置组网图



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 202.38.160.1 255.255.255.0
```
创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 202.38.160.111。
```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```
设置 Switch A 在备份组中的优先级为 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
```
设置备份组的认证方式为 SIMPLE 认证，认证字为 hello。
```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```
设置 Master 发送 VRRP 报文的间隔时间为 4 秒。
```
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 4
```
设置 Switch A 工作在抢占方式，以保证 Switch A 故障恢复后，能再次抢占成为 Master，即只要 Switch A 正常工作，就由 Switch A 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。
```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```
配置 Switch A 监视上行接口——VLAN 接口 3，当 VLAN 接口 3 不可用时，降低 Switch A 在备份组 1 中的优先级。降低后的优先级应低于 Switch B 的优先级 100，即优先级降低数额应大于 10，以保证 Switch B 能够抢占成为 Master。本例中，配置优先级降低数额为 30。
```
[SwitchA-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 3 reduced 30
```
(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 202.38.160.2 255.255.255.0
```
创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 202.38.160.111。
```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```
设置备份组的认证方式为 SIMPLE 认证，认证字为 hello。
```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```
设置 Master 发送 VRRP 报文的间隔时间为 4 秒。
```
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 4
```
设置 Switch B 工作在抢占方式，以保证 Switch A 的优先级降低后，Switch B 可以抢占成为 Master。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。
```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```
(3) 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp verbose** 命令查看配置后的结果。

显示 Switch A 上备份组 1 的详细信息。
```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
```

```
  Interface Vlan-interface2
    VRID           : 1               Adver Timer  : 4
    Admin Status   : Up              State        : Master
    Config Pri     : 110             Running Pri  : 110
    Preempt Mode   : Yes             Delay Time   : 5
    Auth Type      : Simple          Key          : ******
    Virtual IP     : 202.38.160.111
    Virtual MAC    : 0000-5e00-0101
    Master IP      : 202.38.160.1
  VRRP Track Information:
    Track Interface: Vlan3          State : Up               Pri Reduced : 30
```

显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 4
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.1
```

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

Switch A 连接 Internet 的 VLAN 接口 3 不可用时，在 Host A 上仍然可以 ping 通 Host B。通过 **display vrrp verbose** 命令查看备份组的信息。

Switch A 的 VLAN 接口 3 不可用时，显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 4
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 80
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.2
   VRRP Track Information:
     Track Interface: Vlan3          State : Down             Pri Reduced : 30
```

Switch A 的 VLAN 接口 3 不可用时，显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer   : 4
     Admin Status   : Up             State         : Master
     Config Pri     : 100            Running Pri   : 100
     Preempt Mode   : Yes            Delay Time    : 5
     Auth Type      : Simple         Key           : ******
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.2
```

以上显示信息表示 Switch A 的 VLAN 接口 3 不可用时，Switch A 的优先级降低为 80，成为 Backup 路由器，Switch B 成为 Master 路由器，Host A 发送给 Host B 的报文通过 Switch B 转发。

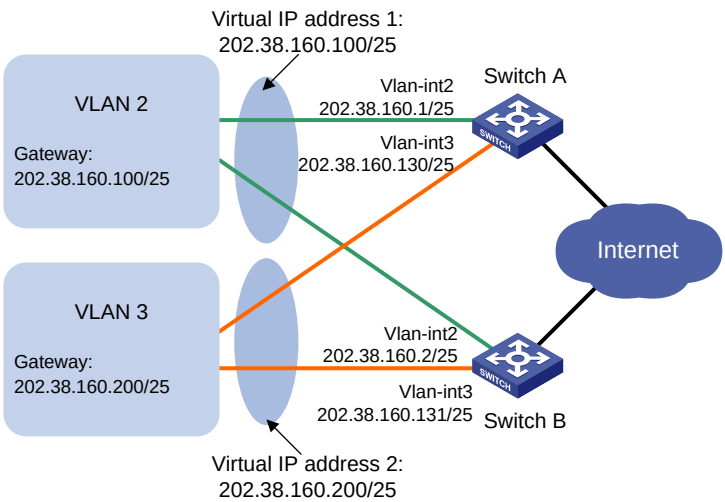
1.6.3 多个VLAN中的VRRP备份组配置举例

1. 组网需求

- VLAN 2 内主机的缺省网关为 202.38.160.100/25；VLAN 3 内主机的缺省网关为 202.38.160.200/25；
- Switch A 和 Switch B 同时属于虚拟 IP 地址为 202.38.160.100/25 的备份组 1 和虚拟 IP 地址为 202.38.160.200/25 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1-13 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] ip address 202.38.160.1 255.255.255.128
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 202.38.160.100。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
```

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 202.38.160.130 255.255.255.128
```

创建备份组 2，并配置备份组 2 的虚拟 IP 地址为 202.38.160.200。

```
[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

(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 202.38.160.2 255.255.255.128
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 202.38.160.100。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
[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 202.38.160.131 255.255.255.128
```

创建备份组 2，并配置备份组 2 的虚拟 IP 地址为 202.38.160.200。

```
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

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
```

(3) 验证配置结果

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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 1
     Admin Status   : Up             State        : Master
     Config Pri     : 110            Running Pri  : 110
     Preempt Mode   : Yes            Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 202.38.160.100
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.1

   Interface Vlan-interface3
     VRID           : 2              Adver Timer  : 1
     Admin Status   : Up             State        : Backup
     Config Pri     : 100            Running Pri  : 100
     Preempt Mode   : Yes            Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 202.38.160.200
     Master IP      : 202.38.160.131
```

显示 Switch B 上备份组的详细信息。

```
[SwitchB-Vlan-interface3] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 1
     Admin Status   : Up             State        : Backup
     Config Pri     : 100            Running Pri  : 100
     Preempt Mode   : Yes            Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 202.38.160.100
     Master IP      : 202.38.160.1

   Interface Vlan-interface3
     VRID           : 2              Adver Timer  : 1
     Admin Status   : Up             State        : Master
```

```
Config Pri      : 110              Running Pri   : 110
Preempt Mode    : Yes              Delay Time    : 0
Auth Type       : None
Virtual IP      : 202.38.160.200
Virtual MAC     : 0000-5e00-0102
Master IP       : 202.38.160.131
```

以上显示信息表示在备份组 1 中 Switch A 为 Master 路由器，Switch B 为 Backup 路由器，缺省网关为 202.38.160.100/25 的主机通过 Switch A 访问 Internet；备份组 2 中 Switch A 为 Backup 路由器，Switch B 为 Master 路由器，缺省网关为 202.38.160.200/25 的主机通过 Switch B 访问 Internet。

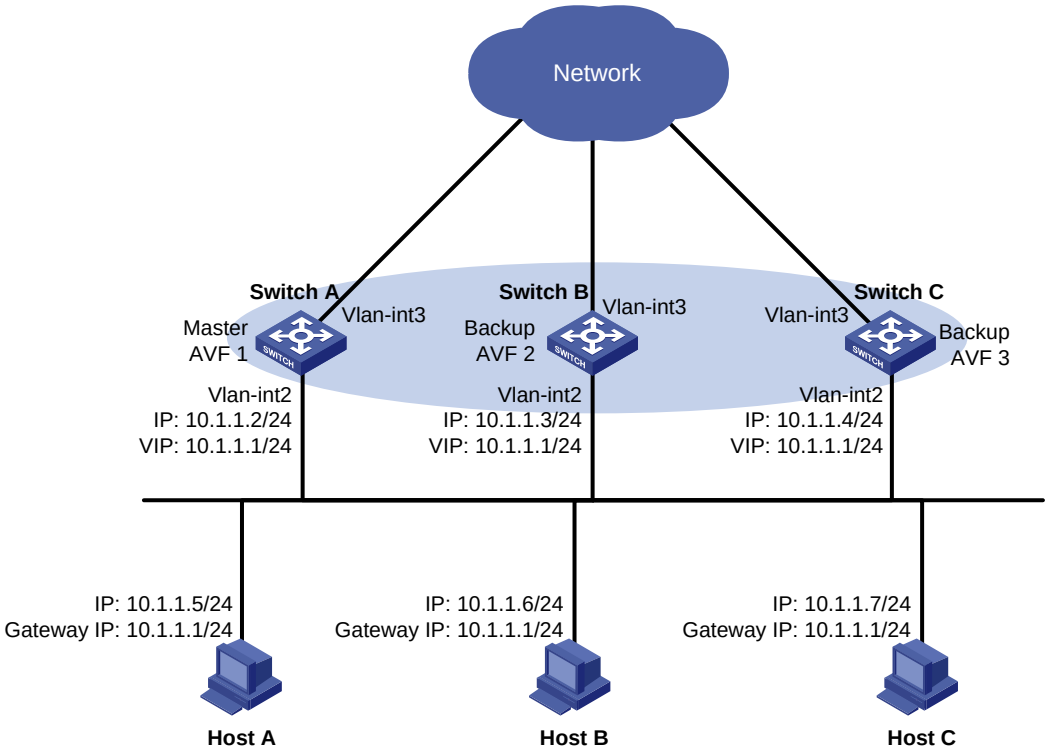
1.6.4 VRRP负载均衡模式配置举例

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，以便其他设备接管它的转发任务；
- 在 Switch C 上通过 Track 项监视 Switch A 和 Switch B 的状态，当 Switch A 或 Switch B 出现故障时，Switch C 立即接管 Switch A 或 Switch B 上的 AVF。

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 VLAN2。

```
<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 5 秒。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[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 并指定权重降低的数额。Track 项的状态为 Negative 时，降低 Switch A 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Switch A 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
```

(2) 配置 Switch B

配置 VLAN2。

```
<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 Swtich 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 5 秒。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[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 并指定权重降低的数额。Track 项的状态为 Negative 时，降低 Switch B 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Switch B 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
```

(3) 配置 Switch C

配置 VLAN2。

```
<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 5 秒。
```
[SwitchC-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[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 并指定权重降低的数额。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，以便其他设备接替 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 weight track 1 reduced 250
[SwitchC-Vlan-interface2] quit
```
分别创建监视 Switch A、Switch B 的 Track 项 2 和 3。如果 Track 项的状态为 Negative，则说明 Switch A 或 Switch B 出现故障。
```
[SwitchC] bfd echo-source-ip 1.2.3.4
[SwitchC] track 2 bfd echo interface vlan-interface 2 remote ip 10.1.1.2 local ip 10.1.1.4
[SwitchC] track 3 bfd echo interface vlan-interface 2 remote ip 10.1.1.3 local ip 10.1.1.4
```
配置虚拟转发器监视 Track 项 2，当 Track 项状态变为 Negative 时，如果 Switch C 上 AVF 地址为 10.1.1.2 的虚拟转发器处于 Listening 状态，则马上将该虚拟转发器切换到 Active 状态，即 Switch C 接管 Switch A 上的 AVF。
```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp vrid 1 track 2 forwarder-switchover member-ip 10.1.1.2
```
配置虚拟转发器监视 Track 项 3，当 Track 项状态变为 Negative 时，如果 Switch C 上 AVF 地址为 10.1.1.3 的虚拟转发器处于 Listening 状态，则马上将该虚拟转发器切换到 Active 状态，即 Switch C 接管 Switch B 上的 AVF。
```
[SwitchC-Vlan-interface2] vrrp vrid 1 track 3 forwarder-switchover member-ip 10.1.1.3
```
(4) 验证配置结果

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 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer   : 1
     Admin Status   : Up              State         : Master
     Config Pri     : 120             Running Pri   : 120
     Preempt Mode   : Yes             Delay Time    : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
```

```
                    10.1.1.4 (Backup)
  Forwarder Information: 3 Forwarders 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 Standby Information:
    Run Mode       : Load Balance
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1               Adver Timer  : 1
    Admin Status   : Up              State        : Backup
    Config Pri     : 110             Running Pri  : 110
    Preempt Mode   : Yes             Delay Time   : 5
    Become Master  : 4200ms 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 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms 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
Forwarder Switchover Track Information:
  Track Object   : 2              State : Positive
    Member IP    : 10.1.1.2
  Track Object   : 3              State : Positive
    Member IP    : 10.1.1.3
```

以上显示信息表示在备份组 1 中 Switch A 为 Master 路由器，Switch B 和 Switch C 为 Backup 路由器。Switch A、Switch B 和 Switch C 上各自存在一个 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 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 1
     Admin Status   : Up             State        : Master
     Config Pri     : 120            Running Pri  : 120
     Preempt Mode   : Yes            Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : 10.1.1.4
    Forwarder 02
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 0
     Active         : 10.1.1.3
    Forwarder 03
```

```
    State           : Initialize
    Virtual MAC     : 000f-e2ff-0013 (Learnt)
    Owner ID        : 0000-5e01-1105
    Priority        : 0
    Active          : 10.1.1.4
  Forwarder Weight Track Information:
    Track Object    : 1             State : Negative       Weight Reduced : 250
```

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 Standby Information:
     Run Mode        : Load Balance
     Run Method      : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID            : 1               Adver Timer  : 1
     Admin Status    : Up              State        : Backup
     Config Pri      : 100             Running Pri  : 100
     Preempt Mode    : Yes             Delay Time   : 5
     Become Master   : 4200ms 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
     Redirect Time   : 93 secs
     Time-out Time   : 1293 secs
    Forwarder 02
     State           : Listening
     Virtual MAC     : 000f-e2ff-0012 (Learnt)
     Owner ID        : 0000-5e01-1103
     Priority        : 85
     Active          : 10.1.1.3
    Forwarder 03
     State           : Active
     Virtual MAC     : 000f-e2ff-0013 (Owner)
     Owner ID        : 0000-5e01-1105
     Priority        : 255
     Active          : local
   Forwarder Weight Track Information:
```

```
    Track Object   : 1              State : Positive       Weight Reduced : 250
  Forwarder Switchover Track Information:
    Track Object   : 2              State : Positive
      Member IP    : 10.1.1.2
    Track Object   : 3              State : Positive
      Member IP    : 10.1.1.3
```

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 Initialized，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 Standby Information:
    Run Mode       : Load Balance
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1               Adver Timer  : 1
    Admin Status   : Up              State        : Backup
    Config Pri     : 100             Running Pri  : 100
    Preempt Mode   : Yes             Delay Time   : 5
    Become Master  : 4200ms 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
  Forwarder Switchover Track Information:
    Track Object   : 2              State : Positive
      Member IP    : 10.1.1.2
    Track Object   : 3              State : Positive
      Member IP    : 10.1.1.3
```

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

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 路由器。

Switch B 出现故障后，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 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/1
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
```

```
  Auth Type       : None
  Virtual IP      : 10.1.1.1
  Member IP List  : 10.1.1.4 (Local, Master)
Forwarder Information: 2 Forwarders 2 Active
  Config Weight   : 255
  Running Weight  : 255
 Forwarder 02
  State           : Active
  Virtual MAC     : 000f-e2ff-0012 (Take Over)
  Owner ID        : 0000-5e01-1103
  Priority        : 85
  Active          : local
  Redirect Time   : 93 secs
  Time-out Time   : 1293 secs
 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
Forwarder Switchover Track Information:
  Track Object    : 2               State : Negative
    Member IP     : 10.1.1.2
  Track Object    : 3               State : Negative
    Member IP     : 10.1.1.3
```

以上显示信息表示 Switch B 出现故障后，Switch C 切换成为 Master，并且 Switch C 上 Forwarder 02 马上切换到 Active 状态，即 Switch C 立即接管 Switch B 上的 AVF。

1.7 基于IPv6的VRRP典型配置举例

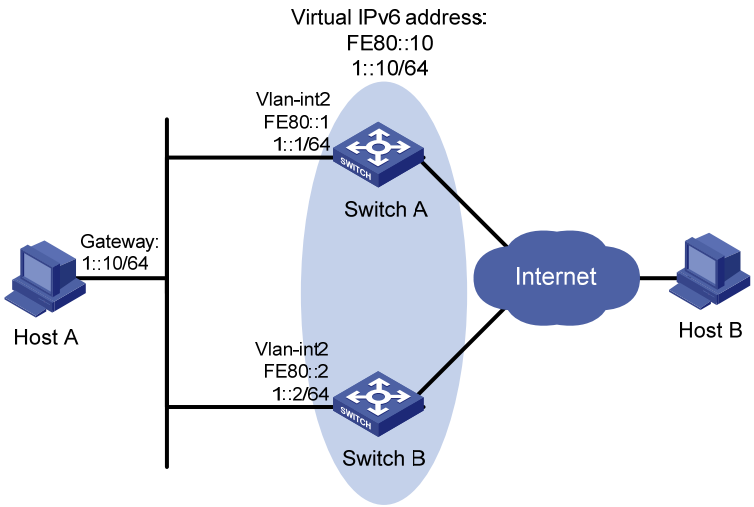
1.7.1 VRRP单备份组配置举例

1. 组网需求

- Switch A 和 Switch B 属于虚拟 IPv6 地址为 1::10/64 和 FE80::10 的备份组 1；
- 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1-15 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] ipv6
[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 5 秒。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

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 VLAN2。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
[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 5 秒。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

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
```

(3) 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp 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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 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   : 5
     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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 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   : 5
     Become Master  : 4200ms left
     Auth Type      : None
```

```
    Virtual IP     : FE80::10
                     1::10
    Master IP      : FE80::1
```

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

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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 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   : 5
     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 路由器，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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 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   : 5
     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。

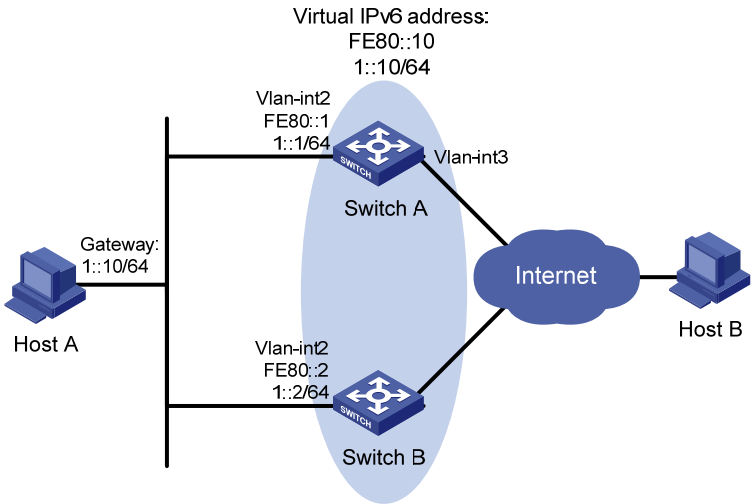
1.7.2 VRRP监视接口配置举例

1. 组网需求

- Switch A 和 Switch B 属于虚拟 IPv6 地址为 1::10/64 和 FE80::10 的备份组 1；
- 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 连接 Internet 的 VLAN 接口 3 不可用时，Host A 发送给 Host B 的报文通过 Switch B 转发；
- 为了防止非法用户构造报文攻击备份组，通过简单字符认证方法验证备份组 1 中的 VRRP 报文，认证字为 hello。

2. 组网图

图1-16 VRRP 监视接口配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 VLAN2。

```
<SwitchA> system-view
[SwitchA] ipv6
[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
```
设置备份组的认证方式为 SIMPLE，认证字为 hello。
```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 authentication-mode simple hello
```
设置 VRRP 通告报文发送的间隔时间为 400 厘秒。
```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 400
```
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，就由 Switch A 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。
```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```
配置 Switch A 监视上行接口——VLAN 接口 3，当 VLAN 接口 3 不可用时，降低 Switch A 在备份组 1 中的优先级。降低后的优先级应低于 Switch B 的优先级 100，即优先级降低数额应大于 10，以保证 Switch B 能够抢占成为 Master。本例中，配置优先级降低数额为 30。
```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 3 reduced 30
```
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 VLAN2。
```
<SwitchB> system-view
[SwitchB] ipv6
[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
```
设置备份组的认证方式为 SIMPLE，认证字为 hello。
```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 authentication-mode simple hello
```
设置 VRRP 通告报文发送的间隔时间为 400 厘秒。
```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 400
```
配置 Switch B 工作在抢占方式，以保证 Switch A 的优先级降低后，Switch B 可以抢占成为 Master。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。
```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```
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
```
(3) 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp 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 Standby Information:
     Run Mode       : Standard
```

```
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 400
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : Simple          Key          : ******
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Interface: Vlan3          State : Up                Pri Reduced : 30
```

显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 400
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::1
```

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

Switch A 连接 Internet 的 VLAN 接口 3 不可用时，在 Host A 上仍然可以 ping 通 Host B。通过 **display vrrp ipv6 verbose** 命令查看备份组的信息。

Switch A 的 VLAN 接口 3 不可用时，显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 400
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 80
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : Simple          Key          : ******
```

```
    Virtual IP      : FE80::10
                      1::10
    Master IP       : FE80::2
  VRRP Track Information:
    Track Interface: Vlan3         State : Down              Pri Reduced : 30
```

Switch A 的 VLAN 接口 3 不可用时，显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode        : Standard
     Run Method      : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID            : 1               Adver Timer   : 400
     Admin Status    : Up              State         : Master
     Config Pri      : 100             Running Pri   : 100
     Preempt Mode    : Yes             Delay Time    : 5
     Auth Type       : Simple          Key           : ******
     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 的 VLAN 接口 3 不可用时，Switch A 的优先级降低为 80，成为 Backup 路由器，Switch B 成为 Master 路由器，Host A 发送给 Host B 的报文通过 Switch B 转发。

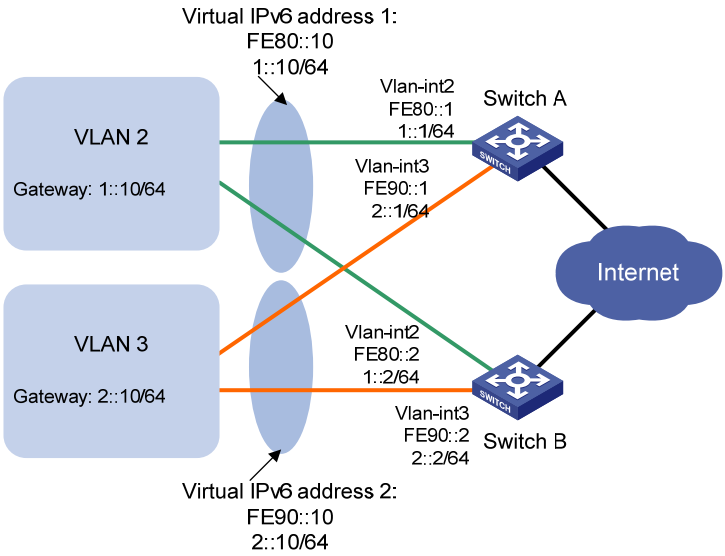
1.7.3 多个VLAN中的VRRP备份组配置举例

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1-17 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] ipv6
[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] ipv6
[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
```
(3) 验证配置结果

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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 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   : 2200ms left
    Auth Type       : None
    Virtual IP      : FE90::10
                      2::10
    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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 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   : 2200ms left
     Auth Type       : None
     Virtual IP      : FE80::10
                       1::10
     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 路由器，Switch B 为 Backup 路由器，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 路由器，Switch B 为 Master 路由器，缺省网关为 2::10/64 的主机通过 Switch B 访问 Internet。

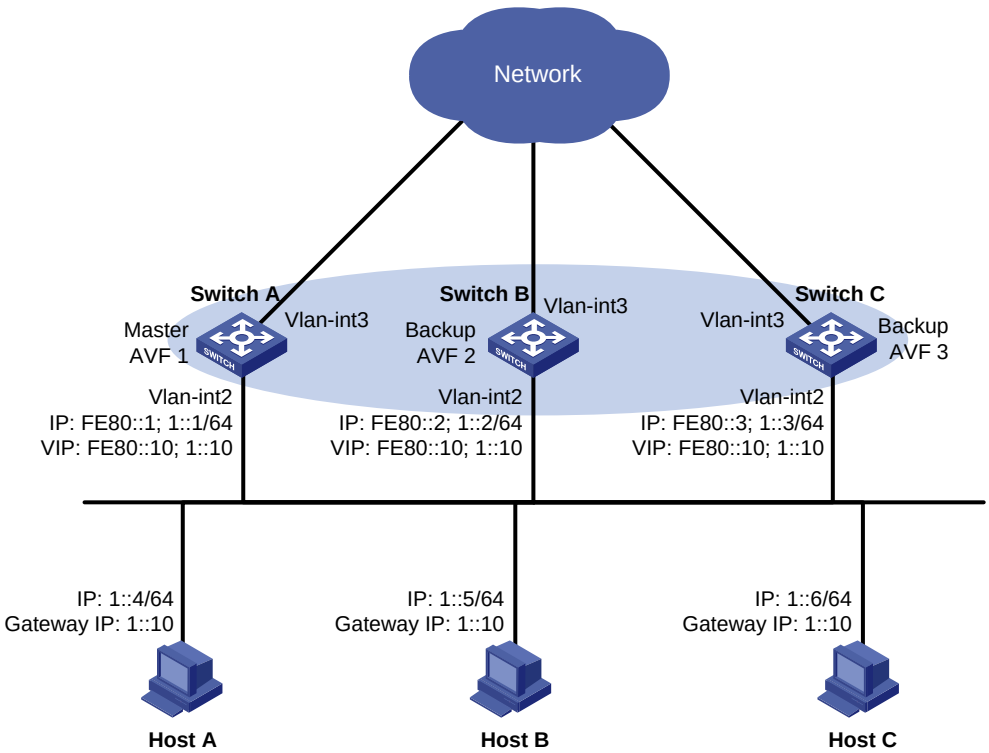
1.7.4 VRRP负载均衡模式配置举例

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，以便其他设备接管它的转发任务。

2. 组网图

图1-18 VRRP 负载均衡模式配置组网图



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
```
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 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 5 秒。
```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```
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 并指定权重降低的数额。Track 项的状态为 Negative 时，降低 Switch A 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Switch A 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。
```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
```
(2)　配置 Switch B

配置 VLAN2。
```
<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 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 Swtich 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 5 秒。
```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```
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 并指定权重降低的数额。Track 项的状态为 Negative 时，降低 Switch B 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Switch B 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。
```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
```
(3) 配置 Switch C

配置 VLAN2。
```
<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 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 5 秒。
```
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```
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 并指定权重降低的数额。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，以便其他设备接替 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 weight track 1 reduced 250
```
(4) 验证配置结果

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 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 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   : 5
     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 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 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    : 5
    Become Master  : 2200ms 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 Standby Information:
    Run Mode       : Load Balance
    Run Method     : Virtual MAC
 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    : 5
    Become Master  : 4200ms 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 路由器，Switch B 和 Switch C 为 Backup 路由器。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 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 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   : 5
     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 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 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   : 5
     Become Master  : 4200ms 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
```

```
    Redirect Time  : 93 secs
    Time-out Time  : 1293 secs
  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 Initialized，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 Standby Information:
    Run Mode       : Load Balance
    Run Method     : Virtual MAC
 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   : 5
    Become Master  : 4200ms 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 Standby Information:
    Run Mode       : Load Balance
    Run Method     : Virtual MAC
 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   : 5
    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 路由器。

1.8 VRRP常见错误配置举例

1. 频频出现配置错误的提示

原因分析：

- 可能是备份组内的另一台路由器配置不一致造成的。
- 可能是有的机器试图发送非法的 VRRP 报文。

解决方法：

- 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，则是有些机器有不良企图，应当通过非技术手段来解决。

2. 同一个备份组内出现多个Master路由器

原因分析：

- 若短时间内存在多个 Master 路由器，属于正常情况，无需进行人工干预。
- 若多个 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。

解决方法：先在多个 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、通告报文的发送时间间隔和认证方式完全一样。

3. VRRP的状态频繁转换

原因分析：这种情况一般是由于 VRRP 通告报文发送时间间隔太短造成的。

解决方法：增加通告报文的发送时间间隔或者设置抢占延迟都可以解决这种故障。

目 录

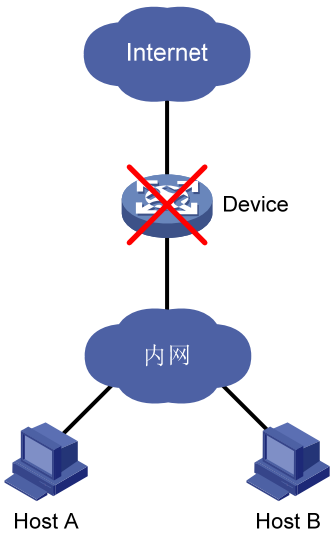
1 双机热备配置

1.1 双机热备简介

1.1.1 双机热备概述

随着用户对网络可靠性的要求越来越高，如何保证网络的不间断传输，已成为一个必须解决的问题。特别是在一些重要业务的入口或接入点上，需要保证网络的不间断运行，如企业的Internet接入点、银行的数据库服务器等。在这些业务点上如果只使用一台设备，无论其可靠性多高，系统都必然要承受因单点故障而导致网络业务中断的风险，如 图 1-1 所示。

图1-1 非双机热备组网



为解决上述问题，引入了双机热备机制，如 图 1-2 所示。双机热备机制主要包括两方面内容：双机业务备份和流量倒换。其基本流程为：

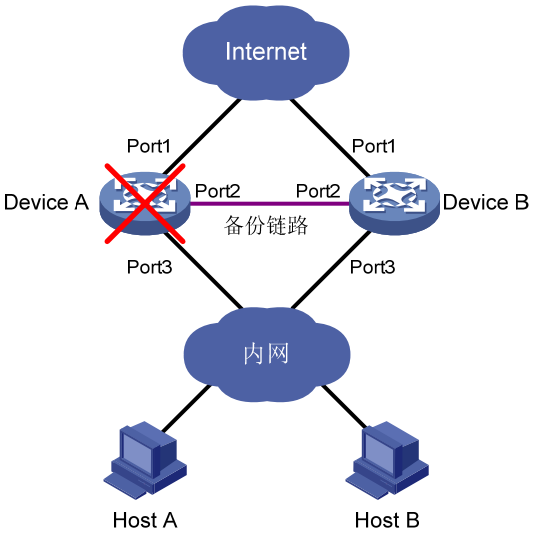
(1) 建立备份链路，即将两台设备上的备份接口连接起来。

(2) 两台设备通过备份链路定时互相发送状态协商报文，当设备进入同步状态后，开始备份对端设备上的业务，直至两台设备上的业务状态完全一致。

(3) 当其中一台设备发生故障时，利用 VRRP 或动态路由（例如 OSPF）机制将业务流量切换到对端设备，业务数据流便可以从对端设备上通过，从而在很大程度上避免了网络业务的中断。

本文仅描述双机热备中双机业务备份，当前仅支持对 Portal 业务信息进行备份。

图1-2 双机热备组网



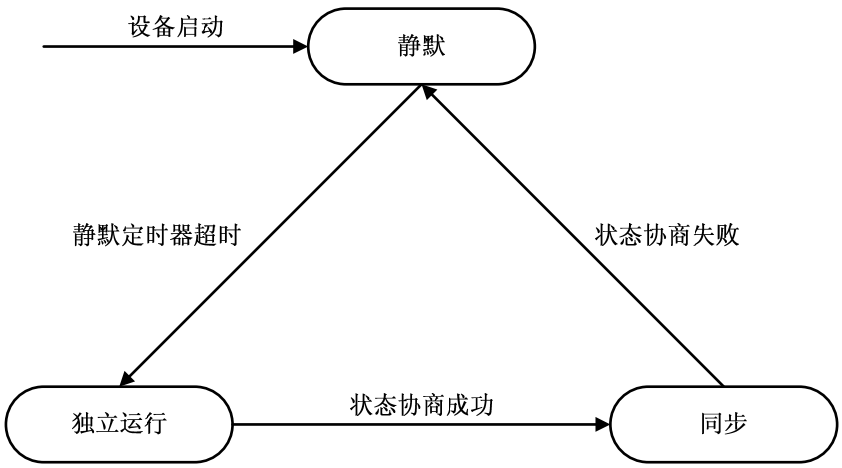
1.1.2 热备状态简介

设备的热备状态有静默、独立运行和同步三种。

- 静默：表示设备刚启动正在等待系统稳定，或者热备状态正在从同步向独立运行转换的中间状态。
- 独立运行：表示静默定时器超时，但是设备没有与其它设备建立备份连接。
- 同步：表示设备与对端设备状态协商成功，可以进行业务备份。

三种状态之间的转换关系如 图 1-3 所示。

图1-3 热备状态转换关系图



1.2 双机热备配置任务简介

要实现两台设备之间互为热备份，必须进行以下配置：

- 路由相关配置。在本设备以及上、下层设备上进行 VRRP 或者动态路由配置，以保证当一台设备故障时，流量能够自动切换到备份设备。
- 业务备份配置，用于实现两台设备之间业务相关信息的实时备份。

本文仅描述业务备份配置。

表1-1 业务备份配置任务简介

配置任务	说明	详细配置
使能业务备份功能	必选	1.3
配置备份VLAN	必选	1.4
业务模块的相关配置	可选	除了“使能业务备份功能”、“配置备份VLAN”，还需要其它配置，才能将Portal业务的相关信息自动备份到备份设备，相关配置请参见“安全配置指导”中的“Portal”

1.3 使能业务备份功能

在开启双机热备业务备份功能时，可以指定 **dissymmetric-path** 和 **symmetric-path** 参数。其中

- **dissymmetric-path** 表示业务备份支持非对称路径。使用该参数时，同一条会话中的数据流进入内网时经过双机热备中的一台设备，从内网出去时经过的设备是随机的，可以是进入时经过的设备，也可以是另一台设备。两台设备均处理业务，互为备份。
- **symmetric-path** 表示业务备份仅支持对称路径。使用该参数时，要求同一条会话中的数据流进入内网和从内网出去时必须经过双机热备中的同一台设备。一台设备处理业务，另一台设备只用作备份。

在实际应用中，选用 **dissymmetric-path** 还是 **symmetric-path**，需要参考组网环境和可使用的网络资源，但本设备和对端设备的配置必须一致，要么均为 **dissymmetric-path**，要么均为 **symmetric-path**。

表1-2 配置业务备份

操作	命令	说明
进入系统视图	**system-view**	-
开启双机热备业务备份功能	**dhbk enable backup-type { dissymmetric-path | symmetric-path }**	必选 缺省情况下，双机热备业务备份功能处于关闭状态

1.4 配置备份VLAN

本特性所指的备份 VLAN 是专用于双机热备的 VLAN。将某 VLAN 配置为备份 VLAN 后，该 VLAN 内的接口就能作为备份接口用于传输双机热备相关报文。

表1-3 配置备份 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
创建VLAN并将接口加入指定VLAN	请参见“二层技术-以太网交换配置指导”中的“VLAN”	必选
退回到系统视图	**quit**	-
将指定VLAN配置为备份VLAN	**dhbk vlan** *vlan-id*	必选 缺省情况下，系统没有配置备份VLAN

说明

- 设备使用 VLAN tag+私有协议号来标识双机热备报文，并在备份 VLAN 内使用广播方式将双机热备报文发送到对端。因此，建议在备份 VLAN 下不要配置其它业务（比如将备份 VLAN 配置为 MAC VLAN、Voice VLAN 等），以免影响是双机热备功能的运行。
- 接口加入备份 VLAN 后，除了传输双机热备报文还可用于转发其它报文。

1.5 双机热备显示和维护

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双机热备功能的运行情况，通过查看显示信息验证配置的效果。

表1-4 双机热备显示和维护

操作	命令
显示双机热备管理的运行状态和相关信息	**display dhbk status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

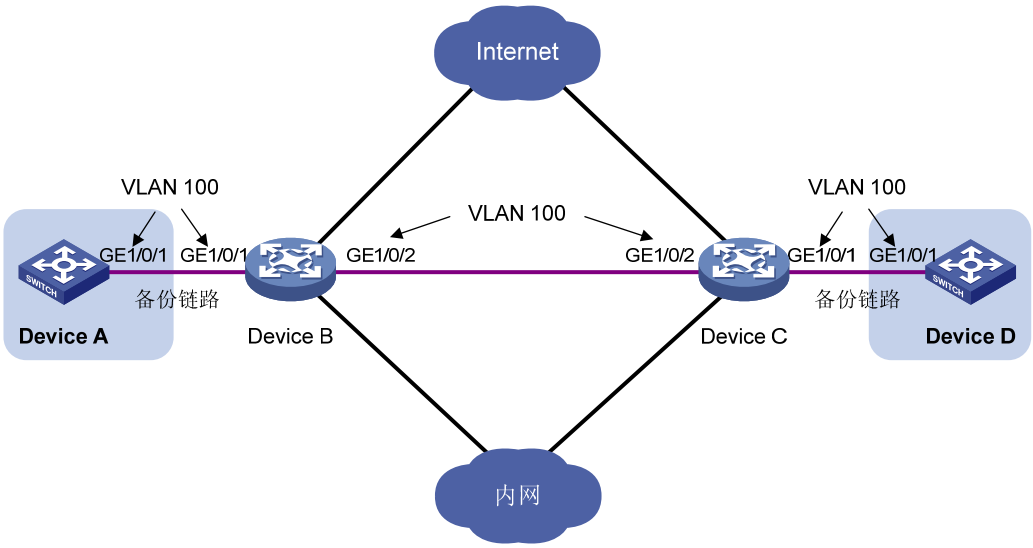
1.6 双机热备典型配置举例

1. 组网需求

如 图 1-4 所示，Device B和Device C作为某企业内部网络的网关，Device A和Device D通过旁挂方式分别与Device B和Device C相连，为企业内部用户提供Portal接入认证。现要求Device A和Device D两设备互为备份，当其中一台设备故障时，另一台设备能迅速接替工作，保证网络业务不中断。

2. 组网图

图1-4 双机热备管理典型组网图



3. 配置步骤

(1) Device A 的配置

创建 VLAN 100。

```
<DeviceA> system-view
[DeviceA] vlan 100
```

将端口 GigabitEthernet1/0/1 加入 VLAN 100。

```
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

设置 VLAN 100 为备份 VLAN

```
[DeviceA] dhbk vlan 100
```

使能双机热备业务备份功能，且支持对称路径。

```
[DeviceA] dhbk enable backup-type symmetric-path
```

(2) Device B 的配置

创建 VLAN 100。

```
<DeviceB> system-view
[DeviceB] vlan 100
```

将端口 GigabitEthernet1/0/1 加入 VLAN 100。

```
[DeviceB-vlan100] port gigabitethernet 1/0/1
[DeviceB-vlan100] quit
```

将端口 GigabitEthernet1/0/2 加入 VLAN 100。

因为 Device B 和 Device C 之间可能要传输多个 VLAN 的报文，所以需要将 GigabitEthernet1/0/2 的类型设置为 Trunk，并允许 VLAN 100 通过。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100
 Please wait... Done.
```

(3) Device C 上的配置与 Device B 上的配置一致，不再赘述。

(4) Device D 上的配置与 Device A 上的配置一致，不再赘述。

1.7 注意事项

配置双机热备时需要注意如下事项：

- 双机热备目前只支持两台设备进行备份，不支持多台设备备份。
- 备份业务涉及的接口必须在双机热备的两台设备上同时存在，否则会导致备份数据不生效，业务报文丢失的情况。比如，设备 A 上的会话使用接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/3 传输信息，要成功进行热备，设备 B 上也必须有接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/3，反之亦然。

目 录

1 BFD配置

说明

- 本文所指的路由器代表运行了路由协议的三层设备。
- BFD 功能中所指的“接口”为三层口，包括 VLAN 接口、三层以太网端口等。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

1.1 BFD简介

为了减小设备故障对业务的影响、提高网络的可用性，设备需要能够尽快检测到与相邻设备间的通信故障，以便能够及时采取措施，从而保证业务继续进行。

现有的故障检测方法主要包括以下几种：

- 硬件检测：例如通过 SDH（Synchronous Digital Hierarchy，同步数字系列）告警检测链路故障。硬件检测的优点是可以很快发现故障，但并不是所有介质都能提供硬件检测。
- 慢 Hello 机制：通常采用路由协议中的 Hello 报文机制。这种机制检测到故障所需时间为秒级。对于高速数据传输，例如吉比特速率级，超过 1 秒的检测时间将导致大量数据丢失；对于时延敏感的业务，例如语音业务，超过 1 秒的延迟也是不能接受的。并且，这种机制依赖于路由协议。
- 其他检测机制：不同的协议有时会提供专用的检测机制，但在系统间互联互通时，这样的专用检测机制通常难以部署。

BFD（Bidirectional Forwarding Detection，双向转发检测）就是为了解决上述检测机制的不足而产生的，它是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况，保证邻居之间能够快速检测到通信故障，从而快速建立起备用通道恢复通信。

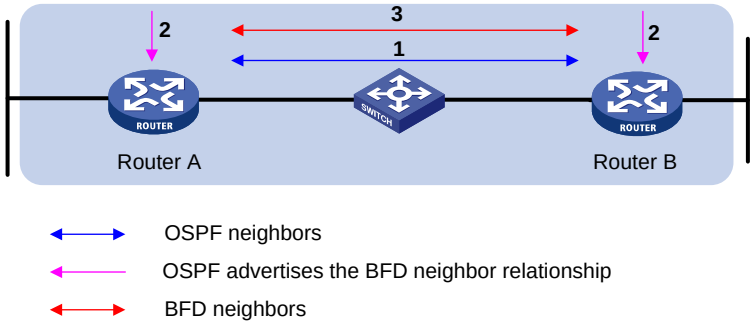
1.1.1 BFD工作机制

BFD 提供了一个通用的、标准化的、介质无关、协议无关的快速故障检测机制，可以为各上层协议如路由协议、MPLS 等统一地快速检测两台路由器间双向转发路径的故障。

BFD 在两台路由器上建立会话，用来监测两台路由器间的双向转发路径，为上层协议服务。BFD 本身并没有发现机制，而是靠被服务的上层协议通知其与谁建立会话，会话建立后如果在检测时间内没有收到对端的 BFD 控制报文则认为发生故障，通知被服务的上层协议，上层协议进行相应的处理。

1. BFD工作流程

图1-1 BFD 会话建立流程图（以 OSPF 为例）



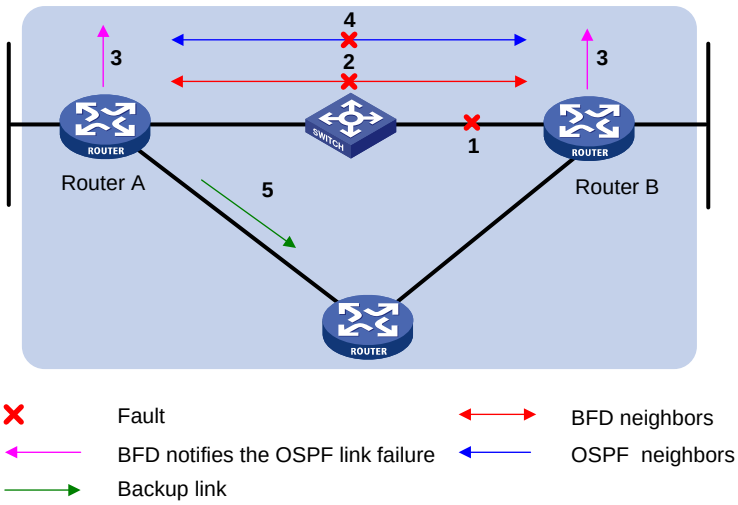
BFD 会话建立过程：

(1) 上层协议通过自己的 Hello 机制发现邻居并建立连接；

(2) 上层协议在建立了新的邻居关系时，将邻居的参数及检测参数都（包括目的地址和源地址等）通告给 BFD；

(3) BFD 根据收到的参数进行计算并建立邻居。

图1-2 BFD 处理网络故障流程图（以 OSPF 为例）



当网络出现故障时：

(1) BFD 检测到链路/网络故障；

(2) 拆除 BFD 邻居会话；

(3) BFD 通知本地上层协议进程 BFD 邻居不可达；

(4) 本地上层协议中止上层协议邻居关系；

(5) 如果网络中存在备用路径，路由器将选择备用路径。

说明

BFD 草案中没有规定检测的时间精度，目前支持 BFD 的设备大多数提供的是毫秒级检测。

2. BFD检测方式

- 单跳检测：BFD 单跳检测是指对两个直连系统进行 IP 连通性检测，这里所说的“单跳”是 IP 的一跳。
- 多跳检测：BFD 可以检测两个系统间的任意路径，这些路径可能跨越很多跳，也可能在某些部分发生重叠。
- 双向检测：BFD 通过在双向链路两端同时发送检测报文，检测两个方向上的链路状态，实现毫秒级的链路故障检测。（BFD 检测 LSP 是一种特殊情况，只需在一个方向发送 BFD 控制报文，对端通过其他路径报告链路状况。）

3. BFD会话的工作方式

- 控制报文方式：链路两端会话通过控制报文交互监测链路状态。
- Echo 报文方式：链路某一端通过发送 Echo 报文由另一端转发回来，实现对链路的双向监测。

4. BFD运行模式

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。

在会话初始化过程中，通信双方至少要有一个运行在主动模式才能成功建立起会话。

BFD 会话建立后通信双方均运行在异步模式：以异步模式运行的设备周期性地发送 BFD 控制报文，如果在检测时间内对端没有收到 BFD 控制报文，则认为会话 down。

说明

当 BFD 会话工作于 echo 报文方式时，不受运行模式控制。

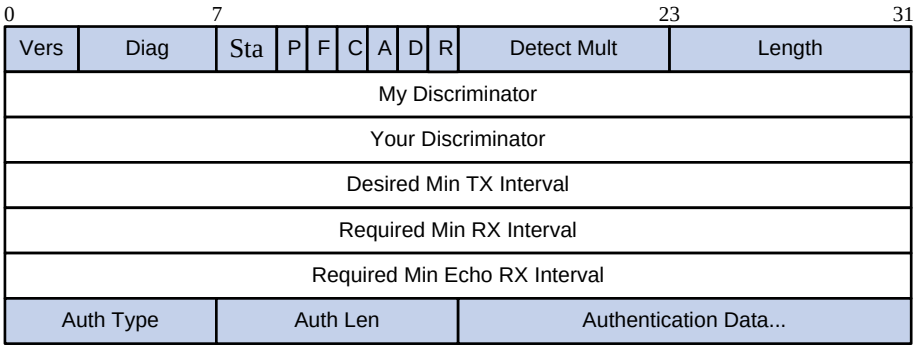
5. 动态改变BFD参数功能

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。

1.1.2 BFD报文格式

BFD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（也可配置为 3784，具体参见配置任务）。BFD echo报文与BFD控制报文格式类似（区别在于字段Desired Min TX Interval和Required Min RX Interval为空），其UDP目的端口号为 3785。报文格式如 图 1-3 所示。

图1-3 BFD 报文格式图



- Vers：协议的版本号，协议版本为 1。
- Diag：本地会话最后一次从up状态转换到其他状态的原因如 表 1-1：

表1-1 Diag 原因描述

Diag	描述
0	无诊断信息（No Diagnostic）
1	控制检测超时（Control Detection Time Expired）
2	回声功能失效（Echo Function Failed）
3	邻居通知会话down（Neighbor Signaled Session Down）
4	转发平面重启（Forwarding Plane Reset）
5	通道失效（Path Down）
6	连接通道失效（Concatenated Path Down）
7	管理down（Administratively Down）
8	反向链路down（Reverse Concatenated Path Down）
9～31	保留位（Reserved for future use）

- State（Sta）：BFD 会话当前状态，取值为：0 代表 AdminDown，1 代表 Down，2 代表 Init，3 代表 Up。
- Poll（P）：设置为 1，表示发送方请求进行连接确认，或者发送请求参数改变的确认；设置为 0，表示发送方不请求确认。
- Final（F）：设置为 1，表示发送方响应一个接收到 P 比特为 1 的 BFD 控制报文；设置为 0，表示发送方不响应一个接收到 P 比特为 1 的 BFD 控制报文。
- Control Plane Independent（C）：设置为 1，表示发送方的 BFD 实现不依赖于它的控制平面（即，BFD 报文在转发平面传输，即使控制平面失效，BFD 仍然能够起作用）；设置为 0，表示 BFD 报文在控制平面传输。
- Authentication Present（A）：如果设置为 1，则表示控制报文包含认证字段，并且会话是被认证的。

- Demand（D）：设置为 1，表示发送方希望操作在查询模式；设置为 0，表示发送方不区分是否操作在查询模式，或者表示发送方不能操作在查询模式。
- Reserved（R）：在发送时设置为 0，在接收时忽略。
- Detect Mult：检测时间倍数。即接收方允许发送方发送报文的最大连续丢包数，用来检测链路是否正常。
- Length：BFD 控制报文的长度，单位字节。
- My Discriminator：发送方产生的一个唯一的、非 0 鉴别值，用来区分两个协议之间的多个 BFD 会话。
- Your Discriminator：接收方收到的鉴别值“My Discriminator”，如果没有收到这个值就返回 0。
- Desired Min Tx Interval：发送方发送 BFD 控制报文时想要采用的最小间隔，单位毫秒。
- Required Min Rx Interval：发送方能够支持的接收两个 BFD 控制报文之间的间隔，单位毫秒。
- Required Min Echo Rx Interval：发送方能够支持的接收两个 BFD 回声报文之间的间隔，单位毫秒。如果这个值设置为 0，则发送不支持接收 BFD 回声报文。
- Auth Type：BFD 控制报文使用的认证类型。
- Auth Len：认证字段的长度，包括认证类型与认证长度字段。

1.1.3 BFD支持的应用

- OSPF 与 BFD 联动：详细情况请参见“三层技术-IP 路由配置指导”中的“OSPF”。
- OSPFv3 与 BFD 联动：详细情况请参见“三层技术-IP 路由配置指导”中的“OSPFv3”。
- IS-IS 与 BFD 联动：详细情况请参见“三层技术-IP 路由配置指导”中的“IS-IS”。
- IPv6 IS-IS 与 BFD 联动：详细情况请参见“三层技术-IP 路由配置指导”中的“IPv6 IS-IS”。
- RIP 与 BFD 联动：详细情况请参见“三层技术-IP 路由配置指导”中的“RIP”。
- 静态路由与 BFD 联动：详细情况请参见“三层技术-IP 路由配置指导”中的“静态路由”。
- BGP 与 BFD 联动：详细情况请参见“三层技术-IP 路由配置指导”中的“BGP”。
- IPv6 BGP 与 BFD 联动：详细情况请参见“三层技术-IP 路由配置指导”中的“IPv6 BGP”。
- PIM 与 BFD 联动：详细情况请参见“IP 组播配置指导”中的“PIM”。
- IPv6 PIM 与 BFD 联动：详细情况请参见“IP 组播配置指导”中的“IPv6 PIM”。
- MPLS 与 BFD 联动：详细情况请参见“MPLS 配置指导”中的“MPLS 基本配置”。
- Track 与 BFD 联动：详细情况请参见“可靠性配置指导”中的“Track”。
- IP 快速重路由：目前支持快速重路由的有 OSPF、RIP、IS-IS 和静态路由。详细情况请参见“三层技术-IP 路由配置指导”中的“OSPF”、“IS-IS”、“RIP”和“静态路由”。

1.1.4 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 5884：Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)
- RFC 5885：Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)

1.2 配置BFD基本功能

BFD 基本功能配置，是配置其他协议和 BFD 联动应用的基础。

1.2.1 配置准备

在配置 BFD 基本功能之前，需完成以下任务：

- 配置接口的网络层地址，使相邻节点之间网络层可达
- 配置可支持 BFD 的路由协议

1.2.2 配置步骤

表1-2 配置 BFD 基本功能

操作	命令	说明
进入系统视图	**system-view**	-
配置BFD会话建立前的会话模式	**bfd session init-mode** { **active** | **passive** }	可选 缺省情况下，BFD会话建立前的会话模式为**active**
配置多跳BFD控制报文的目的端口号	**bfd multi-hop destination-port** *port-number*	可选 缺省情况下，多跳BFD控制报文的目的端口号为4784
配置echo报文源IP地址	**bfd echo-source-ip** *ip-address*	可选 需要注意的是，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BFD echo报文的源IP地址配置为属于该设备任何一个接口所在网段
进入接口视图	**interface** *interface-type interface-number*	-
配置接收echo报文的最小时间间隔	**bfd min-echo-receive-interval** *value*	可选 请参见1.1.2 BFD报文格式中的参数Required Min Echo Rx Interval 缺省情况下，接收echo报文的最小时间间隔为400毫秒

操作	命令	说明
配置发送BFD控制报文的最小时间间隔	**bfd min-transmit-interval** *value*	可选 请参见1.1.2 BFD报文格式中的参数Desired Min Tx Interval 缺省情况下，发送BFD控制报文的最小时间间隔为400毫秒
配置接收BFD控制报文的最小时间间隔	**bfd min-receive-interval** *value*	可选 请参见1.1.2 BFD报文格式中的参数Required Min Rx Interval 缺省情况下，接收BFD控制报文的最小时间间隔为400毫秒
配置检测时间倍数	**bfd detect-multiplier** *value*	可选 请参见1.1.2 BFD报文格式中的参数Detect Mult 缺省情况下，检测时间倍数为5

如 图 1-1 所示，假如Router A的Desired Min Tx Interval为 100 毫秒，Required Min Rx Interval为300 毫秒，Detect Mult为 5；Router B的Desired Min Tx Interval为 150 毫秒，Required Min Rx Interval为 400 毫秒，Detect Mult为 10。那么会有以下结果：

- Router A 的实际发送时间为 Router A 发送控制报文的最小时间间隔和 Router B 接收控制报文的最小时间间隔之间的较大值＝Max（100，400）＝400 毫秒。
- Router B 的实际发送时间为 Router B 发送控制报文的最小时间间隔和 Router A 接收控制报文的最小时间间隔之间的较大值＝Max（150，300）＝300 毫秒。
- Router A 的实际检测时间为 Router B 的检测时间倍数和 Router B 的实际发送时间的乘积＝10×300＝3000 毫秒。
- Router B 的实际检测时间为 Router A 的检测时间倍数和 Router A 的实际发送时间的乘积＝5×400＝2000 毫秒。

1.3 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1-3 BFD 显示和维护

操作	命令
显示使能的BFD接口信息	**display bfd interface** [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示使能的BFD调试信息开关	**display bfd debugging-switches** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示BFD会话信息	**display bfd session** [**slot** *slot-number* [**all** | **verbose**] | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
清除BFD会话统计信息	**reset bfd session statistics** [**slot** *slot-number*]

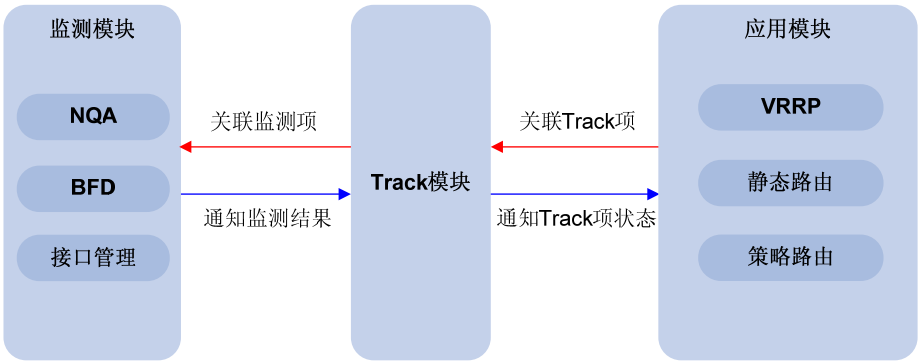
目 录

1 Track配置

1.1 Track简介

1.1.1 联动功能介绍

图1-1 联动功能实现示意图



Track的用途是实现联动功能。如 图 1-1 所示，联动功能通过在监测模块、Track模块和应用模块之间建立关联，实现这些模块之间的联合动作。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，在静态路由、Track和NQA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。

如果应用模块直接与监测模块关联，由于不同监测模块通知给应用模块的监测结果形式各不相同，应用模块需要分别处理不同形式的监测结果。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。

1.1.2 联动功能工作原理

联动功能的工作原理分为两部分：

- Track 模块与监测模块联动
- Track 模块与应用模块联动

1. Track模块与监测模块联动

Track 模块和监测模块之间通过 Track 项建立关联。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 Invalid。

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）
- 接口管理

2. Track模块与应用模块联动

Track 模块和应用模块之间通过 Track 项建立关联。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。

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

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。

1.1.3 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。

1.2 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。

表1-1 Track 配置任务简介

配置任务		说明	详细配置
配置Track与监测模块联动	配置Track与NQA联动	三者必选其一	1.3.1
	配置Track与BFD联动		1.3.2
	配置Track与接口管理联动		1.3.3
配置Track与应用模块联动	配置Track与VRRP联动	三者必选其一	1.4.1
	配置Track与静态路由联动		1.4.2
	配置Track与策略路由联动		1.4.3

1.3 配置Track与监测模块联动

1.3.1 配置Track与NQA联动

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”。

表1-2 配置 Track 与 NQA 联动

操作	命令	说明
进入系统视图	**system-view**	-
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* } *]	必选 缺省情况下，没有创建与NQA测试组中指定联动项关联的Track项

说明

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 Invalid。

1.3.2 配置Track与BFD联动

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”。

1. 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”。

2. 配置过程

表1-3 配置 Track 与 BFD 联动

操作	命令	说明
进入系统视图	**system-view**	-
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* **local ip** *local-ip* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]	必选 缺省情况下，没有创建和BFD会话关联的Track项

说明

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。

1.3.3 配置Track与接口管理联动

接口管理用来监视接口的物理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，则当接口的物理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；接口的物理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。

表1-4 配置 Track 与接口管理联动

操作	命令	说明
进入系统视图	**system-view**	-
创建和接口管理关联的Track项，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* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]	二者必选其一 缺省情况下，没有创建和接口管理关联的Track项
创建和接口管理关联的Track项，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* } *]	

1.4 配置Track与应用模块联动

1.4.1 配置Track与VRRP联动

VRRP 是一种容错协议，它将一组承担网关功能的路由器加入到备份组中，形成一台虚拟路由器。备份组中的路由器根据优先级，选举出 Master 路由器，承担转发任务。优先级越高，越有可能成为 Master 路由器。其他路由器作为 Backup 路由器，当 Master 路由器发生故障时，取代 Master 承担转发任务，从而保证网络内的主机通过虚拟路由器不间断地与外部网络进行通信。

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，处于 Active 状态的虚拟转发器）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，处于 Listening 状态的虚拟转发器）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。

表1-5 配置 Track 与 VRRP 备份组联动

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
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*	必选 缺省情况下，没有创建备份组
配置VRRP备份组监视指定的Track项	**vrrp** [**ipv6**] **vrid** *virtual-router-id* **track** *track-entry-number* [**reduced** *priority-reduced* | **switchover**]	必选 缺省情况下，没有指定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

表1-6 配置 Track 与 VRRP 虚拟转发器联动

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
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*	必选 缺省情况下，没有创建备份组
配置虚拟转发器监视指定的Track项	**vrrp** [**ipv6**] **vrid** *virtual-router-id* **weight track** *track-entry-number* [**reduced** *weight-reduced*]	二者至少选择其一 缺省情况下，没有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负载均衡模式下本配置才会起作用
配置LVF通过Track功能监视AVF的状态	**vrrp** [**ipv6**] **vrid** *virtual-router-id* **track** *track-entry-number* **forwarder-switchover member-ip** *ip-address*	

说明

- 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 Invalid 后，对应的路由器优先级或虚拟转发器优先级会自动恢复。
- 可以通过 **vrrp vrid track** 命令或 **vrrp vrid weight track** 命令指定监视的 Track 项后，再通过 **track** 命令创建该 Track 项。
- VRRP 配置的详细介绍，请参见“可靠性配置指导”中的“VRRP”。

1.4.2 配置Track与静态路由联动

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没有指定出接口，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 Invalid 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。

表1-7 配置 Track 与静态路由联动

操作	命令	说明
进入系统视图	**system-view**	-
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* | *mask-length* } { *next-hop-address* | **vpn-instance** *d-vpn-instance-name next-hop-address* } **track** *track-entry-number* [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*] **ip route-static vpn-instance** *s-vpn-instance-name*&<1-6> *dest-address* { *mask* **|** *mask-length* } { *next-hop-address* [**public**] **track** *track-entry-number* **| vpn-instance** *d-vpn-instance-name next-hop-address* **track** *track-entry-number* } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	二者必选其一 缺省情况下，没有配置Track与静态路由联动

说明

- 静态路由关联的 Track 项可以是未创建的 Track 项。通过 **track** 命令创建 Track 项后，联动功能开始生效。
- 如果 Track 模块通过 NQA 探测私网静态路由中下一跳的可达性，静态路由下一跳的 VPN 实例名与 NQA 测试组配置的实例名必须相同，才能进行正常的探测。
- 需要注意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。
- 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”。

1.4.3 配置Track与策略路由联动

策略路由是一种依据用户制定的策略进行路由选择的机制。与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由基于到达报文的源地址等信息灵活地进行路由选择。

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，需要通过指定的下一跳转发。当该下一跳所在的链路出现故障时，策略路由无法感知链路故障，仍然通过该下一跳转发报文，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 Invalid 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
- 设置报文的缺省下一跳

1. 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。

2. 配置过程

表1-8 配置 Track 与策略路由联动

操作	命令	说明
进入系统视图	**system-view**	-
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*	必选
设置ACL匹配条件	**if-match acl** *acl-number*	可选 缺省情况下，所有报文都会通过该节点的过滤
设置报文的下一跳，并与Track项关联	**apply ip-address next-hop** *ip-address* [**direct**] [**track** *track-entry-number*] [*ip-address* [**direct**] [**track** *track-entry-number*]]	二者中至少选择其一
设置报文缺省下一跳，并与Track项关联	**apply ip-address default next-hop** *ip-address* [**track** *track-entry-number*] [*ip-address* [**track** *track-entry-number*]]	

说明

- 策略路由关联的 Track 项可以是未创建的 Track 项。通过 **track** 命令创建 Track 项后，联动功能开始生效。
- 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”。

1.5 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1-9 Track 显示和维护

操作	命令
显示Track项的信息	**display track** { *track-entry-number* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.6 Track典型配置举例

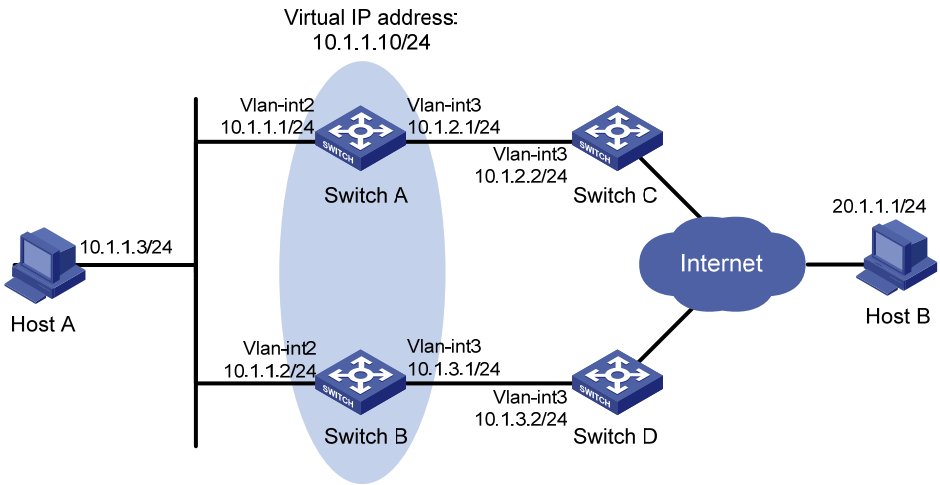
1.6.1 VRRP、Track与NQA联动配置举例（Master监视上行链路）

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] nqa entry admin test
```

配置测试类型为 ICMP-echo。

```
[SwitchA-nqa-admin-test] type icmp-echo
```

配置目的地址为 10.1.2.2。

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.1.2.2
```

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
```

(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 nqa entry admin test reaction 1
```

(4) 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
```

设置备份组的认证方式为 SIMPLE，认证字为 hello。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

设置 Master 发送 VRRP 报文的间隔时间为 5 秒。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

设置 Switch A 工作在抢占方式，抢占延迟时间为 5 秒。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

设置监视 Track 项。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 30
```

(5) 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
```

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 hello
```

设置 Master 发送 VRRP 报文的间隔时间为 5 秒。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

设置 Switch B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

(6) 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp** 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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 5
     Admin Status   : Up             State        : Master
     Config Pri     : 110            Running Pri  : 110
     Preempt Mode   : Yes            Delay Time   : 5
```

```
    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 Standby Information:
    Run Mode       : Standard
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
    VRID           : 1               Adver Timer  : 5
    Admin Status   : Up              State        : Backup
    Config Pri     : 100             Running Pri  : 100
    Preempt Mode   : Yes             Delay Time   : 5
    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 Standby Information:
    Run Mode       : Standard
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
    VRID           : 1               Adver Timer  : 5
    Admin Status   : Up              State        : Backup
    Config Pri     : 110             Running Pri  : 80
    Preempt Mode   : Yes             Delay Time   : 5
    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 Standby Information:
    Run Mode       : Standard
    Run Method     : Virtual MAC
```

```
Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1               Adver Timer   : 5
    Admin Status   : Up              State         : Master
    Config Pri     : 100             Running Pri   : 100
    Preempt Mode   : Yes             Delay Time    : 5
    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。

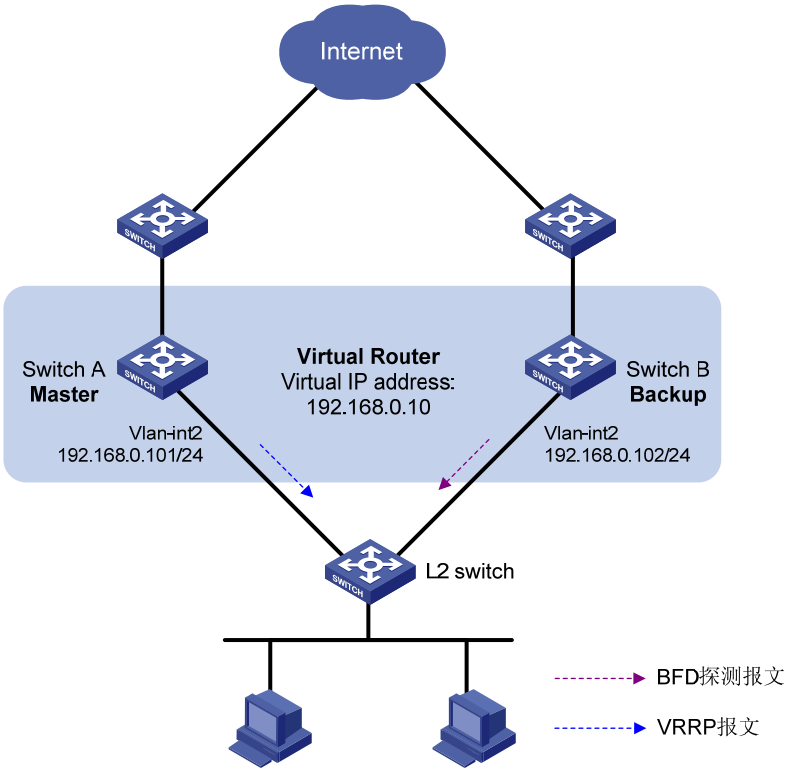
1.6.2 VRRP、Track与BFD联动配置举例（Backup监视Master）

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
```

(6) 验证配置结果

显示 Switch A 上备份组的详细信息。

```
<SwitchA> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 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
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
```

```
    Packet type: Echo
    Interface  : Vlan-interface2
    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 事件调试信息开关。

```
<SwitchB> terminal debugging
<SwitchB> terminal monitor
<SwitchB> debugging vrrp state
<SwitchB> debugging bfd event
```

Switch A 出现故障时，Switch B 上输出如下调试信息。

```
*Dec 17 14:44:34:142 2012 SwitchB BFD/7/EVENT:Send sess-down Msg,
[Src:192.168.0.102,Dst:192.168.0.101,Vlan-interface2,Echo], instance:0, protocol:Track
*Dec 17 14:44:34:144 2012 SwitchB VRRP/7/DebugState: 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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer   : 1
     Admin Status   : Up              State         : Master
     Config Pri     : 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。

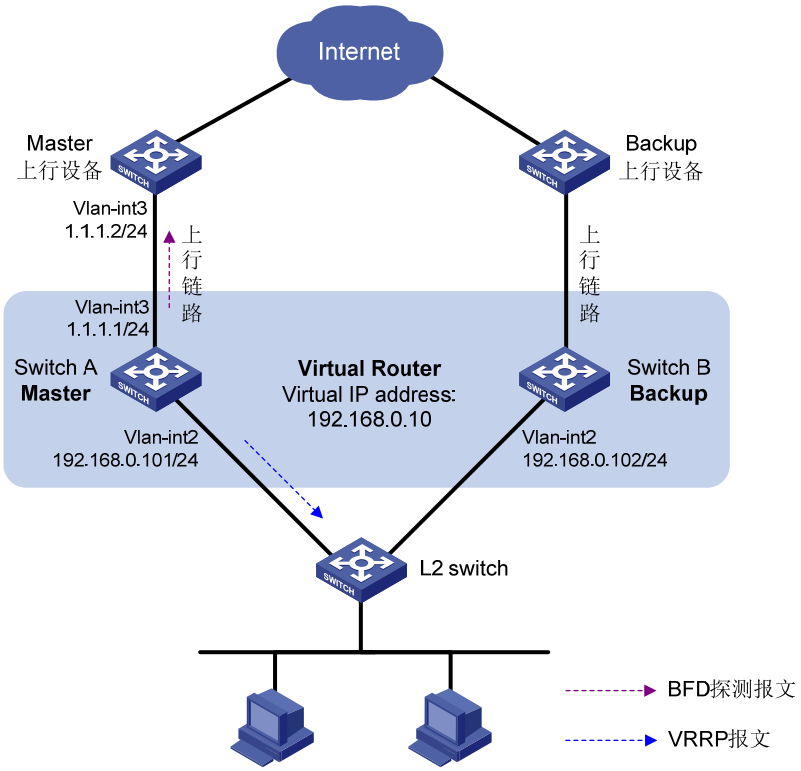
1.6.3 VRRP、Track与BFD联动配置举例（Master监视上行链路）

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 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
```

(6) 验证配置结果

显示 Switch A 上备份组的详细信息。

```
<SwitchA> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     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
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface  : Vlan-interface2
    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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 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
  Status: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface  : Vlan-interface2
    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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 1
     Admin Status   : Up             State        : Backup
     Config Pri     : 110            Running Pri  : 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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 1
     Admin Status   : Up             State        : Master
     Config Pri     : 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。

1.6.4 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：

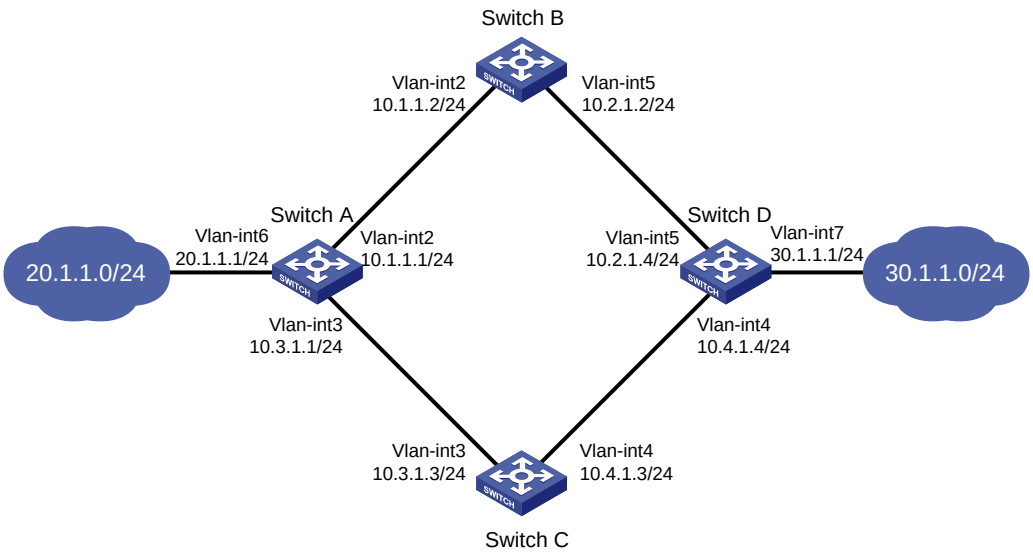
- 下一跳为 Switch B 的静态路由优先级高，作为主路由。该路由可达时，Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路作为备份路由。
- 在 Switch A 上通过静态路由、Track 与 NQA 联动，实时判断主路由是否可达。当主路由不可达时，备份路由生效，Switch A 通过 Switch C 将报文转发到 30.1.1.0/24 网段。

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 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 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
```

(6) 验证配置结果

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
Track ID: 1
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table
Routing Tables: Public
         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
  Status: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table
Routing Tables: Public

         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
--- 30.1.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/2 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
  --- 20.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

1.6.5 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：

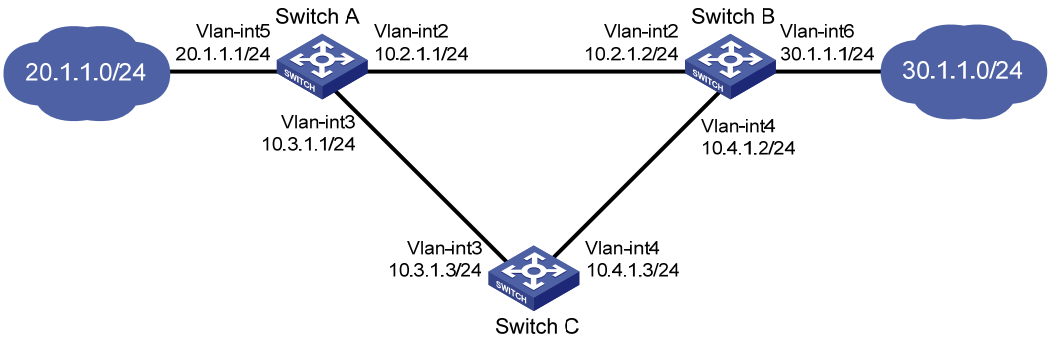
- 下一跳为 Switch B 的静态路由优先级高，作为主路由。该路由可达时，Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路作为备份路由。
- 在 Switch A 上通过静态路由、Track 与 BFD 联动，实时判断主路由是否可达。当主路由不可达时，BFD 能够快速地检测到路由故障，使得备份路由生效，Switch A 通过 Switch C 和 Switch B 将报文转发到 30.1.1.0/24 网段。

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 能够快速地检测到路由故障，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
```

(5) 验证配置结果

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
Track ID: 1
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD Session:
    Packet type: Echo
    Interface  : Vlan-interface2
    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
Routing Tables: Public
         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
  Status: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD Session:
    Packet type: Echo
    Interface  : Vlan-interface2
    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
Routing Tables: Public
         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
  --- 30.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 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
  --- 20.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

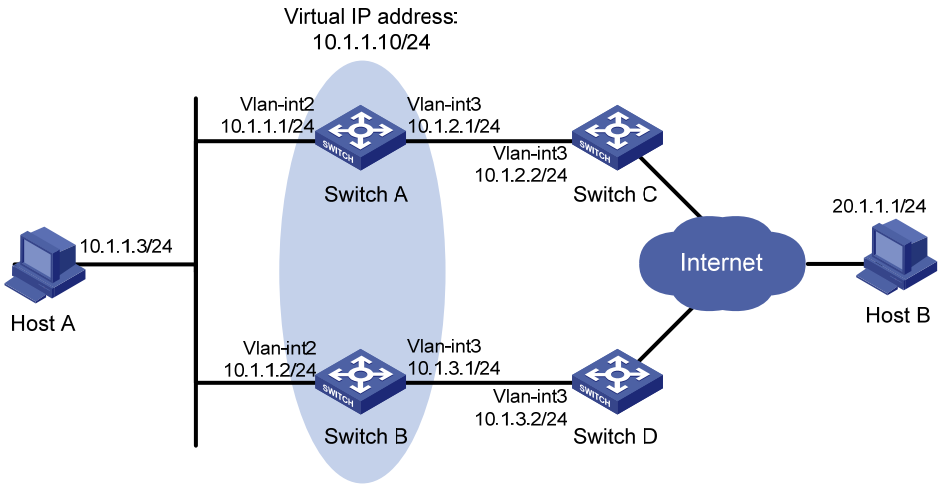
1.6.6 VRRP、Track与接口管理联动配置举例（Master监视上行接口）

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 的物理状态关联。

```
[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 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
```

(5) 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp** 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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 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 Standby Information:
     Run Mode       : Standard
```

```
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 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 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 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。