



配置指南-可靠性

本分册介绍可靠性配置指南相关内容，包括以下章节：

1. REUP
2. RLDP
3. DLDP
4. PCAP
5. VRRP
6. VRRP Plus
7. BFD
8. IP Event Dampening
9. VSU
10. RNS

1 REUP

1.1 概述

REUP (Rapid Ethernet Uplink Protection Protocol，快速以太网上链保护协议) 提供一个快速上链保护功能。

在双上行组网方式中，REUP 用来保证链路的正常通信，阻塞冗余链路，避免链路环路，起到快速备份的作用。

REUP 的上链端口是成对配置的，两个端口都正常的情况下，有一个端口处于备份状态，处于备份状态的端口是不转发数据报文。当处于转发状态的端口发生故障时，备份端口会马上切换成转发状态，提供数据传输，此外 REUP 还会向上游设备发送地址更新报文，使得上游设备可以即时更新 MAC 地址信息。REUP 的这种功能可以保证当链路出现故障后，用户的二层数据流能够在 50ms 以内恢复。

REUP 和 STP(Spanning Tree Protocol，生成树协议)是基于端口互斥的。此时该设备对下运行 STP 协议，对上使用 REUP 来实现上链的备份以及故障保护。REUP 使得用户在关闭 STP 的情况下，仍提供基本的链路冗余，同时提供比 STP 更快的毫秒级故障恢复。

协议规范

- REUP 是锐捷网络私有协议，无标准协议参考。

1.2 典型应用

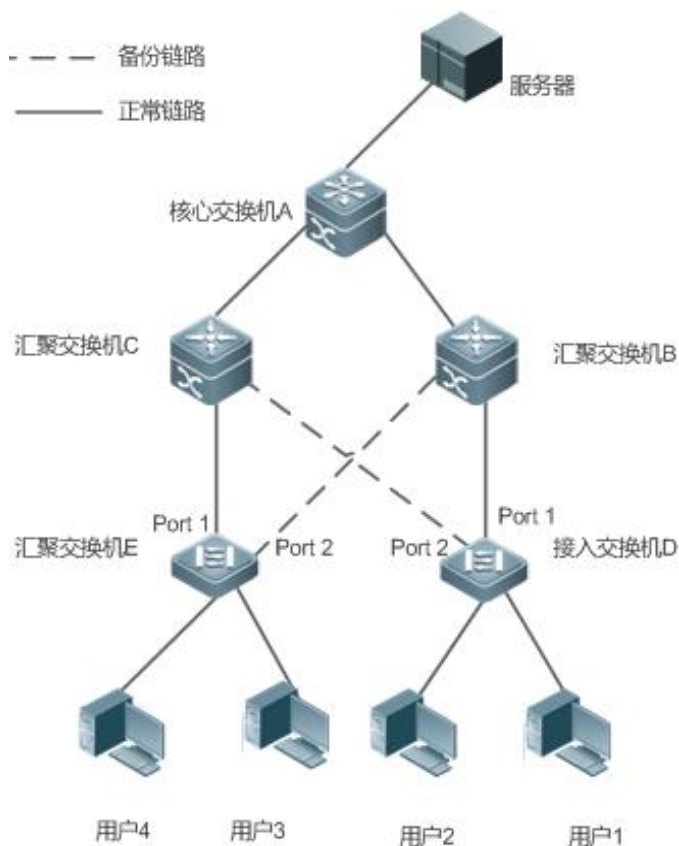
典型应用	场景描述
在双上行组网中通信	在双上行组网中进行报文转发

1.2.1 在双上行组网中通信

应用场景

在双上行组网中进行通信中，接入交换机有两条上行通路，其应该场景如下图所示。

图 1-1 双上行组网方式



功能部署

- 在接入交换机 D/E 的 port1 和 port2 上同时开启 REUP 协议，在链路发生故障时进行快速切换。
- 在交换机 A/B/C 相连接的端口上开启 REUP 的 MAC 地址更新消息接收功能，在链路发生故障时，能快速清除接口上的 MAC 地址。

1.3 功能详解

基本概念

➤ REUP 对

通过指定一个端口作为另外一个端口的备用端口来配置一个 REUP 对，其中一个端口为主端口(Active)，另一个端口为从端口(Backup)。在两个端口都正常的情况下，有一个端口会被设置成转发端口(Forward)，另一个端口会被设置成备份端口(Standby)，如何判断哪个端口该设置为 Standby 可以由用户配置决定，请参考“配置 REUP 的抢占模式和延迟时间”章节获取相关信息。

➤ MAC 地址更新消息

MAC 地址更新消息是指锐捷网络通过私有组播给上链设备发送 FLUSH 报文，当锐捷网络上链设备打开接收 MAC 地址更新消息功能时，并且接收 MAC 地址更新消息，便执行对相应接口上 MAC 更新工作。

MAC 地址更新组

把几个端口同时加入到一个组里面，在该组中，如果有一个接口接收到了 MAC 地址更新消息，就会消更新组内其他端口的 MAC 地址，则该组叫 MAC 地址更新组。

MAC 地址更新报文

为了支持友商的上链设备，而需要进行 MAC 地址更新而发送的报文叫 MAC 地址更新报文。

链路跟踪组

把同一个设备的上链端口与下链端口同时加入一个组内，当该组的所有上链端口都 down 时，则强制让该组内的所有下链端口也 down 的组叫链路跟踪组。

功能特性

功能特性	作用
REUP 双链路备份	当一条链路发生故障时，另外一条链路可以快速地切换成转发状态。
REUP 的抢占模式和延迟时间	两条链路同时正常时，通过抢占模式来决定哪条链路来转发数据，通过延迟时间来决定过多久来切换。
MAC 地址更新	链路进行切换时，对端口上的 MAC 地址进行更新，加快报文的收敛性。
VLAN 负载均衡	两条链路同时正常时，最大限度的利用链路的宽带，
链路跟踪	上链链路发生故障时，让下链链路进行切换。

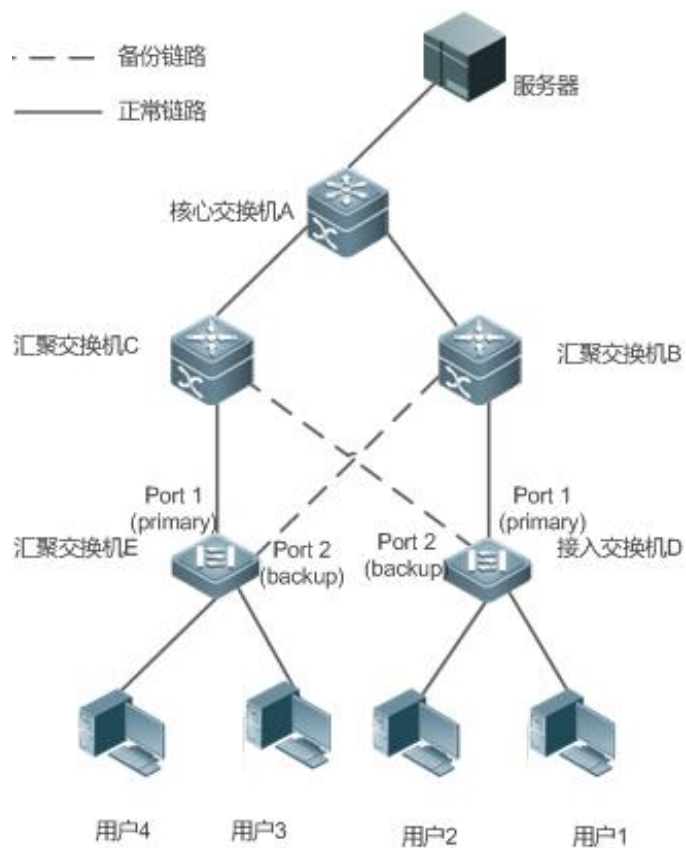
1.3.1 REUP 双链路备份功能

当活动链路发生故障时，处于备用状态的条链路会迅速切换到转发状态，开始转发数据，最大程度的减小链路故障造成的业务中断。

工作原理

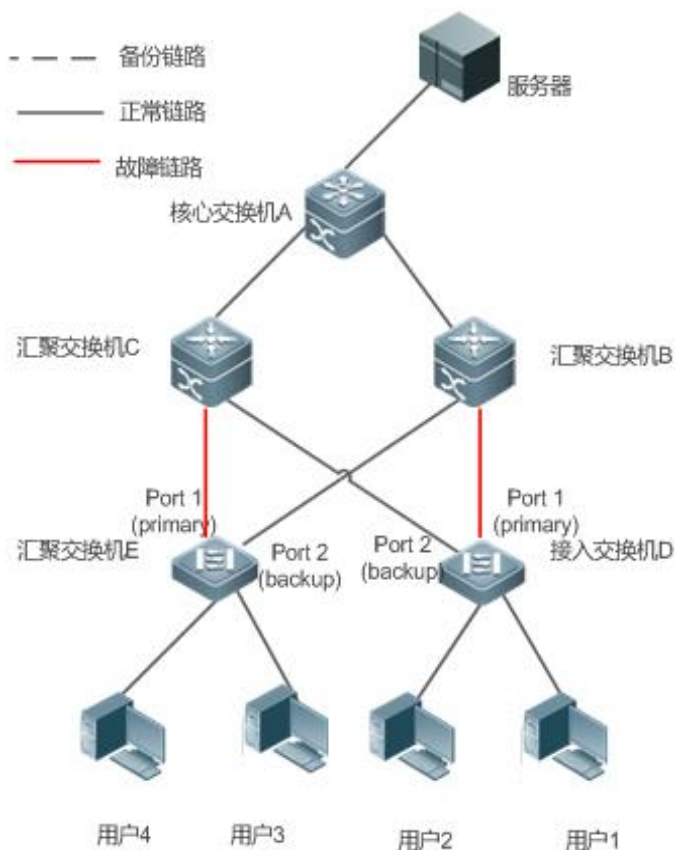
通过指定一个端口作为另外一个端口的备用端口来配置一个 REUP 对。当两个端口正常时，其中的一条链路处于转发状态（转发数据报文），另外一条链路处于备份状态（不转发数据报文）。当活动链路发生故障时，处于备用状态的另外一条链路会迅速切换到转发状态，开始转发数据；当故障链路恢复后，进入备份状态，不转发数据报文。当然，用户可以通过配置抢占模式来指定从故障中恢复的链路是否抢占当前处于转发状态的链路。

图 1-2 两条链路都正常的拓扑



如上图，交换机 D (E) 的端口 1, 2 连接到上链交换机 B, C (C, B) 上，在端口 1, 2 上配置 REUP。在链路正常的情况下，端口 1 处于转发状态，负责转发数据报文；端口 2 处于备份状态，不转发数据报文。

图 1-3 交换机 D(E)端口 1 故障后的拓扑



一旦端口 1 发生故障，端口 2 会立即开始转发数据报文，恢复交换机的上链传输。在非抢占模式下，当端口 1 的链路恢复后，端口 1 会处于备份状态，不转发数据报文，端口 2 则继续转发数据报文。

相关配置

启动接口上的双链路备份功能

缺省情况下，接口上的双链路备份功能关闭。

通过配置 **switchport backup interface** 来配置一个物理二层口(或者二层 AP 口)作为备用端口，开启 REUP 的双链路备份功能。

必须在接口上启用 REUP 双链链路备份功能，接口发生故障时才能参与 REUP 协议的链路切换工作。

- ❗ REUP 和 ERPS、RERP 不共用端口。
- ❗ 启用 REUP 的设备，需要关闭所有二层端口的风暴控制功能。

1.3.2 REUP 的抢占模式和延迟时间。

工作原理

可以通过配置 REUP 的抢占模式来决定优先使用哪条链路。如果将抢占模式配置为带宽(Bandwith)优先模式,则 REUP 会优先使用一条带宽比较大的链路;当然可以通过把抢占模式设置为强制(Forced)模式,来强制优先使用一条比较稳定可靠的链路。

为了避免异常故障导致频繁的主备链路切换,REUP 提供了一个抢占延迟的功能。当两条链路恢复后,延迟一定时间(默认 35s),等故障链路稳定后再进行链路的切换。

相关配置

配置 REUP 的抢占模式和延迟时间功能

缺省情况下,抢占模式功能关闭,延迟时间为 35s。

通过使用 **switchport backup interface preemption mode** 命令来配置抢占模式功能。

通过使用 **switchport backup interface preemption delay** 命令来配置延迟时间。

延迟时间越短,链路故障恢复后抢占切换越频繁。

- i REUP 对于 AP 口的 Bandwidth 属性值采用的是 AP 口的实际带宽,等于 AP 的 Link UP 成员口数*成员口的 Speed 属性值。
- i 当上链打开 STP 时,REUP 的抢占延迟时间要大于 35 秒。

1.3.3 MAC 地址更新

链路进行切换时,对端口上的 MAC 地址进行更新,加快报文的收敛性。

工作原理

图 1-2 中,在交换机 D (E) 的端口 port1, port2 上启用 REUP 双链路备份功能,端口 port1 作为主端口,在正常的通讯过程中,交换机 A 会在连接交换机 B (C) 的端口上学习到用户 1 和 2 (用户 3 和 4) 的 MAC 地址。

当交换机 D (E) 的端口 port1 发生故障后,端口 port2 会快速变成转发状态,开始转发数据报文。此时交换机 A 暂时没有从连接交换机 B (C) 的端口上学习到用户 1 和 2 (用户 3 和 4) 的 MAC 地址,服务器发往用户 1 和 2 (用户 3 和 4) 的数据报文会被交换机 A 转发给交换 C (B),导致服务器到用户 1 和 2 (用户 3 和 4) 报文丢失。

为避免出现以上问题,可在交换机 D (E) 上开启 MAC 地址更新功能,在 port2 开始转发报文时,交换机 D (E) 会往 port2 发送一个 MAC 地址的更新消息。交换机 A 收到 MAC 地址更新消息后,会更新交换机 A 端口上的 MAC 地址。这样交换机 A 就会把服务器发往用户的报文同时转发到连接交换机 B (C) 的端口上,加快报文传输的收敛。

此外,引入一个 MAC 地址更新组的设置,即将多个端口归在一个组里,当该组的某个端口收到地址更新消息时,便更新该组内其它端口上的 MAC 地址信息,以减少 MAC 地址更新所引发泛洪的副作用。

为了兼容不支持 MAC 地址更新消息的上游设备，在 port2 口变成转发状态时，交换机 D (E) 会替用户 1 和 2 (用户 3 和 4) 往上发出 MAC 地址更新报文，让交换机 A 把用户 1 和 2 (用户 3 和 4) 的 MAC 地址更新到相应的口上，恢复交换机 A 的下行数据传输。

相关配置

启动接口上的 MAC 地址更新消息发送功能

缺省情况下，接口上的 MAC 地址更新消息发送功能关闭。

通过使用 **mac-address-table move update transit** 命令启用设备的所有接口上发送 MAC 地址更新消息的功能。

如果没有启用 MAC 地址更新消息发送功能，则在进行 REUP 双链路备份切换时不会发送 MAC 地址更新消息。

启动接口上的 MAC 地址更新消息接收功能

缺省情况下，接口上的 MAC 地址更新消息接收功能关闭。

通过使用 **mac-address-table move update receive** 命令启用设备的所有接口上接收 MAC 地址更新消息的功能。

如果没有启用 MAC 地址更新消息接收功能，则在设备上不会接收到下链设备在进行 REUP 双链路备份切换时发送出来的 MAC 地址更新消息，从而不会进行 MAC 地址更新工作。

配置发送 MAC 地址更新消息的 VLAN

缺省情况下，发送 MAC 地址更新消息的 vlan 为接口所属的缺省的 vlan。

通过使用命令 **mac-address-table move update transit vlan** 命令配置接口在哪个 vlan 中发送 MAC 地址更新消息。

如果配置了接口发送 MAC 地址更新消息的 vlan，则在配置的 vlan 中进行发送，否则在接口所属的缺省的 vlan 进行发送。

配置接收 MAC 地址更新消息的 VLAN

缺省情况下，在所有 vlan 中接收 MAC 地址更新消息。

通过使用命令 **no mac-address-table move update receive vlan** 命令配置接口在哪个 vlan 中不接收 MAC 地址更新消息，剩余的 vlan 都接收 mac 地址更新消息。

如果没有配置了接口接收 MAC 地址更新消息的 vlan，则在配置的所有的 vlan 中都接收 MAC 地址更新消息，否则在剩余的 vlan 中接收。

配置 MAC 地址更新组

缺省情况下，不存在 MAC 地址更新组。

使用命令 **mac-address-table update group** 把端口加入 mac 地址更新组，默认加入第一个更新组。

如果没有配置 MAC 地址更新组，接收到 MAC 地址更新报文时，不会进行 MAC 地址更新工作。

配置每秒发送最大的 MAC 地址更新报文数量

缺省情况下，每秒发送最大的 MAC 地址更新报文数量为 150 个。

使用命令 **mac-address-table move update max-update-rate** 配置每秒发送 MAC 地址更新报文的最大个数。

配置发送的个数越大，发送的所占的 cpu 时间越多，下行报文丢失的越少。

1.3.4 VLAN 负载均衡

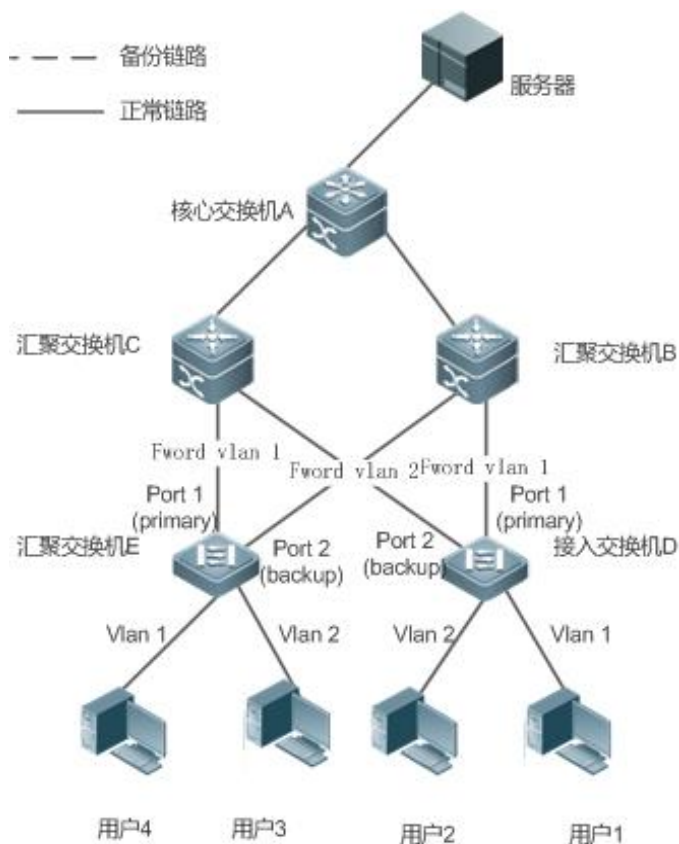
工作原理

VLAN 负载均衡功能允许 REUP 对的两个端口同时转发互斥 VLAN 的数据报文，以便充分利用链路带宽。

如下图所示，在交换机 D 的两个 port1, port2 上配置 REUP 双链路备份并启用 REUP 的 VLAN 负载均衡功能，把 VLAN 1 映射到实例 1、VLAN2 映射到实例 2。VLAN 1(实例 1)的数据由端口 1 传输，其它所有 VLAN2 (实例 2)的数据由端口 2 传输。在交换机 E 上也进行同样的处理。

当其中的一个端口发生故障时，由另外一个端口负责所有 VLAN 的传输；当发生故障的端口恢复过来，并在抢占延迟时间内不再故障，则把故障恢复的端口负责的 VLAN 的传输从另外一个端口上切换过来。

图 1-4 负载均衡两条链路都正常的拓扑




相关配置

启动接口上的 VLAN 负载均衡功能

缺省情况下，接口上的 VLAN 负载均衡功能关闭。

使用命令 **switchport backup interface prefer instance** 启用 vlan 负载均衡功能。

如果没有启用此功能，在两条链路都正常的情况下转发报文时无法充分利用链路带宽。必须在接口上启用 VLAN 负载均衡功能，接口才能参与 VLAN 负载均衡工作。

 REUP 的 VLAN 负载均衡的实例映射由 MSTP 模块统一控制，具体如何配置实例请参见《配置 MSTP》的说明。

 VLAN 负载均衡的功能只能在 trunk 口、uplink 口或 hybrid 口上进行配置。

1.3.5 链路状态跟踪

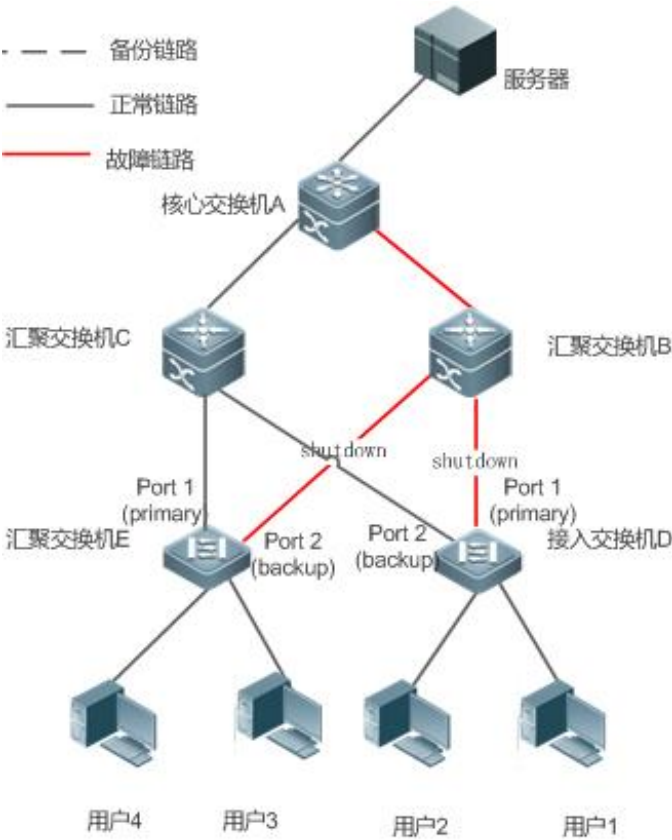
链路跟踪是指当上行链链路发生故障时，由下行链链路进行切换，使得备份端口能继续转发报文。

工作原理

链路状态跟踪(Link state tracking)提供上行链路都发生故障，通告下链设备进行链路切换的功能。链路状态同步通过配置链路状态跟踪组的下行端口和下行端口，把多个下行端口的链路状态绑定到多个上行链路的端口上。当跟踪组内所有的上行链路都发生故障，则把下行链路的端口强制 shutdown，使下行链路的传输从主链路切换到备份链路上。

如下图，当交换机 B 的上行链路发生故障时，Link State Tracking 会把 B 的下行端口快速 Shutdown，使得交换机 D 的上行传输就会被切换到交换机 C 上。

图 1-5 主链路上链发生故障后的拓扑



相关配置

启动链路跟踪功能

缺省情况下，链路跟踪功能关闭。

使用命令 **link state track [number]** 启用一个链路跟踪组。number 的范围为 1-2，默认启用第一个链路跟踪组(默认 number 的值为 1)。

如果未启用链路跟踪功能，则无法检测到相应的上链口的状态，导致无法进行及时的报文转发切换。

端口加入链路跟踪组

缺省情况下，端口不加入跟踪组中。

使用命令 **link state group [number] {upstream | downstream}** 设置链路跟踪组的上行端口(upstream)和下行端口(downstream)。number 的范围为 1-2，默认加入第一个链路跟踪组(默认 number 的值为 1)。

如果端口未加入跟踪组中，则无法检测到相应的上链口的状态，导致无法进行及时的报文转发切换。

1.4 配置详解

配置项	配置建议&相关命令
-----	-----------

配置 REUP 基本功能	 必须配置。启动 REUP 双链路备份功能。	
	switchport backup interface	启动 REUP 双链路备份功能
配置 REUP 的链路抢占模式与延迟时间	 可选配置。用于决定抢占模式和延迟时间，不配置都有默认值。	
	switchport backup interface preemption mode	设置抢占模式。
	switchport backup interface preemption delay	设置抢占的延迟时间。
配置 MAC 地址更新功能	 可选配置。启动 MAC 地址快速更新功能。	
	mac-address-table update group	设置交换机的 MAC 地址更新组 ID
	mac-address-table move update transit	打开发送 MAC 地址更新消息的开关
	mac-address-table move update transit vlan	打开发送 MAC 地址更新消息的 VLAN ID
	mac-address-table move update	每秒发送的最大 MAC 地址更新报文数量。 可选范围为 0-32000，默认为 150 个。
	mac-address-table move update receive	打开接收 MAC 地址更新消息的开关
	mac-address-table move update receive vlan	配置处理 MAC 地址更新消息的 VLAN 范围
配置 VLAN 负载均衡功能	 可选配置。启动 VLAN 负载均衡功能。	
	switchport backup interface prefer instance	配置 REUP 的链路 VLAN 负载均衡
配置链路跟踪功能	 可选配置。启动链路跟踪功能功能。	
	link state track up-delay	启用链路状态跟踪组下连链路延时 up
	link state track	启用链路状态跟踪组
	link state group	将端口加入指定的链路状态跟踪组的上行接口或下行口

1.4.1 配置 REUP 基本功能

配置效果

- 在一条链路发生故障时，另一条正常的链路立即切换成转发状态从而转发报文。

注意事项

- 一个端口只能属于一个 REUP 对，每一条活动链路只能有一条备用链路，一条备用链路只能作为一条活动链路的备用链路，活动链路和备用链路必须是不同的端口。

- REUP 支持二层物理端口和二层 AP 口，但不支持 AP 成员口。
- 主从端口不必为同一类型的端口，主端口和从端口的速率也可以不同。例如，可以将 AP 口作为主端口，物理口设置为从端口。
- 配置了 REUP 的端口不参与 STP 计算。
- 每台设备最多可以配置 16 个 REUP 对。
- 对已经配置 REUP 成功的端口，需要禁止把端口变成三层口或者把端口加入 AP。

配置方法

启动 REUP 双链路备份功能

- 必须配置。
- 若无特殊要求，应在接收交换机的端口上启动 REUP 双链路备份功能。

检验方法

使用 **show interfaces switchport backup [detail]**命令查看是否配置。

相关命令

启动 REUP 双链路备份功能

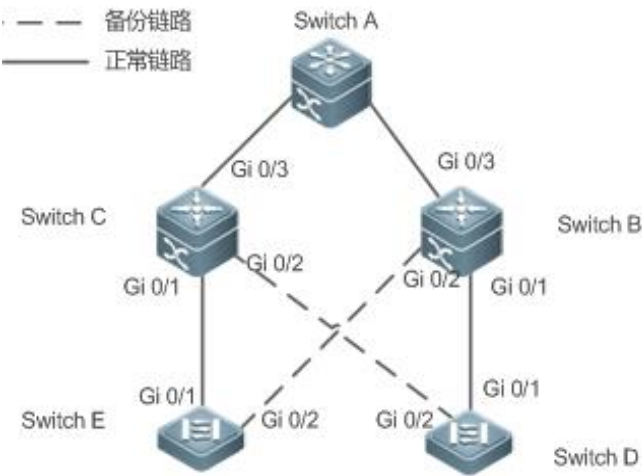
- 【命令格式】 **switchport backup interface *interface-id***
- 【参数说明】 *interface-id*：备接口 id。
- 【命令模式】 接口模式
- 【使用指导】 模式所在的端口为主端口，参数中的 *interface-id* 所对应的端口为备份端口。当活动链路发生故障后，快速恢复备份链路的传输

配置举例

在启动 REUP 双链路备份功能

【网络环境】 如下图，交换机 D 到交换机 A 有二条上行链，分别为交换机 D->交换机 B->交换机 A；交换机 D->交换机 C->交换机 A。交换机 E 到交换机 A 有二条上行链，分别为交换机 E->交换机 B->交换机 A；交换机 E->交换机 C->交换机 A。

图 1-6 双上行组网



【配置方法】 ● 在接入交换机上 D (E) 上配置 REUP 双链路备份 (Gi0/1 口为主端口，Gi0/2 口为从端口)。

D

```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# interface GigabitEthernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface GigabitEthernet 0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

E

```
SwitchE> enable
SwitchE# configure terminal
SwitchE(config)# interface GigabitEthernet 0/1
SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchE(config-if-GigabitEthernet 0/1)#switchport backup interface GigabitEthernet 0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

【检验方法】 ● 检查交换机 D (E) 配置的双链路备份信息。

D

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi0/1                 Gi0/2                 Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
```

E

```

Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)

SwitchE#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi0/1                 Gi0/2                 Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)

```

常见错误

- 配置的接口上已配置其他的 REUP 对。
- 配置的接口非二层物理口或二层 ap 口。

1.4.2 配置 REUP 的抢占模式和延迟功能

配置效果

- 限制 REUP 链路切换的抢占的模式和延迟抢占的时间。

注意事项

- 必须配置 REUP 双链路备份功能。

配置方法

- 可选配置。
- 若需要主链路一直转发报文或根据链路带宽来决定哪条链路来转发报文要求，应配置上相应的抢占模式和延迟时间。

检验方法

使用 **show interfaces switchport backup [detail]** 命令查看是否配置的抢占模式与延迟时间。

相关命令

配置 REUP 的抢占模式

【命令格式】 **switchport backup interface** *interface-id* **preemption mode** {forced|bandwidth|off}

【参数说明】 *interface-id* : 备接口 id。

mode : 设置抢占模式 :

forced: 表示强制模式

bandwidth:表示带宽模式

off:表示关闭模式。

【命令模式】 接口模式

【使用指导】 抢占模式分为强制、带宽和关闭三种模式，其中带宽模式为优先选择带宽较大的端口来传输数据；强制模式为优先选择主端口来传输数据；关闭模式则不抢占。默认为关闭模式。

配置 REUP 延迟时间

【命令格式】 **switchport backup interface** *interface-id* **preemption delay** *delay-time*

【参数说明】 *interface-id* : 备接口 id。

delay-time : 延迟时间

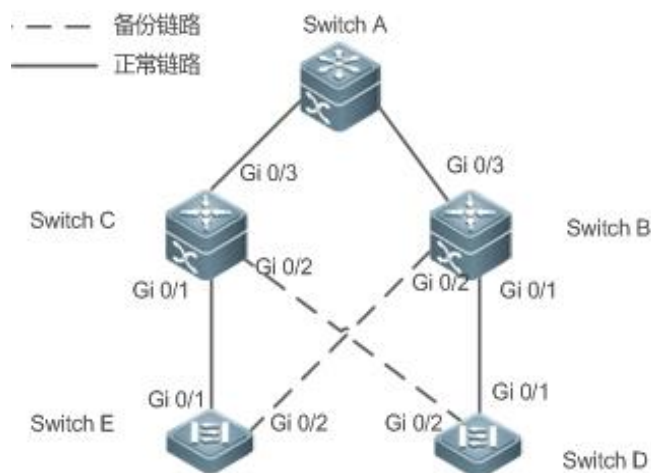
【命令模式】 接口模式

【使用指导】 抢占延迟是指故障链路恢复后，到链路重新切换的延迟时间。

配置举例

配置 REUP 抢占模式与延迟时间

【网络环境】 在图 1-6 中，交换机 D 到交换机 A 有二条上行链，分别为交换机 D->交换机 B->交换机 A；交换机 D->交换机 C->交换机 A。交换机 E 到交换机 A 有二条上行链，分别为交换机 E->交换机 B->交换机 A；交换机 E->交换机 C->交换机 A。



【配置方法】 ● 在接入交换机 D (E) 上配置抢占模式为 bandwidth，延迟时间为了 40S。

D

```
SwitchD> enable
```



```
SwitchD# configure terminal
SwitchD(config)# interface GigabitEthernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preemption mode bandwidth
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preemption delay 40
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

E

```
SwitchE> enable
SwitchE# configure terminal
SwitchD(config)# interface GigabitEthernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preemption mode bandwidth
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preemption delay 40
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

【检验方法】 ● 检查交换机 D (E) 配置的双链路备份信息。

D

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi0/1                 Gi0/2                 Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)
```

E

```
SwitchE#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi0/1                 Gi0/2                 Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)
```

常见配置错误

- 配置的接口非二层物理口或二层 ap 口

1.4.3 配置 MAC 地址更新功能

配置效果

- 在链路进行切换时能快速的消除、更新接口中的 MAC 地址信息，从而加快报文的收敛性。

注意事项

- 必须配置 REUP 双链路备份功能。
- 每台设备最多可以配置 8 个地址更新组。每个地址更新组最多可以有 8 个成员口，一个端口可以属于多个地址更新组

配置方法

- 必选配置。
- 若无特殊要求，应配置上 MAC 地址更新功能。

检验方法

使用 **show mac-address-table update group [detail]**命令查看更新组配置信息。

相关命令

配置交换机的 MAC 地址更新组 ID

- 【命令格式】 **mac-address-table update group [group-num]**
- 【参数说明】 *group-num*：MAC 地址更新组 ID。。
- 【命令模式】 接口模式
- 【使用指导】 为了减少因为 MAC 地址更新而导致的大量泛洪，影响交换机的正常数据传输，我们增加了一个 MAC 地址更新组的设置。只有把切换路径上的所有端口加入到同一个 MAC 地址更新组中，才能达到快速恢复下行数据传输的功能。

配置打开发送 MAC 地址更新消息的开关

- 【命令格式】 **mac-address-table move update transit**
- 【参数说明】 -
- 【命令模式】 配置模式
- 【使用指导】 为了减少链路切换时，下行数据流的丢失，需要在发生切换的交换机上打开发送 MAC 地址更新消息的功能。

配置打开发送 MAC 地址更新消息的 VLAN ID

- 【命令格式】 **mac-address-table move update transit vlan vid**
- 【参数说明】 *vid*：发送 MAC 地址更新消息的 VLAN ID

【命令模式】 接口模式

【使用指导】 链路切换时，打开发送 MAC 地址更新消息的功能时，会向上链设备发出 MAC 地址更新消息。

配置每秒发送的最大 MAC 地址更新报文数量。

▾ 配置每秒发送的最大 MAC 地址更新报文数量

【命令格式】 **mac-address-table move update max-update-rate***pkts-per-second*

【参数说明】 *pkts-per-second*：每秒发送的最大 MAC 地址更新报文数量。可选范围为 0-32000，默认为 150 个

【命令模式】 配置模式

【使用指导】 链路切换时，REUP 会向上链设备每秒发出特定数量的 MAC 地址更新报文，恢复上链设备的下行数据传输。

▾ 配置打开接收 MAC 地址更新消息的开关

【命令格式】 **mac-address-table move update receive**

【参数说明】 -

【命令模式】 配置模式

【使用指导】 当双链路备份发生切换时，由于上链交换机的 MAC 地址表没有及时更新，会导致下行数据流丢失。为了减少二层数据流的丢失，需要对上链交换机进行 MAC 地址表更新的处理。这就需要在链交换机上打开接收 MAC 地址更新消息的开关。

▾ 配置处理 MAC 地址更新消息的 VLAN 范围

【命令格式】 **mac-address-table move update receive vlan***vlan-range*

【参数说明】 *vlan-range*：处理 MAC 地址更新消息的 VLAN 范围

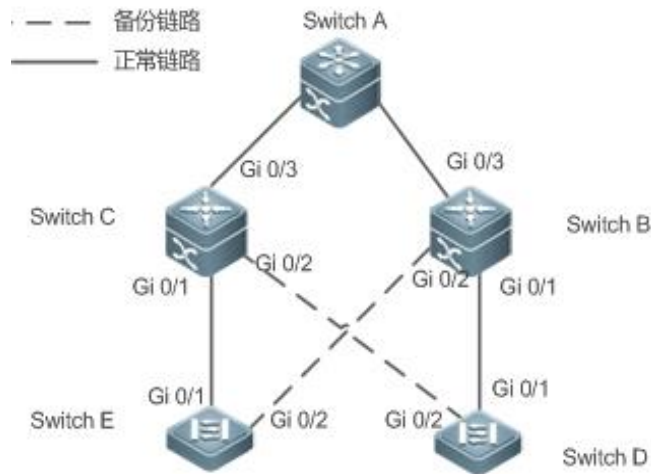
【命令模式】 配置模式

【使用指导】 通过此命令关闭某些 VLAN 上的处理 MAC 地址更新消息功能。关闭处理 MAC 地址更新消息的 VLAN 仍然可以通过 MAC 地址更新报文来恢复上链设备的下链传输，但是链路故障的收敛性能会降低。

配置举例

▾ 配置 MAC 地址更新

【网络环境】 在图 1-6 中，交换机 D 到交换机 A 有二条上行链，分别为交换机 D->交换机 B->交换机 A；交换机 D->交换机 C->交换机 A。交换机 E 到交换机 A 有二条上行链，分别为交换机 E->交换机 B->交换机 A；交换机 E->交换机 C->交换机 A。



【配置方法】

- 在接入交换机 D (E) 上打开发送 MAC 地址更新消息功能
- 在交换机 B (C) 上打开接收 MAC 地址更新报文功能
- 将 REUP 切换路径上的所有端口加入同一个 MAC 地址更新组
- 在环境中，在交换机 B 中 Gi0/1 和 Gi0/3 为 SwitchD 上行链路切换路径上接口，Gi0/3 和 Gi0/2 为 SwitchE 上行链路切换路径上接口，可以把 Gi0/1、Gi0/2 和 Gi0/3 同时加入一个地址更新组。同理可得出交换机 C 上的配置。
- 在交换机 A 上打开接收 MAC 地址更新报文功能。
- 在交换机 A 上的 REUP 切换路径上的所有端口加入同一个 MAC 地址更新组

D

```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# mac-address-table move update transit
SwitchD(config)# exit
```

E

```
SwitchE> enable
SwitchE# configure terminal
SwitchE((config)# mac-address-table move update transit
SwitchE(config)# exit
```

B SwitchB# configure terminal
SwitchB(config)# mac-address-table move update receive
SwitchB(config)# interface range gigabitEthernet 0/1 -3
SwitchB(config-if-range)#switchport mode trunk
SwitchB(config-if-range)# mac-address-table update group 1
SwitchB(config-if-range)# end

C SwitchC# configure terminal
SwitchC(config)# mac-address-table move update receive
SwitchC(config)# interface range gigabitEthernet 0/1 -3
SwitchC(config-if-range)#switchport mode trunk
SwitchC(config-if-range)# mac-address-table update group 1
SwitchC(config-if-range)# end

A SwitchA# configure terminal
SwitchA(config)# mac-address-table move update receive
SwitchA(config)# interface range gigabitEthernet 0/1 -2
SwitchA(config-if-range)# switchport mode trunk
SwitchA(config-if-range)# mac-address-table update group 1
SwitchA(config-if-range)# end

【检验方法】 检查交换机 D/E/C/B/A 显示地址更新组的信息

D SwitchD# show run | incl mac-ad
mac-address-table move update transit

E SwitchE# show run | incl mac-ad
mac-address-table move update transit

B SwitchB# show mac-address-table update group detail
show mac-address-table update group detailMac-address-table Update Group:1
Received mac-address-table update message count:0

Group member	Receive Count	Last Receive Switch-ID	Receive Time
Gi0/1	0	0000.0000.0000	
Gi0/2	0	0000.0000.0000	
Gi0/3	0	0000.0000.0000	

C SwitchC# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0

Group member	Receive Count	Last Receive Switch-ID	Receive Time
Gi0/1	0	0000.0000.0000	

A

```

Gi0/2          0          0000.0000.0000
Gi0/3          0          0000.0000.0000
SwitchA# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member      Receive Count    Last Receive Switch-ID    Receive Time
-----
Gi0/1             0             0000.0000.0000
Gi0/2             0             0000.0000.0000

```

常见配置错误

- 配置的接口非二层物理口或二层 ap 口

1.4.4 配置 VLAN 负载均衡功能

配置效果

- 最大限度的利用链路宽带。

注意事项

- 必须配置 REUP 双链路备份功能。
- VLAN 负载均衡不支持 Access 端口，支持和 STP 共用。
- 对于配置 VLAN 负载均衡成功的端口，禁止修改端口的属性，但可以修改端口 VLAN 属性。

配置方法

- 如果不要求最大限度的利用宽带，则为可选配置。
- 若有 VLAN 负载均衡功能要求，则进行相应配置。

检验方法

使用 **show interfaces switchport backup [detail]**命令查看是否配置了 VLAN 负载均衡功能。

相关命令

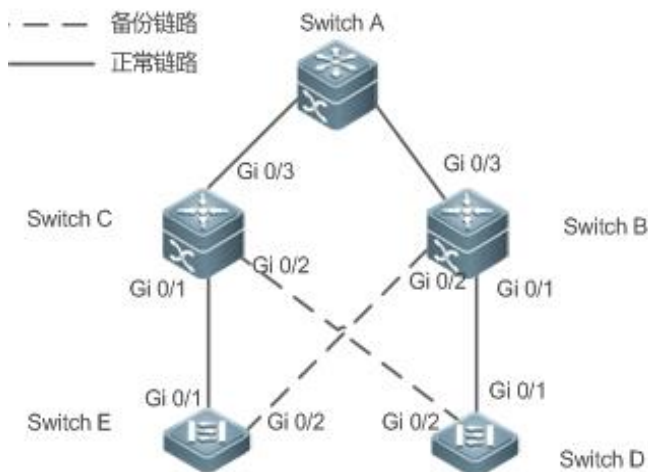
🔗 配置 VLAN 负载均衡功能

- 【命令格式】 **switchport backup interface** *interface-id* **prefer instance** *instance-range*
- 【参数说明】 *interface-id* : 备接口 id。
instance-range : 备份端口负载实例范围
- 【命令模式】 接口模式
- 【使用指导】 可以通过 MSTP 的实例映射功能来修改实例和 VLAN 的对应关系。

配置举例

配置 VLAN 负载均衡功能

- 【网络环境】 在图 1-6 中，交换机 D 到交换机 A 有二条上行链，分别为交换机 D->交换机 B->交换机 A；交换机 D->交换机 C->交换机 A。交换机 E 到交换机 A 有二条上行链，分别为交换机 E->交换机 B->交换机 A；交换机 E->交换机 C->交换机 A。



- 【配置方法】
- 在交换机 D (E) 上进行实现映射配置，把 VLAN 1 映射到实例 1、VLAN2 映射到实例 2，把 VLAN 3 映射到实例 3、VLAN4 映射到实例 4 这步可参考《MSTP 配置指南》
 - 在交换机 D (E) 上进行 VLAN 负载均衡功能配置

D

```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# interface GigabitEthernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi0/2 prefer instance 2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

E

```
SwitchE> enable
SwitchE# configure terminal
SwitchE(config)# interface GigabitEthernet 0/1
SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi0/2 prefer instance 4
```

```
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

【检验方法】 ● 检查交换机 D (E) 配置的双链路备份信息。

D

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi0/1                 Gi0/2                 Active Up/Backup Up

Instances Preferred on Active Interface: Instance 0-1, 3-64
Mapping VLAN 1, 3-4094

Instances Preferred on Backup Interface: Instance 2
Mapping VLAN 2

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : balance
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(800 kbits), Gi0/2(100000 kbits)
```

E

```
SwitchE#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi0/1                 Gi0/2                 Active Up/Backup Up

Instances Preferred on Active Interface: Instance 0-3, 5-64
Mapping VLAN 1-3, 5-4094

Instances Preferred on Backup Interface: Instance 4
Mapping VLAN 4

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : balance
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(800 kbits), Gi0/2(100000 kbits)
```

常见错误

- 没有配置好 VLAN id 与实例的映射关系

1.4.5 配置链路跟踪功能

配置效果

- 感知上行链路断开后，强制让下行链路也断开，从而使得链路进行切换。

注意事项

- 必须配置 REUP 双链路备份功能。
- 对于 Link State Tracking 功能，每个端口只能属于一个链路状态跟踪组，每台设备最多可以配置 2 个链路状态跟踪组。每个链路状态跟踪组可以有 8 个上行端口(Up Stream)，256 个下行端口(Down Stream)。

配置方法

- 必选配置。
- 若无特殊要求，应配置上链路跟踪功能。

检验方法

使用 **show link state group** 命令查看配置的链路跟踪信息。

相关命令

配置启用链路状态跟踪组

- 【命令格式】 **link state track [num]**
- 【参数说明】 *num*：链路状态跟踪组 ID。
- 【命令模式】 配置模式
- 【使用指导】 必须先创建链路跟踪组，然后才能将端口加入指定的跟踪组。

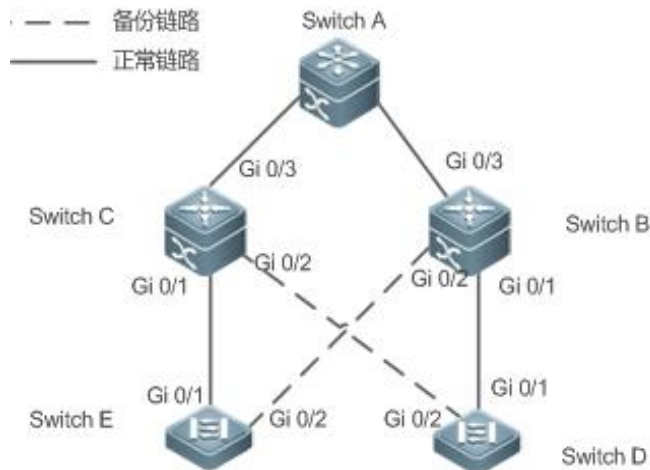
配置接口加入链路跟踪组

- 【命令格式】 **ink stategroup num {upstream | downstream}**
- 【参数说明】 *num*：链路状态跟踪组 ID。
upstream：将端口加入跟踪组的上链接口中
downstream：将端口加入跟踪组的下链接口中
- 【命令模式】 接口模式
- 【使用指导】 必须先创建链路跟踪组，然后才能将端口加入指定的跟踪组。

配置举例

配置链路跟踪组

【网络环境】 在图 1-6 中，交换机 D 到交换机 A 有二条上行链，分别为交换机 D->交换机 B->交换机 A；交换机 D->交换机 C->交换机 A。交换机 E 到交换机 A 有二条上行链，分别为交换机 E->交换机 B->交换机 A；交换机 E->交换机 C->交换机 A。



- 【配置方法】
- 在交换机 B (C) 上，创建一个链路跟踪组 1
 - 在交换机 B (C) 上，把接口 Gi0/1 和 Gi0/2 加入链路跟踪组的下链接口中，把接口 Gi0/3 加入链路跟踪组的上链接口中

B

```
SwitchB> enable
SwitchB# configure terminal
SwitchB(config)# link state track 1
SwitchB(config)# interface GigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#link state group 1
SwitchB(config-if-GigabitEthernet 0/1)#exit
SwitchB(config)# interface GigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)# link state group 1 downstream
SwitchB(config-if-GigabitEthernet 0/2)#exit
SwitchB(config)# interface GigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#link state group 1 upstream
SwitchB(config-if-GigabitEthernet 0/3)#exit
```

C

```
SwitchC> enable
SwitchC# configure terminal
SwitchC(config)# link state track 1
SwitchC(config)# interface GigabitEthernet 0/1
SwitchC(config-if-GigabitEthernet 0/1)#link state group 1
downstreamSwitchC(config-if-GigabitEthernet 0/1)#exit
SwitchC(config)# interface GigabitEthernet 0/2
SwitchC(config-if-GigabitEthernet 0/2)# link state group 1 downstream
SwitchC(config-if-GigabitEthernet 0/2)#exit
SwitchC(config)# interface GigabitEthernet 0/3
SwitchC(config-if-GigabitEthernet 0/3)#link state group 1 upstream
SwitchC(config-if-GigabitEthernet 0/3)#exit
```

【检验方法】**检查交换机 B (C) 配置的链路跟踪组信息****B**

```
SwitchB#show link state group
Link State Group:1  Status: enabled, Down
Upstream Interfaces :Gi0/3(Down)
Downstream Interfaces : Gi0/2(Down)

Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :

(Up):Interface up    (Down):Interface Down    (Dis):Interface disabled
```

C

```
SwitchC#show link state group
Link State Group:1  Status: enabled, Down
Upstream Interfaces :Gi0/3(Down)
Downstream Interfaces : Gi0/2(Down)

Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :

(Up):Interface up    (Down):Interface Down    (Dis):Interface disabled
```

常见配置错误

- 没有启用链路跟踪组就把端口加入组中

1.5 监视与维护

清除各类信息

作用	命令
-	-

查看运行情况

作用	命令
查看 REUP 双链路备份信息	show interfaces[<i>interface-id</i>]switchport backup [detail]
查看地址 MAC 地址更新组的配置信息	show mac-address-table update group [detail]
查看 REUP 对发送 MAC 地址更新消息的统计信息	show mac-address-table move update
查看链路状态跟踪组的信息	show link state group

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 REUP 所在调试开关	debug reup all
打开 REUP 的正常用运行过程的开关	debug reup process
打开 REUP 的 MAC 地址更新消息的开关	debug reup packet
打开 REUP 的 MAC 地址更新报文的开关	debug reup macupdt
打开热备开关	debug reup ha
打开整个 REUP 运行出错误的开关	debug reup error
打开接收到事件的开关	debug reup evnet
打开 show 操作时相关统计的开关	debug reup status

2 RLDP

2.1 概述

RLDP (Rapid Link Detection Protocol , 快速链路检测协议) 是一种以太网链路故障检测协议 , 用于快速检测单向链路故障、双向链路故障以及下联环路故障。如果发现故障存在 , RLDP 会根据用户配置的故障处理方式自动关闭或通知用户手工关闭相关端口 , 以避免流量的错误转发或者防止以太网二层环路。

协议规范

- 无

2.2 典型应用

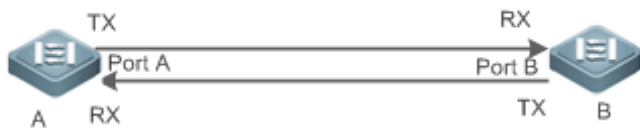
典型应用	场景描述
单向链路检测	检测链路单向故障
双向链路检测	检测链路双向故障
下联环路检测	检测链路环路故障

2.2.1 单向链路检测

应用场景

如下图所示 , 设备 A 与设备 B 之间通过光纤相连 , 图中的两条线分别表示光纤的 Tx 线与 Rx 线 , A 与 B 分别使能 RLDP 的单向链路检测功能。如果端口 A 的 Tx 与端口 B 的 Rx 或者端口 A 的 Rx 与端口 B 的 Tx 中任意一个出现故障 , 那么协议可以检测出单向故障并做出相应的处理。故障如果被恢复 , 管理员可以手工在 A 和 B 上恢复协议状态并重新开始检测。

图 2-1



- 【注释】
- A、B 为二层或者三层交换机。
 - A 上的 Port A 的 TX 与 B 上的 Port B 的 RX 连接。
 - A 上的 Port A 的 RX 与 B 上的 Port A 的 TX 连接。

功能部署

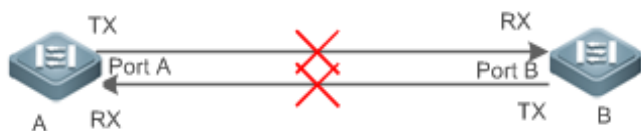
- 全局配置 RLDP 使能。
- 接口下配置 RLDP 的单向链路检测功能并指定单向故障发生时的处理方式。

2.2.2 双向链路检测

应用场景

如下图所示，设备 A 与设备 B 之间通过光纤相连，图中的两条线分别表示光纤的 Tx 线与 Rx 线，A 与 B 分别使能 RLDP 的双向链路检测功能。如果端口 A 的 Tx 与端口 B 的 Rx 以及端口 A 的 Rx 与端口 B 的 Tx 同时出现故障，那么协议可以检测出双向故障并做出相应的处理。故障如果被恢复，管理员可以手工在 A 和 B 上恢复协议状态并重新开始检测。

图 2-2



【注释】 A、B 为二层或者三层交换机。
A 上的 Port A 的 TX 与 B 上的 Port B 的 RX 连接。
A 上的 Port A 的 RX 与 B 上的 Port A 的 TX 连接。

功能部署

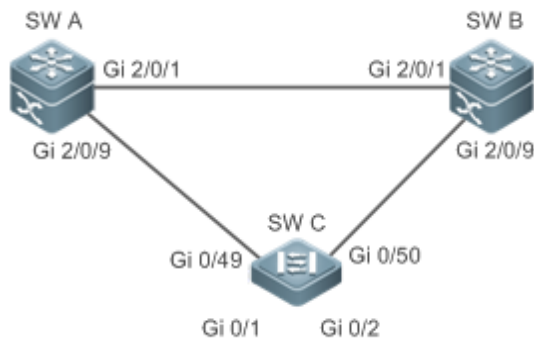
- 全局配置 RLDP 使能。
- 接口下配置 RLDP 的双向链路检测功能并指定双向故障发生时的处理方式。

2.2.3 下联环路链路检测

应用场景

如下图所示，设备 A、设备 B 以及设备 C 之间连成网络环路，A 使能 RLDP 的下联环路检测功能，协议此时可以检测出环路故障并做响应的。

图 2-3



【注释】 A、B、C 为二层或者三层交换机。
A、B、C 通过交换口两两互连。

功能部署

- A 上全局配置 RLDP 使能。
- A 与 B 的连接端口、A 与 C 的连接端口分别配置 RLDP 下联环路检测功能并指定环路故障发生时的处理方式。

2.3 功能详解

一般的以太网链路检测机制都只是利用物理连接的状态，通过物理层的自动协商来检测链路的连通性。但是这种检测机制存在一定的局限性，有些情况下物理层虽然处于连通状态并能正常工作，但是实际对应的二层链路却是无法通信或者存在异常。RLDP 协议通过与邻居设备交互探测报文、探测响应报文或者环路报文来识别邻居设备并检测链路是否存在故障。

基本概念

📌 链路单向故障

光纤交叉连接、一条光纤未连接、一条光纤断路、双绞线中的一条线路断路或者两台设备之间的中间设备出现单向断路等情况下会出现链路单向故障，这种链路一边能通而另一边不能通会导致流量被错误转发或者环路保护协议（比如 STP）功能失效。

📌 链路双向故障

两条光纤断路、双绞线中的两条线路断路或者两台设备之间的中间设备出现双向断路等情况下会出现链路双向故障，这种链路双向都不通会导致流量被错误的转发。

📌 链路环路故障

设备下联被用户错误的接入其他设备形成了环路，这种会在网络中引起广播风暴。

📌 RLDP 协议报文

协议定义了三种类型的报文：探测报文（Prob）、探测响应报文（Echo）以及环路报文（Loop）。

- Prob 报文为二层组播报文，用于邻居协商、单向或者双向链路检测，报文的默认封装格式为 SNAP 类型，如果邻居发出的报文格式为 EthernetII 格式则封装方式自动变更为 EthernetII；
- Echo 报文为响应 Prob 报文的二层单播报文，用于单向或者双向链路检测，报文的默认封装格式为 SNAP 类型，如果邻居发出的报文格式为 EthernetII 格式则封装方式自动变更为 EthernetII；
- Loop 报文为二层组播报文，用于下联环路检测，这类报文只会被发送方所接收，报文的封装格式为 SNAP 封装方式。

📌 RLDP 探测间隔及最大探测次数

RLDP 可以配置探测间隔与最大探测次数。探测间隔决定了 Prob 报文与 Loop 报文的发送周期，设备在接收到 Prob 报文后会立即响应 Echo 报文。探测间隔与最大探测次数决定了单向或者双向链路探测的最大探测时间（探测间隔 × 最大探测次数 + 1），最大探测时间内如果无法正确接收到邻居的 Prob 报文或者 Echo 报文可以触发单向或者双向故障的处理。

📌 RLDP 邻居协商

配置了单向或者双向检测功能的端口可以学习到对端设备作为邻居，一个端口支持学习一个邻居，邻居可变化。协商功能启用后，端口下协商到邻居后才开始单向或者双向检测，协商过程中如果成功接收到邻居发送的 Prob 报文就认为协商成功。但是，在已存在故障的情况下才使能协议，会出现无法正常学习邻居而导致检测不能启动，建议此时先恢复链路的错误状态。

📌 RLDP 端口故障时的处理方式

- warning：只打印相关的 Syslog 说明当前的故障端口和故障类型。
- Shutdown SVI：打印 Syslog 的基础上，如果故障端口为物理交换口或者 L2 AP 成员口，那么会根据端口所属的 Access VLAN 或者 Native VLAN 查询出对应的 SVI 并执行 Shutdown 操作。
- 端口违例：打印 Syslog 的基础上，设置故障端口为违例状态，此时端口物理上会进入 Linkdown 状态。
- Block：打印 Syslog 的基础上，设置故障端口的转发状态为 Block，此时端口不对收到的报文进行转发。

📌 RLDP 端口故障后的恢复方式

- 手工执行 Reset：手工将所有故障端口恢复到初始化状态，此时会重新启动链路检测。
- 手工或者自动执行 Errdisable Recovery：手工或者定时（默认每 30s，可配置）恢复所有故障端口到初始化状态并重新启动链路检测。
- 自动恢复：单向或者双向链路检测的情况下，如果指定的故障处理方式不是端口违例，那么可以依赖与邻居交互的 Prob 报文自动恢复到初始化状态并重新启动链路检测。

📌 RLDP 端口状态

- normal：端口下配置启动检测后的状态。
- error：端口下检测出链路故障后的状态，可以是单向、双向或者环路故障导致。

📌 功能特性

功能特性	作用
建立 RLDP 检测	启用单向、双向或者下联环路检测功能，永远检测单向、双向或者环路故障并进行相应的故障处理。

2.3.1 建立 RLDP 检测

RLDP 的链路检测模式主要包括单向链路检测、双向链路检测以及下联环路检测等。

工作原理

RLDP 单向链路检测

单向链路检测启动后，端口后周期的发送 Prob 报文并接收邻居响应的 Echo 报文，同时接收邻居的 Prob 报文并及时响应 Echo 报文给邻居。在最大探测时间内，如果只能接收到邻居的 Prob 报文但无法接收到邻居的 Echo 报文或者既不能接收到邻居的 Prob 报文也不能接收到邻居的 Echo 报文，那么会触发单向故障的处理并停止检测。

RLDP 双向链路检测

双向链路检测启动后，端口后周期的发送 Prob 报文并接收邻居响应的 Echo 报文，同时接收邻居的 Prob 报文并及时响应 Echo 报文给邻居。在最大探测时间内，如果既不能接收到邻居的 Prob 报文也不能接收到邻居的 Echo 报文，那么会触发双向故障的处理并停止检测。

RLDP 下联环路检测

下联环路检测启动后，端口会周期的发送 Loop 报文，同一个设备的相同端口或者不同端口接收到 Loop 报文后，如果报文发送端口与接收端口为路由口或者 L3 AP 成员口并且发送口与接收后相同则触发环路故障，或者报文发送端口与接收端口为交换口或者 L2 AP 成员口并且端口的默认 VLAN 相同同时转发状态均为 Forward 则触发环路故障，故障发生后按相应的故障处理方式来处理并停止检测。

相关配置

- 配置 RLDP 检测功能

缺省情况下，检测功能不生效。

使用 RLDP 全局命令 **rldp enable** 和接口命令 **rldp port** 可以启动 RLDP 检测功能，并指定检测类型与故障处理方式。

用户可以根据实际环境通过 **rldp neighbor-negotiation** 指定邻居协商、**rldp detect-interval** 指定探测间隔、**rldp detect-max** 指定探测次数、**rldp reset** 恢复故障端口状态等。

2.4 配置详解

配置项	配置建议&相关命令	
配置 RLDP 基本功能	 全局模式，必须配置。配置全局开启 RLDP 探测功能	
	rldp enable	全局下启动 RLDP 检测，生效到所有端口。

 接口模式，必须配置。指定接口下的探测类型以及故障处理方式。	
rldp port	端口下启动 RLDP 检测，指定具体的检测类型以及发生故障后的处理方式。
 全局模式，可选配置。指定探测过程中的探测间隔、探测次数、是否需要邻居协商。	
rldp detect-interval	全局修改 RLDP 配置参数，包括探测间隔、最大探测次数以及邻居协商，可生效到所有端口下的 RLDP 检测。
rldp detect-max	
rldp neighbor-negotiation	
 特权模式，可选配置。	
rldp reset	特权下恢复故障端口的状态，可生效到所有端口下的 RLDP 检测。

2.4.1 配置 RLDP 基本功能

配置效果

- 启用 RLDP 单向、双向或者下联环路检测，用于发现单向、双向或者环路故障。

注意事项

- 对于 AP 成员口上的 RLDP 配置，如果是配置环路检测，则会同步配置到该 AP 的所有成员口，如果是配置单向链路检测和双向链路检测，则直接在 AP 成员口生效。
- 对于物理口加入 AP 的情况，新加入的 AP 成员口的环路检测配置需要和该 AP 现有的成员口的环路检测配置一致。这里分 3 种情况：1) 如果新加入的 AP 成员口没有配置环路检测，而该 AP 现有的成员口有配置环路检测，则新加入的 AP 成员口同步环路检测的配置和检测结果。2) 如果新加入的 AP 成员口的环路检测配置和该 AP 现有的成员口的环路检测配置不一致，则新加入的 AP 成员口同步环路检测的配置和检测结果。
- AP 成员口配置 RLDP 时，故障处理方法只能配置为“shutdown-port”，如果故障处理方法配置为非“shutdown-port”时，将转换成“shutdown-port”的配置并生效。
- 配置了“shutdown-port”故障处理的端口在出现故障后将无法主动恢复 RLDP 探测，如果用户确认故障已经解决，则可以使用 **rldp reset** 命令或者 **errdisable recovery** 命令来恢复并重新启动检测，**errdisable recovery** 的配置可以参考 <<SWITCH-INTF-SCG.doc>>。

配置方法

📌 全局配置使能

- 必须配置。
- 全局模式下配置，配置后各端口的检测可以启动。

✎ 全局配置邻居协商

- 可选配置。
- 全局模式下配置，配置后各端口检测的启动依赖于邻居协商的成功。

✎ 全局配置探测间隔

- 可选配置。
- 全局模式下配置，可以指定具体的时间间隔。

✎ 全局配置最大探测次数

- 可选配置。
- 全局模式下配置。
- 可以指定具体的最大探测次数。

✎ 接口下配置检测功能

- 必须配置。
- 接口模式下配置。
- 在接口下配置 RLDP 功能，可以选择单向、双向或者下联环路检测类型，同时指定对应的故障处理方式。

✎ 特权下配置恢复所有故障端口状态

- 可选配置。
- 特权模式下配置，配置后可以恢复所有故障状态端口，重新启动检测。

检验方法

- 查看设备的 RLDP 信息，包括全局、端口以及邻居的相关信息。

相关命令

✎ 全局使能 RLDP 检测功能

- | | |
|--------|-----------------|
| 【命令格式】 | rldp enable |
| 【参数说明】 | - |
| 【命令模式】 | 全局模式。 |
| 【使用指导】 | 全局启用 RLDP 检测功能。 |

接口下启动 RLDP 检测功能

- 【命令格式】 **rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port | block }**
- 【参数说明】 **unidirection-detect**：单向链路检测。
bidirection-detect：双向链路检测。
loop-detect：下联环路检测。
warning：故障处理方式告警。
shutdown-svi：故障处理方式为关闭接口所在的 SVI 口。
shutdown-port：故障处理方式为端口违例。
block：故障处理方式为关闭端口的学习转发能力。
- 【命令模式】 接口模式
- 【使用指导】 接口包括：2 层交换口、3 层路由口、L2AP 下的成员口、L3AP 下的成员口等接口。

全局修改 RLDP 检测参数

- 【命令格式】 **rldp {detect-interval interval | detect-max num | neighbor-negotiation }**
- 【参数说明】 **detect-interval interval**：探测间隔。
detect-max num：最大探测次数。
neighbor-negotiation：邻居协商。
- 【命令模式】 全局模式
- 【使用指导】 当实际环境变化，需要修改所有 RLDP 检测的参数时，对所有端口生效。

恢复 RLDP 故障端口状态

- 【命令格式】 **rldp reset**
- 【参数说明】 -
- 【命令模式】 特权模式
- 【使用指导】 恢复 RLDP 所有故障端口状态到初始状态并重新启动检测。

查看 RLDP 状态信息

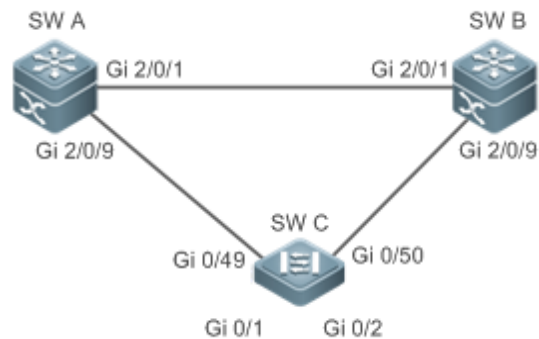
- 【命令格式】 **show rldp [interface interface-name]**
- 【参数说明】 **interface-name**：指定要查看的具体接口
- 【命令模式】 特权模式、全局模式、接口模式
- 【使用指导】 查看 RLDP 状态信息。

配置举例

在环网拓扑中开启 RLDP 检测功能

- 【网络环境】 如下图所示，汇聚与接入为环网拓扑，环网中各设备均开启 STP 来防止环路并提供冗余保护，为了防止环路中链路出现单向或者双向故障进而导致 STP 协议失效，汇聚设备与汇聚设备之间以及汇聚与接入设备之间启用 RLDP 单向和双向检测，为了防止汇聚设备下联被错误的接入而出现环路，汇聚设备与接入设备的下联口
- 图 2-4

均开启 RLDP 环路检测；为了防止接入设备下联被错误的接入而出现环路，接入设备的下联口均开启 RLDP 环路检测



- 【配置方法】
- SW A、SW B 作为汇聚，SW C 作为接入，SW C 下联可以接用户设备，三台设备组成环网拓扑，每台设备开启 STP，STP 配置参考相关配置指南。
 - SW A 开启 RLDP，两个端口需要配置单向和双向链路检测，下联端口需要配置开启环路检测。
 - SW B 开启 RLDP，两个端口需要配置单向和双向链路检测，下联端口需要配置开启环路检测。
 - SW C 开启 RLDP，上联两个端口需要配置单向和双向链路检测，下联两个端口需要配置开启环路检测

A

```

A#configure terminal
A(config)#rldp enable
A(config)#interface GigabitEthernet 2/0/1
A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)# exit
A(config)#interface GigabitEthernet 2/0/9
A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port loop-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#exit
  
```

B

同 A 的配置

C

```

C#configure terminal
C(config)#rldp enable
C(config)#interface GigabitEthernet 0/49
C(config-if-GigabitEthernet 0/49)#rldp port unidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/49)#rldp port bidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/49)# exit
C(config)#interface GigabitEthernet 0/50
C(config-if-GigabitEthernet 0/50)#rldp port unidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/50)#rldp port bidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/50)#exit
C(config)#interface GigabitEthernet 0/1
C(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port
  
```

```
C(config-if-GigabitEthernet 0/1)#exit
C(config)#interface GigabitEthernet 0/2
C(config-if-GigabitEthernet 0/2)# rldp port loop-detect shutdown-port
C(config-if-GigabitEthernet 0/2)#exit
```

【检验方法】 ● 检查 A、B、C 设备的 RLDP 状态信息，以 A 为例。

A

```
A#show rldp
rldp state          : enable
rldp hello interval: 3
rldp max hello      : 2
rldp local bridge   : 00d0.f822.33aa
-----
Interface GigabitEthernet 2/0/1
port state          : normal
neighbor bridge    : 00d0.f800.51b1
neighbor port      : GigabitEthernet 2/0/1
unidirection detect information:
    action: shutdown-port
    state : normal
bidirection detect information:
    action: shutdown-port
    state : normal

Interface GigabitEthernet 2/0/9
port state          : normal
neighbor bridge    : 00d0.f800.41b0
neighbor port      : GigabitEthernet 0/49
unidirection detect information:
    action: shutdown-port
    state : normal
bidirection detect information:
    action: shutdown-port
    state : normal
loop detect information:
    action: shutdown-port
    state : normal
```

常见错误

- 与私有组播地址认证或者 TPP 等功能不可以同时开启。
- 配置单双向检测时不指定邻居协商，要求邻居设备在全局和接口下使能 RLDP，否则会被检测为单向或者双向故障。

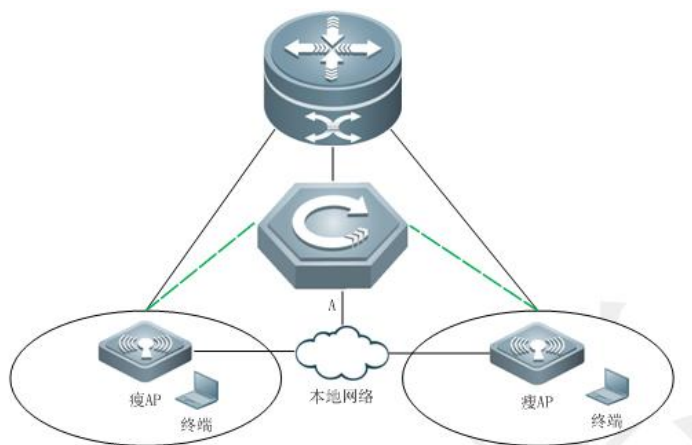
- 配置单双向检测时如果指定了先协商邻居后开始检测 那么在已存在故障的情况下由于无法学习到邻居而导致不能正常检测，建议先恢复链路错误状态。
- 路由口下建议不要指定故障处理方式为 Shutdown SVI。
- STP 等环路保护协议使能的端口下建议不要指定故障处理方式为 Block。

在无线 AP 场景下配置 RLDP 环路检测功能

【网络环境】

如下图所示，无线 AP 场景下，由于环境中存在大量 AP，如果通过逐个登入 AP 设备进行 RLDP 环路检测功能的配置及修订，将十分繁琐。因此可通过无线控制器 AC 将 RLDP 环路检测功能配置下发至在线的所有 AP（或单独某 AP）上。

图 2-5



【配置方法】

- 进入无线控制器 AC 上进入 ap-config 模式。
- 在对应的 AP 有线口上开启 RLDP 环路检测功能。
- 在对应的 AP 全局打开 RLDP 功能。
- 在对应的 AP 全局配置被 RLDP 设置违例的端口恢复时间。

A

```
A#configure terminal
A(config)#ap-config all
A(config-ap)#exec-cmd mode "int gi 0/1" cmd "rldp port loop-detect shutdown-port"
A(config-ap)#exec-cmd mode configure cmd "rldp enable"
A(config-ap)#exec-cmd mode configure cmd "errdisable recovery interval 600"
```

【检验方法】

- 在 AC 上查看 RLDP 环路检测配置是否生效。

A

```
A# show run
!
ap-config all
  exec-cmd mode "int gi 0/1" cmd "rldp port loop-detect shutdown-port"
  exec-cmd mode configure cmd "rldp enable"
  exec-cmd mode configure cmd "errdisable recovery interval 600"
!
```

常见错误

- 执行 exec-cmd 进行接口配置时，对应的 AP 有线口输入错误。
- 更改 RLDP 环路检测配置时，没有配置 no exec-cmd 删除原来的配置，或者没有重新通过 exec-cmd 进行反向的配置。

2.5 监视与维护

查看运行情况

作用	命令
查看 RLDP 运行状态。	show rldp [interface <i>interface-name</i>]

3 DLDP

3.1 概述

DLDP (Data Link Detection Protocol , 数据链路检测协议) , 是一种基于快速检测以太网链路故障的检测协议。

一般的以太网链路检测机制都只是利用物理连接的状态, 通过物理层的自动协商来检测链路的连通性。但是该方法对于三层的数据连通性检测, 如物理连接状态正常但三层数据通信异常的场景, 存在一定的局限性。

DLDP 在这类场景中, 为用户提供可靠的三层链路检测信息。同时, 在检测出故障后, DLDP 主动 SHUTDOWN 三层接口的逻辑状态, 促使三层协议快速收敛。

协议规范

- 无

3.2 典型应用

典型应用	场景描述
同网段 DLDP 检测	检测端口的源 IP 与检测 IP 属于同一网段。
跨网段 DLDP 检测	检测端口的源 IP 与检测 IP 属不同网段

3.2.1 同网段 DLDP 检测

应用场景

检测端口的源 IP 与检测 IP 属于同一网段的基本应用场景。

以下图为例, 设备 A 上的三层口 Gi 0/1 与设备 C 上的三层口 Gi 0/2 属同网段, 若要检测 Gi 0/1 到 Gi 0/2 三层线路的连通性, 仅需在 A 或 C 的相应三层口开启 DLDP 检测功能即可。

图 3-1



【注释】 Gi 0/1 与 Gi 0/2 均为三层口, 且属同一网段。

B 为同网段网络。

功能部署

- 在 Gi 0/1 或 Gi 0/2 上开启 DLDP 检测即可。

3.2.2 跨网段 DLDP 检测

应用场景

检测端口的源 IP 与检测 IP 在不同网段的应用场景。

以下图为例,设备 A 上的三层口 Gi 0/1 与设备 D 上的三层口 Gi 0/4 在不同网段,若要检测 Gi 0/1 到 Gi 0/4 三层线路的连通性,则需在 A 的 Gi 0/1 开启 DLDP 功能的同时还需再配置 DLDP 下一跳 IP 地址(设备 B 上的 Gi 0/2 的 IP 地址)。

图 3-2



【注释】 Gi 0/1 与 Gi 0/4 均为三层口,但在不同网段。

功能部署

- 在 Gi 0/1 上开启 DLDP 并配置 DLDP 下一跳 IP 地址。

3.3 功能详解

基本概念

DLDP 的探测间隔及重传次数

探测间隔:指 DLDP 探测报文(ICMP echo)的发送间隔。

重传次数:指 DLDP 探测失效所需的发包次数。

当网络设备在“探测间隔”×“重传次数”的时间周期内没有收到对端的应答报文,则认为三层链路故障,主动 SHUTDOWN 三层接口逻辑状态(实际物理链路还是连通的)。一旦三层链路正常通讯,则恢复三层接口逻辑状态 UP。

DLDP 检测模式

DLDP 的检测模式包括：主动模式和被动模式。

主动模式：指主动发送 ICMP 探测报文的模式，缺省配置为主动模式。

被动模式：指被动接收 ICMP 探测报文的模式。

DLDP 的下一跳

下一跳：指跨网段 DLDP 检测中，检测 IP 对应的路由下一节点。

在某些情形下，DLDP 需要检测非直连网段 IP 的可达性。这时需要配置该接口的下一跳 IP，以便 DLDP 能够通过 ARP 报文获取下一跳 MAC 地址，正确的封装 ICMP 报文并发出。

但在这种情形下，需避免响应报文从其他链路回应的情况，否则会造成 DLDP 误判该接口没有收到 ICMP 应答。

DLDP 的恢复次数

恢复次数：指 DLDP 从故障中恢复需连续收到的响应报文（ICMP reply）次数。

在有些情形下，检测链路可能不太稳定，比如 PING 断了三次，通一次，又断了多次。如果按简单的逻辑，其中的 DLDP 检测就是 UP、DOWN 多次，实际可能加剧环网的不稳定。

恢复次数表示链路从 DOWN 状态为设置为 UP 状态前，需要收到连续的 DLDP 检测报文响应次数。恢复次数缺省为 3 次，即只有该链路上连续 PING 通了 3 次才会设置为 UP。在这种情况下，虽然降低了链路检测的灵敏度，但增加其稳定性，同时相关参数在实际应用中还可根据网络情况进行调整。

DLDP 的绑定 MAC

绑定 MAC：指 DLDP 检测 IP 所绑定的 MAC 地址

在复杂的网络环境下，检测链路中可能存在异常 ARP 报文（ARP 欺骗），使得 DLDP 则获取到非法的 MAC 地址，从而导致检测无法正常工作。

在此种环境下，通过配置绑定 MAC 地址，可将检测 IP(或下一跳 IP)与静态 MAC 地址进行绑定，不再受异常 ARP 报文欺骗而引起 DLDP 功能失效。

功能特性

功能特性	作用
建立 DLDP 检测	实现 DLDP 三层链路连通性检测，在三层链路异常时，主动 SHUTDOWN 掉对应三层口。
绑定 MAC 地址	当网络中存在 ARP 欺骗等异常情况，可将检测 IP 与设备 MAC 地址进行绑定，避免协议异常发生。
DLDP 被动模式	当检测链路两端都开启 DLDP，其中一端可配置为被动模式，以节省带宽资源和设备 CPU 资源。

3.3.1 建立 DLDP 检测

DLDP 三层链路连通性检测，在检测出三层链路异常时，主动 SHUTDOWN 掉对应三层口。

工作原理

启动 DLDP 功能后，DLDP 会通过 ARP 报文获取被检测设备或者到达被检测设备的下一跳设备的 mac 地址和出接口，然后通过周期性的 IPv4 ICMP echo 报文进行通路检测。如果在指定时间内被检测设备没有回应 IPv4 ICMP reply 报文，则认为这个接口通路出现问题，将该接口设置为“三层接口 DOWN”。

相关配置

- 配置 DLDP 检测功能

缺省情况下，接口上不开启 DLDP 检测功能。

使用 dldp 命令并指定要检测的目的 IP 地址就可以启动 DLDP 检测功能。

用户可以根据实际环境选择是否配置下一跳 IP、MAC 地址、发送间隔、重传次数、恢复次数等参数。

3.3.2 绑定 MAC 地址

网络中存在 ARP 欺骗等异常情况，可将检测 IP（或下一跳 IP）与设备 MAC 地址进行绑定，避免协议发生异常情况。

工作原理

网络中存在 ARP 欺骗的情况下，通过配置绑定 MAC 地址，可将检测 IP(或下一跳 IP)与静态 MAC 地址进行绑定，不再受异常 ARP 报文欺骗而引起 DLDP 功能失效。

相关配置

缺省情况下开启 DLDP 检测功能时不指定 MAC 地址绑定。

通过 dldp 命令开启检测时并同时指定要绑定的 MAC 地址，若存在下一跳 IP 地址，则配置的是下一跳设备的 MAC 地址，否则配置目的检测设备的 MAC 地址。

配置开启后，DLDP 探测过程中发送的 ARP 报文与 ICMP 报文中的目的 IP 与目的 MAC 是固定的，如果接收的报文中源 IP 与源 MAC 和绑定的 IP 与 MAC 不匹配，则不会进行处理。

3.3.3 DLDP 被动模式

当检测链路两端都开启 DLDP，其中一端可配置为被动模式，以节省带宽资源和设备 CPU 资源。

工作原理

一端设备使用 ICMP echo 发包，另一端用同样的检测参数来确认报文的及时可达，一样能达到双方设备检测链路通路的效果，同时也节省了带宽资源和设备 CPU 资源。

相关配置

缺省情况下不开启 DLDP 被动检测模式。

通过 `dldp passive` 命令开启被动检测。

配置开启后，DLDP 将不再主动发起 ICMP echo 报文进行探测，只需要在接收到 ICMP echo 报文后响应 ICMP Reply 报文即可，在指定时间内如果没有收到 ICMP echo 报文则认为接口通路出现问题。

3.4 配置详解

配置项	配置建议&相关命令	
配置 DLDP 检测功能	 必须配置，接口模式，开启 DLDP 检测功能	
	dldp	配置 DLDP 检测功能
	 可选配置，接口模式，开启被动检测功能。	
	dldp passive	配置接口被动模式
	 可选配置，全局模式，指定探测过程中的探测间隔、重传次数以及恢复次数。	
	dldp interval	全局修改 DLDP 配置参数，可生效到所有 DLDP 检测
	dldp retry	
	dldp resume	

3.4.1 配置 DLDP 检测功能

配置效果

- 实现 DLDP 三层链路连通性检测，在三层链路异常时，主动 SHUTDOWN 掉对应三层口。

注意事项

- 一个三层接口下，DLDP 可以配置多个 IP 检测，当所有 IP 都没有 ICMP 响应时，才认为接口 DOWN；而一旦有一个 IP 恢复通讯，则认为接口恢复 UP。
- DLDP 使用该三层接口的第一个 IP 地址作为报文的源 IP 地址进行通讯。

配置方法

启动 DLDP 检测功能

- 必须配置。
- 在接口下配置 DLDP 功能：根据实际环境选择是否配置下一跳 IP、MAC 地址、发送间隔、重传次数、恢复次数等参数。

配置 DLDP 检测模式

- 可选配置。
- 在接口下配置 DLDP 检测模式：根据实际环境选择配置为主动或被动模式。
- 如当三层链路两端都需要开启 DLDP 功能，为节省了带宽资源和设备 CPU 资源，可将其中一端的 DLDP 检测模式改为被动模式。

全局配置 DLDP 参数

- 可选配置。
- 根据需求，可在全局下修改所有 DLDP 检测的参数，包括：检测报文的发送间隔、检测报文的重传次数、恢复次数。

检验方法

- 查看设备的 DLDP 信息，包括所有 DLDP 检测的状态信息以及其统计信息。

相关命令

启动 DLDP 检测功能

【命令格式】 **dldp** *ip-address* [*next-hop-ip*] [**mac-address** *mac-addr*] [**interval** *tick*] [**retry** *retry-num*] [**resume** *resume-num*]

【参数说明】 *ip-address*：DLDP 检测 IP 地址。
next-hop-ip：下一跳 IP 地址。
mac-addr：绑定 MAC 地址，若存在下一跳 IP 地址，则配置的是下一跳设备的 MAC 地址。
tick：检测报文的发送间隔，取值范围：5-6000 tick（1 tick = 10 毫秒），缺省值 100 tick（1 秒）。
retry-num：取值范围：1-3600，缺省值 4。
resume-num：恢复次数，取值范围：1-200，缺省值 3。

【命令模式】 接口模式

【使用指导】 接口必须是三层接口，包括：路由口、L3AP、SVI 等接口。

配置 DLDP 检测模式

【命令格式】 **dldp passive**

- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 接口下必须先开启 DLDP 检测功能后才能配置 DLDP 检测模式。

✎ 全局修改 DLDP 检测参数

- 【命令格式】 **dldp { interval tick | retry retry-num | resume resume-num }**
- 【参数说明】 *tick* : 检测报文的发送间隔, 取值范围 : 5-6000 tick (1 tick =10 毫秒), 缺省值 100 tick (1 秒)。
- retry-num* : 检测报文的重传次数, 取值范围 : 1-3600, 缺省值 4。
- resume-num* : 恢复次数, 取值范围 : 1-200, 缺省值 3。
- 【命令模式】 全局模式
- 【使用指导】 当实际环境变化, 需要修改所有 DLDP 检测的参数时, 可使用该命令快速生效。

✎ 查看 DLDP 状态信息

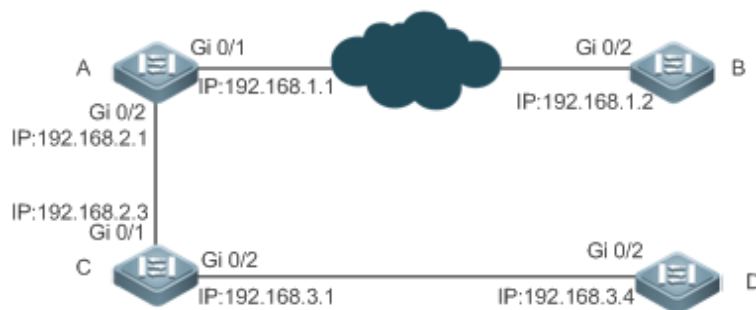
- 【命令格式】 **show dldp statistic [interface interface-name]**
- 【参数说明】 *interface-name* : 查看信息的三层接口
- 【命令模式】 特权模式、全局模式、接口模式
- 【使用指导】 查看接口下的 DLDP 工作状态信息。
- 查看所有 DLDP 检测的统计信息。

配置举例

✎ 在三层网络上开启 DLDP 检测功能, 分别控制 A、B 设备的三层口

【网络环境】

图 3-3



- 【配置方法】
- 在设备 A 上的路由口 (Gi 0/1、Gi 0/2) 开启 DLDP 功能, 检测 A 到 B 和 D 的三层网络的链通性。
 - 若需控制 B 设备的路由口 (Gi 0/2), 则在该接口上开启 DLDP 功能, 并配置为被动模式。

A

```
A#configure terminal
A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#dldp 192.168.1.2
A(config-if-GigabitEthernet 0/1)# exit
A(config)#interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/1)#dldp 192.168.3.4 192.168.2.3
```

```

B
B#configure terminal
B(config)#interface GigabitEthernet 0/2
B(config-if-GigabitEthernet 0/1)#dldp 192.168.1.1
B(config-if-GigabitEthernet 0/1)#dldp passive

```

【检验方法】 ● 检查 A、B 设备的 DLDP 状态信息，检测 DLDP 检测是正常开启并工作。

```

A
A# show dldp
Interface  Type      Ip      Next-hop  Interval  Retry  Resume  State
-----
Gi0/1     Active   192.168.1.2      100      4      3      Up
Gi0/1     Active   192.168.3.4  192.168.2.3  100      4      3      Up

B
B# show dldp
Interface  Type      Ip      Next-hop  Interval  Retry  Resume  State
-----
Gi0/2     Passive  192.168.1.1      100      4      3      Up

```

常见错误

- IPv4 单播路由不可达，误以为 DLDP 检测失效。
- 对端设备不支持 arp/icmp 回应导致 DLDP 功能失效。
- 跨网段检测没有配置下一跳 IP 地址。

3.5 监视与维护

清除各类信息

作用	命令
清除 DLDP 统计信息。	clear dldp [interface <i>interface-name</i> [<i>ip-address</i>]]

查看运行情况

作用	命令
查看 DLDP 运行状态。	show dldp [interface <i>interface-name</i>]
查看 DLDP 的 down/up 统计信息	show dldp statistic

4 PCAP

4.1 概述

PCAP (Packet Capture) 是网络设备中常用的一种维护功能。

类似运行于个人电脑上的抓包软件，PCAP 功能可以将进入网络设备和从网络设备发出的报文抓取下来，保存在文件中，或者直接显示出来。

协议规范

4.2 典型应用

典型应用	场景描述
抓取报文	在日常维护过程中，发现网络内某种报文不通，指定抓包点及抓包方向，输入报文特征，启动抓包，观察报文是否到达设备及被转发走。

4.2.1 抓取报文

应用场景

在日常维护过程中，发现网络内某种报文不通，指定抓包点及抓包方向，输入报文特征，启动抓包，观察报文是否到达设备或从设备发出。

功能部属

用户按照以下步骤操作：

- 创建抓包特征规则，并为规则取名
- 创建抓包点，指定抓包点名称、抓包位置（物理口、控制面）、抓包方向、抓包特征。抓包点仅控制面抓包时需要指定，转发面抓包则不需要。
- 指定保存文件名。
- 启动抓包点抓包
- 等待抓包结束。
- 把文件上传到 PC

- 使用 PC 上的抓包软件打开观察抓到的报文内容。

4.3 功能详解

功能特性

功能特性	作用
控制面抓取报文	抓取指定控制面的收发报文。
转发面抓取报文	抓取指定规则的转发面入口报文。

4.3.1 控制面抓取报文

用户可以定义抓包点，指定抓包位置、方向、匹配的规则信息、抓包数量、保存文件名称等信息，然后启动抓包过程。

工作原理

用户通过定义抓包点来定义抓包的规则，为了同时抓取多种类型报文，允许用户定义多个抓包点，抓包点间以名称进行区别。这些抓包规则包括：

- 1) 抓包的位置，可以选择在某个物理端口、系统控制面作为抓包位置，每个抓包点只能定义一个抓包位置。
- 2) 抓包方向，可以选择出方向、入方向、双向抓包。
- 3) 匹配的 7 元组信息，可以匹配源 MAC、目的 MAC、二层协议类型、源 IP、目的 IP、三层协议类型、TCP/UDP 端口信息。
- 4) 抓包数量，可以选择指定抓包数量或者抓包文件大小。
- 5) 保存文件名称，指定的抓包文件名称，抓取的报文将保存为 pcap 文件格式。配置好规则后，用户通过命令启动抓包，在达到抓包数量或者文件大小或者超时后，抓包将自动停止。用户也可输入命令手动停止抓包。

4.3.2 转发面抓取报文

用户可以指定 ACL ID 和物理接口匹配规则（ACLID 必须指定，物理接口可选）、抓包数量、保存文件名称等信息，然后启动抓包过程。

工作原理

1. 支持指定 ACLID 和物理接口这 2 个匹配规则的抓包，物理接口为可选。
2. 支持多条 ACLID 跟物理接口组件的规则抓包。
3. 抓包方向，支持入口抓包。

4. 无需指定抓包点，也不支持 7 元组匹配信息。
5. 抓包数量，可以选择指定抓包数量或者抓包文件大小。
6. 保存文件名称，指定的抓包文件名称，抓取的报文将保存为 pcap 文件格式。配置好规则后，用户通过命令启动抓包，在达到抓包数量或者文件大小或者超时后，抓包将自动停止。用户也可输入命令手动停止抓包。

4.4 配置详解

配置项	配置建议&相关命令	
控制面抓取报文	packet capture rule rule-name filter [src-mac smac] [dst-mac dmac][etype type ip arp] [ipv4-sip sip sip-mask] [ipv4-dip dip dip-mask] [ipv6-sip sipv6 sipv6-prefix] [ipv6_dip dipv6 dipv6-prefix] [v6_protocol protocol tcp udp] [ipv6_sport sport] [ipv6_dport dport] [v4_protocol protocol tcp udp] [ipv4_sport sport] [ipv4_dport dport]	定义抓包匹配规则。
	packet capture point capture-point-name rule rule-name location{interfaceinterface-name control-plane} {in out both}	创建抓包点，指定抓包位置、匹配规则、抓包方向
	packet capture file filename [buffer-size buf-size] [packet-numpkt-num] [timeouttimeout]	指定保存的文件名
	packet capture {start stop}	开始/停止抓包
转发面抓取报文	packet capture rule rule-name filter acl aclid / aclname [interfaceinterface-name]	定义抓包匹配规则。
	packet capture file filename [buffer-size buf-size][packet-numpkt-num] [timeouttimeout]	指定保存的文件名
	packet capture {start stop}	开始/停止抓包

4.4.1 控制面抓取报文

配置效果

- 定义抓包匹配规则；
- 创建抓包点；

- 指定保存的文件名
- 开始抓包。
- 停止抓包

注意事项

无

配置方法

📌 定义抓包匹配规则

- 必选配置。用户用此命令定义抓包规则。

【命令格式】 **packet capture rule rule-name filter [src-mac smac] [dst-mac dmac] [etype type | ip | arp] [ipv4_sip sip sip-mask] [ipv4_dip dip dip-mask] [ipv6_sip sipv6 sipv6-prefix] [ipv6_dip dipv6 dipv6-prefix][v6_protocol protocol | tcp | udp] [ipv6_sport sport] [dst-port dport] [v4_protocol protocol | tcp | udp] [ipv4_sport sport] [dst-port dport]**

【参数说明】 rule-name：匹配规则名称
 smac：源 MAC
 dmac：目的 MAC
 type | ip | arp：二层协议类型
 sip：源 IP
 sip-mask：源 IP 掩码
 dip：目的 IP
 dip-mask：目的 IP 掩码
 sipv6：源 IPv6 地址
 sipv6-prefix：源 IPv6 前缀
 dipv6：目的 IPv6 地址
 dipv6-prefix：目的 IPv6 前缀
 Protocol | tcp | udp：三层协议类型
 sport：tcp/udp 协议源端口
 dport：tcp/udp 协议目的端口

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 1、用户可以定义多个不同的抓包规则，以规则名称区分不同规则。定义规则以后，规则需要被抓包点引用才会实际生效。
 2、删除抓包规则之前，需要删除所有引用该规则的抓包点。

📌 创建抓包点

- 必选配置。本命令用于创建抓包点。

- 【命令格式】 **packet capture point** *capture-point-name* **rule** *rule-name* **location**{*interface**interface-name* | **control-plane**} {**in** | **out** | **both**}
- 【参数说明】
capture-point-name : 抓包点名称
rule-name : 匹配的规则名称, 由 **packet capture rule** 命令定义。
interface-name : 抓包的端口名称
control-plane : 控制面抓包
in | out | both : 抓包方向, 入口、出口、或者双向。
- 【缺省配置】 -
- 【命令模式】 特权模式
- 【使用指导】
 1、根据需要, 用户可以在同一位置定义多个不同的抓包点, 匹配不同的抓包规则或者报文方向。多个抓包点可以同时工作, 互不影响。
 2、抓包过程中, 如果修改抓包点定义, 不会立即生效, 将在下次启动抓包时生效。

📌 指定保存文件名

- 可选配置。本命令用于指定保存文件名。

- 【命令格式】 **packet capture file** *filename* [**buffer-size** *buf-size*][**packet-num***pkt-num*][**timeout***timeout*]
- 【参数说明】
filename : 保存的文件名
buf-size : 缓冲区大小。不选择默认按照 2M 大小存放, 文件达到指定大小自动停止抓包。目前最大支持 200M。
pkt-num : 抓包数量。抓包达到指定数量后, 自动停止。不选择默认持续抓取 1024 报文。
timeout : 抓包超时, 超过该时间自动停止抓包。不选择默认抓包时间 10 分钟。最大支持连续 120 分钟抓包。
- 【缺省配置】 -
- 【命令模式】 特权模式
- 【使用指导】 1、设置保存文件名后, 下次启动抓包后生效。

📌 开始/停止抓包

- 必选配置。输入此命令开始或停止抓包。

- 【命令格式】 **packet capture {start | stop}**
- 【参数说明】
start : 开始抓包。
stop : 停止抓包。
- 【缺省配置】 -
- 【命令模式】 特权模式
- 【使用指导】
 1、开始抓包以后, 如果不输入停止抓包命令, 抓包数量满足后, 抓包点将自动停止抓包。如果抓包的停止条件尚未满足, 输入停止抓包命令后, 立即停止抓包。
 2、输入开始抓包后, 所有抓包点同时开始抓包。

检验方法

使用 **show packet capture status** 命令查看抓包信息。

【命令格式】 **show packet capture status**

【参数说明】 -

【命令模式】 特权用户模式

【使用指导】 执行本命令可以查看抓包的状态信息。

【命令展示】 查看抓包的状态信息

```
Ruijie#show packet capture status
```

```
Capture rules:
```

```
Capture rules tcp:
```

```
etype: 0x0800
```

```
source MAC: 2222.2222.2222
```

```
destination MAC: 1111.1111.1111
```

```
protocol: 0x6
```

```
source IP: 10.10.10.3
```

```
destination IP: 10.10.10.10
```

```
source port: 5
```

```
destination port: 10
```

```
Capture points:
```

```
Capture point controlplane:
```

```
Capture rules: tcp
```

```
location: control-plane
```

```
direction: all
```

```
Capture file:
```

```
Filename: /tmp/tcp.pcap
```

```
Buffer size: 2(MB)
```

```
Capture Statistic:
```

```
Status: stop
```

```
Stop reason: Normal
```

```
Start time: 2017-5-20 9:24:19
```

```
End time: 2017-5-20 9:28:19
```

```
Timeout: 10(minutes)
```

```
Packets limit: 1024
```

```
Packet capture cnts:10  
Ruijie#
```

配置举例

📄 抓取报文

- 【网络环境】 ● 用户环境，发现设备端口 0/1 下的设备某应用 TCP 连接不上，需要抓取该端口 TCP 报文进行分析。
- 【配置方法】 ● 使用抓包命令将 TCP 报文保存在 tcp.pcap 文件中，上传到 PC 查看抓取到的内容。

```
Ruijie# packet capture rule tcp filter etype ip v4_protocol tcp  
Ruijie# packet capture point tcppoint rule tcp location interface gi0/1 both  
Ruijie# packet capture file usb0:tcp.pcap packet-num 1500  
Ruijie# packet capture start
```

- 【检验方法】 ● 输入 **show packet capture status** 命令，发现已经开始抓包。

```
Ruijie#show packet capture status
```

Capture rules:

Capture rules tcp:

etype: 0x0800

protocol: 0x6

Capture points:

Capture point tcppoint:

Capture rules: tcp

location: Gi0/1

direction: all

Capture file:

Filename: /mnt/usb0/tcp.pcap

Buffer size: 2(MB)

Capture Statistic:

Status: running

Timeout: 10(minutes)

Packets limit: 1500

Packet capture cnts:10

常见错误

4.4.2 转发面抓取报文

配置效果

- 定义抓包匹配规则；
- 指定保存的文件名
- 开始抓包。
- 停止抓包

注意事项

无

配置方法

📌 定义抓包匹配规则

- 必选配置。用户用此命令定义抓包规则。

【命令格式】 **packet capture rule** *rule-name* **filter acl** *aclid* [**interface** *interface-name*]

【参数说明】 *rule-name*：匹配规则名称
aclid：转发面匹配的 aclid
interface-name：转发面匹配的接口

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 1、用户可以定义多个不同的抓包规则，以规则名称区分不同规则。

📌 指定保存文件名

- 可选配置。本命令用于指定保存文件名。

【命令格式】 **packet capture file** *filename* [**buffer-size** *buf-size*][**packet-num** *pkt-num*][**timeout** *timeout*]

【参数说明】 *filename*：保存的文件名
buf-size：缓冲区大小。不选择默认按照 2M 大小存放，文件达到指定大小自动停止抓包。目前最大支持 200M。
pkt-num：抓包数量。抓包达到指定数量后，自动停止。不选择默认持续抓取 1024 报文。
timeout：抓包超时，超过该时间自动停止抓包。不选择默认抓包时间 10 分钟。最大支持连续 120 分钟抓包。

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 1、设置保存文件名后，下次启动抓包后生效。

开始/停止抓包

- 必选配置。输入此命令开始或停止抓包。

【命令格式】 **packet capture {start | stop}**

【参数说明】 **start**：开始抓包。

stop：停止抓包。

【缺省配置】 -

【命令模式】 特权模式

【使用指导】 开始抓包以后，如果不输入停止抓包命令，抓包数量满足后，将自动停止抓包。如果抓包的停止条件尚未满足，输入停止抓包命令后，立即停止抓包。

检验方法

使用 **show packet capture status** 命令查看抓包信息。

【命令格式】 **show packet capture status**

【参数说明】 -

【命令模式】 特权用户模式

【使用指导】 执行本命令可以查看抓包的状态信息。

【命令展示】 查看抓包的状态信息

```
Ruijie#show packet capture status
```

```
Capture rules:
```

```
Capture rules rule1:
```

```
acl_id: 1
```

```
Capture file:
```

```
Filename: /tmp/vsd/0/test.pcap
```

```
Buffer size: 2(MB)
```

```
Capture Statistic:
```

```
Status: stopped
```

```
Stopped reason: Normal
```

```
Timeout: 10(minutes)
```

```
Packets limit: 1024  
Write file packet count: 0  
Ruijie#
```

配置举例

📄 抓取报文

- 【网络环境】
- 用户环境，发现设备端口 0/1 下的某流量异常，不确定流量是否到设备，需要抓取该端口转发报文进行确认
- 【配置方法】
- 使用抓包命令将匹配 ACL 规则且指定端口 0/1 下面的流量，保存在 tcp.pcap 文件中，上传到 PC 查看抓取到的内容。

```
Ruijie(config)#access-list 100 permit tcp host 1.1.1.1 any  
Ruijie(config)#exit  
Ruijie#packet capture rule rule1 filter acl 100 interface tenGigabitEthernet 0/1  
Ruijie# packet capture file usb0:tcp.pcap packet-num 1500  
Ruijie# packet capture start
```

- 【检验方法】
- 输入 **show packet capture status** 命令，发现已经开始抓包。

```
Ruijie#show packet capture status  
  
Capture rules:  
  
Capture rules rule1:  
    acl_id: 100  
    acl_ifx: TenGigabitEthernet 0/1  
  
Capture file:  
    Filename: /tmp/vsd/0/test.pcap  
    Buffer size: 2(MB)  
  
Capture Statistic:  
    Status: running  
    Start time: 2018-6-4 16:34:55  
    Timeout: 10(minutes)  
    Packets limit: 1024
```

```
Write file packet count: 4
```

常见错误

4.5 监视与维护

查看运行情况

作用	命令
查看抓包信息	show packet capture status

4.6 抓包功能限制说明

1. 不支持 mgmt 口抓包，支持物理口抓包。
2. 不支持 svi 口和 vsl 口抓包。
3. efmplib进程重启或者设备重启，抓包配置会丢失，不支持保存。
4. 不支持非主成员设备接口配置为抓包口，但支持成员口包含非主成员设备接口的聚合口配置为抓包口。
5. 不支持 vsu 配置同步，在主上面配置抓包，主备切换后抓包配置会丢失。
6. show packet capture raw-packet 命令作隐藏命令，内部使用。
7. 控制面/转发面抓包规则一次只能配置一种，两者互斥。

5 VRRP

5.1 概述

VRRP (Virtual Router Redundancy Protocol , 虚拟路由冗余协议) 是一种路由容错协议。

VRRP 设计采用主备模式 , 以保证当主路由设备发生故障时 , 备份路由设备可以在不影响内外数据通信的前提下进行功能切换 , 且不需要再修改内部网络的参数。VRRP 组内多个路由设备都映射为一个虚拟的路由设备。VRRP 保证同时有且只有一个路由设备在代表虚拟路由设备进行包的发送 , 而主机则是把数据包发向该虚拟路由设备 , 这个转发数据包的路由设备被选择成为主路由设备。如果这个主路由设备在某个时候由于某种原因而无法工作的话 , 则处于备份状态的路由设备将被选择来代替原来的主路由设备。VRRP 使得局域网内的主机看上去只使用了一个路由设备 , 并且即使在它当前所使用的首跳路由设备失败的情况下仍能够保持路由的连通性。

- VRRP 适用于需要对局域网中设备的路由出口进行冗余备份的场景。

 下文仅介绍 VRRP 的相关内容。

协议规范

- RFC2338 : Virtual Router Redundancy Protocol
- RFC3768 : Virtual Router Redundancy Protocol (VRRP)
- RFC5798 : Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

5.2 典型应用

典型应用	场景描述
路由冗余	局域网中路由设备配置单备份组实现简单的路由冗余。
负载均衡	局域网中路由设备配置多备份组实现流量的负载均衡。

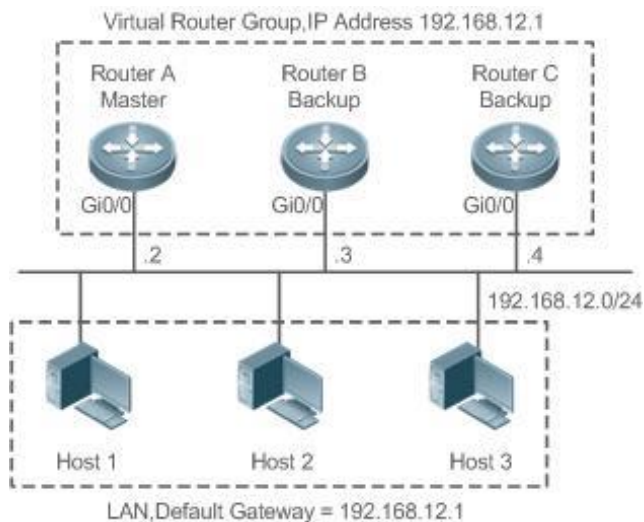
5.2.1 路由冗余

应用场景

在连接局域网的路由设备上配置单备份组 , 局域网中的主机以该备份组的虚拟 IP 作为默认网关。

- 局域网内主机 1、2 以及 3 发往其它网络的数据包将由选举出来的主路由设备(在图 4-1 中是路由设备 A)进行路由转发。
- 一旦主路由设备 A 失效 , 将在路由设备 B 与 C 之间选举出新的主路由设备来承担虚拟路由设备的路由转发功能 , 由此实现了简单路由冗余。

图 4-1



功能部署

- 路由设备 A、B 以及 C 均使用以太网口与局域网连接。
- 路由设备 A、B 以及 C 在与局域网连接的以太网接口上设置了 VRRP。
- 路由设备 A、B 以及 C 在与局域网连接的以太网接口上处于同一个 VRRP 组并且该 VRRP 组的虚拟 IP 地址为 192.168.12.1。
- 局域网内的主机 1、2 以及 3 以虚拟路由设备的 IP 地址 192.168.12.1 作为网关。

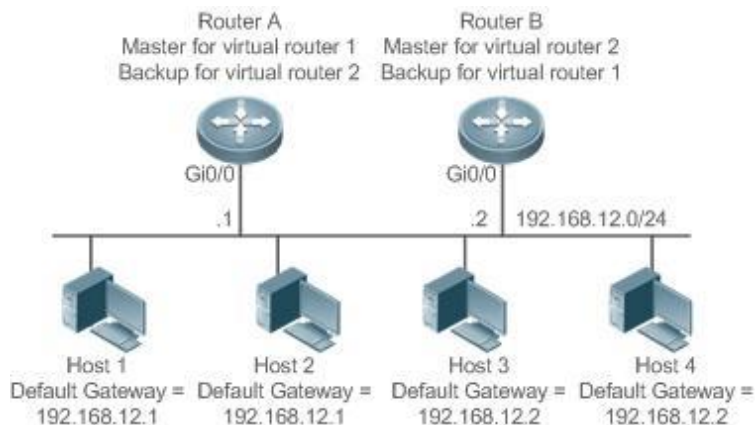
5.2.2 负载均衡

应用场景

在连接局域网的路由设备上配置多个备份组，局域网中的主机分别以各备份组的虚拟 IP 作为网关，路由设备互相作为主路由设备和备份路由设备。

- 以虚拟路由器 1 的虚拟 IP 地址作为默认网关的主机 1 和 2 发往其它网络的数据包将由主路由设备(在图 4-2 中是路由设备 A)进行路由转发。
- 以虚拟路由器 2 的虚拟 IP 地址作为默认网关的主机 3 和 4 发往其它网络的数据包将由主路由设备(在图 4-2 中是路由设备 B)进行路由转发。
- 路由设备 A 和 B 实现了路由冗余，并同时分担了来自局域网的流量即实现了负载均衡。

图 4-2



功能部属

- 路由设备 A 和 B 均使用以太网口与局域网连接。
- 路由设备 A 和 B 在与局域网连接的以太网接口上设置了两个虚拟路由设备。
- 设置了两个虚拟路由设备。对于虚拟路由设备 1，路由设备 A 使用以太网口 Gi0/0 的 IP 地址 192.168.12.1 作为虚拟路由设备的 IP 地址，这样路由设备 A 就成为主路由设备，而路由设备 B 成为备份路由设备。
- 对于虚拟路由设备 2，路由设备 B 使用以太网口 Gi0/0 的 IP 地址 192.168.12.2 作为虚拟路由设备的 IP 地址，这样路由设备 B 就成为主路由设备，而路由设备 A 成为备份路由设备。
- 在局域网内，主机 1 和主机 2 使用虚拟路由设备 1 的 IP 地址 192.168.12.1 作为默认网关，主机 3 和主机 4 使用虚拟路由设备 2 的 IP 地址 192.168.12.2 作为默认网关。

5.3 功能详解

基本概念

虚拟路由器

又称 VRRP 备份组，被当作一个共享局域网内主机的缺省网关。包括一个虚拟路由器标识符和一组虚拟 IP 地址。

虚拟 IP 地址

虚拟路由器的 IP 地址，一个虚拟路由器可以配置有一个或多个虚拟 IP 地址。

IP 地址拥有者

如果 VRRP 组的虚拟 IP 地址与所在以太网接口上的 IP 一致，那么就认为该 VRRP 组占用(Own)了以太网接口实际 IP 地址，认为该设备是 IP 地址拥有者，此时该 VRRP 组的优先级为 255，如果对应的以太网接口可用，那么该 VRRP 组将自动处于 Master 状态。IP 地址拥有者接收处理目的 IP 地址为虚拟路由器的 IP 地址的报文。

虚拟 MAC 地址

VRRP 的虚拟 MAC 地址就是协议规定的、由国际标准统一分配的：00-00-5E-00-01-{VRID}，其中前五个字节固定，最后一个字节是备份组的组号。当虚拟路由器回应 ARP 请求时，使用虚拟 MAC 地址，而不是接口的实 MAC 地址。

Master 路由器

在一个 VRRP 备份组中，只有 Master 路由器负责 ARP 响应和转发 IP 数据包。如果该设备是 IP 地址拥有者，通常它将成为 Master 路由器。

Backup 路由器

在一个 VRRP 备份组中，Backup 路由器不承担 ARP 响应和转发 IP 数据包的任务，只负责监听 Master 路由器的状态。当 Master 路由器出现故障时，它们将有机会通过选举成为新的 Master 路由器。

抢占模式

如果 VRRP 组工作在抢占模式，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主路由设备。

功能特性

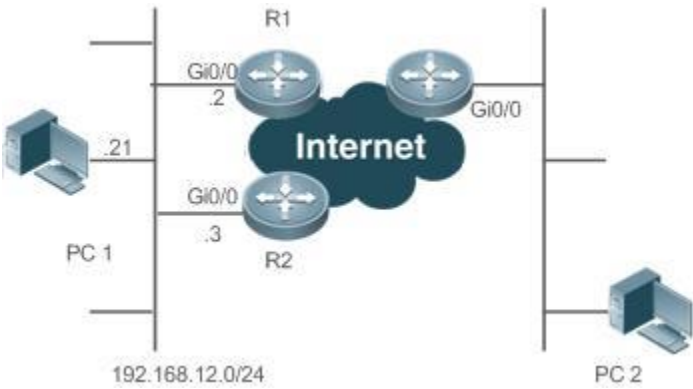
功能特性	作用
VRRP	通过启动 VRRP 功能，VRRP 对共享多存取访问介质（如以太网）上终端设备的默认网关进行冗余备份，从而在其中一台路由设备宕机时，备份路由设备及时接管转发工作，向用户提供透明的切换，提高了网络服务质量。

5.3.1 VRRP

通过启动 VRRP 功能，当主路由设备发生故障时，备份路由设备可以在不影响内外数据通信的前提下进行功能切换，且不需要再修改内部网络的参数。

工作原理

图 4-3 VRRP 工作原理



VRRP 的运作方式

RFC 2338、RFC3768、RFC5798 中定义了 VRRP 类型的 IP 报文格式及其运作机制，VRRP 报文是一类指定目的地址的组播报文，该报文由主路由设备定时发出来标志其运行正常同时该报文也用于选举主路由设备。VRRP 允许为 IP 局域网承担路由转发功能的路由设备失效后，局域网中另外一个路由设备将自动接管失效的路由设备，从而实现 IP 路由的热备份与容错，同时也保证了局域网内主机通讯的连续性和可靠性。一个 VRRP 应用组通过多台路由设备来实现冗余，但是任何时候只有一台路由设备作为主路由设备来承担路由转发功能，其他的为备份路由设备，VRRP 应用组中不同路由设备间的切换对局域网内的主机则是完全透明的。

📌 路由设备的切换规则

RFC 规定了路由设备的切换规则：

- VRRP 协议采用简单竞选的方法选择主路由设备。首先比较同一个 VRRP 组内的各台路由设备对应接口上设置的 VRRP 优先级的大小，优先级最大的为主路由设备，它的状态变为 Master。若路由设备的优先级相同，则比较对应网络接口的主 IP 地址大小，主 IP 地址大的就成为主路由设备，由它提供实际的路由转发服务。
- 主路由设备选出后，其它路由设备作为备份路由设备(状态变为 Backup)，并通过主路由设备定时发出的 VRRP 报文监测主路由设备的状态。当正常工作时，主路由设备会每隔一段时间发送一个 VRRP 组播报文，称为通告报文，以通知备份路由设备：主路由设备处于正常工作状态。如果组内的备份路由设备在设定的时间段没有接收到来自主路由设备的报文，则将自己状态转为 Master。当组内有多台状态为 Master 路由设备时，重复 1) 的竞选过程。通过这样一个过程就会将优先级最大的路由设备选成新的主路由设备，从而实现 VRRP 的备份功能。

一旦在一个 VRRP 备份组选举出它的主路由设备，局域网内的主机将通过主路由设备进行路由转发。

📌 通讯过程

通讯过程可以由上图来说明。在图中，路由设备 R1 和 R2 均通过以太网口 Gi0/0 与局域网 192.168.12.0/24 连接，路由设备 R1 与 R2 的 Gi 0/0 接口上设置了 VRRP，局域网内的主机都以该 VRRP 组的虚拟路由设备 IP 地址作为默认网关。对于局域网内的主机而言，它们只能感受到由 VRRP 组的虚拟路由设备，而实际承担路由转发功能的 VRRP 组的主路由设备对它们而言则是透明的。譬如，局域网内的主机 PC 1 如果要与其它网络内的主机 PC 2 通讯，PC 1 会以虚拟路由设备为默认网关来发送通向 PC 2 的网络数据包，VRRP 组中的主路由设备在接收到该数据包后会将该数据包转发给 PC 2。在这个通讯过程中，PC 1 只能感受到虚拟路由设备而不知道扮演虚拟路由设备角色的主路由设备究竟是 R1 还是 R2，在这个 VRRP 组中的主路由设备是在 R1 与 R2 之间选举产生的，一旦主路由设备失效，那么另外一台将自动成为主路由设备。

相关配置

📌 配置启动 VRRP 功能

缺省情况下，接口上 VRRP 功能关闭。

在接口模式下，使用 `vrrp group ip ipaddress [secondary]` 或者 `vrrp group ipv6 ipv6-address` 命令设置备份组号和虚拟 IP 地址来启用 VRRP 功能。

必须在接口上配置启动 VRRP 功能，才能参与 VRRP 协议工作。

📌 设置 IPv4 VRRP 的验证字符串

缺省状态下，VRRP 处于无验证模式。

使用 **vrrp group authentication string** 命令可以设置 IPv4 VRRP 的验证字符串的同时也设定该 VRRP 组处于明文密码验证模式。在明文密码验证模式下，明文密码长度不能超过 8 个字节。

VRRP 备份组成员必须处于相同的验证模式下才可能正常通讯。明文密码验证模式下，在同一个 VRRP 组中的路由设备必须设置相同的验证口令。明文验证口令不能保证安全性，它只是用来防止/提示错误的 VRRP 配置。

📌 设置 VRRP 备份组的通告发送间隔

缺省状态下，系统默认主路由设备的 VRRP 通告发送间隔为 1 秒。

使用 **vrrp [ipv6] group timers advertise { advertise-interval | csec centisecond-interval }** 可以调整 VRRP 备份组的通告发送间隔。

在没有设置 VRRP 定时设备学习功能的时候，同一个 VRRP 备份组要设置相同的 VRRP 通告发送间隔，否则处于备份状态的路由设备将会丢弃接收到的 VRRP 通告。

📌 设置路由设备在 VRRP 备份组中的抢占模式

缺省情况下，VRRP 组工作在抢占模式下。

使用 **vrrp [ipv6] group preempt [delay seconds]** 设置 VRRP 组工作在抢占模式下，可选参数 **delay seconds** 缺省为 0 秒。

如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主路由设备。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主路由设备。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主路由设备。可选参数 Delay Seconds 定义了处于备份状态的 VRRP 路由设备准备宣告自己拥有 Master 身份之前的延迟。

📌 设置 IPv6 VRRP 虚拟路由器的 Accept_Mode 模式

缺省状态下，IPv6 VRRP 组没有配置 Accept_Mode 模式。

使用 **vrrp ipv6 group accept_mode** 命令可以设置 IPv6 VRRP 组处于 Accept_Mode 模式。

如果配置了 Accept_Mode 模式，则表示 Master 状态的 IPv6 VRRP 虚拟路由器需接收处理任何目的 IP 为虚拟路由器的 IP 地址的报文，如果未配置 Accept_Mode 模式，则表示 Master 状态的 IPv6 VRRP 虚拟路由器需丢弃处理任何目的 IP 为虚拟路由器的 IP 地址的报文，但不丢弃 NA 和 NS 报文。另外，Owner 状态的 IPv6 VRRP Master 状态虚拟路由器，不管有没有配置 Accept_Mode 模式，都会接收处理任何目的 IP 为虚拟路由器的 IP 地址的报文。

📌 设置路由设备在 VRRP 备份组中的优先级

缺省状态下，VRRP 组默认其优先级为 100。

使用 **vrrp [ipv6] group priority level** 可以调整 VRRP 组的优先级。

工作在抢占模式下具有最高优先级并且已获得虚拟 IP 地址的路由设备将成为该备份组的活动的(或主)路由设备，同一个备份组中低于该路由设备优先级的其它路由设备将成为备份的(或监听的)路由设备。

📌 设置 VRRP 备份组监视的接口

缺省状态下，没有设置 VRRP 备份组监视的接口。

使用 **vrrp group track { interface-type interface-number | bfd interface-type interface-number ipv4-address } [priority]** 或者 **vrrp ipv6 group track interface-type interface-number [priority]** 命令可以设置监视接口。

配置了 VRRP 备份组监视的接口后，系统将根据所监视接口的状态动态地调整本路由设备的优先级。一旦所监视的接口状态变为不可用就按照设置的数值减少本路由设备在 VRRP 备份组中的优先级，而此时同一个备份组中接口状态更稳定并且优先级更高的其它路由设备就可以成为该 VRRP 备份组的活动的(或主)路由设备。

📌 设置 VRRP 备份组监视的 IP/IPv6 地址

缺省状态下，没有设置 VRRP 备份组监视的 IP 地址。

使用 **vrrp group track ip-address [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]** 或者 **vrrp ipv6 group track { ipv6-global-address | { ipv6-linklocal-address interface-type interface-number } } [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]** 命令可以设置监视 IP/IPv6 地址。

配置了 VRRP 备份组监视的 IP 地址后，系统将根据所监视的地址是否可达来动态地调整本设备的优先级。一旦所监视的 IP 地址变为不可达，即 ping 不通，就按照设置的数值减少本设备在 VRRP 备份组中的优先级，而此时同一个备份组中优先级更高的其它路由设备就可以成为该 VRRP 备份组的活动的(或主)路由设备。

📌 设置 VRRP 通告定时设备学习功能

缺省状态下，系统没有为 VRRP 组设置定时设备学习功能。

使用 **vrrp [ipv6] group timers learn** 命令设置 VRRP 组启用定时设备学习功能。

一旦启用了定时设备学习功能，如果当前路由设备是 VRRP 备份路由设备，在设置了定时设备学习功能后，它会从主路由设备的 VRRP 通告中学习 VRRP 通告发送间隔，并由此来计算 Master 路由设备失效判断间隔，而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现 Backup 路由设备与 Master 路由设备的 VRRP 通告发送定时设备同步。

📌 设置路由设备在 VRRP 备份组的描述字符串

缺省状态下，系统没有设置 VRRP 组描述符。

使用 **vrrp [ipv6] group description text** 命令可以设置 VRRP 组描述符。

为 VRRP 组设置描述符，可以便于区分 VRRP 组。当设置的描述符超过 80 个字节，提示配置错误。

📌 设置 VRRP 备份组延迟启动

缺省状态下，系统没有设置 VRRP 备份组延迟启动。

使用 **vrrp delay { minimum min-seconds | reload reload-seconds }** 可以设置 VRRP 备份组延迟启动，两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。

本命令配置某个接口上 VRRP 备份组的延迟启动时间；延迟时间有两种：系统启动时的延迟时间，与接口状态变为活动时的延迟时间，可以分别配置，也可同时配置。配置本命令后，当系统启动，或者接口状态变为活动时，该接口上的 VRRP 备份组不会立即启动；而是等待相应的延迟时间后再启动 VRRP 备份组，保证非抢占配置不会失效。如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文，则会取消延迟，立即启动 VRRP 协议。

配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

📌 设置 IPv4 VRRP 的 VRRP 报文发送标准

缺省状态下，IPv4 VRRP 的 VRRP 报文使用 VRRPv2 标准。

使用 **vrrp group version { 2 | 3 }** 命令设置 IPv4 VRRP 的 VRRP 报文发送标准。

参数配置为 2，则 IPv4 VRRP 的 VRRP 报文使用 VRRPv2 标准；参数配置为 3，则 IPv4 VRRP 的 VRRP 报文使用 VRRPv3 标准。

📌 设置 Super VLAN 中 IPv4 VRRP 报文的发送方式

缺省状态下，只往 Super VLAN 的第一个 UP 的 Sub VLAN 发送。

使用 **vrrp detection-vlan first-subvlan** 命令可以设置 Super VLAN 中 IPv4 VRRP 报文只往 Super VLAN 的第一个 UP 的 Sub VLAN 发送；使用 **vrrp detection-vlan subvlan-id** 命令可以设置 Super VLAN 中 IPv4 VRRP 报文向指定的 Sub VLAN 发送。Super VLAN 接口如果同时启用 VRRP 和 VRRP PLUS 功能，则 VRRP 协议报文往 Super VLAN 接口所有 UP 的 Sub VLAN 口发送。

设置 IPv4 VRRP 协议报文只往 Super VLAN 中的第一个 UP 的、或者往指定的 Sub VLAN 发送，可以减少 VRRP 协议报文数量，避免影响设备的性能和占用网络带宽。但是要求组成 IPv4 VRRP 备份组的设备必须能够在该 Super VLAN 的第一个 UP 的、或者指定的 Sub VLAN 互通。

📌 设置 IPv4 VRRP 组和 BFD 联动

缺省状态下，接口上没有指定 IPv4 VRRP 组和 BFD 联动。

使用 **vrrp group bfd ip-address** 命令可以设置 IPv4 VRRP 组和 BFD 联动。

对于备份路由器，执行这条命令，使该 IPv4 VRRP 组和 BFD 联动，并不关心配置的 IP 地址。而对于主路由器，由于不知道备份路由器接口的主 IP 地址，所以只能由管理员指定备份路由器的 IP 地址。

配置时首先确保配置的接口配置了 IP 和 BFD 会话参数。

通过指定 IPv4 VRRP 组和 BFD 联动，当主路由器出现故障时，可以把备份路由器检出主路由器故障的时间缩短到 1 秒钟以内。

📌 设置全局 IPv4 VRRP BFD

缺省状态下，VRRP 不采用全局 IPv4 VRRP BFD 方式检测 master 是否处于活动状态。



使用 **vrrp bfd interface-type interface-number ip-address** 命令可以设置全局 VRRP BFD。


配置全局 IPv4 VRRP BFD，使得多个 IPv4 VRRP 备份组可以共用该全局 BFD 会话，实现快速检测、主备快速切换。

配置时首先确保配置的接口配置了 IP 和 BFD 会话参数。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置 IPv4 VRRP	⚠️ 必须配置。用于启动 IPV4 VRRP 备份功能。	
	vrrp group ip ipaddress [secondary]	启用 IPv4 VRRP
	⚠️ 可选配置。用于配置 IPV4 VRRP 备份组参数。	
	vrrp group authentication string	设置 IPv4 VRRP 的验证字符串

	vrrp group timers advertise { advertise-interval csec centisecond-interval }	设置 IPv4 VRRP 主路由设备 VRRP 通告间隔
	vrrp group preempt [delay seconds]	设置 IPv4 VRRP 备份组处于抢占模式
	vrrp group priority level	设置 IPv4 VRRP 备份组的优先级
	vrrp group track { interface-type interface-number bfd interface-type interface-number ipv4-address } [priority]	设置 IPv4 VRRP 备份组监视的接口
	vrrp group track ip-address [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]	设置 IPv4 VRRP 备份组监视的 IP 地址
	vrrp group timers learn	设置 IPv4 VRRP 定时设备学习功能
	vrrp group description text	设置 IPv4 VRRP 组描述字符串
	vrrp delay { minimum min-seconds reload reload-seconds }	设置接口上 VRRP 备份组延迟启动时间
	vrrp group version { 2 3 }	设置 IPv4 VRRP 的 VRRP 报文标准
	vrrp detection-vlan { first-subvlan subvlan-id }	设置 IPv4 VRRP 协议报文只往 Super VLAN 中的第一个 UP 的、或者往指定的 Sub VLAN 发送
	vrrp group bfd ip-address	设置 IPv4 VRRP 组和 BFD 联动
	vrrp bfd interface-type interface-number ip-address	设置全局 IPv4 VRRP BFD
配置 IPv6 VRRP	 必须配置。用于启动 IPV6 VRRP 备份功能。	
	vrrp group ipv6 ipv6-address	接口启用 IPv6 VRRP
	 可选配置。用于配置 IPV6 VRRP 备份组参数。	
	vrrp ipv6 group timers advertise { advertise-interval csec centisecond-interval }	设置 IPv6 VRRP 主路由设备 VRRP 通告间隔
	vrrp ipv6 group preempt [delay seconds]	设置 IPv6 VRRP 备份组处于抢占模式
	vrrp ipv6 group accept_mode	设置 IPv6 VRRP 备份组的 Accept_Mode 模式
	vrrp ipv6 group priority level	设置 IPv6 VRRP 备份组的优先级
	vrrp ipv6 group track interface-type interface-number [interface-priority]	设置 IPv6 VRRP 备份组监视的接口
	vrrp ipv6 group track { ipv6-global-address { ipv6-linklocal-address interface-type interface-number } } [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]	设置 IPv6 VRRP 备份组监视的 IP 地址

	vrrp ipv6 group timers learn	设置 IPv6 VRRP 定时设备学习功能
	vrrp ipv6 group description text	设置者 IPv6 VRRP 组描述字符串
	vrrp delay { minimum min-seconds reload reload-seconds }	设置接口上 VRRP 备份组延迟启动时间
配置 VRRP+MSTP	 VRRP 的基本配置跟 IPv4VRRP 配置一样。	

5.4.1 配置 IPv4 VRRP

配置效果

- 配置单备份组时，通过设置备份组号和虚拟 IP 地址，可以在指定的局域网段上添加一个备份组，从而启动对应接口的 VRRP 单备份功能。
- 配置多备份组时，在同一个以太网接口上配置多个 VRRP 备份组，可以实现负载均衡同时通过互相备份来提供更稳定可靠的网络服务。
- 通过设置监视接口，动态的调整备份组的优先级，实现动态故障监测，实现备份组的状态切换。

注意事项

- 同一个 VRRP 备份组内路由设备上 VRRP 需要配置相同的虚拟 IPv4 地址。
- 实现 IPv4 VRRP 多备份组相互备份，需要通过在接口上配置多个相同的 IPv4 VRRP 备份组，且通过配置不同优先级等形式形成互为主备关系，从而实现 IPv4 VRRP 多备份组功能。
- 启动 VRRP 需要在三层口上配置。

配置方法

📌 启用 IPv4 VRRP

- 默认接口上没有启用 IPv4 VRRP，如果接口要启用 IPv4 VRRP 备份功能则必须配置。

📌 设置 IPv4 VRRP 的验证字符串

- 默认 VRRP 处于无验证模式，如果需要 VRRP 处于明文密码验证模式则配置。

📌 设置 IPv4 VRRP 主路由设备 VRRP 通告间隔

- 默认 VRRP 的主路由设备 VRRP 通告间隔为 1 秒，如果需要手动设置则配置。

📌 设置 IPv4 VRRP 备份组处于抢占模式

- 默认 VRRP 处于抢占模式，抢占延迟时间缺省为 0 秒。

📌 设置 IPv4 VRRP 备份组的优先级

- 默认 VRRP 组优先级为 100，如果需要手动设置则配置。

📌 设置 IPv4 VRRP 备份组监视的接口

- 默认 IPv4 VRRP 组未配置监视接口，缺省优先级改变值为 10，如果需要通过监视接口来实现故障检测则配置。

📌 设置 IPv4 VRRP 定时设备学习功能

- 默认 VRRP 组未开启定时设备学习功能，如果备份路由设备需要学习主路由设备的 VRRP 通告间隔则配置。

📌 设置 IPv4 VRRP 组描述字符串

- 默认 VRRP 组未配置描述字符串，如果需要便于区分 VRRP 组则配置。

📌 设置接口上 VRRP 备份组延迟启动时间

- 默认 VRRP 组未配置延迟启动时间，如果为了保证非抢占模式不失效则配置。

📌 设置 IPv4 VRRP 的 VRRP 报文标准

- 默认 IPv4 VRRP 使用 VRRPv2 标准，如果需要手动设置则配置。

📌 设置 Super VLAN 中 IPv4 VRRP 报文的发送方式

- 默认 IPv4 VRRP 协议报文只往 Super VLAN 中的第一个 UP 的 Sub VLAN 发送，可以设置往指定的 Sub VLAN 发送。

📌 设置 IPv4 VRRP 组和 BFD 联动

- 默认接口上没有指定 IPv4 VRRP 组和 BFD 联动，如果需要手动设置则配置。

📌 设置全局 IPv4 VRRP BFD

- 默认 VRRP 不采用全局 IPv4 VRRP BFD 方式检测 master 是否处于活动状态，如果需要手动设置则配置。

检验方法

- `show vrrp` 命令显示配置是否生效

相关命令

📌 启用 IPv4 VRRP

【命令格式】 `vrrp group ip ipaddress [secondary]`

【参数说明】 `group`：VRRP 组号，不同产品型号取值范围不同。
`ipaddress`：虚拟设备的 IP 地址。
`secondary`：标明是该虚拟设备的次 IP 地址。

【命令模式】 接口模式

【使用指导】 如果不指定虚拟 IP 地址，路由设备就不会参与 VRRP 备份组。如果不使用 `Secondary` 参数，那么设置的 IP 地址将成为虚拟路由设备的主 IP 地址。

设置 IPv4 VRRP 的验证字符串

【命令格式】 **vrrp group authentication string**

【参数说明】 *group* : VRRP 组号。

string : 用于 VRRP 组验证的字符串(不能超过 8 个字节, 这里的验证口令是明文口令)。

【命令模式】 接口模式

【使用指导】 在同一个 VRRP 组中的设备必须设置相同的验证口令。明文验证口令不能保证安全性, 它只是用来防止/提示错误的 VRRP 配置。

此命令只对 VRRPv2 报文适用, 对于 VRRPv3 不适用。

VRRPv3 (IPv4 VRRP 和 IPv6 VRRP) 已经废除了认证功能, 如果用户在 IPv4 VRRP 选择的是 VRRPv2, 则对 VRRPv2 生效, 如果选择的是 VRRPv3, 则对 VRRPv3 不生效。

设置 IPv4 VRRP 主路由设备 VRRP 通告间隔

【命令格式】 **vrrp group timers advertise { advertise-interval | csec centisecond-interval }**

【参数说明】 *group* : VRRP 组号。

advertise-interval : VRRP 通告发送间隔(以秒为单位)。

csec centisecond-interval : 备份组中 Master 发送 VRRP 报文的时间间隔。整数形式, 取值范围是 50 ~ 99。单位是厘秒。无缺省值。

只对 VRRPv3 生效, 如果 VRRPv2 配置了此命令, 则取默认的主设备的通告发送间隔, 即 1 秒。

【命令模式】 接口模式

【使用指导】 如果当前设备成为 VRRP 组中的主设备, 它将以设定的间隔发送 VRRP 通告来通告自己的 VRRP 状态、优先级以及其它信息。

根据 RFC 标准, 配置了组播报文发送标准为 VRRPv3 的 IPv4 VRRP 组, 其组播报文中最大的报文通告间隔为 40 秒, 所以如果配置的报文通告间隔超过 40 秒, 则取最大的通告间隔 40 秒, 但该通告间隔配置是生效的。

设置 IPv4 VRRP 备份组处于抢占模式

【命令格式】 **vrrp group preempt [delay seconds]**

【参数说明】 *group* : VRRP 组号。

delay seconds : 准备宣告自己拥有 Master 身份之前的延迟。缺省值为 0 秒。

【命令模式】 接口模式

【使用指导】 如果 VRRP 组工作在抢占模式下, 一旦它发现自己的优先级高于当前 Master 的优先级, 它将抢占成为该 VRRP 组的主设备。如果 VRRP 组工作在非抢占模式下, 即便它发现自己的优先级高于当前 Master 的优先级, 它也不会抢占成为该 VRRP 组的主设备。VRRP 组使用以太网接口 IP 地址情况下, 抢占模式是否设置意义不大, 因为此时该 VRRP 组具有最大优先级, 它自动成为该 VRRP 组中的主设备。

设置 IPv4 VRRP 备份组的优先级

【命令格式】 **vrrp group priority level**

【参数说明】 *group* : VRRP 组号。

level : VRRP 组的优先级。

【命令模式】 接口模式

【使用指导】 该命令将手动设置 VRRP 组的优先级。

✎ 设置 IPv4 VRRP 备份组监视的接口

- 【命令格式】 **vrrp group track** {*interface-type interface-number* | **bfd** *interface-type interface-number ipv4-address* } [*priority*]
- 【参数说明】 *group* : VRRP 组号。
interface-type interface-number : 被监视的接口。
bfd *interface-type interface-number ipv4-address* : 通过 BFD 跟踪指定的邻居 IP。
priority : 被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。
- 【命令模式】 接口模式
- 【使用指导】 被监视的接口只允许是三层可路由的逻辑接口(如 Routed Port、SVI、Loopback、Tunnel 等等)。
如果 VRRP 组占用(Own)了以太网接口实际 IP 地址, 此时该 VRRP 组的优先级为 255, 不能配置监视接口。

✎ 设置 IPv4 VRRP 备份组监视的 IP 地址

- 【命令格式】 **vrrp group track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
- 【参数说明】 *group* : VRRP 组号。
ipv4-address : 被监视的 IPv4 地址。
interval *interval-value* : 发送探测报文的时间间隔。单位为秒。如果不设定, 系统缺省值为 3 秒。
timeout *timeout-value* : 发送探测报文后等待应答的超时时间。如果超时时间到了, 没有收到应答, 则认为不可达。单位为秒。如果不设定, 系统缺省值为 1 秒。
retry *retry-value* : 确认不可达的次数, 如果在连续 *retry-value* 次都没有收到应答, 则认为不可达。单位为次数, 如果不设定, 系统缺省值为 3 次。
priority : 被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。
- 【命令模式】 接口模式
- 【使用指导】 如果是监视主机, 对于 IPv4 虚拟路由器, 指定主机的 IPv4 地址。
如果 VRRP 组占用(Own)了以太网接口实际 IP 地址, 此时该 VRRP 组的优先级为 255, 不能配置监视 IP 地址。

✎ 设置 IPv4 VRRP 定时设备学习功能

- 【命令格式】 **vrrp group timers learn**
- 【参数说明】 *group* : VRRP 组号。
- 【命令模式】 接口模式
- 【使用指导】 一旦启用了定时器学习功能, 如果当前设备是 VRRP 备份设备, 在设置了定时器学习功能后, 它会从主设备的 VRRP 通告中学习 VRRP 通告发送间隔, 并由此来计算 Master 设备失效间隔, 而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现与 Master 设备的 VRRP 通告发送定时器同步。

✎ 设置 IPv4 VRRP 组描述字符串

- 【命令格式】 **vrrp group description** *text*
- 【参数说明】 *group* : VRRP 组号。
text : VRRP 组描述符。
- 【命令模式】 接口模式
- 【使用指导】 为 VRRP 组设置描述符, 可以便于区分 VRRP 组。当设置的描述符超过 80 个字节, 提示配置错误。

设置接口上 VRRP 备份组延迟启动时间

【命令格式】 **vrrp delay { minimum min-seconds | reload reload-seconds }**

【参数说明】 **minimum min-seconds** : 接口状态变为活动时的延迟时间。

reload reload-seconds : 系统启动时的延迟时间。

【命令模式】 接口模式

【使用指导】 配置本命令后, 当系统启动, 或者接口状态变为活动时, 该接口上的 VRRP 备份组不会立即启动; 而是等待相应的延迟时间后再启动 VRRP 备份组, 保证非抢占配置不会失效。如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文, 则会取消延迟, 立即启动 VRRP 协议。两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。

配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

设置 IPv4 VRRP 的 VRRP 报文标准

【命令格式】 **vrrp group version { 2 | 3 }**

【参数说明】 **2** : 使用 VRRPv2 报文发送标准。

3 : 使用 VRRPv3 报文发送标准。

【命令模式】 接口模式

【使用指导】 对于 IPv4 VRRP 考虑到 VRRPv2 和 VRRPv3 的兼容性问题, 用户可以根据网络实际环境选择 VRRP 报文的发送标准。VRRPv2 基于 RFC3768, VRRPv3 基于 RFC 5798。

此命令只适用于 IPv4 VRRP。

设置 IPv4 VRRP 协议报文只往 Super VLAN 中的第一个 UP 的 Sub VLAN 发送

【命令格式】 **vrrp detection-vlan {first-subvlan | subvlan-id}**

【参数说明】 **first-subvlan** : 只往 Super VLAN 中的第一个 UP 的 Sub VLAN 发送

subvlan-id : 往指定的 Sub VLAN 发送

【命令模式】 接口模式

【使用指导】 本命令用于配置 Super VLAN 接口中 IPv4 VRRP 协议报文的发送方式。IPv4 VRRP 协议报文在 Super VLAN 中的发送方式包括三种: 只往 Super VLAN 中的第一个 UP 的 Sub VLAN 发送; 往 Super VLAN 中指定的那个 Sub VLAN 发送; 往 Super VLAN 中的所有 Sub VLAN 发送。Super VLAN 接口如果同时启用 VRRP 和 VRRP PLUS 功能, 则 VRRP 协议报文往 Super VLAN 接口所有 UP 的 Sub VLAN 口发送。

本命令在 VLAN 接口上配置, 只对 Super VLAN 口生效。

设置 IPv4 VRRP 组和 BFD 联动

【命令格式】 **vrrp group bfd ip-address**

【参数说明】 **group** : VRRP 组号。

ip-address : 指定的邻居 IP。

【命令模式】 接口模式

【使用指导】 对于备份路由器, 执行这条命令, 使该 IPv4 VRRP 组和 BFD 联动, 并不关心配置的 IP 地址。而对于主路由器, 由于不知道备份路由器接口的主 IP 地址, 所以只能由管理员指定备份路由器的 IP 地址。

如果配置了全局 IPv4 VRRP BFD, 不能配置 IPv4 VRRP 组和 BFD 联动。

配置时首先确保配置的接口配置了 IP 和 BFD 会话参数。

设置全局 IPv4 VRRP BFD

- 【命令格式】
vrrp bfd interface-type interface-number ip-address
- 【参数说明】
interface-type interface-number：配置接口类型和接口编号。
ip-address：指定的邻居 IP。
- 【命令模式】
全局配置模式
- 【使用指导】
如果配置了全局 IPv4 VRRP BFD，会删除所有配置的 IPv4 VRRP 组和 BFD 联动。
配置时首先确保配置的接口配置了 IP 和 BFD 会话参数。
全局 IPv4 VRRP BFD 会话只适用于两台设备组成的 IPv4 VRRP 虚拟路由器。

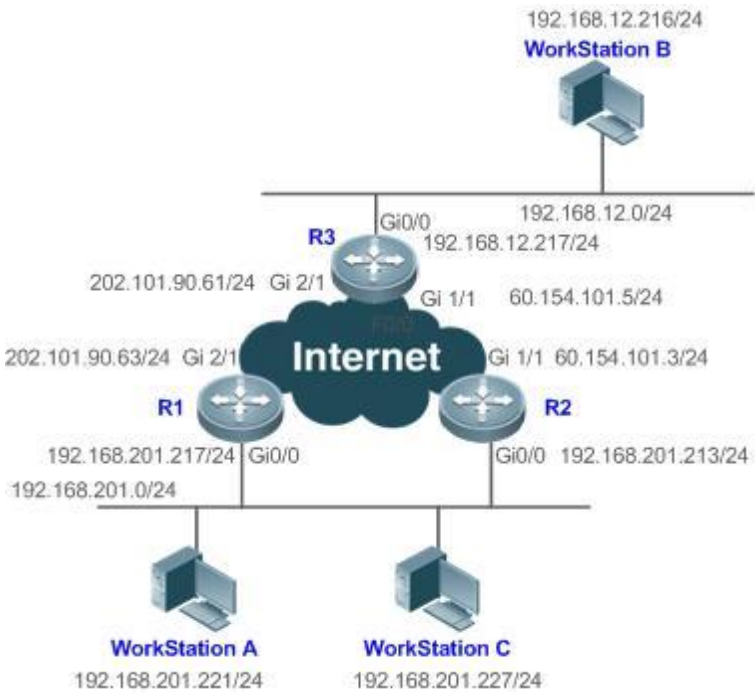
配置举例

以下配置举例，仅介绍与 VRRP 相关的配置。

在 IPv4 的 VRRP 单备份组和监视接口

【网络环境】

图 4-4



- 【配置方法】
- 用户工作站群(192.168.201.0/24)使用路由设备 R1 与 R2 组成的备份组，并将其网关指向该备份组设置的虚拟路由设备的 IP 地址 192.168.201.1，经由虚拟路由设备 192.168.201.1 访问远程用户工作站群(其工作网络为 192.168.12.0/24)。
 - 路由设备 R1 中设置了 VRRP 监视接口 GigabitEthernet 2/1。
 - 路由设备 R3 上没有配置 VRRP 而只是配置了普通路由功能。

R3

```
R3#configure terminal
R3(config)#interface GigabitEthernet 0/0
// "no switchport"命令只有在交换机上才需要
```

```
R3(config-if-GigabitEthernet 0/0)#no switchport
R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0
R3(config-if-GigabitEthernet 0/0)#exit
R3(config)#interface GigabitEthernet 1/1
// "no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 1/1)#no switchport
R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0
R3(config-if-GigabitEthernet 1/1)#exit
R3(config)#interface GigabitEthernet 2/1
// "no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 2/1)#no switchport
R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0
R3(config-if-GigabitEthernet 2/1)#exit
R3(config)#router ospf
R3(config-router)#network 202.101.90.0 0.0.0.255 area 10
R3(config-router)#network 192.168.12.0 0.0.0.255 area 10
R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
```

R1

```
R1#configure terminal
R1(config)#interface GigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0
R1(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120
R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R1(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 2/1 30
R1(config-if-GigabitEthernet 0/0)#exit
R1(config)#interface GigabitEthernet 2/1
R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0
R1(config-if-GigabitEthernet 2/1)#exit
R1(config)#router ospf
R1(config-router)#network 202.101.90.0 0.0.0.255 area 10
R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

R2

```
R2#configure terminal
R2(config)#interface GigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0
R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R2(config-if-GigabitEthernet 0/0)#exit
R2(config)#interface GigabitEthernet 1/1
// "no switchport"命令只有在交换机上才需要
R2(config-if-GigabitEthernet 1/1)#no switchport
R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0
```

```
R2(config-if-GigabitEthernet 1/1)#exit
R2(config)#router ospf
R2(config-router)#network 60.154.101.0 0.0.0.255 area 10
R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

【检验方法】 通过 **show vrrp** 命令显示验证。

- 检查当路由设备 R1 在作为 Master 路由设备状态下发现与广域网的接口 GigabitEthernet 2/1 不可用，路由设备 R1 是否降低自己的 VRRP 备份组优先级 30 而成为 90，这样路由设备 R2 就会成为 Master 路由设备。
- 检查当路由设备 R1 发现自己的与广域网的接口 GigabitEthernet 2/1 恢复可用，是否增加自己的 VRRP 备份组优先级 30 而恢复到 120，这样路由设备 R1 将再次成为主路由设备。

R1

```
R1#show vrrp
GigabitEthernet 0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
  Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
    up  GigabitEthernet 2/1 priority decrement=30
```

R2

```
R2#show vrrp
GigabitEthernet 0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is 192.168.201.217 , priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

常见错误

- 同一个 VRRP 备份组内路由设备上 VRRP 的虚拟 IP 地址不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。

- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致,并且未设置定时设备学习功能导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 协议报文版本不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 对于 VRRPv2,同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式相同均为明文密码模式,但是验证字符串不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。

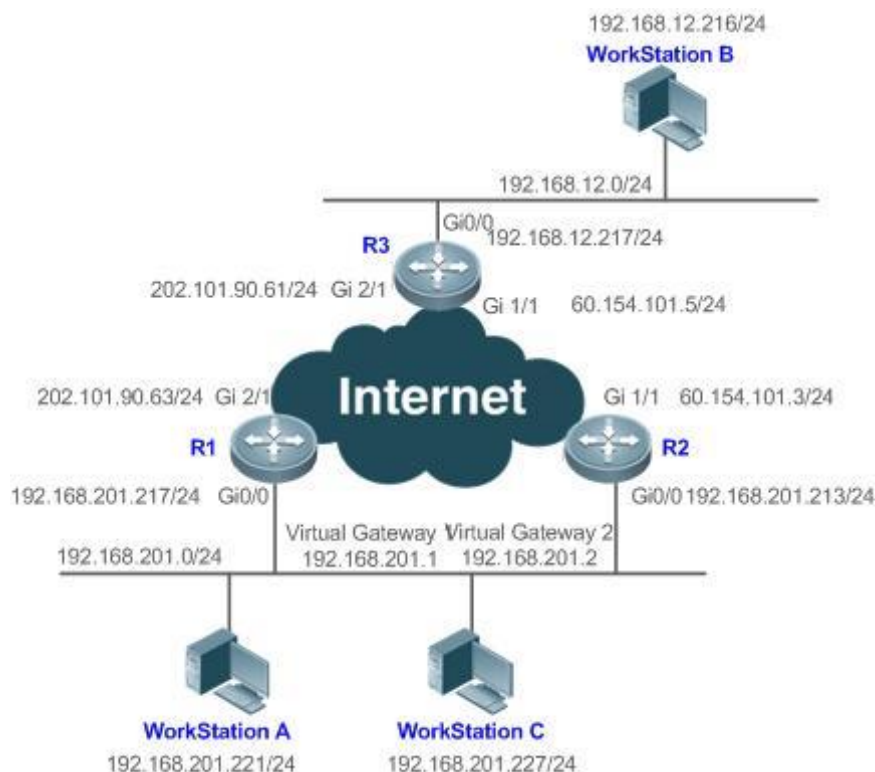
配置举例

i 以下配置举例, 仅介绍与 VRRP 相关的配置。

在 IPv4 的 VRRP 多备份组

【网络环境】

图 4-5



【配置方法】

- 用户工作站群(192.168.201.0/24)使用路由设备 R1 与 R2 组成的备份组,其中部分用户工作站(如 A)将其网关指向备份组 1 的虚拟 IP 地址 192.168.201.1,部分用户工作站(如 C)则将其网关指向备份组 2 的虚拟 IP 地址 192.168.201.2。在所有路由器上启动 IPv4 组播路由功能。
- 路由设备 R1 在备份组 2 中作为主路由设备,在备份组 1 中作为备份路由设备。
- 路由设备 R2 在备份组 2 中作为备份路由设备,在备份组 1 中作为主路由设备。

R3

```
R3#configure terminal
R3(config)#interface GigabitEthernet 0/0
// "no switchport"命令只有在交换机上才需要
```

```
R3(config-if-GigabitEthernet 0/0)#no switchport
R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0
R3(config-if-GigabitEthernet 0/0)#exit
R3(config)#interface GigabitEthernet 1/1
// "no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 1/1)#no switchport
R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0
R3(config-if-GigabitEthernet 1/1)#exit
R3(config)#interface GigabitEthernet 2/1
// "no switchport"命令只有在交换机上才需要
R3(config-if-GigabitEthernet 2/1)#no switchport
R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0
R3(config-if-GigabitEthernet 2/1)#exit
R3(config)#router ospf
R3(config-router)#network 202.101.90.0 0.0.0.255 area 10
R3(config-router)#network 192.168.12.0 0.0.0.255 area 10
R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
```

R1

```
R1#configure terminal
R1(config)#interface GigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0
R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R1(config-if-GigabitEthernet 0/0)#vrrp 2 priority 120
R1(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3
R1(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2
R1(config-if-GigabitEthernet 0/0)#vrrp 2 track GigabitEthernet 2/1 30
R1(config-if-GigabitEthernet 0/0)#exit
R1(config)#interface GigabitEthernet 2/1
R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0
R1(config-if-GigabitEthernet 2/1)#exit
R1(config)#router ospf
R1(config-router)#network 202.101.90.0 0.0.0.255 area 10
R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

R2

```
R2#configure terminal
R2(config)#interface GigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0
R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R2(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120
R2(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2
R2(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3
```

```
R2(config-if-GigabitEthernet 0/0)#exit
R2(config)#interface GigabitEthernet 1/1
R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0
R2(config-if-GigabitEthernet 1/1)#exit
R2(config)#router ospf
R2(config-router)#network 60.154.101.0 0.0.0.255 area 10
R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

【检验方法】 通过 **show vrrp** 命令显示验证。

- 检查当路由设备 R1 在 VRRP 组 2 中作为 Master 路由设备状态下发现与广域网的接口 GigabitEthernet 2/1 不可用，路由设备 R1 是否降低自己的 VRRP 备份组优先级 30 而成为 90，这样 VRRP 组 2 中路由设备 R2 就会成为 Master 路由设备。
- 检查当路由设备 R1 发现自己的与广域网的接口 GigabitEthernet 2/1 恢复可用，是否增加自己的 VRRP 备份组优先级 30 而恢复到 120，这样路由设备 R1 将再次成为 VRRP 组 2 主路由设备。

R1

```
R1#show vrrp
GigabitEthernet 0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is 192.168.201.213 , priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
GigabitEthernet 0/0 - Group 2
  State is Master
  Virtual IP address is 192.168.201.2 configured
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
    up  GigabitEthernet 2/1 priority decrement=30
```

R2

```
R2#show vrrp
GigabitEthernet 0/0 - Group 1
```

```
State is Master
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
    min delay is 0 sec
Priority is 120
Master Router is 192.168.201.213 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.59 sec
GigabitEthernet 0/0 - Group 2
State is Backup
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
    min delay is 0 sec
Priority is 100
Master Router is 192.168.201.217 , priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.82 sec
```

常见错误

- 同一个 VRRP 备份组内路由设备上 VRRP 的虚拟 IP 地址不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致,并且未设置定时设备学习功能导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 协议报文版本不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 对于 VRRPv2, 同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式相同均为明文密码模式,但是验证字符串不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。

5.4.2 配置 IPv6 VRRP

配置效果

- 配置 IPv6 VRRP 单备份组,通过设置备份组号和虚拟 IPv6 地址,可以在指定的局域网段上添加一个备份组,从而启动对应接口的 VRRP 单备份功能。
- 配置 IPv6 VRRP 多备份组,在同一个以太网接口上配置多个 IPv6 VRRP 备份组,可以实现负载均衡同时通过互相备份来提供更稳定可靠的网络服务。

- 通过设置监视接口，动态的调整备份组的优先级，实现动态故障监测，实现备份组的状态切换。

注意事项

- 同一个 VRRP 备份组内路由设备上 VRRP 需要配置相同的虚拟 IPv6 地址。
- 实现 IPv6 VRRP 多备份组相互备份，需要通过在接口上配置多个相同的 IPv6 VRRP 备份组，且通过配置不同优先级等形式形成互为主备关系，从而实现 IPv6 VRRP 多备份组功能。
- 启动 VRRP 需要在三层口上配置。

配置方法

▾ 接口启用 IPv6 VRRP

- 默认接口上没有启用 IPv6 VRRP，如果接口要启用 IPv6 VRRP 备份功能则必须配置。

▾ 设置 IPv6 VRRP 主路由设备 VRRP 通告间隔

- 默认 VRRP 的主路由设备 VRRP 通告间隔为 1 秒，如果需要手动设置则配置。

▾ 设置 IPv6 VRRP 备份组处于抢占模式

- 默认 VRRP 处于抢占模式，抢占延迟时间缺省为 0 秒。

▾ 设置 IPv6 VRRP 备份组的 Accept_Mode 模式

- 默认 IPv6 VRRP 未配置 Accept_Mode 模式，如果要求处于 Master 状态的 IPv6 VRRP 虚拟路由器接收处理目的 IP 地址为虚拟路由器的 IP 地址的报文，则配置 Accept_Mode 模式。

▾ 设置 IPv6 VRRP 备份组的优先级

- 默认 VRRP 组优先级为 100，如果需要手动设置则配置。

▾ 设置 IPv6 VRRP 备份组监视的接口

- 默认 IPv6 VRRP 组未配置监视接口，缺省优先级改变值为 10，如果需要通过监视接口来实现故障检测则配置。

▾ 设置 IPv6 VRRP 备份组监视的 IP 地址

- 默认 IPv6 VRRP 组未配置监视 IP 地址，缺省优先级改变值为 10，如果需要通过监视接 IP 地址来实现故障检测则配置。

▾ 设置 IPv6 VRRP 定时设备学习功能

- 默认 VRRP 组未开启定时设备学习功能，如果备份路由设备需要学习主路由设备的 VRRP 通告间隔则配置。

▾ 设置 IPv6 VRRP 组描述字符串

- 默认 VRRP 组未配置描述字符串，如果需要便于区分 VRRP 组则配置。

▾ 设置接口上 VRRP 备份组延迟启动时间

- 默认 VRRP 组未配置延迟启动时间，如果为了保证非抢占模式不失效则配置。

检验方法

- `show ipv6 vrrp` 命令显示配置是否生效

相关命令

▾ 接口启用 IPv6 VRRP

- 【命令格式】 `vrrp group ipv6 ipv6-address`
- 【参数说明】 `group`：VRRP 组号，不同产品型号取值范围不同。
`ipv6-address`：虚拟设备的 IPv6 地址。
- 【命令模式】 接口模式
- 【使用指导】 IPv6 的 VRRP 与 IPv4 的 VRRP 共用 1 ~ 255 的组号。同一个接口一个相同的 VRRP 组号可以同时适用于 IPv4 VRRP 和 IPv6 VRRP。第一个配置的地址必须是链路本地地址，链路本地地址必须在其它虚拟地址删除后才能删除。

▾ 设置 IPv6 VRRP 主路由设备 VRRP 通告间隔

- 【命令格式】 `vrrp ipv6 group timers advertise { advertise-interval | csec centisecond-interval }`
- 【参数说明】 `group`：VRRP 组号。
`advertise-interval`：VRRP 通告发送间隔(以秒为单位)。
`csec centisecond-interval`：备份组中 Master 发送 VRRP 报文的时间间隔。整数形式，取值范围是 50 ~ 99。单位是厘秒。无缺省值。只对 VRRPv3 生效，如果 VRRPv2 配置了此命令，则取默认的主设备的通告发送间隔，即 1 秒。
- 【命令模式】 接口模式
- 【使用指导】 如果当前设备成为 VRRP 组中的主设备，它将以设定的间隔发送 VRRP 通告来通告自己的 VRRP 状态、优先级以及其它信息。
根据 RFC 标准，组播报文发送标准为 VRRPv3 的 IPv6 VRRP 备份组，其组播报文中最大的报文通告间隔为 40 秒，所以如果配置的报文通告间隔超过 40 秒，则取最大的通告间隔 40 秒，但该通告间隔配置是生效的。

▾ 设置 IPv6 VRRP 备份组处于抢占模式

- 【命令格式】 `vrrp ipv6 group preempt [delay seconds]`
- 【参数说明】 `group`：VRRP 组号。
`delay seconds`：准备宣告自己拥有 Master 身份之前的延迟。缺省值为 0 秒。
- 【命令模式】 接口模式
- 【使用指导】 如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主设备。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主设备。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主设备。

▾ 设置 IPv6 VRRP 备份组的 Accept_Mode 模式

- 【命令格式】 **vrrp ipv6 group accept_mode**
- 【参数说明】 *group* : VRRP 组号。
- 【命令模式】 接口模式
- 【使用指导】 缺省情况下, Master 状态的 IPv6 VRRP 是不允许接收目的 IPv6 地址为虚拟路由器的 IPv6 地址的报文的。但是 NA 和 NS 报文不管是否配置 Accept_Mode 都必须接收。另外, Owner 状态的 IPv6 VRRP Master 状态虚拟路由器, 不管有没有配置 Accept_Mode 模式, 都会接收处理任何目的 IPv6 为虚拟路由器的 IPv6 地址的报文。

📌 设置 IPv6 VRRPVRRP 备份组的优先级

- 【命令格式】 **vrrp ipv6 group priority level**
- 【参数说明】 *group* : VRRP 组号。
level : VRRP 组的优先级。
- 【命令模式】 接口模式
- 【使用指导】 该命令将手动设置 VRRP 组的优先级。

📌 设置 IPv6 VRRP 备份组监视的接口

- 【命令格式】 **vrrp ipv6 group track interface-type interface-number [priority]**
- 【参数说明】 *group* : VRRP 组号。
interface-type interface-number : 被监视的接口。
priority : 被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。
- 【命令模式】 接口模式
- 【使用指导】 被监视的接口只允许是三层可路由的逻辑接口(如 Routed Port、SVI、Loopback、Tunnel 等等)。
如果 VRRP 组占用(Own)了以太网接口实际 IP 地址, 此时该 VRRP 组的优先级为 255, 不能配置监视接口。

📌 设置 IPv6 VRRP 备份组监视的 IP 地址

- 【命令格式】 **vrrp ipv6 group track { ipv6-global-address | ipv6-linklocal-address interface-type interface-number } [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]**
- 【参数说明】 *group* : VRRP 组号。
ipv6-global-address : IPv6 全球单播地址。
ipv6-linklocal-address : IPv6 链路本地地址。
interface-type interface-number : 被监视的接口。
interval interval-value : 发送探测报文的时间间隔。单位为秒。如果不设定, 系统缺省值为 3 秒。
timeout timeout-value : 发送探测报文后等待应答的超时时间。如果超时时间到了, 没有收到应答, 则认为不可达。单位为秒。如果不设定, 系统缺省值为 1 秒。
retry retry-value : 确认不可达的次数, 如果在连续 *retry-value* 次都没有收到应答, 则认为不可达。单位为次数, 如果不设定, 系统缺省值为 3 次。
priority : 被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。
- 【命令模式】 接口模式
- 【使用指导】 如果是监视主机, 对于 IPv6 虚拟路由器, 指定主机的 IPv6 地址。
如果被跟踪的主机地址是链路本地地址, 必须指定网络接口。
如果 VRRP 组占用(Own)了以太网接口实际 IP 地址, 此时该 VRRP 组的优先级为 255, 不能配置监视 IP 地

址。

📌 设置 IPv6 VRRP 定时设备学习功能

【命令格式】 **vrrp ipv6 group timers learn**

【参数说明】 *group* : VRRP 组号。

【命令模式】 接口模式

【使用指导】 一旦启用了定时器学习功能，如果当前设备是 VRRP 备份设备，在设置了定时器学习功能后，它会从主设备的 VRRP 通告中学习 VRRP 通告发送间隔，并由此来计算 Master 设备失效间隔，而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现与 Master 设备的 VRRP 通告发送定时器同步。

📌 设置 IPv6 VRRP 组描述字符串

【命令格式】 **vrrp ipv6 group description text**

【参数说明】 *group* : VRRP 组号。

text : VRRP 组描述符。

【命令模式】 接口模式

【使用指导】 为 VRRP 组设置描述符，可以便于区分 VRRP 组。当设置的描述符超过 80 个字节，提示配置错误。

📌 设置接口上 VRRP 备份组延迟启动时间

【命令格式】 **vrrp delay { minimum *min-seconds* | reload *reload-seconds* }**


【参数说明】 **minimum** *min-seconds* : 接口状态变为活动时的延迟时间。

reload *reload-seconds* : 系统启动时的延迟时间。

【命令模式】 接口模式

【使用指导】 配置本命令后，当系统启动，或者接口状态变为活动时，该接口上的 VRRP 备份组不会立即启动；而是等待相应的延迟时间后再启动 VRRP 备份组，保证非抢占配置不会失效。如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文，则会取消延迟，立即启动 VRRP 协议。两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

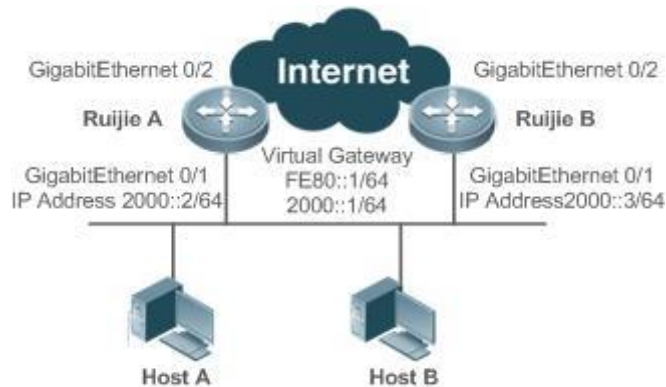
配置举例

 以下配置举例，仅介绍与 VRRP 相关的配置。

📌 在 IPv6 的 VRRP 单备份组和监视接口

【网络环境】

图 4-6



【配置方法】

- Host A Host B 需要通过网关访问 Internet 上的资源，它们的缺省网关为 2000::1/64。
- Ruijie A 和 Ruijie B 属于虚拟 IPv6 路由器的备份组 1，其虚拟地址为 2000::1/64 和 FE80::1。
- Ruijie A 监视与 Internet 链接的接口 GigabitEthernet 0/2，当 GigabitEthernet 0/2 不可用时，Ruijie A 的 VRRP 1 降低自己的优先级，由 Ruijie B 执行网关功能。

RuijieA

```
RuijieA#configure terminal
RuijieA(config)#interface GigabitEthernet 0/1
RuijieA(config-if-GigabitEthernet 0/1)#no switchport
RuijieA(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 track GigabitEthernet 0/2 50
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
```

RuijieB

```
RuijieB#configure terminal
RuijieB(config)#interface GigabitEthernet 0/1
RuijieB(config-if-GigabitEthernet 0/1)#no switchport
RuijieB(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
```

【检验方法】

通过 **show ipv6 vrrp** 命令显示验证。

- 检查当路由设备 Ruijie A 作为 Master 路由设备状态下发现与广域网的接口 GigabitEthernet 0/2 不可用，路由设备 Ruijie A 是否降低自己的 VRRP 备份组优先级 50 而成为 70，这样 VRRP 中路由设备 Ruijie B 就会成为 Master 路由设备。
- 检查当路由设备 Ruijie A 发现自己的与广域网的接口 GigabitEthernet 0/2 恢复可用，是否增加自己的 VRRP 备份组优先级 50 而恢复到 120，这样路由设备 Ruijie A 将再次成为主路由设备。

RuijieA

```
RuijieA#show ipv6 vrrp 1
GigabitEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
    up GigabitEthernet 0/2 priority decrement=50
```

RuijieB

```
RuijieB#show ipv6 vrrp 1
GigabitEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

常见错误

- 同一个VRRP备份组内路由设备上VRRP的虚拟IPv6地址不一致导致同一个VRRP备份组内出现多个Master路由设备。
- 同一个VRRP备份组内路由设备上VRRP的通告发送间隔不一致,并且未设置定时设备学习功能导致同一个VRRP备份组内出现多个Master路由设备。

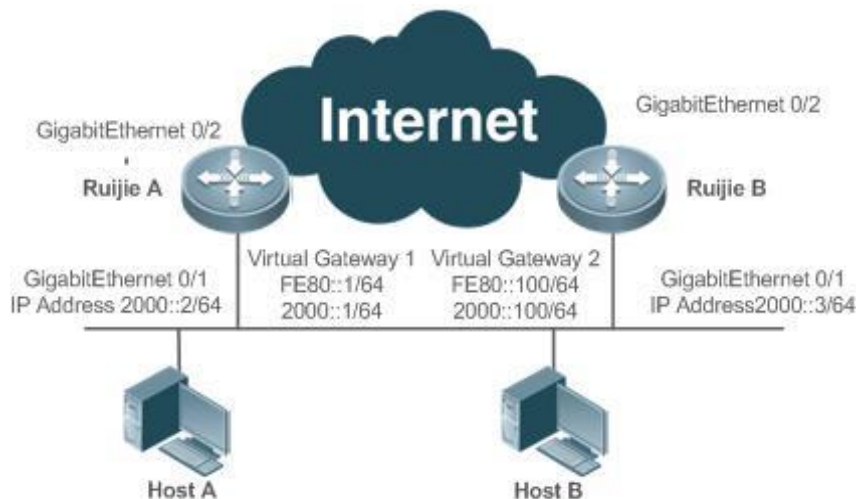
配置举例

i 以下配置举例，仅介绍与 VRRP 相关的配置。

在 IPv6 的 VRRP 多备份组

【网络环境】

图 4-7



【配置方法】

- Host A Host B 需要通过网关访问 Internet 上的资源，它们的缺省网关分别为 2000::1/64 和 2000::100/64。
- Ruijie A 和 Ruijie B 属于虚拟 IPv6 路由器的备份组 1，其虚拟地址为 2000::1/64 和 FE80::1。
- Ruijie A 和 Ruijie B 也属于虚拟 IPv6 路由器的备份组 2，其虚拟地址为 2000::100/64 和 FE80::100。
- Ruijie A 和 Ruijie B 同时作为网关转发流量，同时作为另外一台设备的备份。

RuijieA

```
RuijieA#configure terminal
RuijieA(config)#interface GigabitEthernet 0/1
RuijieA(config-if-GigabitEthernet 0/1)#no switchport
RuijieA(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
RuijieA(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100
RuijieA(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 100
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3
RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode
```

RuijieB

```
RuijieB#configure terminal
RuijieB(config)#interface GigabitEthernet 0/1
RuijieB(config-if-GigabitEthernet 0/1)#no switchport
RuijieB(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1
```

```
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
RuijieB(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100
RuijieB(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 120
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3
RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode
```

【检验方法】 通过 **show ipv6 vrrp** 命令显示验证。

RuijieA

```
RuijieA#show ipv6 vrrp
GigabitEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
GigabitEthernet 0/1 - Group 2
  State is Backup
  Virtual IPv6 address is as follows:
    FE80::100
    2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::5678, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

RuijieB

```
RuijieB#show ipv6 vrrp
```



```
GigabitEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
GigabitEthernet 0/1 - Group 2
  State is Master
  Virtual IPv6 address is as follows:
    FE80::100
    2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::5678(local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
```

常见错误

- 同一个VRRP备份组内路由设备上VRRP的虚拟IPv6地址不一致导致同一个VRRP备份组内出现多个Master路由设备。
- 同一个VRRP备份组内路由设备上VRRP的通告发送间隔不一致,并且未设置定时设备学习功能导致同一个VRRP备份组内出现多个Master路由设备。

5.4.3 配置 VRRP+MSTP

配置效果

- MTSP 和 VRRP 同时使用可以达到链路级备份和网关级备份,极大提高网络健壮性。

注意事项

- 同一个 VRRP 备份组内路由设备上 VRRP 需要配置相同的虚拟 IPv4 地址。
- 启动 VRRP 需要在三层口上配置。

配置方法

📌 启用 IPv4 VRRP

- 默认接口上没有启用 IPv4 VRRP，如果接口要启用 IPv4 VRRP 备份功能则必须配置。

📌 设置 IPv4 VRRP 的验证字符串

- 默认 VRRP 处于无验证模式，如果需要 VRRP 处于明文密码验证模式则配置。

📌 设置 IPv4 VRRP 主路由设备 VRRP 通告间隔

- 默认 VRRP 的主路由设备 VRRP 通告间隔为 1 秒，如果需要手动设置则配置。

📌 设置 IPv4 VRRP 备份组处于抢占模式

- 默认 VRRP 处于抢占模式，抢占延迟时间缺省为 0 秒。

📌 设置 IPv4 VRRP 备份组的优先级

- 默认 VRRP 组优先级为 100，如果需要手动设置则配置。

📌 设置 IPv4 VRRP 备份组监视的接口

- 默认 IPv4 VRRP 组未配置监视接口，缺省优先级改变值为 10，如果需要通过监视接口来实现故障检测则配置。

📌 设置 IPv4 VRRP 定时设备学习功能

- 默认 VRRP 组未开启定时设备学习功能，如果备份路由设备需要学习主路由设备的 VRRP 通告间隔则配置。

📌 设置 IPv4 VRRP 组描述字符串

- 默认 VRRP 组未配置描述字符串，如果需要便于区分 VRRP 组则配置。

📌 设置接口上 VRRP 备份组延迟启动时间

- 默认 VRRP 组未配置延迟启动时间，如果为了保证非抢占模式不失效则配置。

📌 设置 IPv4 VRRP 的 VRRP 报文标准

- 默认 IPv4 VRRP 使用 VRRPv2 标准，如果需要手动设置则配置。

📌 设置 Super VLAN 中 IPv4 VRRP 报文的发送方式

- 默认 IPv4 VRRP 协议报文只往 Super VLAN 中的第一个 UP 的 Sub VLAN 发送，可以设置往指定的 Sub VLAN 发送。

✎ 设置 IPv4 VRRP 组和 BFD 联动

- 默认接口上没有指定 IPv4 VRRP 组和 BFD 联动，如果需要手动设置则配置。

✎ 设置全局 IPv4 VRRP BFD

- 默认 VRRP 不采用全局 IPv4 VRRP BFD 方式检测 master 是否处于活动状态，如果需要手动设置则配置。

检验方法

- **show vrrp** 命令显示配置是否生效

相关命令

✎ 启用 IPv4 VRRP

【命令格式】 **vrrp group ip** *ipaddress* [**secondary**]

【参数说明】 *group* : VRRP 组号，不同产品型号取值范围不同。

ipaddress : 虚拟设备的 IP 地址。

secondary : 标明是该虚拟设备的次 IP 地址。

【命令模式】 接口模式

【使用指导】 如果不指定虚拟 IP 地址，路由设备就不会参与 VRRP 备份组。如果不使用 Secondary 参数，那么设置的 IP 地址将成为虚拟路由设备的主 IP 地址。

✎ 设置 IPv4 VRRP 的验证字符串

【命令格式】 **vrrp group authentication** *string*

【参数说明】 *group* : VRRP 组号。

string : 用于 VRRP 组验证的字符串(不能超过 8 个字节，这里的验证口令是明文口令)。

【命令模式】 接口模式

【使用指导】 在同一个 VRRP 组中的设备必须设置相同的验证口令。明文验证口令不能保证安全性，它只是用来防止/提示错误的 VRRP 配置。

此命令只对 VRRPv2 报文适用，对于 VRRPv3 不适用。

VRRPv3 已经废除了认证功能，如果用户在 IPv4 VRRP 选择的是 VRRPv2，则对 VRRPv2 生效，如果选择的是 VRRPv3，则对 VRRPv3 不生效。

✎ 设置 IPv4 VRRP 主路由设备 VRRP 通告间隔

【命令格式】 **vrrp group timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

【参数说明】 *group* : VRRP 组号。

advertise-interval : VRRP 通告发送间隔(以秒为单位)。

csec *centisecond-interval* : 备份组中 Master 发送 VRRP 报文的时间间隔。整数形式，取值范围是 50 ~ 99。单位是厘秒。无缺省值。

只对 VRRPv3 生效，如果 VRRPv2 配置了此命令，则取默认的主设备的通告发送间隔，即 1 秒。

- 【命令模式】 接口模式
- 【使用指导】 如果当前设备成为 VRRP 组中的主设备，它将以设定的间隔发送 VRRP 通告来通告自己的 VRRP 状态、优先级以及其它信息。
- 根据 RFC 标准，配置了组播报文发送标准为 VRRPv3 的 IPv4 VRRP 组，其组播报文中最大的报文通告间隔为 40 秒，所以如果配置的报文通告间隔超过 40 秒，则取最大的通告间隔 40 秒，但该通告间隔配置是生效的。

✎ 设置 IPv4 VRRP 备份组处于抢占模式

- 【命令格式】 **vrrp group preempt [delay seconds]**
- 【参数说明】 *group* : VRRP 组号。
- delay seconds** : 准备宣告自己拥有 Master 身份之前的延迟。缺省值为 0 秒。
- 【命令模式】 接口模式
- 【使用指导】 如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主设备。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主设备。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主设备。

✎ 设置 IPv4 VRRP 备份组的优先级

- 【命令格式】 **vrrp group priority level**
- 【参数说明】 *group* : VRRP 组号。
- level* : VRRP 组的优先级。
- 【命令模式】 接口模式
- 【使用指导】 该命令将手动设置 VRRP 组的优先级。

✎ 设置 IPv4 VRRP 备份组监视的接口

- 【命令格式】 **vrrp group track {interface-type interface-number | bfd interface-type interface-number ipv4-address } [priority]**
- 【参数说明】 *group* : VRRP 组号。
- interface-type interface-number* : 被监视的接口。
- bfd interface-type interface-number ipv4-address** : 通过 BFD 跟踪指定的邻居 IP。
- priority* : 被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。
- 【命令模式】 接口模式
- 【使用指导】 被监视的接口只允许是三层可路由的逻辑接口(如 Routed Port、SVI、Loopback、Tunnel 等等)。
- 如果 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，不能配置监视接口。

✎ 设置 IPv4 VRRP 备份组监视的 IP 地址

- 【命令格式】 **vrrp group track ipv4-address [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]**
- 【参数说明】 *group* : VRRP 组号。
- ipv4-address* : 被监视的 IPv4 地址。
- interval interval-value** : 发送探测报文的时间间隔。单位为秒。如果不设定，系统缺省值为 3 秒。
- timeout timeout-value** : 发送探测报文后等待应答的超时时间。如果超时时间到了，没有收到应答，则认为不

可达。单位为秒。如果不设定，系统缺省值为 1 秒。

retry *retry-value* : 确认不可达的次数，如果在连续 *retry-value* 次都没有收到应答，则认为不可达。单位为次数，如果不设定，系统缺省值为 3 次。

priority : 被监视的接口状态改变时其 VRRP 优先级改变的尺度。缺省值为 10。

【命令模式】 接口模式

【使用指导】 如果是监视主机，对于 IPv4 虚拟路由器，指定主机的 IPv4 地址。

如果 VRRP 组占用(Own)了以太网接口实际 IP 地址，此时该 VRRP 组的优先级为 255，不能配置监视 IP 地址。

📌 设置 IPv4 VRRP 定时设备学习功能

【命令格式】 **vrrp group timers learn**

【参数说明】 *group* : VRRP 组号。

【命令模式】 接口模式

【使用指导】 一旦启用了定时器学习功能，如果当前设备是 VRRP 备份设备，在设置了定时器学习功能后，它会从主设备的 VRRP 通告中学习 VRRP 通告发送间隔，并由此来计算 Master 设备失效间隔，而不是使用自己本地设置的 VRRP 通告发送间隔来计算。本命令可以实现与 Master 设备的 VRRP 通告发送定时器同步。

📌 设置 IPv4 VRRP 组描述字符串

【命令格式】 **vrrp group description text**

【参数说明】 *group* : VRRP 组号。

text : VRRP 组描述符。

【命令模式】 接口模式

【使用指导】 为 VRRP 组设置描述符，可以便于区分 VRRP 组。当设置的描述符超过 80 个字节，提示配置错误。

📌 设置接口上 VRRP 备份组延迟启动时间

【命令格式】 **vrrp delay { minimum min-seconds | reload reload-seconds }**

【参数说明】 **minimum** *min-seconds* : 接口状态变为活动时的延迟时间。

reload *reload-seconds* : 系统启动时的延迟时间。

【命令模式】 接口模式

【使用指导】 配置本命令后，当系统启动，或者接口状态变为活动时，该接口上的 VRRP 备份组不会立即启动；而是等待相应的延迟时间后再启动 VRRP 备份组，保证非抢占配置不会失效。如果在延迟启动 VRRP 时该接口上接收到 VRRP 报文，则会取消延迟，立即启动 VRRP 协议。两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。

配置此命令将对接口的 IPv4 VRRP 和 IPv6 VRRP 备份组同时生效。

📌 设置 IPv4 VRRP 的 VRRP 报文标准

【命令格式】 **vrrp group version { 2 | 3 }**

【参数说明】 **2** : 使用 VRRPv2 报文发送标准。

3 : 使用 VRRPv3 报文发送标准。

【命令模式】 接口模式

【使用指导】 对于 IPv4 VRRP 考虑到 VRRPv2 和 VRRPv3 的兼容性问题，用户可以根据网络实际环境选择 VRRP 报文的

发送标准。VRRPv2 基于 RFC3768，VRRPv3 基于 RFC 5798。

此命令只适用于 IPv4 VRRP。

📌 设置 Super VLAN 中 IPv4 VRRP 报文的发送方式

【命令格式】 **vrrp detection-vlan {first-subvlan | subvlan-id}**

【参数说明】 **first-subvlan**：只往 Super VLAN 中的第一个 UP 的 Sub VLAN 发送

subvlan-id：往指定的 Sub VLAN 发送

【命令模式】 接口模式

【使用指导】 本命令用于配置 Super VLAN 接口中 IPv4 VRRP 协议报文的发送方式。IPv4 VRRP 协议报文在 Super VLAN 中的发送方式有三种：只往 Super VLAN 中的第一个 UP 的 Sub VLAN 发送；往指定的 Sub VLAN 发送；往 Super VLAN 中的所有 Sub VLAN 发送。Super VLAN 接口如果同时启用 VRRP 和 VRRP PLUS 功能，则往 Super VLAN 中的所有 Sub VLAN 发送。

本命令在 VLAN 接口上配置，只对 Super VLAN 口生效。

📌 设置 IPv4 VRRP 组和 BFD 联动

【命令格式】 **vrrp group bfd ip-address**

【参数说明】 **group**：VRRP 组号。

ip-address：指定的邻居 IP。

【命令模式】 接口模式

【使用指导】 对于备份路由器，执行这条命令，使该 IPv4 VRRP 组和 BFD 联动，并不关心配置的 IP 地址。而对于主路由器，由于不知道备份路由器接口的主 IP 地址，所以只能由管理员指定备份路由器的 IP 地址。

如果配置了全局 IPv4 VRRP BFD，不能配置 IPv4 VRRP 组和 BFD 联动。

配置时首先确保配置的接口配置了 IP 和 BFD 会话参数。

📌 设置全局 IPv4 VRRP BFD

【命令格式】 **vrrp bfd interface-type interface-number ip-address**

【参数说明】 **interface-type interface-number**：配置接口类型和接口编号。

ip-address：指定的邻居 IP。


【命令模式】 全局配置模式

【使用指导】 如果配置了全局 IPv4 VRRP BFD，会删除所有配置的 IPv4 VRRP 组和 BFD 联动。

配置时首先确保配置的接口配置了 IP 和 BFD 会话参数。

全局 IPv4 VRRP BFD 会话只适用于两台设备组成的 IPv4 VRRP 虚拟路由器。

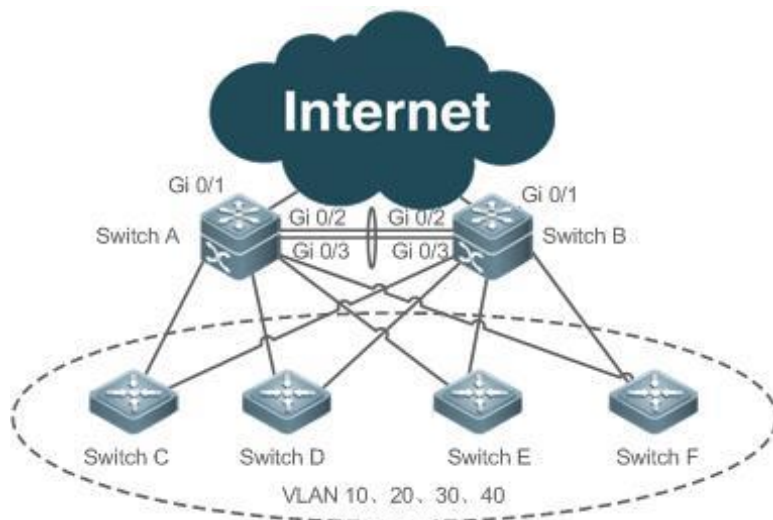
配置举例

 以下配置举例，仅介绍与 VRRP 相关的配置。

📌 配置 VRRP+MSTP

【网络环境】

图 4-8



【配置方法】

- 在设备上（本例为 Switch A、B、C、D、E、F）使能 MSTP 功能，配置 VLAN-Instance 之间的实例映射（本例将 VLAN 10、20 对应 Instance 1，VLAN 30、40 对应 Instance 2，其余 VLAN 对应 Instance 0），并设置网关设备（本例为 Switch A 和 Switch B）为对应实例的根桥。
- 将各 VLAN 的 SVI 加入相应的 VRRP 备份组，并设置网关设备为对应备份组的 Master 路由设备和 Backup 路由设备。本例具体配置如下表所示：

网关设备	VLAN ID	SVI	备份组	虚拟 IP 地址	状态
Switch A	10	192.168.10.2	VRRP 10	192.168.10.1	Master
Switch B		192.168.10.3			Backup
Switch A	20	192.168.20.2	VRRP 20	192.168.20.1	Master
Switch B		192.168.20.3			Backup
Switch A	30	192.168.30.2	VRRP 30	192.168.30.1	Backup
Switch B		192.168.30.3			Master
Switch A	40	192.168.40.2	VRRP 40	192.168.40.1	Backup
Switch B		192.168.40.3			Master

- 将对应备份组的 Master 路由设备的上链口（本例为 Switch A 和 Switch B 的端口 Gi 0/1）设置为 Master 路由设备的监视接口。
- 第一步，在设备上创建 VLAN，在 Switch A、B 上创建 VLAN 10、20、30、40
- 第二步，配置 MST 域，在 Switch A、B 上配置 VLAN 10、20 对应 Instance 1，VLAN 20、30 对应 Instance 2，其余 VLAN 对应 Instance 0。
- 第三步，配置 Switch A 为 MST 0 和 MST 1 的根桥，Switch B 为 MST 2 的根桥。
- 第四步，使能 MSTP。
- 第五步，配置各 VLAN 的 SVI，并加入对应的备份组，同时设置备份组的虚拟 IP 地址。对应配置参见上表。

- 第六步，配置各备份组对应的 Master 路由设备和 Backup 路由设备。
- 第七步，将备份组的 Master 路由设备的上链口配置为 VRRP 组的监视接口。注意：监视接口必须为三层接口。

第八步，配置双核心设备的互联端口为 AP 口。

SwitchA

```
//在Switch A 上创建 VLAN 10、20、30、40
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#vlan range 10,20,30,40
SwitchA(config-vlan-range)#exit
//配置 VLAN 10、20 对应 Instance 1，VLAN 30、40 对应 Instance 2，其余 VLAN 对应 Instance 0。
SwitchA(config)#spanning-tree mst configuration
SwitchA(config-mst)#instance 1 vlan 10,20
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchA(config-mst)#instance 2 vlan 30,40
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchA(config-mst)#exit
//在Switch A 上设置 MST 0 和 MST 1 的优先级为 4096，MST 2 的优先级为 8192。
SwitchA(config)#spanning-tree mst 0 priority 4096
SwitchA(config)#spanning-tree mst 1 priority 4096
SwitchA(config)#spanning-tree mst 2 priority 8192
//开启 MSTP
SwitchA(config)#spanning-tree
Enable spanning-tree.
//配置各 VLAN 的 SVI，并加入对应的备份组，同时设置备份组的虚拟 IP 地址。
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0
SwitchA(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0
SwitchA(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchA(config-if-VLAN 20)#exit
SwitchA(config)#interface vlan 30
SwitchA(config-if-VLAN 30)#ip address 192.168.30.2 255.255.255.0
SwitchA(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchA(config-if-VLAN 30)#exit
SwitchA(config)#interface vlan 40
SwitchA(config-if-VLAN 40)#ip address 192.168.40.2 255.255.255.0
SwitchA(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchA(config-if-VLAN 40)#exit
```


SwitchB

```
//将 Switch A 的备份组 10、20 的优先级调高为 120
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#vrrp 10 priority 120
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#vrrp 20 priority 120
SwitchA(config-if-VLAN 20)#exit

//配置 Switch A 的端口 Gi 0/1 为 Route Port，并设置 IP 地址为 10.10.1.1/24
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#exit

//将 Switch A 的端口 Gi 0/1 配置为备份组 10、20 的监视接口，并设置 Priority decrement 为 30。
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#vrrp 10 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#vrrp 20 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 20)#exit

//配置端口 Gi 0/2 和 Gi 0/3 属于 AP 口，并设置 AP 口为 trunk 口。
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#interface range gigabitEthernet 0/2-3
SwitchA(config-if-range)#port-group 1
SwitchA(config)#interface aggregateport 1
SwitchA(config-if-AggregatePort 1)#switchport mode trunk

//在 Switch B 上创建 VLAN 10、20、30、40
SwitchB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchB(config)#vlan range 10,20,30,40
SwitchB(config-vlan-range)#exit

//配置 VLAN 10、20 对应 Instance 1，VLAN 30、40 对应 Instance 2，其余 VLAN 对应 Instance 0。
SwitchB(config)#spanning-tree mst configuration
SwitchB(config-mst)#instance 1 vlan 10,20
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchB(config-mst)#instance 2 vlan 30,40
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchB(config-mst)#exit

//在 Switch B 上设置 MST 2 的优先级为 4096，MST 0 和 MST 1 的优先级为 8192
SwitchB(config)#spanning-tree mst 2 priority 4096
SwitchB(config)#spanning-tree mst 0 priority 8192
```

```
SwitchB(config)#spanning-tree mst 1 priority 8192
//开启 MSTP
SwitchB(config)#spanning-tree
Enable spanning-tree.
//配置各 VLAN 的 SVI，并加入对应的备份组，同时设置备份组的虚拟 IP 地址。
SwitchB(config)#interface vlan 10
SwitchB(config-if-VLAN 10)#ip address 192.168.10.3 255.255.255.0
SwitchB(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchB(config-if-VLAN 10)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if-VLAN 20)#ip address 192.168.20.3 255.255.255.0
SwitchB(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchB(config-if-VLAN 20)#exit
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#ip address 192.168.30.3 255.255.255.0
SwitchB(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#ip address 192.168.40.3 255.255.255.0
SwitchB(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchB(config-if-VLAN 40)#exit
//将 Switch B 的 VRRP 30、40 的优先级调高为 120。
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#vrrp 30 priority 120
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#vrrp 40 priority 120
SwitchB(config-if-VLAN 40)#exit
//配置 Switch B 的端口 Gi 0/1 为 Route Port，并设置 IP 地址为 10.10.2.1/24
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#no switchport
SwitchB(config-if-GigabitEthernet 0/1)#ip address 10.10.2.1 255.255.255.0
SwitchB(config-if-GigabitEthernet 0/1)#exit
//将 Switch B 的端口 Gi 0/1 配置为备份组 30、40 的监视接口，并设置 Interface -Priority 为 30。
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#vrrp 30 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#vrrp 40 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 40)#exit
//配置端口 Gi 0/2 和 Gi 0/3 属于 AP 口，并设置 AP 口为 trunk 口。
```

```
SwitchB #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchB (config)#interface range gigabitEthernet 0/2-3
SwitchB (config-if-range)#port-group 1
SwitchB (config)#interface aggregateport 1
SwitchB (config-if-AggregatePort 1)#switchport mode trunk
```

【检验方法】**SwitchA**

//查看设备的配置信息。

```
SwitchA#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
    instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
    instance 1 vlan 10, 20
    instance 2 vlan 30, 40
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
interface GigabitEthernet 0/1
    no switchport
    no ip proxy-arp
    ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
    port-group 1
!
interface GigabitEthernet 0/3
    port-group 1
!
interface AggregatePort 1
    switchport mode trunk
!
interface VLAN 10
```

```

no ip proxy-arp
ip address 192.168.10.2 255.255.255.0
vrrp 10 priority 120
vrrp 10 ip 192.168.10.1
vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
no ip proxy-arp
ip address 192.168.20.2 255.255.255.0
vrrp 20 priority 120
vrrp 20 ip 192.168.20.1
vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
no ip proxy-arp
ip address 192.168.30.2 255.255.255.0
vrrp 30 ip 192.168.30.1
!
interface VLAN 40
no ip proxy-arp
ip address 192.168.40.2 255.255.255.0
vrrp 40 ip 192.168.40.1
//查看设备的 VRRP 状态
SwitchA#show vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
VLAN 10 10 120 3 - P Master 192.168.10.2 192.168.10.1
VLAN 20 20 120 3 - P Master 192.168.20.2 192.168.20.1
VLAN 30 30 100 3 - P Backup 192.168.30.3 192.168.30.1
VLAN 40 40 100 3 - P Backup 192.168.40.3 192.168.40.1
//断开 Switch A 的上行链路，查看设备的 VRRP 状态
SwitchA#show vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
VLAN 10 10 90 3 - P Backup 192.168.10.3 192.168.10.1
VLAN 20 20 90 3 - P Backup 192.168.20.3 192.168.20.1
VLAN 30 30 100 3 - P Backup 192.168.30.3 192.168.30.1
VLAN 40 40 100 3 - P Backup 192.168.40.3 192.168.40.1

```

SwitchB

```

//查看设备的配置信息。
SwitchB#show running-config
!

```

```
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
    instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
    instance 1 vlan 10, 20
    instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
    no switchport
    no ip proxy-arp
    ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
    port-group 1!
interface GigabitEthernet 0/3
    port-group 1
!
interface AggregatePort 1
    switchport mode trunk
!
interface VLAN 10
    no ip proxy-arp
    ip address 192.168.10.3 255.255.255.0
    vrrp 10 ip 192.168.10.1
!
interface VLAN 20
    no ip proxy-arp
    ip address 192.168.20.3 255.255.255.0
    vrrp 20 ip 192.168.20.1
!
interface VLAN 30
    no ip proxy-arp
```

```
ip address 192.168.30.3 255.255.255.0
vrrp 30 priority 120
vrrp 30 ip 192.168.30.1
vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
no ip proxy-arp
ip address 192.168.40.3 255.255.255.0
vrrp 40 priority 120
vrrp 40 ip 192.168.40.1
vrrp 40 track GigabitEthernet 0/1 30
//查看设备的 VRRP 状态
SwitchB#show vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
VLAN 10 10 100 3 - P Backup 192.168.10.2 192.168.10.1
VLAN 20 20 100 3 - P Backup 192.168.20.2 192.168.20.1
VLAN 30 30 120 3 - P Master 192.168.30.3 192.168.30.1
VLAN 40 40 120 3 - P Master 192.168.40.3 192.168.40.1
//断开 Switch B 的上行链路，查看设备的 VRRP 状态如下
SwitchB#show vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
VLAN 10 10 100 3 - P Master 192.168.10.3 192.168.10.1
VLAN 20 20 100 3 - P Master 192.168.20.3 192.168.20.1
VLAN 30 30 120 3 - P Master 192.168.30.3 192.168.30.1
VLAN 40 40 120 3 - P Master 192.168.40.3 192.168.40.1
```

常见错误

- 同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式不同导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 对于 VRRPv2，同一 VRRP 备份组内各路由设备以太网接口上 VRRP 组验证模式相同均为明文密码模式，但是验证字符串不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的通告发送间隔不一致，并且未设置定时设备学习功能导致同一个 VRRP 备份组内出现多个 Master 路由设备。
- 同一个 VRRP 备份组内路由设备上 VRRP 的虚拟 IP 地址不一致导致同一个 VRRP 备份组内出现多个 Master 路由设备。

5.5 监视与维护

清楚各类信息

无

查看运行情况

作用	命令
查看 IPv4 VRRP 或者 IPv6 VRRP 的概况或者细节。	show [ipv6] vrrp [brief group]
查看指定接口上的 IPv4 VRRP 组或者 IPv6 VRRP 组的情况。	show [ipv6] vrrp interface <i>type number</i> [brief]
查看 VRRP 报文收发的统计信息。	show vrrp packet statistics [<i>interface-type interface-number</i>]

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 VRRP 出错提示、VRRP 事件、VRRP 报文以及状态调试开关。	debug [ipv6] vrrp
打开 VRRP 出错提示调试开关。	debug [ipv6] vrrp errors
打开 VRRP 事件提示调试开关。	debug [ipv6] vrrp events
打开 VRRP 数据包调试开关。	debug vrrp packets [acl <i>acl-id</i> [icmp protocol] interface <i>type number</i> [group]] debug ipv6 vrrp packets [acl <i>acl-name</i> [icmp protocol] interface <i>type number</i> [group]]
打开 VRRP 状态调试开关。	debug [ipv6] vrrp state

6 VRRP Plus

6.1 概述

VRRP Plus (Virtual Router Redundancy Protocol Plus , 扩展虚拟路由冗余协议) 功能是对 VRRP 协议的扩展 , 利用 VRRP 协议进行 IEEE 802.3 局域网内的网关备份和负载均衡。

VRRP 协议有个不足之处是 : 处于备份状态的路由设备 , 没有承担报文转发的任务。如果要用 VRRP 实现负载均衡 , 则需要手工配置多个 VRRP 组 并将局域网内主机的网关指向不同 VRRP 组的虚拟 IP 地址。这将增大网络管理员的工作量 , VRRP Plus 就是为了解决上述不足而设计的。

VRRP Plus 的好处是 : 自动实现负载均衡 , 即自动将不同主机的流量分配到 VRRP Plus 组成员中 , 无需配置多个 VRRP 组以及设置局域网内主机网关指向不同的 VRRP 组的虚拟 IP 地址。从而大大减轻网络管理员的负担。

 下文仅介绍 VRRP Plus 的相关内容。

协议规范

6.2 -典型应用

典型应用	场景描述
在一个 VRRP 组内启动负载均衡转发	实现 VRRP 组的负载均衡转发 , 无需配置多个组及为每台主机配置不同默认网关。

6.2.1 在一个 VRRP 组内启动负载均衡转发策略

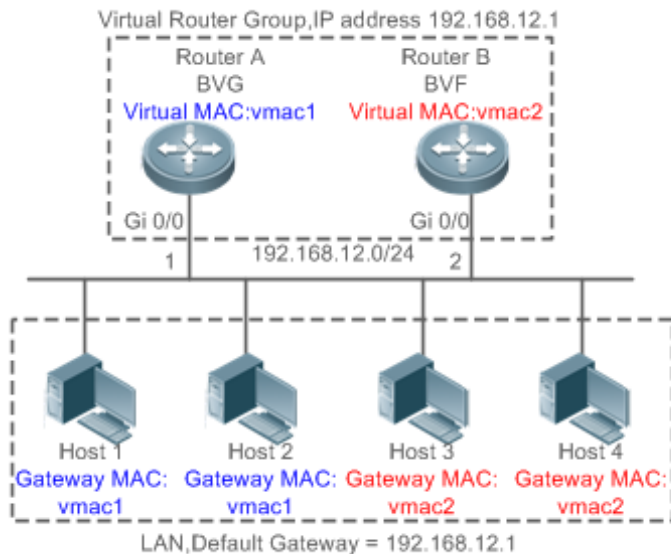
应用场景

在一个 VRRP 组内启动负载均衡转发策略 , 无需配置多个 VRRP 组 , 也不用为每台主机配置不同的默认网关。

以下图 5-1 为例 :

- 配置由 Router A 和 Router B 组成的 VRRP 组 , 并启动 VRRP Plus 功能。
- 每台主机将自己的默认网关设置为 VRRP 组的主虚 IP 地址。

图 5-1 IPv4 VRRP Plus 应用拓扑示意图



【注释】

1. 两台三层设备 Router A 和 Router B 组成一个 VRRP Plus 组，虚拟 IP 地址为 192.168.12.1。Router A 是 VRRP 的 Master 设备，承担 BVG 职责。Router B 是 VRRP 的 Backup 设备，承担 BVF 职责。
2. Host1~Host4 是网段为 192.168.12.0/24 的局域网中的主机，默认网关都指向 VRRP Plus 的虚 IP：192.168.12.1。
3. 对于不同的主机的 ARP 请求，根据在设备上配置的均衡策略进行对应的 ARP 应答。比如 Host1 和 Host2 请求网关 ARP 后，响应的 MAC 为 0000.5e00.0101，Host3 和 Host4 请求网关 ARP 后，响应的 MAC 为 001A.A916.0201。这样 Host1 和 Host2 与外网通讯的报文就发送到 Router A，Host3 和 Host4 与外网通讯的报文就发送到 Router B，从而达到了负载均衡的目的。

功能部署

- 在 Router A 和 Router B 部署 VRRP Plus 策略，实现对本地主机的负载均衡转发。

6.3 功能详解

基本概念

➤ BVG (Balancing Virtual Gateway, 均衡的虚拟网关)

负责 VRRP Plus 组成员虚拟 MAC 的分配，局域网中针对网关 ARP/ND 的应答，同时也承担局域网中主机报文的转发。

➤ BVF (Balancing Virtual Forwarder, 均衡的虚拟转发者)

负责局域网中主机报文的转发，若分配到虚 MAC，则会参与转发，否则不会参与转发。

功能特性

功能特性	作用
VRRP Plus 功能	对 VRRP 协议进行扩展，利用 VRRP 协议进行 IEEE 802.3 局域网内的网关备份和负载均衡。

6.3.1 VRRP Plus 功能

自动实现负载均衡，自动将不同主机的流量分配到 VRRP Plus 组成员中，无需配置多个 VRRP 组以及设置局域内主机网关指向不同的 VRRP 组的虚拟 IP 地址。

基本原理

VRRP Plus 的基本原理是：局域网中的主机使用统一的网关 IP（即 VRRP 组的虚拟 IP），但不同主机在请求网关 ARP 时，由 BVG 应答不同的虚拟 MAC，从而将不同主机的流量分配到 VRRP Plus 的不同成员上，实现负载均衡。

📌 VRRP Plus 与 VRRP 关系

VRRP Plus 是依赖于 VRRP 协议运行的，其运行规则如下：

VRRP 中 Master 的角色，对应 VRRP Plus 中 BVG 角色，VRRP 中 Backup 的角色，对应 VRRP Plus 中 BVF 角色。局域网内主机的网关指向 VRRP 的虚拟 IP 地址。

📌 BVG 和 BVF 的 MAC 地址分配规则

BVG 负责给 BVF 分配虚拟 MAC。对于 IPv4 VRRP Plus，为和 VRRP 兼容，BVG 直接使用 VRRP 的虚拟 MAC，即 00-00-5E-00-01-{VRID}（其中 VRID 为 VRRP 组号）；BVF 使用的虚拟 MAC 为 00-1A-A9-16-{MemberID}-{VRID}（其中 MemberID 为 VRRP Plus 组成员的编号）。目前 VRRP Plus 支持 4 个成员，BVG 使用成员编号 01，其它三个 BVF 使用成员编号 02~04。

📌 VRRP Plus 负载均衡策略

BVG 负责响应局域网内主机的网关 ARP/NS 请求，根据均衡策略的不同，BVG 使用不同的虚拟 MAC 进行应答。均衡策略有三种：基于主机响应，轮询响应和基于权重响应。

- 1) 基于主机响应是指对于特定的主机，使用特定的虚拟 MAC 地址进行应答；
- 2) 轮流响应是指对于收到的主机的网关地址 ARP/NS 请求，轮流使用备份组的各个虚拟 MAC 地址进行应答；
- 3) 基于权重是指根据设备的转发能力进行 ARP/NA 报文的应答。

如果在不同的负载均衡模式下切换，则最终都是新的模式下实现负载均衡，如之前使用的是基于轮询的负载均衡模式，之后使用基于权重的负载均衡模式，则是在新的模式下实现负载均衡，即不考虑设备之前的应答情况。如果基于权重策略，且 VRRP Plus 组内虚拟路由器总的权重值为 0，则不会应答 ARP/NS 请求。

📌 虚拟 MAC 地址的代理

当备份组中某台已经分配了虚拟 MAC 的设备出现故障时，此时使用该虚拟 MAC 作为网关 MAC 地址的用户的流量便会中断。

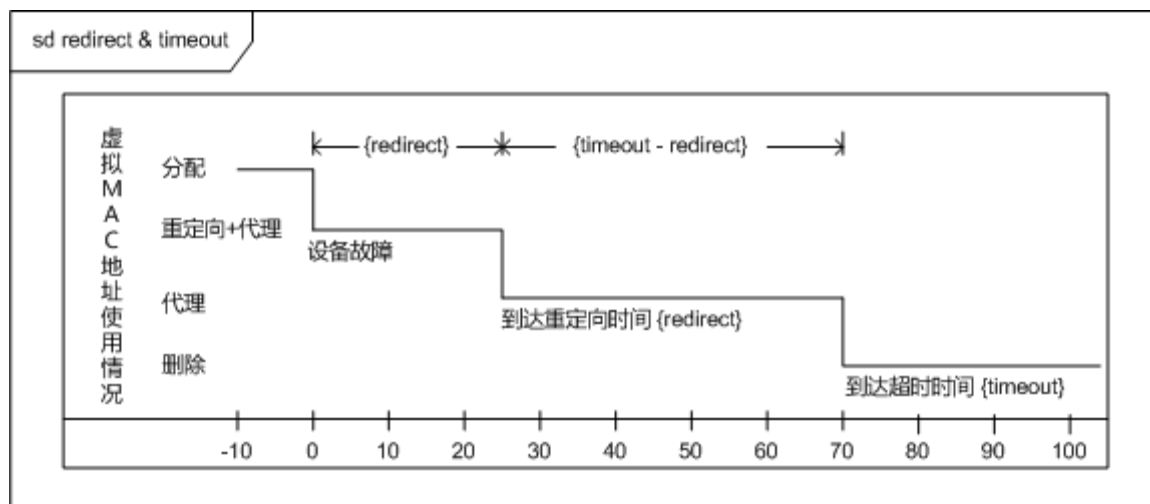
VRRP Plus 备份组中负责管理虚 MAC 地址的 BVG 设备应能够快速检测到该故障，并将该故障的 BVF 设备的虚拟 MAC 地址自动分配给备份组中的其他设备，代替故障设备对该虚 MAC 地址的报文进行转发，由该代理设备承担原用户的流量，避免用户流量中断。对于备份组中某台设备分配得到的虚 MAC 地址，可称为主虚 MAC 地址；对于由它代理的虚 MAC 地址，称为代理虚 MAC 地址。

代理虚 MAC 的重定向时间和超时时间

VRRP Plus 提供虚拟 MAC 地址的代理功能，对已经分配了虚拟 MAC 地址且出现了故障的设备进行代理转发。如果 BVF 从故障中恢复，则应该恢复其转发角色，继续承担该虚拟 MAC 地址的报文转发任务。但如果原设备一直未能恢复，则备份组应该停止重定向流量到该虚拟 MAC 地址，即再收到对网关地址的 ARP 请求时，不再使用该虚拟 MAC 地址进行应答；而且，经过足够长的时间后，我们可以认为原来使用该虚拟 MAC 地址作为网关 MAC 的用户已经更新了网关地址的 ARP/ND 表项、流量已经由其他设备承担，此时便可以删除该虚拟 MAC 地址，发往该虚拟 MAC 地址的报文应该被丢弃。

为此，VRRP Plus 支持设置备份组的重定向时间和超时时间。当设备出现故障后，备份组将其虚拟 MAC 地址分配给其他设备进行代理。在重定向时间内，备份组继续使用该虚拟 MAC 地址应答 ARP/NS 请求；超过重定向时间后，便不再使用该虚拟 MAC 地址进行应答。经过超时时间后，备份组应删除该虚拟 MAC 地址，停止对该虚 MAC 进行代理转发。虚拟 MAC 地址在重定向时间和超时时间内的角色变化如图 5-2 所示：

图 5-2



基于权重的转发

VRRP Plus 支持备份组的权重配置。为不同的设备设置不同的权重值，以使权重值大者分担较多流量，权重值小者分担较少流量，使不同设备的转发性能得到充分利用。当备份组中 BVF 设备的权重值低于下阈值时，将自动退出转发角色，当权重值恢复、高于上阈值时，自动申请为转发角色，能否恢复转发角色，取决于当前是否有剩余的虚 MAC 地址或者代理的虚 MAC 地址。

VRRP Plus 与 BFD 联动

VRRP Plus 支持与链路检测协议联动、根据链路状态调整权重值。备份组中各台设备可以各自关联相应的链路状态，当该链路出现异常、不通时，该设备应自动降低其权重值；如果权重过低、则应该可以退出转发角色。若备份组正在使用基于权重的负载均衡策略，便可以根据其新的权重值为其分配相应的流量。当关联的链路状态得以恢复时，该设备能够自动恢复权重值、恢

转发角色；对于采用基于权重的负载均衡方式的备份组，根据其恢复后的权重值为其分配不同主机的流量。IPv6 VRRP Plus 暂时不支持与 bfd 的联动。

基于权重的转发抢占

VRRP Plus 支持转发角色的抢占功能。VRRP Plus 中参与负载均衡的设备数量上限为四台，即一个 VRRP Plus 备份组中最多会产生四个虚拟 MAC 地址，当有超过四台设备加入一个 VRRP Plus 组时，只有四台设备会参与报文转发，其余的设备则不参与，仅监听其他设备的状况；只有当参与转发的设备出现故障时，才会替换其角色，开始对报文进行转发。当已经有四台设备组成 VRRP Plus 备份组，并均在负责报文转发，此时有第五台设备加入 VRRP Plus 组，且这台设备转发能力较强，或者原有转发角色出现链路故障、导致转发能力降低，如果配置允许抢占模式，则第五台设备可以抢占其他权重较低（即转发能力较低）的设备。为转发能力较强的设备配置较高的权重值，当发现处于监听状态的设备的权重值比正在负责转发的设备的权重值更高时，使监听设备自动抢占转发设备的角色，由转发能力更强的设备负责报文转发，较低的设备进行监听。这样可以尽量减少资源的浪费。

由于备份组中的 BVG 设备负责管理虚 MAC 地址分配，故 BVG 的角色不可以被抢占；只有 BVF 的转发角色可以被抢占。如果 BVG 所在的设备出现故障，VRRP 会重新选举 Master，因此 BVG 也会在新的 Master 设备上生成。

影响转发策略的几个因素

- 在配置了 VRRP Plus 后，若收到主机的 ARP/NS 请求报文，可以基于不同的负载均衡策略进行应答，以实现对这些主机的负载均衡；但是对于配置 VRRP Plus 之前、已经学习到了 VRRP 虚网关地址的主机，不支持对这些主机的负载均衡。因此，如果待 VRRP 状态切换为 Master 之后才配置 VRRP Plus，则在主机学到的 ARP/ND 老化之前，无法真正的实现负载均衡；待主机记录的网关 ARP/ND 老化、重新请求网关地址时，才会负载均衡。
- 接口的定时发送免费 ARP 的功能也会影响 VRRP Plus 的负载均衡功能。当打开了 VRRP Plus 时，便屏蔽虚地址的免费 ARP/NA 的发送。当虚 IP 地址、实 IP 地址重叠时，不再发送该地址的免费 ARP/NA 报文。
- 当发现有主机与本设备地址出现冲突时，ARP/ND 模块也会广播发送该地址的免费 ARP/NA 报文。如果发生冲突的是 VRRP Plus 的虚地址，那么发送的免费 ARP/NA 报文就会导致主机的网关 MAC 地址被重新学习，破坏 VRRP Plus 的负载均衡功能，此情况暂不支持 VRRP Plus 的负载均衡功能。

6.4 配置详解

配置项	配置建议 & 相关命令	
配置 VRRP Plus	 必须配置。开启 VRRP Plus 功能。	
	vrrp balance	接口下启动指定组号的 VRRP 备份组的 VRRP Plus 功能。
	 可选配置。配置 VRRP Plus 备份组参数。	
	vrrp load-balancing	接口下设置 VRRP Plus 负载均衡策略。
	vrrp timers redirect	接口下设置 VRRP Plus 备份组的代理虚 MAC 地址的重定向时间和超时时间。
	vrrp weighting	接口下设置 VRRP Plus 备份组的权重和上下限值。
	vrrp forwarder preempt	接口下设置 VRRP Plus 备份组的转发抢占功能。

6.4.1 配置 VRRP Plus

配置效果

- 启动 VRRP Plus 功能（缺省未开启接口 VRRP Plus 功能）。
- 设置 VRRP Plus 权重值的跟踪对象。

注意事项

- 启动 VRRP Plus 功能，必须在相应的备份组上配置 VRRP 虚地址。

配置方法

▾ 接口启动 VRRP Plus 功能

- VRRP Plus 默认关闭，如果要具备 VRRP Plus 功能则必须配置。

▾ 设置 VRRP Plus 负载均衡策略

- 启动了 VRRP Plus 后，默认使用基于主机均衡的转发策略，即 host-dependent。

▾ 设置 VRRP Plus 备份组的代理虚 MAC 地址的重定向时间和超时时间

- 启动了 VRRP Plus 后，默认配置了该功能，redirect 缺省值为 300 秒，timeout 的缺省值为 14400 秒。

▾ 设置 VRRP Plus 备份组的权重和上下限值。

- 启动了 VRRP Plus 后，默认配置了该功能。备份组的权重值缺省值为 100，权重值下限缺省值为 1，上限缺省值为 100。

▾ 设置 VRRP Plus 备份组的转发抢占功能

- 启动了 VRRP Plus 后，默认打开了允许转发抢占功能。

▾ 设置 VRRP Plus 备份组的权重值的跟踪对象

- VRRP Plus 权重值跟踪对象默认关闭，如果要具备跟踪功能则必须配置。

检验方法

- 通过 **show group vrrp balance** 命令显示验证，如果该备份组有承担负载转发的任务，则显示的转发者 forwarders 中会显示 “local”，且显示该备份组分配到的虚拟 MAC 地址。

相关命令

▾ 接口启动 VRRP Plus 功能

- 【命令格式】 **vrrp group balance**
- 【参数说明】 *group* : VRRP 组号，不同产品型号取值范围不同。
- 【命令模式】 接口配置模式
- 【使用指导】 需要配置 VRRP 组，VRRP PLUS 功能才能启动。。

配置 VRRP Plus 备份组的负载均衡策略

- 【命令格式】 **vrrp group load-balancing { host-dependent | round-robin | weighted }**
- 【参数说明】 *group* : VRRP 组号。
- host-dependent** : 表示基于主机的均衡转发策略。
- round-robin** : 表示基于轮询的均衡策略。
- weighted** : 表示基于备份组权重的均衡。
- 【命令模式】 接口配置模式
- 【使用指导】 启动了 VRRP Plus 后，默认使用基于主机均衡的转发策略，即 **host-dependent**。整个备份组的负载均衡策略由配置在 BVG 上的均衡策略决定，若用户希望在 BVG 设备角色更换后还使用同样的均衡策略，则需要在备份组内的所有设备配置相同的均衡策略。

配置 VRRP Plus 备份组的代理虚 MAC 地址的重定向时间和超时时间

- 【命令格式】 **vrrp group timers redirect redirect timeout**
- 【参数说明】 *group* : VRRP 组号。
- redirect* : 重定向时间，取值范围为 0 ~ 3600 秒，缺省值为 300 秒（即 5 分钟）。
- timeout* : 超时时间，取值范围为（*redirect* + 600）- 64800 秒，缺省值为 14400 秒（即 4 小时）。
- 【命令模式】 接口配置模式
- 【使用指导】 启动了 VRRP Plus 后，默认配置了该功能，*redirect* 缺省值为 300 秒，*timeout* 的缺省值为 14400 秒。当设备出现故障后，备份组将其虚拟 MAC 地址分配给其他设备进行代理。在重定向时间内，备份组继续使用该虚拟 MAC 地址应答 ARP/NS 请求；超过重定向时间后，便不再使用该虚拟 MAC 地址进行应答。经过超时时间后，备份组应删除该虚拟 MAC 地址。

配置 VRRP Plus 备份组的权重和上下限值。

- 【命令格式】 **vrrp group weighting maximum [lower lower] [upper upper]**
- 【参数说明】 *maximum* : 备份组的权重值，取值范围 2-254，缺省值为 100。
- lower lower** : 备份组的权重下限值，取值范围 1 ~ (*maximum* - 1)，缺省值为 1。
- upper upper** : 备份组的权重上限值，取值范围 *lower* ~ *maximum*，缺省值为 100。
- 【命令模式】 接口配置模式
- 【使用指导】 启动了 VRRP Plus 后，默认配置了该功能。用户通过此命令不同的设备设置不同的权重值，以使权重值大者分担较多流量，权重值小者分担较少流量。当备份组中 BVF 设备的权重值低于下限值时，将自动退出转发角色，当权重值恢复、高于上限值时，应该自动恢复转发角色。

配置 VRRP Plus 备份组的转发抢占功能

- 【命令格式】 **vrrp group forwarder preempt**
- 【参数说明】 *group* : VRRP 组号。
- 【命令模式】 接口模式

- 【使用指导】 启动了 VRRP Plus 后，默认打开了转发抢占功能。VRRP Plus 允许设置备份组的转发抢占功能，当发现处于监听状态的设备的权重值比正在负责转发的设备的权重值更高时，使监听设备自动抢占转发设备的角色，由转发能力更强的设备负责报文转发，较低的设备进行监听。

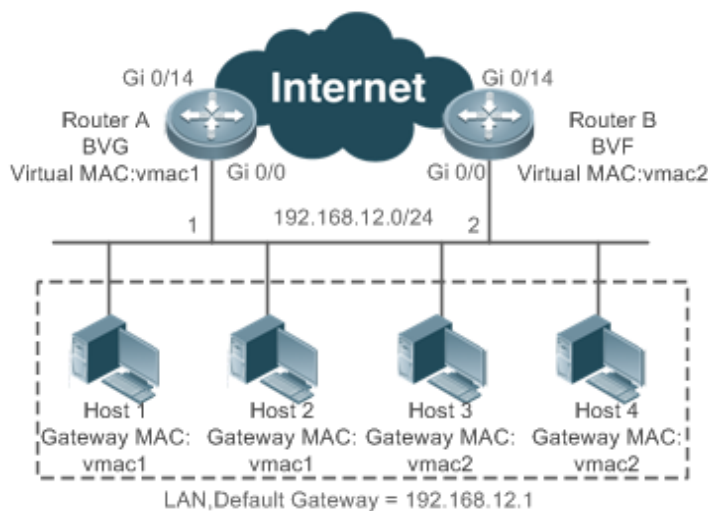
配置举例

以下配置举例，仅介绍与 VRRP Plus 相关的配置。

在一个 IPv4 VRRP 组内启动负载均衡转发策略

【网络环境】

图 5-3



- 【配置方法】
- 在 Router A 和 Router B 配置 VRRP 组，并开启 VRRP Plus 功能；通过配置本地 IP 地址使得 Router A 为 BVG (Master) 设备，Router B 为 BVF (Backup) 设备。
 - 配置 VRRP Plus 为基于权重的负载均衡策略，并设置权重值的跟踪对象，减少权重值为 100。
 - 备份组权重和阈值，重定向时间和超时时间以及是否允许转发抢占功能都采用默认配置。
 - 本地局域网的主机 Host1 ~ Host4 默认网关指向 VRRP 的虚 IP 地址即 192.168.12.1。

Router A

```
RuijieA#config
RuijieA(config)#interface GigabitEthernet 0/0
// 'no switchport'在交换机上使用
RuijieA(config-if-GigabitEthernet 0/0)#no switchport
RuijieA(config-if-GigabitEthernet 0/0)#ip address 192.168.12.3 255.255.255.0
RuijieA(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.12.1
RuijieA(config-if-GigabitEthernet 0/0)#vrrp 1 balance
RuijieA(config-if-GigabitEthernet 0/0)#vrrp 1 load-balancing weighted
```

Router B

```
RuijieB#config
RuijieB(config)#interface GigabitEthernet 0/0
RuijieB(config-if-GigabitEthernet 0/0)#no switchport
RuijieB(config-if-GigabitEthernet 0/0)#ip address 192.168.12.2 255.255.255.0
RuijieB(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.12.1
```

```
RuijieB(config-if-GigabitEthernet 0/0)#vrrp 1 balance
RuijieB(config-if-GigabitEthernet 0/0)#vrrp 1 load-balancing weighted
```

【检验方法】 通过 **show vrrp balance** 显示 VRRP PLUS 备份组的配置情况，如果该备份组有承担负载转发的任务，则显示的转发者 Forwarder 中会显示 “local”，且显示该备份组分配到的虚拟 MAC 地址。

Router A

```
RuijieA# show vrrp balance interface GigabitEthernet 0/0
State is BVG
Virtual IP address is 192.168.12.1
Hello time 1 sec, hold time 3 sec
Load balancing: weighted
Redirect time 300 sec, forwarder time-out 14400 sec
Weighting 100 (configured 100), thresholds: lower 1, upper 100
There are 2 forwarders
Forwarder 1 (local)
MAC address:
    0000.5e00.0101
Owner ID is 0000.0001.0006
Preemption disabled (BVG cannot be preempted)
Forwarder 2
MAC address:
    001a.a916.0201
Owner ID is 00d0.f822.33a3
Preemption enabled
```

Router B

```
RuijieB# show vrrp balance interface GigabitEthernet 0/0
State is BVF
Virtual IP address is 192.168.12.1
Hello time 1 sec, hold time 3 sec
Load balancing: weighted
Redirect time 300 sec, forwarder time-out 14400 sec
Weighting 100 (configured 100), thresholds: lower 1, upper 100
There are 2 forwarders
Forwarder 1
MAC address:
    0000.5e00.0101
Owner ID is 0000.0001.0006
Preemption disabled (BVG cannot be preempted)
Forwarder 2 (local)
MAC address:
    001a.a916.0201
Owner ID is 00d0.f822.33a3
Preemption enabled
```


常见错误

- 没有在相应的组上配置 VRRP 虚地址，则配置 VRRP PLUS 功能不生效。

6.5 监视与维护


清除各类信息

无

查看运行情况

作用	命令
显示 VRRP Plus 的概况或者细节	show vrrp balance
显示指定接口上的 VRRP Plus 组的操作情况	show vrrp balance interface

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 VRRP Plus 功能所有调试开关	debug vrrp balance
打开错误信息调试开关	debug vrrp balance error
打开 VRRP Plus 组事件的调试开关	debug vrrp balance event
打开与 VRRP 模块间的消息调试开关	debug vrrp balance messages
打开 VRRP Plus 协议报文调试开关	debug vrrp balance packets
打开 VRRP Plus 组状态调试开关	debug vrrp balance state
打开 VRRP Plus 组的定时器消息调试开关	debug vrrp balance timer

7 BFD

7.1 概述

为了减小故障对业务的影响，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。BFD（Bidirectional Forwarding Detection，双向转发检测），提供一种轻负载、快速检测两台邻接路由器之间转发路径连通状态的方法。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，加快启用备份转发路径，提升现有网络性能。

 下文仅介绍 BFD 的相关内容。

协议规范

- draft-ietf-bfd-base-09：Bidirectional Forwarding Detection
- draft-ietf-bfd-generic-05：Generic Application of BFD
- draft-ietf-bfd-mib-06：Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-v4v6-1hop-09：BFD for IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-07：BFD for IPv4 and IPv6 (Multihop)
- draft-ietf-bfd-mpls-07：BFD For MPLS LSPs

 目前不支持 draft-ietf-bfd-mib-06 和 draft-ietf-bfd-multihop-07。

7.2 典型应用

典型应用	场景描述
OSPF 与 BFD 联动	OSPF 利用 BFD 快速检测邻居状态
典型应用	场景描述
静态路由与 BFD 联动	静态路由利用 BFD 快速检测路由下一跳的可达性

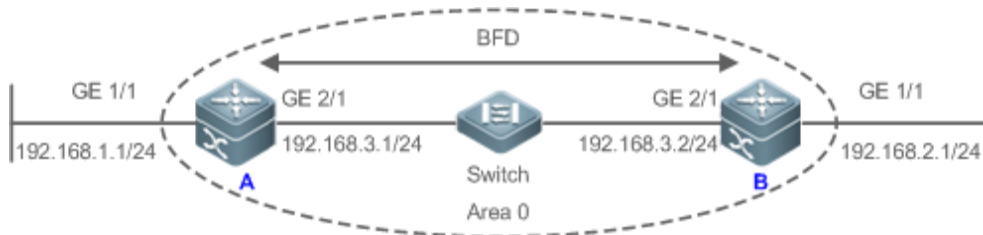
7.2.1 OSPF 与 BFD 联动

应用场景

OSPF 协议通过 Hello 报文动态发现邻居，当 OSPF 启动 BFD 检测功能后，将会为达到 FULL 关系的邻居建立 BFD 会话，通过 BFD 机制检测邻居状态，一旦 BFD 邻居失效，OSPF 会立刻进行网络收敛。收敛的时间可以从 120 秒（缺省情况非广播型网络 OSPF hello 报文的发送间隔为 30 秒，而邻居设备失效的时间是间隔时间的 4 倍，也就是需要 120s）降到 1 秒内。

以下图为例，Router A、Router B 通过二层交换机 switch 互连，在设备上运行 OSPF 协议来建立路由，同时使能允许 OSPF 在双方接口上关联 BFD 应用。在 Router B 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告 OSPF 协议，触发协议快速收敛。

图 6-1



【注释】 A、B 为路由器。
switch 为二层交换机。
A、B 通过二层交换机 switch 互连。

功能部属

- 在 Router A 和 B 相连接口配置 IP 地址
- 在 Router A 和 B 运行 OSPF 协议
- 在 Router A 和 B 相连接口配置 BFD 参数
- 在 Router A 和 B 使能 OSPF 联动 BFD

7.2.2 静态路由与 BFD 联动

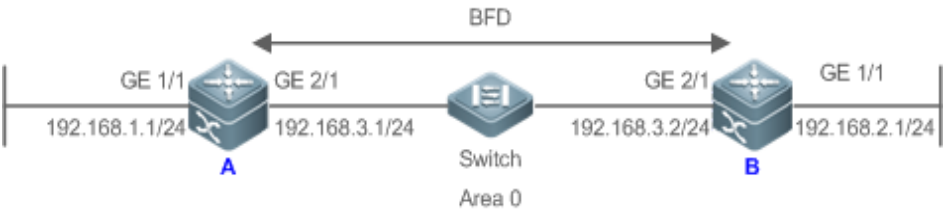
应用场景

静态路由与 BFD 联动，可以避免在配置的静态路由不可达的情况下，路由选路不会选择该静态路由作为转发路径。如果存在备份路由转发路径，将可以快速地切换到该备份转发路径。

与动态路由协议不同，静态路由没有发现邻居的机制，因此，当配置 BFD 与静态路由关联，静态路由的下一跳可达性将依赖于 BFD 会话状态。如果 BFD 会话检测到故障，表示静态路由的下一跳不可达，则该静态路由将不安装到 RIB 中。

以下图为例，Router A、Router B 通过二层交换机 switch 互连，在设备上配置静态路由来建立转发，同时使能允许静态路由在双方接口上关联 BFD 应用。在 Router B 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告静态路由，触发系统将该静态路由从 RIB 中删除，从而避免选路错误。

图 6-2



【注释】 A、 B 为路由器。
switch 为二层交换机。
A、 B 通过二层交换机 switch 互连

功能部属

- 在路由器 A 和 B 相连接口配置 IP 地址
- 在路由器 A 和 B 配置静态路由
- 在路由器 A 和 B 相连接口配置 BFD 参数
- 在路由器 A 和 B 使能静态路由联动 BFD

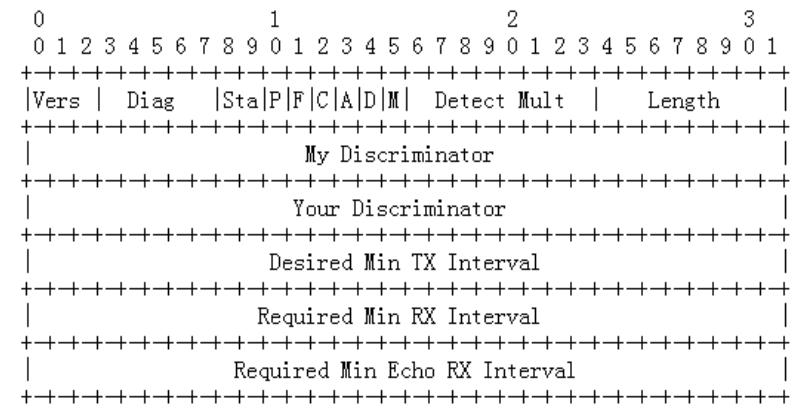
7.3 功能详解

基本概念

📄 报文格式

BFD 发送的检测报文是 UDP 报文，有两种类型分别是控制报文和回声报文。其中回声报文只有 BFD 会话本端系统关心，远端系统不关心，因此协议没有规定其具体格式。协议只规定了控制报文的格式。目前控制报文格式有两个版本(版本 0 和版本 1)，建立 BFD 会话时缺省采用版本 1，如果收到对端系统发送的是版本 0 的报文，将自动切换到版本 0。

图 6-3



字段	说明
Vers	BFD 协议版本号，目前为 1。
Diag	给出本地最后一次从 UP 状态转到其他状态的原因，包括： 0—没有诊断信息 1—控制超时检测 2—回声功能失效 3—邻居通告会话 Down 4—转发面复位 5—通道失效 6—连接通道失效 7—管理 Down
Sta	BFD 本地状态，包括： 0 代表 AdminDown 1 代表 Down 2 代表 Init 3 代表 Up
P	参数发生改变时，发送方在 BFD 报文中置该标志，接收方必须立即响应该报文。
F	响应 P 标志置位的回应报文中必须将 F 标志置位。
C	转发/控制分离标志，一旦置位，控制平面的变化不影响 BFD 检测，如：控制平面为 OSPF，当 OSPF 重启/GR 时，BFD 可以继续检测链路状态。
A	认证标识，置位代表会话需要进行验证。
D	查询请求，置位代表发送方期望采用查询模式对链路进行检测。
M	用于将来应用点到多点时使用，目前必须设置 0。
Detect Mult	检测超时倍数，用于检测方计算检测超时时间。
Length	报文长度。
My Discriminator	BFD 会话连接本端标识符。
Your Discriminator	BFD 会话连接远端标识符。
Desired Min Tx Interval	本地支持的最小 BFD 报文发送间隔。
Required Min RX Interval	本地支持的最小 BFD 报文接收间隔。
Required Min Echo RX Interval	本地支持的最小 Echo 报文接收间隔（如果本地不支持 Echo 功能，则设置 0）。
Auth Type	认证类型(可选)，包括： Simple Password Keyed MD5 Meticulous Keyed MD5 Keyed SHA1 Meticulous Keyed SHA1
Auth Length	认证数据长度。
Authentication Data	认证数据区。

会话状态

BFD 会话有四种基本的状态，分别是 Down、Init、Up 和 AdminDown。

7. Down：会话处于 Down 状态或者刚刚创建。
8. Init：已经和对端系统通信，希望使会话进入 Up 状态。
9. Up：会话已经建立成功。
10. AdminDown：会话处于管理性 Down 状态。

BFD 根据自己的本地会话状态以及接收到的对端 BFD 报文，进行状态机迁移。

BFD 状态机的建立和拆除采用三次握手机制，以确保两端都知道状态的变化。

发送周期和检测时间

BFD 在建立过程中，两端会话会协商 BFD 参数，确定发送周期及检测时间进行会话检测。

在建立 BFD 会话后，可以动态协商 BFD 的相关参数（例如最小发送间隔、最小接收间隔等），两端协议通过发送相应的协商报文后采用新的发送周期和检测时间按，不影响会话的当前状态。

功能特性

功能特性	作用
BFD 会话建立	建立 BFD 会话。
BFD 会话检测	快速检测双向转发路径。
BFD 与关联应用联动	快速通告 BFD 检测结果。
BFD 保护策略	受攻击的情况下保护 BFD 的稳定。
BFD 震荡抑制通告	线路不稳定的情况下保护关联应用的稳定。

7.3.1 BFD 会话建立

BFD 检测开始于 BFD 会话的建立。

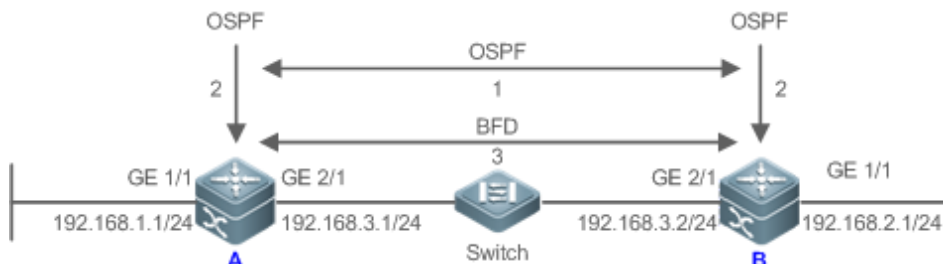
工作原理

会话建立过程

BFD 本身没有发现邻居的能力，需要上层协议通知与哪个邻居建立会话。

如下图所示，两台路由器通过一台二层交换机相连，两台路由器同时运行 OSPF 和 BFD。

图 6-4



BFD 会话建立过程：

11. OSPF 发现邻居后并与邻居建立连接。
12. OSPF 通知 BFD 与该邻居建立会话。
13. BFD 与该邻居建立起会话。

建立 BFD 会话模式

BFD 协议规定建立 BFD 会话的模式，有两种：

- 主动模式

在建立会话前不管是否收到对端发来的建立 BFD 会话的控制报文，都会主动发送建立 BFD 会话的控制报文。

- 被动模式

在建立会话前不会主动发送建立 BFD 会话的控制报文，直到收到对端发过来建立 BFD 会话的控制报文。

i 被动模式暂不支持，且不可配置。

协商 BFD 会话参数

BFD 会话建立过程，两端会进行 BFD 会话的参数协商，从而确定发送周期和检测时间，需要注意以下几点：

14. 必须在两端接口上配置 BFD 会话参数(包括 Desired Min Tx Interval , Required Min RX Interval , Detect Mult) , 否则 BFD 会话无法建立。
15. 在建立 BFD 会话的过程中，两端接口会协商 BFD 会话参数，并依据此会话参数进行会话检测。
16. 在建立 BFD 会话后，可以动态协商 BFD 的相关参数（例如最小发送间隔、最小接收间隔等），两端协议通过发送相应的协商报文后采用新的发送周期和检测时间按，不影响会话的当前状态。

7.3.2 BFD 会话检测

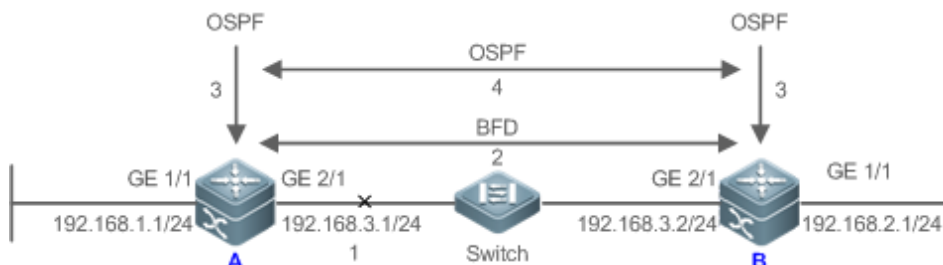
BFD 会话建立后，开始进行链路检测。周期性地发送 BFD 控制报文，如果在检测时间内未收到对端发过来的 BFD 报文，则认为会话 Down，通告联动应用，加快应用协议收敛。

工作原理

检测过程

如下图所示，两台路由器通过一台二层交换机相连，两台路由器同时运行 OSPF 和 BFD。

图 6-5



BFD 会话检测到故障后的处理过程：

1. RouterA 与 Switch 之间的链路通信发生故障。
2. RouterA 和 RouterB 之间的 BFD 会话检测到故障。
3. BFD 通知本地运行的 OSPF 到邻居的转发路径发生故障。
4. OSPF 进行邻居 Down 过程的处理，如果存在备份转发路径那么将进行协议收敛，从而启用备份转发路径。

检测模式

BFD 包含如下几种检测模式。

异步模式

在异步模式下，系统之间相互周期性地发送 BFD 控制报文，如果某个系统在检测时间内没有收到对端发来的 BFD 控制报文，就宣布会话为 Down。

查询模式

在查询模式下，假定每个系统都有一个独立的方法用来确认它连接到其他系统。这样一旦一个 BFD 会话建立起来以后，系统停止发送 BFD 控制报文，除非某个系统需要显式地验证连接性，在需要显式验证连接性的情况下，系统发送一个短序列的 BFD 控制包，如果在检测时间内没有收到返回的报文就宣布会话为 Down，如果收到对端的回应报文，表示转发路径正常。

回声模式

本地系统周期性的发送 BFD 回声报文，远端系统通过它的转发通道将它们环回回来。如果本地在检测周期内连续几个回声报文都没有接收到，会话就被宣布为 Down。回声功能可以和上述两种检测模式一起使用。采用回声报文的检测功能，不需要远端系统的控制面参与，报文通过远端系统的转发面转回，减少了延迟，相对于发送控制报文可以更快的检测到故障。如果在异步模式下启用回声功能，可以大大减少了控制报文的发送，因为检测工作由回声功能完成；如果在查询模式下启用回声功能，在会话建立后可以完全取消发送控制报文。BFD 会话两点必须同时启用回声功能，否则回声功能将不生效。

- i 查询模式暂不支持，且不可配置。
- i 只有 BFD 会话版本 1 支持 BFD 的回声模式
- i 源或者目的地址为链路本地地址的 IPv6 BFD 会话，不支持 ECHO 模式

7.3.3 BFD 与关联应用联动

关联应用通过与 BFD 联动，可以利用 BFD 快速检测故障的优点，提高关联应用协议的收敛性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

工作原理

关联应用配置联动 BFD，下发创建 BFD 会话，BFD 会话建立后进行快速故障检测。当链路出现故障时，BFD 能够快速检测到故障，通告关联应用进行处理，提高关联应用协议的收敛性能。当前 BFD 支持的关联应用有：

- 支持 RIP 联动 BFD

RIP 通过与 BFD 联动，可以利用 BFD 相对于协议自身的“HELLO”机制更快速检测故障的优点，提高协议的收敛性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

 关于 RIP 与 BFD 联动的更多内容，请查阅“RIP”章节

- 支持 OSPF 联动 BFD

OSPF 通过与 BFD 联动，可以利用 BFD 相对于协议自身的“HELLO”机制更快速检测故障的优点，提高协议的收敛性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

 关于 OSPF 与 BFD 联动的更多内容，请查阅“OSPF”章节

- 支持 OSPFv3 联动 BFD

OSPFv3 通过与 BFD 联动，可以利用 BFD 相对于协议自身的“HELLO”机制更快速检测故障的优点，提高协议的收敛性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

 关于 OSPFv3 与 BFD 联动的更多内容，请查阅“OSPFv3”章节

- 支持 BGP 联动 BFD

BGP 通过与 BFD 联动，可以利用 BFD 相对于协议自身的“HELLO”机制更快速检测故障的优点，提高协议的收敛性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

 关于 BGP 与 BFD 联动的更多内容，请查阅“BGP”章节

- 支持 ISIS 联动 BFD

IS-IS 协议通过 Hello 报文动态发现邻居，当 IS-IS 启动 BFD 检测功能后，将会为达到 UP 状态的邻居建立 BFD 会话，通过 BFD 机制检测邻居状态，一旦 BFD 邻居失效，IS-IS 会立刻进行网络收敛。收敛的时间可以从 30 秒(缺省情况点到点网络 IS-IS hello 报文的发送间隔为 10 秒，而邻居设备失效的时间是间隔时间的 3 倍，也就是需要 30s)降到 1 秒内。

 关于 ISIS 与 BFD 联动的更多内容，请查阅“ISIS”章节

- 支持静态路由联动 BFD

静态路由与 BFD 联动，可以避免在配置的静态路由不可达的情况下，路由选路不会选择该静态路由作为转发路径。如果存在备份路由转发路径，将可以快速地切换到该备份转发路径。

与动态路由协议不同，静态路由没有发现邻居的机制。因此，当配置 BFD 与静态路由关联，静态路由的下一跳可达性将依赖于 BFD 会话状态。如果 BFD 会话检测到故障，表示静态路由的下一跳不可达，则该静态路由将不安装到 RIB 中。

如果 BFD 会话建立过程，远端系统删除 BFD 会话，将会造成 BFD 会话状态变为 Down，在这种情况下系统确保不影响静态路由的转发行为。

i 关于静态路由与 BFD 联动的更多内容，请查阅“NSM”章节

- 支持策略路由联动 BFD

策略路由与 BFD 联动，可以避免在配置的策略路由不可达的情况下，路由选路不会选择该策略路由作为转发路径。如果存在备份路由转发路径，将可以快速地切换到该备份转发路径。

与策略路由联动的方式等同于静态路由。通过 BFD 跟踪检测与指定邻居的转发路径，当会话检测到故障，将通知策略路由到达相应下一跳不可达，达到该下一跳的策略路由将不生效。

如果 BFD 会话建立过程，远端系统删除 BFD 会话，将会造成 BFD 会话状态变为 Down，在这种情况下系统确保不影响策略路由的转发行为。

i 关于策略路由与 BFD 联动的更多内容，请查阅“PBR”章节

- 支持 VRRP 联动 BFD

VRRP 与 BFD 联动可以替代 VRRP 自身的“HELLO”机制实现快速检测主备路由器的运行状态，加快了故障时主备路由器的切换，提高网络的性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

VRRP 还可以利用 BFD 来跟踪指定的邻居，如果 BFD 会话检测到与该邻居的转发路径发生故障，则自动降低一定数额的 VRRP 优先级，触发主备路由器进行切换。该配置只有在动态路由协议或者其他应用通知 BFD 与相应邻居创建会话时，才会生效。

i 关于 VRRP 与 BFD 联动的更多内容，请查阅“VRRP”章节

- 支持 VRRP Plus 联动 BFD

VRRP Plus 与 BFD 联动可以替代 VRRP Plus 自身的 BVP 对 BVF 的检测，实现快速检测 BVF 的运行状态，加快了故障时转发实体的切换，提高网络的性能。一般情况下，检测故障的时间可以缩短到 1 秒以内。

VRRP Plus 是基于 VRRP 协议的，所以在于 BFD 关联上，无须进行额外的配置，只需要确保两端的设备均已经开启 VRRP，并且正确的关联了 BFD 会话。

i 关于 VRRP Plus 与 BFD 联动的更多内容，请查阅“VRRP Plus”章节

- 支持 MPLS 联动 BFD


MPLS 与 BFD 联动主要是指 LSP 标签交换路径(Label Switched Path)通过 BFD 进行邻居的快速检测。所支持的检测方式为：

17. BFD 检测静态 LSP
18. BFD 检测 LDP 协议生成的 LSP
19. BFD 检测 LSP 反向路径采用 IP

i 关于 MPLS 与 BFD 联动的更多内容，请查阅“MPLS”章节


- 支持三层接口联动 BFD

BFD 支持修改三层接口状态，在配置模式下，通过 **bfd bind peer-ip** 命令来检测指定的三层接口的直连地址，该 CLI 命令所建立的 BFD 会话状态会产生对应接口的 BFD 状态，比如 BFD Down 或者 BFD Up。常用在各类型 FRR 中，通过 BFD 来检测接口状态，进行快速的 FRR 切换。

 三层接口联动 BFD，暂只支持进行 LDP FRR 切换

- 支持 L3AP 成员口联动 BFD

L3AP 成员口和 BFD 联动后，可以快速检测到成员口的链路故障，从而快速的将该成员链路的流量分配到其他有效成员链路上。一般情况下，检测故障的时间可以缩短到 1 秒以内。

 关于 L3AP 与 BFD 联动的更多内容，请查阅“AP”章节

7.3.4 BFD 保护策略

保护 BFD 由于受到攻击(比如：大量 Ping 报文攻击设备)而发生 BFD 会话震荡。

工作原理

BFD 协议是非常敏感协议，如果所启用 BFD 功能的设备受到攻击（比如：大量 Ping 报文攻击设备）而发生 BFD 会话震荡，可以通过配置启用 BFD 的保护策略进行保护。但如果启用该设备 BFD 功能的同时打开该保护策略，会导致上一跳设备发出的 BFD 报文经过该设备时，该设备会将 BFD 报文丢弃，从而影响上一跳设备与其他设备的 BFD 会话建立。

7.3.5 BFD 震荡抑制通告

主要解决由于线路不稳定导致 BFD 会话在 Down 和 Up 状态之间频繁切换，从而引起关联的应用（比如静态路由）频繁的进行转发路径切换，影响业务的正常运行的问题。

工作原理

BFD 会话在 Down 和 Up 状态之间频繁切换，允许用户配置通告给关联应用会话 Up 状态前所需 Up 状态稳定的时间。在 Up 状态保持在特定时间后，才通告关联应用 BFD Up，否则通告 BFD Down。

7.4 配置详解

配置项	配置建议 & 相关命令	
配置 BFD 基本功能	 必须配置。用于建立 BFD 会话。	
	bfd interval	配置 BFD 参数

	配置关联应用联动 BFD	
	 关联的应用不同，配置命令会不同，具体参见各应用相关章节。此处不一一列出	
	 可选配置。用于配置 BFD 的检测模式、慢速报文发送周期和 BFD 联动三层接口。	
	bfd echo	配置回声模式
	bfd slow-timer	配置慢速发送控制报文周期
配置 BFD 保护策略	bfd bind peer-ip	配置 BFD 联动三层接口
	 可选配置。用于保护 BFD 免受攻击的影响。	
	bfd cpp	配置 BFD 保护策略
配置 BFD 震荡抑制通告	 可选配置。用于关联协议免受 BFD 震荡的影响。	
	bfd up-dampening	配置 BFD 震荡抑制通告

7.4.1 配置 BFD 基本功能

配置效果

- 关联应用联动上 BFD。
- 建立起 BFD 会话
- BFD 会话进行链路故障检测。

注意事项

- 配置 BFD 会话参数，需要注意：
 20. 建议 BFD 会话两端的参数配置一致，这样可以确保关联 BFD 应用协议同时生效，避免由于两端配置的抑制时间不同而出现转发路径单通的情况。
 21. 配置时设置的参数需要考虑不同接口传输上的带宽差异。如果设置最小发送间隔和最小接受间隔过小，可能导致 BFD 占用过大带宽而影响本身的数据传输。
- 配置关联应用联动 BFD，需要注意：
 22. 配置时需要确保 BFD 会话邻居都启用关联应用联动 BFD，否则 BFD 会话将无法建立。但如果已经有动态路由协议或者其他应用通知 BFD 与相应邻居创建会话，那么应用关联 BFD 会话也将建立。
 23. 如果由于 IP 选路而导致 BFD 会话邻居指定的接口和实际 BFD 报文出接口不一致，或创建 BFD 会话时指定的接口和实际 BFD 回来的报文入接口不一致，则无法建立 BFD 会话。
- 配置 BFD 检测模式，需要注意：

24. 本端的回声报文发出,在对端设备转发面处理后返回到本端,这个过程可能由于对端设备拥塞造成回声报文丢失,引发会话检测失败。在这种情况下,需要配置相应的 QOS 策略来确保回声报文优先得到处理或者关闭回声功能。
25. BFD 的回声检测功能不支持多跳检测,所以在配置多跳时,请确认回声功能已经关闭。
26. Echo 模式必须是 BFD 会话的两端系统都使能该模式才能生效。
27. 在 BFD 启用 echo 模式前,需要在 BFD 会话的邻居设备上执行 **no ip redirects** 命令关闭发送 ICMP 重定向报文的功能,执行 **no ip deny land** 命令关闭 DDOS 功能(防止 Land-based 攻击)。

配置方法

配置 BFD 参数

- 必须配置。
- 若无特殊要求,应在 BFD 检测的两端路由器的 BFD 会话出口上配置 BFD 参数。
- 配置时设置的参数需要考虑不同接口传输上的带宽差异。如果设置最小发送间隔和最小接收间隔过小,可能导致 BFD 占用过大带宽而影响本身的数据传输。

【命令格式】 **bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier**

【参数说明】 **interval milliseconds**: 最小发送间隔,单位毫秒。

min_rx milliseconds: 最小接收间隔,单位毫秒。

multiplier interval-multiplier: 检测超时倍数

【缺省配置】 无 BFD 会话参数

【命令模式】 接口配置模式

【使用指导】 在路由器上启用 BFD 功能前,必须先启用快转功能。

配置 BFD 检测模式

- 可选配置,端口默认运行异步模式,如果 BFD 会话要运行于回声模式,则需要配置。
- 在交换机或路由器的端口下配置。
- 只要两端路由器的其中一端配置异步模式,BFD 会话就会运行于异步模式;两端同时默认配置运行于回声模式,则 BFD 会话最终运行于回声模式。

【命令格式】 **bfd echo**

【参数说明】 -

【缺省配置】 BFD 回声模式关闭

【命令模式】 接口配置模式

【使用指导】 该命令不允许在 L3 AP 接口下配置。

缺省情况下配置了 BFD 会话参数的同时系统自动使能 echo 模式。

echo 报文的最小发送间隔和最小接收间隔采用会话配置的 **Interval milliseconds** 和 **min_rx milliseconds** 参数。

在 BFD 启用 echo 模式前,需要在 BFD 会话的邻居设备上执行 **no ip redirects** 命令关闭发送 ICMP 重定向报文的功能,执行 **no ip deny land** 命令关闭 DDOS 功能(防止 Land-based 攻击)。

配置慢速报文发送周期

- 可选配置，默认慢速报文发送周期为 3000ms，如果需要增加或减少 BFD 慢速报文的发送周期，则可以配置。
- 在交换机或路由器的全局配置模式下配置。
- BFD 运行在 ECHO 模式或者 BFD 建立过程，以该周期来发送慢速控制报文，配置周期越大，协商建立 BFD 会话的时间越长，ECHO 模式下发送的慢速 BFD 报文时间越长。

【命令格式】 **bfd slow-timer [milliseconds]**

【参数说明】 *milliseconds*：BFD 的慢速定时器时间，单位为毫秒。可配置范围从 1000 到 30000，未配置缺省值为 3000。

【缺省配置】 慢速控制报文发送周期为 3000ms

【命令模式】 全局配置模式

【使用指导】 此命令用来指定 ECHO 模式下发送慢速控制报文的周期。

📌 配置 BFD 联动三层接口

- 可选配置。目前，BFD 关联三层接口仅在 MPLS LDP 做 FRR 快速切换时使用。
- 在交换机或路由器的端口下配置。

【命令格式】 **bfd bind peer-ip src-address [source-ip dst-address] process-pst**

【参数说明】 *src-address*：接口对端的 ip 地址

dst-address：接口本端 ip 地址

【缺省配置】 缺省无三层口关联 BFD 配置

【命令模式】 接口配置模式

【使用指导】 用于指定三层接口联动 BFD，可快速检测三层接口的连通性。

📌 配置关联应用联动 BFD

- 必须配置。
- 缺省情况下关联应用联动 BFD 未开启。
- 关联的应用不同，配置命令会不同，具体参见各应用相关章节。
- 必须确保两端均配置关联应用联动 BFD，BFD 会话才能建立起来。
- 在 RIP 路由配置模式下，使用 **bfd all interfaces** 命令开启允许所有接口 RIP 关联 BFD，详细配置参考 RIP 相关章节。
- 在 OSPF 路由配置模式下，使用 **bfd all interfaces** 命令开启允许所有接口 OSPF 关联 BFD，详细配置参考 OSPF 相关章节。
- 在 OSPFv3 路由配置模式下，使用 **bfd all interfaces** 命令开启允许所有接口 OSPFv3 关联 BFD，详细配置参考 OSPFv3 相关章节。
- 在 BGP 路由配置模式下，使用 **neighbor address fall-over bfd** 命令开启 BGP 联动 BFD，详细配置参考 BGP 相关章节。
- 在 ISIS 路由配置模式下，使用 **bfd all interfaces** 命令开启允许所有接口 ISIS 关联 BFD，详细配置参考 ISIS 相关章节。
- 在全局配置模式下，使用 **ip route static bfd [vrf vrf-name] interface-type interface-number gateway [source ip-address]** 命令开启静态路由联动 BFD，详细配置参考 NSM 相关章节。
- 在全局配置模式下，使用 **ipv6 route static bfd [vrf vrf-name] interface-type interface-number gateway [source ip-address]** 命令开启静态 IPv6 路由联动 BFD，详细配置参考 NSM 相关章节。

- 使用 **set ip next-hop verify-availability next-hop-address bfd [vrf vrf-name] interface-type interface-number gateway** 命令开启策略路由联动 BFD，详细配置参考 PBR 相关章节。
- 使用 **set ipv6 next-hop verify-availability next-hop-address bfd [vrf vrf-name] interface-type interface-number gateway** 命令开启 IPv6 策略路由联动 BFD，详细配置参考 PBR 相关章节。
- 使用 **vrrp bfd interface-type interface-number ip-address** 命令开启 VRRP 联动 BFD，详细参考见 VRRP 相关章节。
- VRRP Plus 是基于 VRRP 协议的，所以在于 BFD 关联上，无须进行额外的配置，只需要确保两端的设备均已经开启 VRRP，并且正确的关联了 BFD 会话。
- 使用 **bfd bind static-lsp peer-ip ip-address source-ip ip-address [local-discriminator discr-value remote-discriminator discr-value] [process-state]** 命令开启静态 LSP 联动 BFD，详细配置见 MPLS 相关章节。
- 使用 **bfd bind ldp-lsp peer-ip ip-address nexthop ip-address [interface interface-type interface-number] source-ip ip-address [local-discriminator discr-value remote-discriminator discr-value] [process-state]** 命令开启 LDP LSP 联动 BFD，详细配置见 MPLS 相关章节。
- 使用 **bfd bind backward-lsp-with-ip peer-ip ip-address [vrf vrf-name] interface interface-type interface-number [source-ip ip-address] { local-discriminator discr-value remote-discriminator discr-value }** 命令开启动态 LSP 联动 BFD，详细配置见 MPLS 相关章节。

检验方法

- 关联的应用不同，其检验的方式也不尽相同，具体参见各应用相关章节。

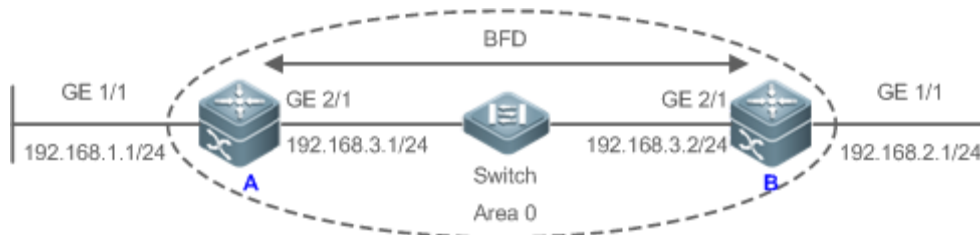
配置举例

i 以下配置举例，仅介绍与 BFD 相关的配置。

OSPF 联动 BFD

【网络环境】

图 6-6



【配置方法】

- 在 Router A 和 Router B 相连接口配置 IP 地址
- 在 Router A 和 Router B 运行 OSPF 协议
- 在 Router A 和 Router B 相连接口配置 BFD 参数
- 在 Router A 和 Router B 使能 OSPF 联动 BFD

A

```
A# configure terminal
A(config)# interface GigabitEthernet2/1
```



```

A(config-if-GigabitEthernet2/1)# no switchport           //路由器无需此配置
A(config-if-GigabitEthernet2/1)# ip address 192.168.3.1 255.255.255.0
A(config-if-GigabitEthernet2/1)# bfd interval 200 min_rx 200 multiplier 5
A(config-if-GigabitEthernet2/1)# exit
A(config)# interface GigabitEthernet1/1
A(config-if-GigabitEthernet1/1)# no switchport           //路由器无需此配置
A(config-if-GigabitEthernet1/1)# ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet1/1)# exit
A(config)# router ospf 123
A(config-router)# log-adj-changes detail
A(config-router)# network 192.168.3.0 0.0.0.255 area 0
A(config-router)# network 192.168.1.0 0.0.0.255 area 0
A(config-router)# bfd all-interfaces
A(config-router)# end

```

B

```

B# configure terminal
B(config)# interface GigabitEthernet2/1
B(config-if-GigabitEthernet2/1)# no switchport           //路由器无需此配置
B(config-if-GigabitEthernet2/1)# ip address 192.168.3.2 255.255.255.0
B(config-if-GigabitEthernet2/1)# bfd interval 200 min_rx 200 multiplier 5
B(config-if-GigabitEthernet2/1)# exit
B(config)# interface GigabitEthernet1/1
B(config-if-GigabitEthernet1/1)# no switchport           //路由器无需此配置
B(config-if-GigabitEthernet1/1)# ip address 192.168.2.1 255.255.255.0
B(config-if-GigabitEthernet1/1)# exit
B(config)# router ospf 123
B(config-router)# log-adj-changes detail
B(config-router)# network 192.168.3.0 0.0.0.255 area 0
B(config-router)# network 192.168.2.0 0.0.0.255 area 0
B(config-router)# bfd all-interfaces
B(config-router)# end

```

【检验方法】 显示验证。**A**

```

A# show bfd neighbors details

```

OurAddr	NeighAddr	LD/RD	RH/RS	Holdown(mult)	State	Int
192.168.3.1	192.168.3.2	1/2	Up	532 (3)	Up	Ge2/1

```

Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196

```


B

```

Registered protocols: OSPF
Uptime: 02:18:49
Last packet: Version: 1      - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 3              - Length: 24
My Discr.: 2                - Your Discr.: 1
Min tx interval: 50000      - Min rx interval: 50000
Min Echo interval: 0

B# show bfd neighbors details
OurAddr      NeighAddr    LD/RD    RH/RS    Holdown(mult)    State    Int
192.168.3.2  192.168.3.1  2/1      Up       532 (5 )         Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: OSPF
Uptime: 02:18:49
Last packet: Version: 1      - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                 - Final bit: 0
Multiplier: 5              - Length: 24
My Discr.: 1                - Your Discr.: 2
Min tx interval: 200000     - Min rx interval: 200000
Min Echo interval: 0

```

常见错误

- 两端设备有一端接口未配置 BFD 参数。
- 没有使能关联应用联动 BFD。
- 两端设备只有一端使能应用联动 BFD。

7.4.2 配置 BFD 保护策略

配置效果

- 如果所启用 BFD 功能的设备受到攻击（比如:大量 Ping 报文攻击设备）而发生 BFD 会话震荡，可以通过配置启用 BFD 的保护策略进行保护。

注意事项

- 必须配置 BFD 基本功能
- 如果启用该设备 BFD 功能的同时打开该保护策略，会导致上一跳设备发出的 BFD 报文经过该设备时，该设备会将 BFD 报文丢弃，从而影响上一跳设备与其他设备的 BFD 会话建立。
- 该功能及限制仅对交换机生效。

配置方法

配置 BFD 保护策略

- 可选配置。
- 在交换机或路由器的全局配置模式下配置。
- BFD 保护策略是用于在设备受到攻击的场景下，提升 BFD 报文的处理优先级，保证 BFD 业务的正常运行。

【命令格式】 **bfd cpp**

【参数说明】 -

【缺省配置】 BFD 保护策略开启

【命令模式】 全局模式

【使用指导】 如果设备受攻击导致的 BFD 震荡，可开启功能进行保护。

检验方法

show running-config 查看对应接口下是否存在该配置。

配置举例

配置 BFD 保护策略

- 【配置方法】
- 在存在攻击行为网络中的交换机上配置。
 - 配置 BFD 保护策略

```
Ruijie# configure terminal
Ruijie(config)# bfd cpp
Ruijie(config)# end
```

【检验方法】 -

常见错误

无

7.4.3 配置 BFD 震荡抑制通告

配置效果

- 线路不稳定导致 BFD 会话在 Down 和 Up 状态之间频繁切换，从而引起关联的应用（比如静态路由）频繁的进行转发路径切换，影响业务的正常运行的问题。
- 用户配置通告给关联应用会话 Up 状态前所需 Up 状态稳定的时间。在 Up 状态保持在特定时间后，才通告关联应用 BFD Up，否则通告 BFD Down。减少线路不稳定导致的关联应用协议的震荡。

注意事项

- 必须配置 BFD 基本功能。
- 如果在 BFD 没有出现 Down 和 Up 状态频繁切换，启用 BFD 震荡抑制通告，会导致延迟通告关联应用会话 Up。

配置方法

配置 BFD 震荡抑制通告

- 可选配置，端口默认未开启 BFD 震荡抑制通告，如果在 BFD 出现 Down 和 Up 状态频繁切换，则可以启用 BFD 震荡抑制通告。
- 在交换机或路由器的端口下配置
- 开启 BFD 震荡抑制通告，可以缓解因 BFD 频繁通告状态变化而导致关联应用的频繁处理，如路由重新计算等；配置的时间越长则 BFD 需要稳定的时间越长，只有在稳定时间达到配置的时间，才会通告相应的应用模块。

【命令格式】 **bfd up-dampening [milliseconds]**

【参数说明】 *milliseconds*：通告给关联应用会话 UP 状态前所需 UP 状态稳定的时间，单位为毫秒。可配置范围从 0 到 300000，配置 0，即当会话的状态从 DOWN 切换为 UP 时将立即通告给应用层。缺省值为 0。。

【缺省配置】 BFD 震荡抑制通告功能未开启

【命令模式】 接口配置模式

【使用指导】 只有在线路不稳定时，才需要开启该功能。

如果在 BFD 没有出现 Down 和 Up 状态频繁切换，配置该命令，会导致延迟通告关联应用会话 Up。

检验方法

show running-config 查看对应接口下是否存在该配置。

配置举例

配置 BFD 震荡抑制通告时间为 60,000 毫秒。

- 【配置方法】
- 在链路不够稳定会导致 BFD 频繁震荡的环境下配置。
 - 配置 BFD 震荡抑制通告时间为 60,000 毫秒

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config)# bfd up-dampening 60000
Ruijie(config)# end
```

【检验方法】 -

常见错误

无

7.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 BFD 会话信息。	show bfd neighbors [vrf <i>vrf-name</i>] [client {ap bgp ospf rip vrrp static-route pbr vrrp-balance ldp-lsp static-lsp backward-lsp-with-ip pst }] [ipv4 <i>ip-address</i> ipv6 <i>ip-address</i>] [details]

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 BFD 事件的调试开关。	debug bfd event [interface <i>interface-type interface-number</i> ipv4 <i>ip-address</i> ipv6 <i>ipv6-address</i>]
打开 BFD 报文的调试开关	debug bfd packet [interface <i>interface-type interface-number</i> ipv4 <i>ip-address</i> ipv6 <i>ipv6-address</i>]

8 IP Event Dampening

8.1 概述

对三层设备来说，当三层网络接口由于人为的开启/关闭或者由于其他外在因素导致状态频繁 UP/DOWN 变化时，会造成本设备上路由表的反复震荡。若配置了路由协议，那么路由协议还可能会将这一震荡扩散到整个网络中，造成邻居路由反复进行路由的更新和重新计算，不仅浪费网络带宽，而且导致整个网络不稳定。从设备本身的角度来说，反复的路由更新和计算需要消耗大量的 CPU 资源。这些都会影响客户网络的正常运行。

IP Event Dampening (IP 事件惩罚) 功能能够检测异常的 UP/DOWN 翻转，并自动抑制接口状态频繁 UP/DOWN，使单点链路故障不会被路由协议扩散出去；当接口恢复稳定后，抑制状态将自动解除，从而减少网络震荡，降低系统的 CPU 资源消耗，增强整网的稳定性。

协议规范

- RFC2439 : BGP Route Flap Damping

i IP Event Dampening 采用的抑制算法核心与 RFC2439 所述的 BGP 路由翻转抑制算法一致。

8.2 典型应用

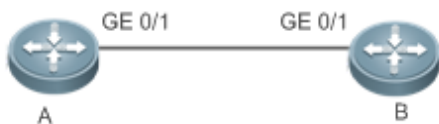
典型应用	场景描述
抑制路由接口震荡	在路由器三层网络接口上监控接口状态变化，对接口的频繁震荡进行抑制。

8.2.1 抑制路由接口震荡

应用场景

在运行路由协议的网络中，两两相连的路由器之间一旦有端口频繁 UP/DOWN，将引起邻居路由反复更新计算路由，进而扩散到整个网络，导致网络震荡。通过在相连的路由口上启用 IP Event Dampening 功能，可以监控接口状态变化，对接口的频繁振荡进行抑制，减少网络震荡，降低系统的 CPU 资源消耗，增强整网的稳定性。


图 8-1



【注释】 A、B 为普通路由器。

功能部属

以上图为例，可以在路由器 A 和 B 的接口 GE0/1 上配置 IP Event Dampening 功能。

 路由器上的子接口和接口虚模板 Virtual template，不支持 dampening 功能。

8.3 功能详解

基本概念

📌 惩罚值 (penalty)

IP Event Dampening 功能采用了一种对接口状态变化事件计算惩罚值的方式，对接口行为进行感知和控制。接口上每进行一次 up→down 翻转，惩罚值将会累加，待接口稳定时，该惩罚值又会按指数递减。通过这种惩罚值计算，使得接口能智能地感知其自身的状态行为，进行相应处理。

📌 抑制门限 (Suppress Threshold)

为了识别接口震荡事件，IP Event Dampening 功能设置了一个抑制门限，当累积惩罚值超过该门限时，认为该接口处于震荡状态，并对接口实施抑制。

📌 半衰期 (Half-Life Period)

半衰期是指在接口稳定情况下惩罚值衰减到原来一半所需要的时间。它定义了惩罚值按指数衰减的速度，半衰期越短，衰减的越快，探测到接口稳定的速度越快，但震荡检测的灵敏度也越低。

📌 解除抑制门限 (Reuse Threshold)

当接口不再震荡，惩罚值衰减到一定程度（减少到抑制门限以下）时，可认为该接口恢复稳定状态，从而解除接口的抑制状态。

📌 最大抑制时间 (Maximum Suppress Time)

为避免接口长时间震荡后，惩罚值过大，导致过久不能恢复使用，算法定义了一个最大抑制时间，即无论接口震荡多久，接口被抑制的时间不会超过最大抑制时间。

功能特性

功能特性	作用
接口震荡抑制	允许用户在接口上配置接口震荡抑制条件和参数，使得交换机或路由器设备能自动对反复震荡的接口进行识别和抑制，确保本机的路由稳定性和避免路由震荡的扩散。

8.3.1 接口震荡抑制

工作原理

当接口上配置了 Dampening 功能时，该接口上会被附上一个与之相关的惩罚值（Penalty）。每当接口 DOWN 的时候，该接口上的 Penalty 增加 1000，该 Penalty 值随时间递减，若递减过程中，接口再次出现 DOWN 事件，则接口上 Penalty 值进行累加，若累计 Penalty 值超过抑制门限（Suppress Threshold）则判断该接口处于抑制（Suppress）状态，之后无论接口的真实状态是什么，对受影响的上层协议来说，该接口始终处于 DOWN 状态。直到 Penalty 递减到解除抑制门限（Reuse Threshold），接口的抑制状态解除，还原接口的真实状态。


当三层接口上未配置 Dampening 功能，或配置了 Dampening 功能但接口未被抑制时，路由协议或其他关心三层接口状态的协议都和正常情况下的行为一样。当接口上配置了 Dampening 且接口被抑制时，上层协议认为接口状态为 down，这期间接口实质上的状态变化不会对路由表以及上层路由协议路由计算和通告造成影响，直到接口解除抑制为止。

相关配置

配置 IP Event Dampening 功能

- 缺省情况下，三层接口上的 IP Event Dampening 功能关闭。
- 使用 **dampening** [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]] 命令可以启动或关闭接口上的 IP Event Dampening 功能。

8.4 配置详解

配置项	配置建议 & 相关命令	
启动 IP Event Dampening	 必须配置。用于抑制三层接口震荡。	
	dampening	配置 IP Event Dampening 功能

8.4.1 启动 IP Event Dampening

配置效果

在配置有 IP Event Dampening 的接口上，若发现震荡情况超过用户预先设定的条件参数时，将该接口状态设置为 down。

注意事项

- 对于交换机接口层次转换（三层口转换为 2 层口），如从 routed port 转换为 switch port，该接口上配置的 **dampening** 命令将被删除。

- 对于路由器来说只有主接口可以配置接口事件抑制功能。该功能可以对配有该命令的主接口的所有子接口生效,但不能直接在子接口上配置该命令。该命令也不支持在 virtual template 上配置。

配置方法

配置 IP Event Dampening 功能

- 必须配置
- 在三层接口模式下配置。
- 配置的时候可以指定半衰期、解除抑制门限、抑制门限、最大抑制时间和初始惩罚值,如果没有指定则使用默认值。

检验方法

可以使用以下两种方法来确认配置是否生效。

- **show running-config**。
- **show interfaces [interface-id] dampening**, 查看接口 IP Event Dampening 配置情况。

相关命令

打开接口上的 Ip Event Dampening 功能

【命令格式】 **dampening** [*half-life-period* [*reuse-threshold* *suppress-threshold* *max-suppress* [**restart** [*restart-penalty*]]]]]

【参数说明】 *half-life-period*: 半衰期, 范围<1-30>, 默认 5s。
reuse-threshold: 解除抑制门限, 范围<1-20000>, 默认 1000。
suppress-threshold: 抑制门限, 范围<1-20000>, 默认 2000。
max-suppress: 最大抑制时间, 范围<1-255>, 默认为 *half-life-period* 的 4 倍。
restart *restart-penalty*: 初始惩罚值, 范围<1-20000>, 默认 2000。

【命令模式】 接口模式

【使用指导】 该功能会影响直连/主机路由, 静态路由, 动态路由和 VRRP。当一个接口满足命令的配置条件, 处于抑制状态时, 以上受影响的模块认为该接口状态为 DOWN, 从而会删除对应的路由, 并且不会从该接口收发数据包。当在一个已经配置了 **dampening** 命令的接口上, 重新配置命令, 会使该接口的所有 dampening 信息清空, 但接口的翻转次数仍会保留, 除非使用 **clear counters** 命令清除接口的统计信息。
如果配置的 *max-suppress* 太小, 导致计算得出的最大惩罚值比抑制门限还要小, 则该接口将永远得不到抑制。这属于配置错误, 此时会打印类似如下的信息, 提示用户配置失败:

```
% Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time
```

另外, 当配置该命令时, 系统内存不足以执行该配置保存, 也会打印配置失败的提示:

```
% No memory, configure dampening fail!
```

配置举例

在三层接口上配置 Ip Event Dampening 功能

【网络环境】

图 8-2



【配置方法】 在路由器 A 和 B 接口 GigabitEthernet 0/1 上开启 IP Event Dampening 功能，半衰期 30 秒，解除抑制门限 1500，开始抑制门限 10000，以及最长抑制时间为 120 秒。

A

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

B

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

【检验方法】 通过 **show interfaces dampening** 命令查看接口的 dampening 的详细信息。

```
Ruijie#show interfaces dampening
GigabitEthernet 0/1
```

Flaps	Penalty	Supp	ReuseTm	HalfL	ReuseV	SuppV	MaxSTm	MaxP	Restart
0	0	FALSE	0	30	1500	1000	100	15119	0

常见错误

- 在三层交换机下配置，接口必须先 **no swithport**，转为路由口后才能配置。

8.5 监视与维护

清除各类信息


作用	命令
清除接口的统计信息。	clear counters

clear counter 命令相关说明请参考“接口”命令的相关章节。

查看运行情况

作用	命令
显示被惩罚的接口统计信息。	show dampening interface
显示接口 IP Event Dampening 配置情况。	show interfaces dampening

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

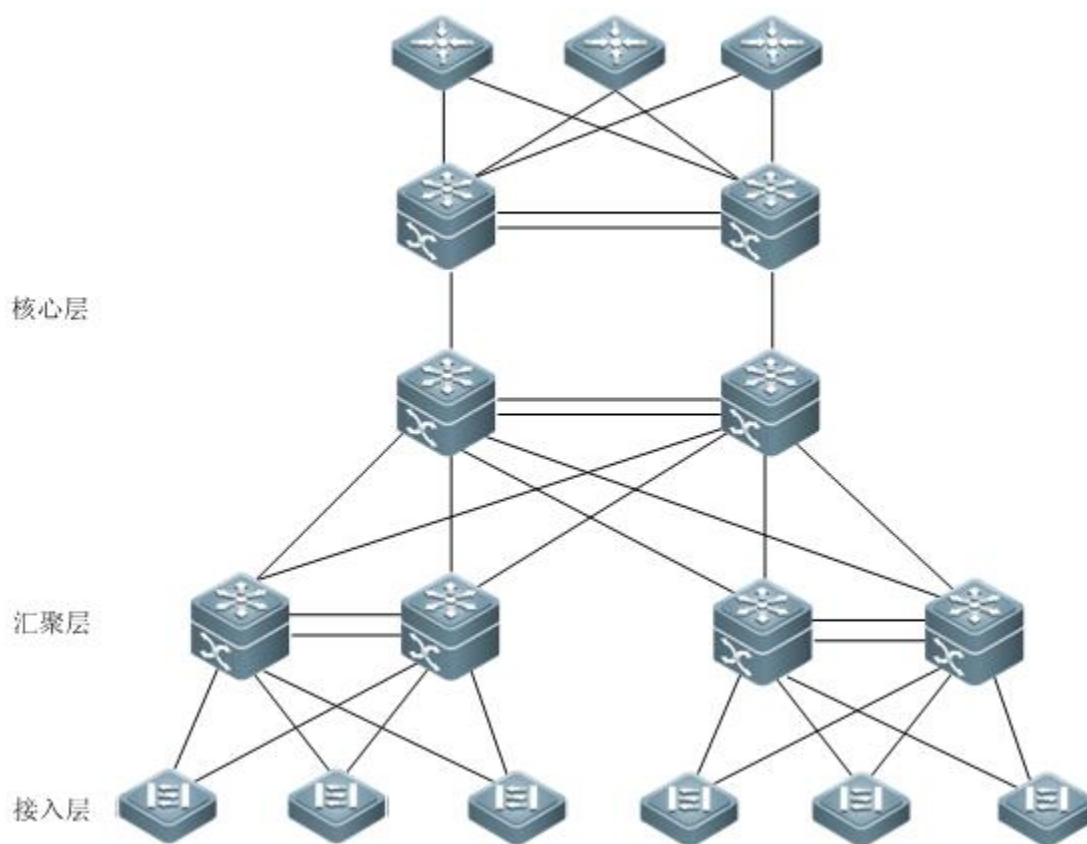
作用	命令
打开 Dampening 功能的调试开关。	debug dampening interface

9 VSU

9.1 概述

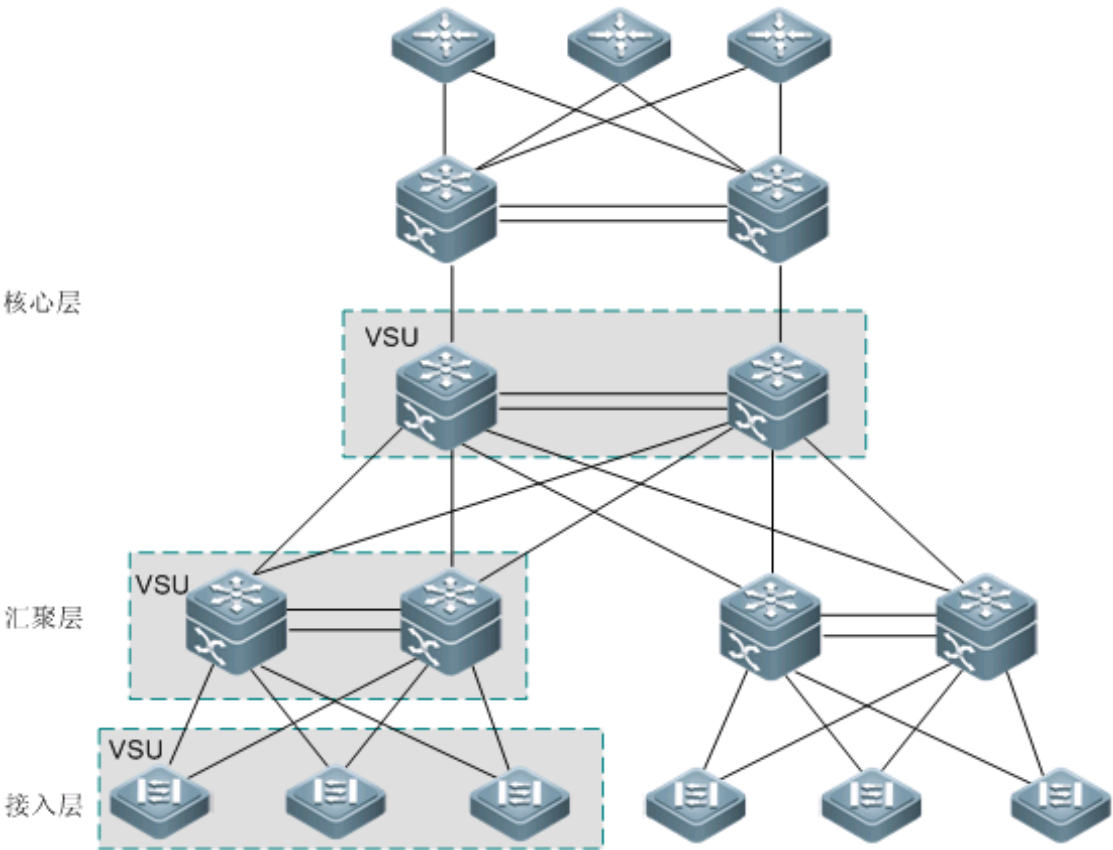
传统的网络中，为了加强网络的可靠性，一般在将核心层和汇聚层配置成双设备，起冗余备份作用，邻居设备分别连接两条链路到双设备上。下图显示的就是这样的一种典型的传统网络架构。冗余的网络架构增加了网络设计和操作的复杂性，同时大量的备份链路也降低了网络资源的利用率，减少了投资回报率。

图 9-1 传统网络结构



VSU(Virtual Switching Unit)是一种网络系统虚拟化技术，支持将多台设备组合成单一的虚拟设备。如下图所示，接入、汇聚、核心层设备都可以组成 VSU，形成整网端到端的 VSU 组网方案。和传统的组网方式相比，这种组网可以简化网络拓扑，降低网络的管理维护成本，缩短应用恢复的时间和业务中断的时间，提高网络资源的利用率。

图 9-2 端到端的 VSU 组网方案



协议规范

- -

9.2 典型应用

典型应用	场景描述
多台设备统一管理	多台物理设备组成一台逻辑设备，统一管理。
简化网络结构	VSU 看做一台逻辑设备，简化网络结构。

9.2.1 多台设备统一管理

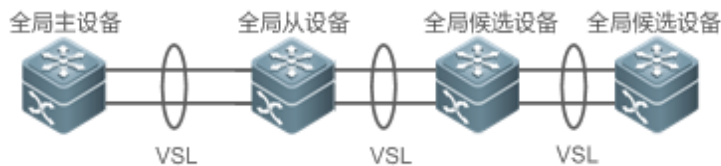
应用场景

当多台物理设备组成 VSU 时，可以看成一台逻辑设备。所有的配置都在全局主设备上管理。

以下图为例四台设备(设备编号从左到右，依次编号为 1、2、3、4)组成 VSU，设备 1 是全局主设备，设备 2 是全局从设备，设备 3 和设备 4 为全局候选设备。

- 对所有设备的管理只要在全局主设备上配置

图 1-3



【注释】 上图设备从左到右，编号依次为 1、2、3、4

VSL 见 1.3.1 描述

设备 1 为全局主设备

设备 2 为全局从设备

设备 3,4 为全局候选设备

功能部署

- 全局主设备负责控制整个 VSU 系统，运行控制面协议并参与数据转发；
- 全局从设备参与数据转发，并不运行控制面协议，并且作为备份当全局主设备发生故障接替全局主设备工作；
- 全局候选设备参与数据转发，并不运行控制面协议。当全局从设备发生故障时，全局候选设备可以接替全局从设备工作，此时设备角色也由此变成全局从设备，全局候选设备不能接替全局主设备工作，因此当全局主设备和全局从设备发生故障，VSU 系统会重启。

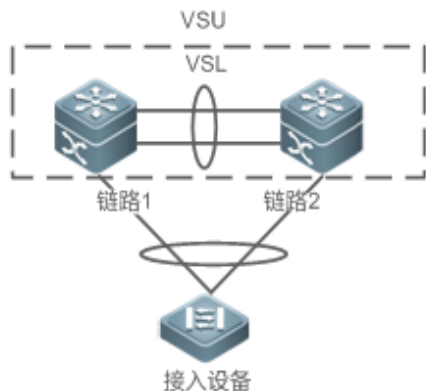
9.2.2 简化网络结构

应用场景

如图 1-1 传统网络中，为了增加网络组网的可靠性，需要增加设备和线路冗余，然而为了防止环路，需要引进许多防止环路的算法。导致网络的组网复杂。VSU 系统中，所有的设备认为是一台逻辑设备。设备之间可以互为备份，不需要引入防止环路算法，就可以简单的组网。

- 两台汇聚交换机组成 VSU。不需要配置防环路算法，两台设备可以互相冗余。
- 接入交换机，通过上联 AP 接入到汇聚交换机。
- 当 VSU 中一台设备出现故障，另一条链路还可以正常工作。

图 1-4



功能部属

- 全局主设备负责控制整个 VSU 系统，运行控制面协议并参与数据转发；
- 全局从设备参与数据转发，并不运行控制面协议，并且作为备份当全局主设备发生故障接替全局主设备工作；
- 接入设备面向用户，用于用户设备的接入。

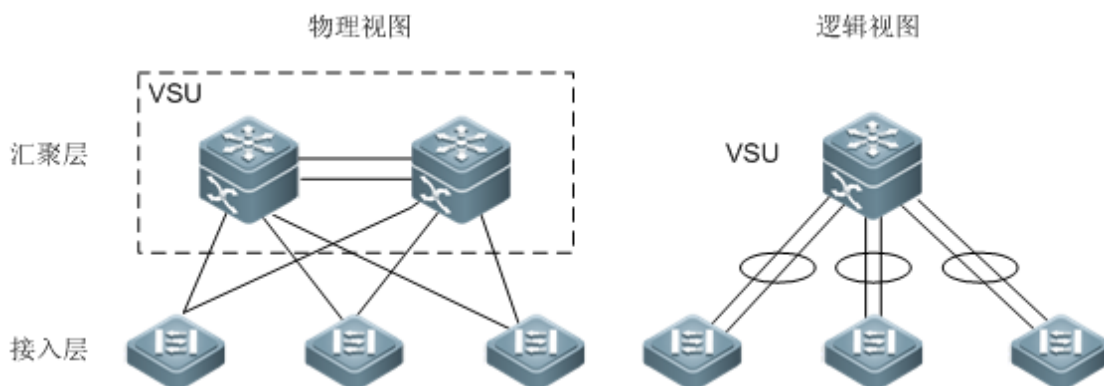
9.3 功能详解

基本概念

VSU 系统

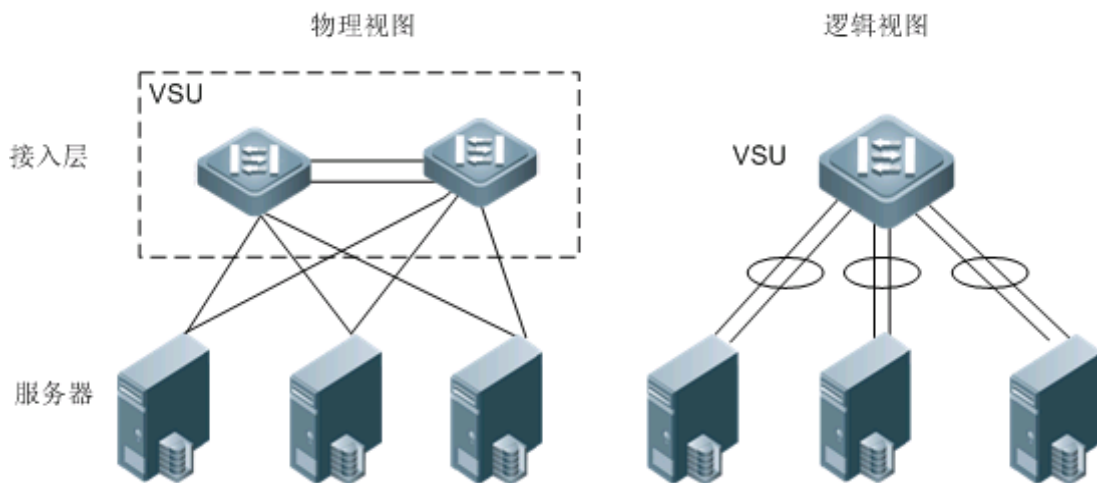
VSU 系统是由传统网络结构中的两台冗余备份的双设备组成的单一的逻辑实体，例如位于下图的汇聚层的 VSU 系统可以看作单独的一台交换机与接入层进行交互。

图 9-5 汇聚层的 VSU



上图的 VSU 网络结构中，成员之间通过内部的链路组成逻辑实体，接入层设备通过聚合链路与 VSU 建立接入到汇聚层。这样在接入层和汇聚层之间避免了二层环路。

图 9-6 接入层的 VSU



除了核心、汇聚层设备外，接入层设备也可以组成 VSU 系统。对于接入可用性要求高的服务器，一般使用“单服务器多网卡绑定为 Aggregate Port 口(简称 AP 口)”技术来与接入层设备相连。由于 AP 要求只能接入在同一台接入设备上，所以单台设备故障的风险增加了。在这种情况下，可以应用 VSU 解决这个问题。在 VSU 模式下，服务器可以使用多网卡绑定为 AP 口，连接同一个 VSU 组内不同的成员设备，这样可以防止接入设备的单点失效，或是单条链路失效导致的网络中断。

VSU 域标识

VSU 域具有唯一标识 Domain ID。只有同一个域标识的设备才能组合在一起形成同一个 VSU 系统。

成员设备编号

VSU 系统的每个成员设备都拥有唯一的编号，即 Switch ID。这个编号用于管理成员设备，以及配置成员设备上的接口等用途。用户在将设备加入 VSU 系统时需要配置该编号，并且保证成员设备编号在同一个 VSU 系统中是唯一的。VSU 系统如果发现成员设备编号冲突，根据优先级保留一台设备。

成员设备角色

VSU 系统由多台设备构成，在组建 VSU 系统时，多台设备通过一定的竞选协议选举出一台全局主设备，在支持 1:N 热备下其余为全局从设备。在支持 1:1 热备下，一台为全局主设备，一台为全局从设备，其余为候选设备。

全局主设备负责控制整个 VSU 系统，运行控制面协议并参与数据转发；其余的设备仅参与数据转发，并不运行控制面协议，所有接收到的控制面数据流都将转发给全局主设备进行处理。

全局从设备同时还实时同步接收全局主设备的状态。与全局主设备构成 1:1 或 1:N 热备份。在全局主设备失效后，全局从设备将切换成全局主角色，来管理整个 VSU 系统。

VSU 系统的主机选举方法为：

28. VSU 系统的主机选举规则如下（如果根据上一条规则不能决定主机，则根据下一条规则继续判断）：
a) 当前运行的主机最优先选为主机（起机时所有设备都不是主机）。
b) 优先级高的成员设备选为主机。
c) 设备号小的优先为主机。
d) MAC 地址小的成员设备选为主机。

29. 在 1:N 热备下，选择从机的时候，优先选择与主机相近的设备为从机，这样可以尽量避免产生双主机，选择从机的条件排序为：最靠近主机/优先级/MAC 地址。
30. VSU 系统支持设备的热加入。即使热加入设备的优先级比当前运行的 VSU 系统主机和从机优先级高，系统也不会进行主、从角色切换。
31. 成员设备的启机顺序可能会影响主机的选举。部分成员设备可能由于启机慢（目前 VSU 系统中，在 5 分钟内没有发现邻居就直接收敛），而没有及时加入 VSU 系统。在这种情况下，该成员设备将做热加入处理，即使优先级比当前运行的 VSU 系统主机高，系统也不会发生角色切换。

功能特性

功能特性	作用
虚拟交换链路	VSU 系统内，用于连接各个设备的虚拟路径。
拓扑	介绍 VSU 系统内连接的拓扑结构。
多主机检测	避免同一个 VSU 域中存在多台主机并存的现象。
VSU 设备外部连接	介绍外部设备与 VSU 设备相连可能出现的状况。
系统管理	用于管理 VSU 系统内部的设备。

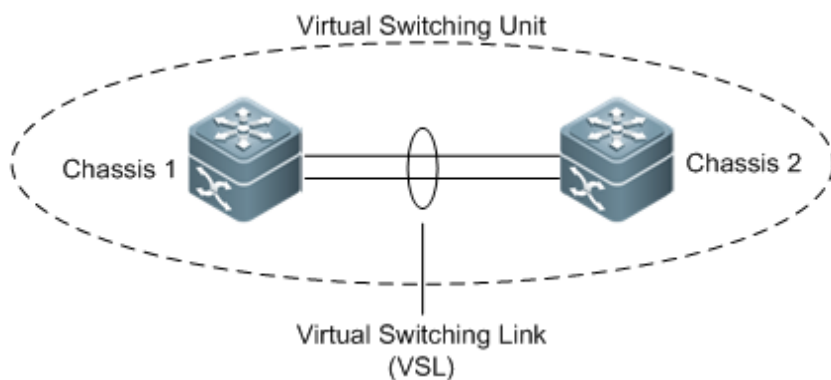
9.3.1 虚拟交换链路

工作原理

📌 VSL 链路

由于 VSU 系统的多台设备作为一个网络实体，因此它们之间需要共享控制信息和部分数据流。虚拟交换链路(Virtual Switching Link，简称 VSL；为方便叙述，下文出现的“虚拟交换链路”均以“VSL”表示)是 VSU 系统的设备间传输控制信息和数据流的特殊链路，目前支持在两台设备间通过万兆接口间建立虚拟交换链路(VSL)。虚拟交换链路在 VSU 系统内的位置如下图所示：

图 9-7 虚拟交换链路



VSL 以聚合端口组的形式存在，由 VSL 传输的数据流根据流量平衡算法在聚合端口的各个成员之间就进行负载均衡。

📌 VSL 链路流量

VSL 链路在设备间传输的控制流分为以下几种情况：

- 成员设备接收到的协议报文，需要通过 VSL 链路转发到全局主设备进行处理。
- 经过全局主设备处理的协议报文，需要通过 VSL 链路转发到其他成员设备的接口，由该接口发送该协议报文到对端设备。

VSL 链路在设备间传输的数据流分为以下几种情况：

- VLAN 内泛洪的数据流。
- 需要跨设备转发的数据流，需要通过 VSL 链路传输。

另外 VSL 链路上也传输 VSU 系统内部的管理类报文，例如热备份交换的协议信息，主机向其他成员设备下发配置信息的报文等等。

i 对于镜像(SPAN)功能，VSL 链路关联的接口既不能作为 SPAN 的源口，也不能作为 SPAN 的目的口。

📌 VSL 链路故障

如果 VSL 聚合端口组的某一成员链路发生故障，VSU 将自动调整 VSL 聚合端口的配置，使得流量不再从故障的成员链接传输。

如果 VSL 聚合端口组的所有成员链路都断开，VSU 拓扑将会发生变化。如果原先是环形拓扑，那么将会发生“环转线”，具体情况请“参考拓扑”变化章节的拓扑环线互转部分。

📌 VSL 口错帧检测

当 VSL 口上出现大量的连续的错帧的时候，需要禁用该端口，切换到其他的 VSL 口中。采用下面的检测方式：

VSL 口上会有错帧，需要进行错帧校正。默认每 5 秒检查一次 vsl 口，如果和上次比较，错帧个数大于 num 则认为是一次错帧，连续 times 次的话，则认为端口异常。在存在多条 vsl 链路的时候，如果发生错帧，vsl 链路会切换。最后一条 vsl 链路，为了防止拓扑分裂，链路不进行切换。

不同用户场景对 num 和 times 要求不一样，默认值 num 为 3，times 为 10 次。用户场景要求严格的这两个值取小值，如果比较宽松需要取大值。

9.3.2 拓扑

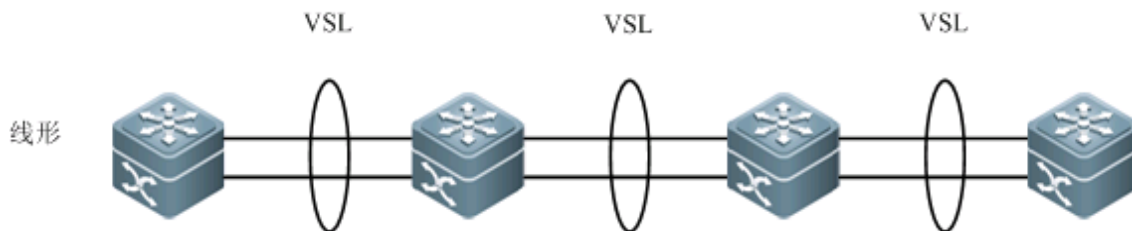
VSU 系统支持线形和环形两种拓扑结构。设备间通过 VSL 链路相连，形成一条线，所以称为线形拓扑。

工作原理

📌 拓扑结构

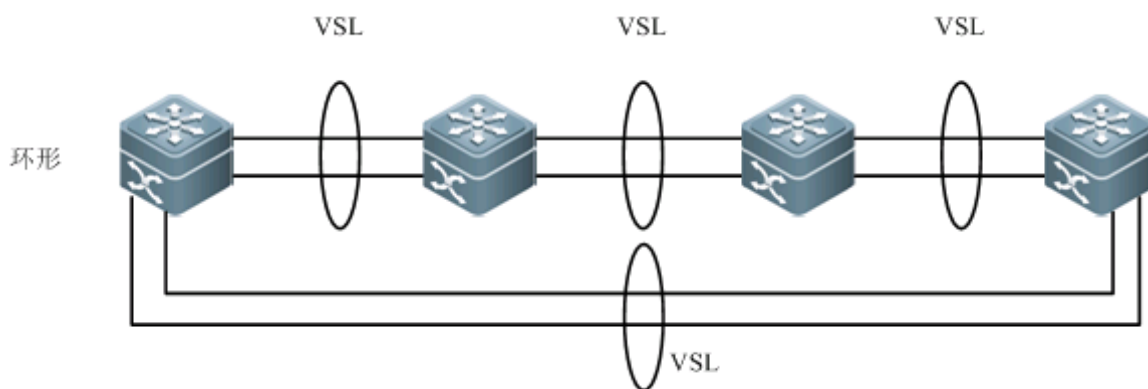
线形拓扑连接简单，使用较少的端口和线缆，但设备间只有一条通信链路，所以 VSL 链路的可靠性较低。

图 9-8 线形拓扑



除了线形拓扑外，如图所示，设备还可以组成环形拓扑，这样设备间的两条通信链路可以相互备份，形成链路冗余，提高 VSU 系统的可靠性。

图 9-9 环形拓扑



- ❗ 用户在选择 VSU 系统的拓扑时，应尽量选择环形拓扑，这样能保证任何单台设备失效、或是任何单条 VSL 链路失效都不会影响整个 VSU 系统的正常运行。
- ❗ 除了选择环形拓扑组网，建议每个 VSL-AP 中配置多根 VSL 链路，以提高单个 VSL-AP 的可靠性。建议最少配置两根链路，最大可以配置 4 根链路。合理的配置是 2 根以上 vsl 链路，并且是跨线卡。

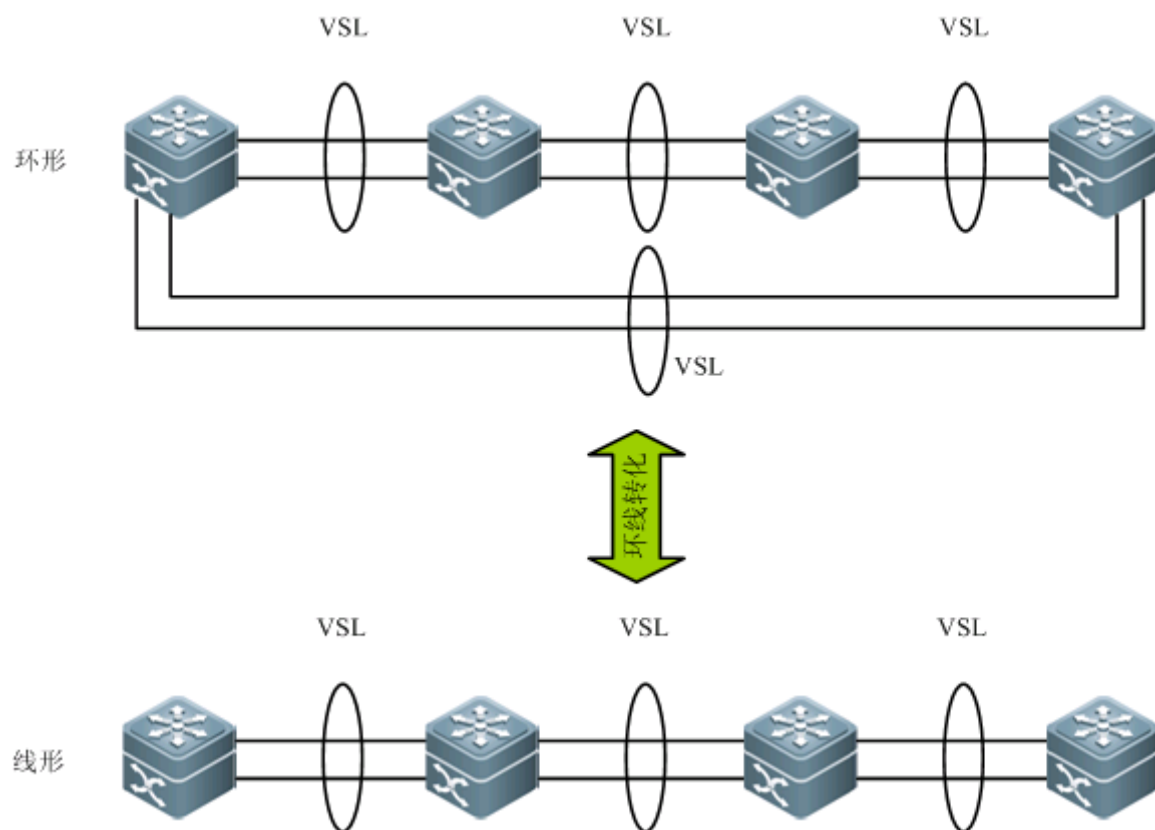
拓扑收敛

在 VSU 系统建立之前，成员设备间需要通过拓扑发现协议来发现邻居，最终确定 VSU 系统中有哪些设备，从而确定管理域的范围。然后选举出一台全局主设备来管理整个 VSU 系统，接着再选举出一台全局从设备作为主设备的备份。到此，整个 VSU 系统的拓扑已经收敛。由于不同的设备的启动时间有所不同，所以拓扑的首次收敛时间也有所不同。

拓扑环线互转

对于环形拓扑，当其中一条 VSL-AP 链路断开时，拓扑将由环形转成线形。这时整个 VSU 系统仍然能够正常工作，不会造成网络的中断。但为了避免其他的 VSL-AP 链路失效、或节点失效，此时应该要及时去排查 VSL 链路故障，将 VSL 链路恢复。VSL-AP 链路恢复后，拓扑将由线形再转回到环形。

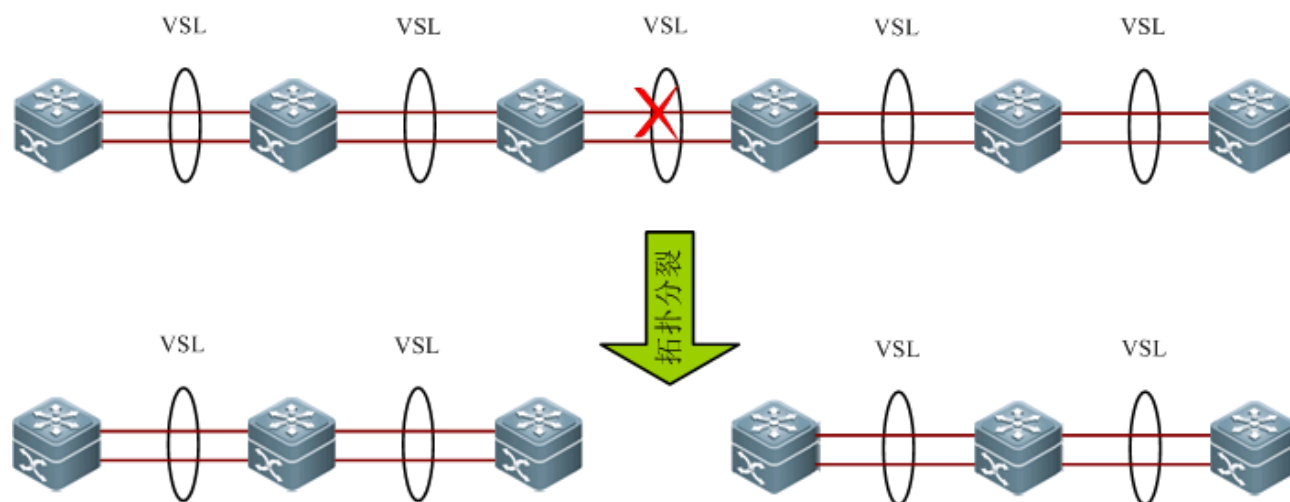
图 9-10 环转线、线转环



拓扑分裂

对于线形拓扑，如果 VSL-AP 链路断开时，拓扑将会发生分裂，如下图所示，一个 VSU 组分裂成两个 VSU 组。这种情况下，可能会导致网络中出现两台配置完全相同的设备，从而令网络无法正常工作。这种情况下需要通过部署多主机检测功能（详见 1.1.4.6 节多主机检测）来解决拓扑分裂问题。

图 9-31 拓扑分裂



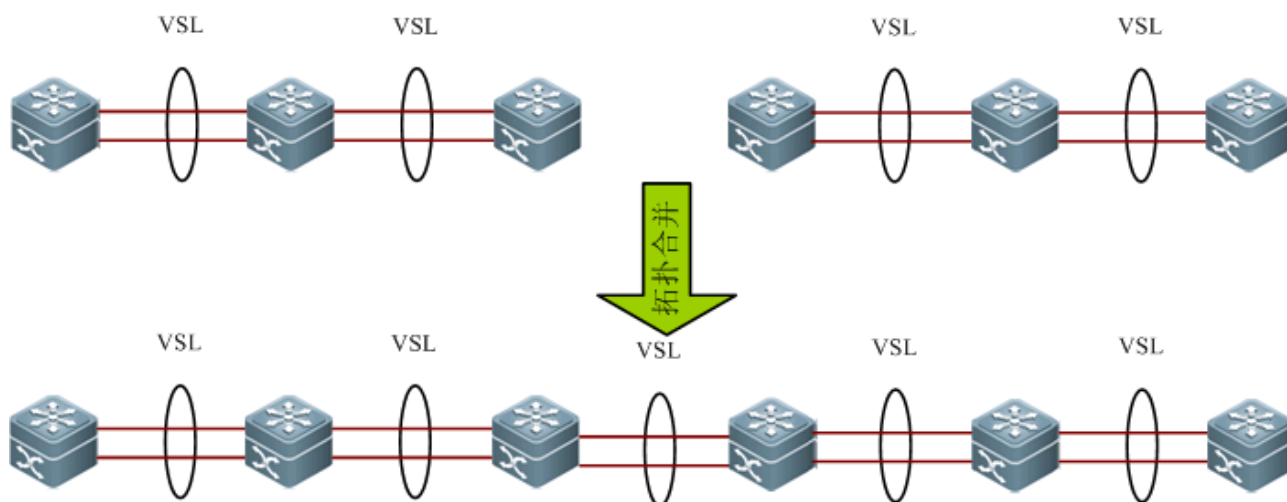
拓扑合并

domain 一致的两个 VSU 组通过 VSL-AP 链路连接，将会发生拓扑合并。在拓扑合并过程中，会重启其中一个 VSU 组，然后热加入另一个 VSU 组。

拓扑合并的原则是：最大限度的降低拓扑合并时对业务所带来的影响。其合并规则如下（从第一条开始判断，如果本条无法选出最优拓扑，继续判断下一条）：

- 用户配置为最高条件，按一堆 VSU 某台设备最高优先级高的那一堆 VSU 保留。
- 上述不能判断，swid 小(以两个全局主为准)的胜出。
- 上述不能判断，以 mac 地址小的保留(以两个全局主为准)。

图 9-12 拓扑合并



i 当两个 VSU 组进行拓扑合并时，需要进行竞选，竞选失败的一方将逐一自动重启并热加入到另一个 VSU 组。

9.3.3 多主机检测

工作原理

当 VSL 断开时，从设备切换成主设备，如果原来的主设备还在运行，那么两台设备都是主角色，由于配置完全相同，在局域网中会引起 IP 地址冲突等一系列问题。在这种情况下，VSU 系统必须检测双主机，并且采取恢复措施。VSU 支持使用两种方式进行多主机检测：

- 基于 BFD 检测
- 基于聚合口检测

多主机检测规则

- 1、一个 VSU 组中优先级高的胜出。
- 2、上述不能判断时，一个 VSU 组中物理设备台数多的胜出。

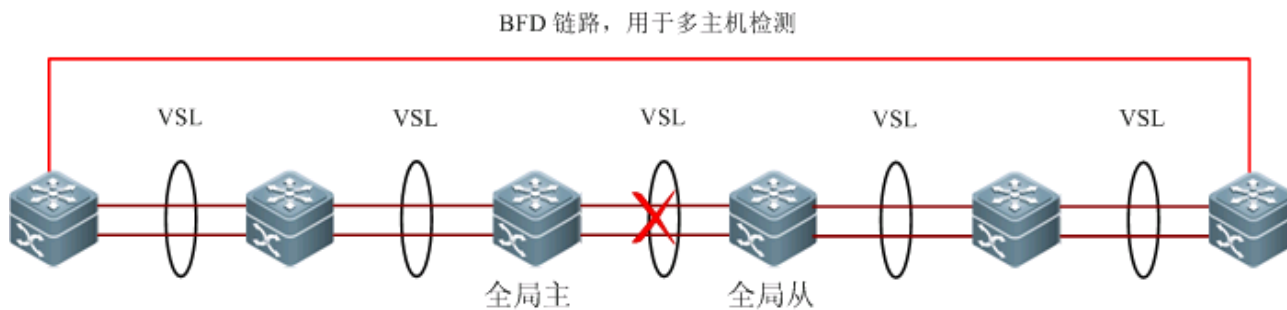
- 3、上述不能判断时，一个 VSU 组中健康度高的胜出。（健康度定义：本拓扑内 UP 的物理端口带宽总和，管理口和 VSL 口除外。）
- 4、上述不能判断时，以两个全局主中 swid 小的胜出。
- 5、上述不能判断时，两个全局主以 mac 地址小的保留。
- 6、上述不能判断时，两个全局主以起机时间大的保留。

! 如果未配置双主机检测，在拓扑分裂后会造成网络中断。

基于 BFD 检测

VSU 支持使用 BFD(Bidirectional Forwarding Detection)检测多主机情况。其拓扑连接如图所示。两个边缘设备增加一条链路，专门用于多主机检测。当全局主和全局从之间的 VSL 链路断开，此时会产生两个主机，如果配置了 BFD 双主机检测功能，则两个主机之间通过 BFD 链路互相发送 BFD 双主机检测报文，从而检测到当前有相同的两个主机存在，最后通过一定的规则（同 1.1.4.4 拓扑合并规则）将其中一个主机所在的 VSU 系统关闭，使其进入 recovery 状态，避免网络异常。

图 9-13 基于 BFD 的多主机检测



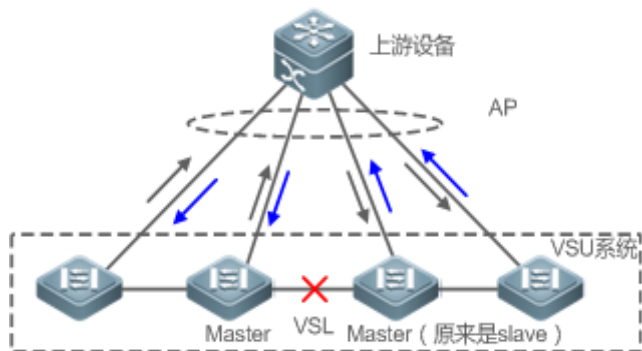
! 只有一对 BFD 检测链路时建议将检测链路部署在拓扑的两端。

! BFD 检测采用扩展 BFD，不能通过现有 BFD 的配置与显示命令配置双主机检测口。

基于聚合口检测

VSU 还支持使用聚合口检测双主机的机制，其连接拓扑如下图所示。在 VSU 系统和上游设备上，都需要支持聚合口多主机检测功能，当发生 VSL 端口断开后，产生两个主机，两个主机向聚合口的每个成员口发送检查报文，检测报文通过上游设备进行中转，到另一个主机。如下图所示，聚合口共有四个成员口，每个成员口连接在 VSU 系统的四个不同设备上，当发生分裂时，四个成员口都会发送和接受检测报文，从而检测到当前有相同的两个主机存在，最后通过一定的规则（同 1.1.4.4 拓扑合并规则）将其中一个主机所在的 VSU 系统关闭，使其进入 recovery 状态，避免网络异常。

图 9-14 聚合口的上下游方式多主机检测



✓ 以上拓扑中，上游设备必须为锐捷设备，该设备需要支持检测报文的转发。

9.3.4 VSU 流量转发

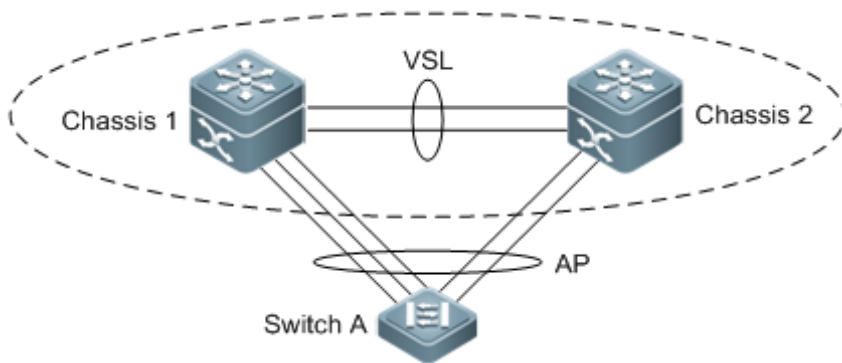
工作原理

跨设备聚合端口组

AP 把多个物理链接捆绑在一起形成一个逻辑链接。VSU 系统支持跨成员设备的 AP。

如下图所示，两台设备组成 VSU 组，外部的接入设备 Switch A 以 AP 的形式链接到 VSU，对于 Switch A 来说，图中的 AP 连接与普通的聚合端口组没有区别。

图 9-15 跨设备聚合端口



故障处理

建议配置跨设备 AP 时，外围设备与 VSU 的每台设备之间均有物理链接。一方面，这可以保留 VSL 链路的带宽(跨机箱 AP 流量优先选择同一机箱的 AP 成员作为出口，避免不必要的流量通过 VSL 链路传输)；另一方面，可以提高网络的可靠性(如果某一机箱发生故障，属于正常设备的成员接口还可以正常工作)。

以下描述跨设备 AP 可能的失败情形及导致的影响：

- 单条链路发生故障

如果跨设备 AP 的单条链路发生故障而其它链路仍然正常工作，则跨设备 AP 在剩余的正常链路之间重新分配流量。

- 全局主设备上的所有跨设备 AP 成员口链路发生故障

如果全局主设备上的所有跨设备 AP 成员口链路发生故障，则只有其它成员设备的成员口继续工作。由该 AP 进入 VSU 系统的数据流，如果数据流的转发出口在全局主设备上，则系统通过 VSL 链路转发到全局主设备对应的出口。

由于控制面协议仍然运行在全局主设备，所以进入 VSU 系统的协议报文通过 VSL 链路转发到全局主设备进行协议运算。

- 与其他成员设备的所有链路发生故障

如果跨设备 AP 与单台成员设备 A 的所有链路发生故障，则只有其它成员设备的成员口继续工作。由该 AP 进入 VSU 系统的数据流，如果数据流的转发出口在成员设备 A 上，则系统通过 VSL 链路转发到成员设备 A 对应的出口。

- 所有链路发生故障

如果跨设备 AP 的所有链路发生故障，与普通 AP 的处理相同，接口的状态变为 Link-Down。

- 全局主设备整机故障

如果主设备整机发生故障，将导致热备份切换，原来的从设备切换为主设备。同时，其它成员设备上的成员口继续工作。通过该 AP 与 VSU 相连的对端设备将检测到链路故障，调整流量平衡算法，将数据流分配到正常的链路。

- 其它成员设备整机故障

如果成员设备整机发生故障，连接在该成员设备的 AP 成员链路将断开，但其他成员链路照常工作。通过该 AP 与 VSU 相连的对端设备将检测到链路故障，调整流量平衡算法，将数据流转发路径分配到正常的链路。

▾ 流量均衡

在 VSU 系统中，流量可能有多个出口。AP 和 ECMP 有各自的流量均衡算法，比如同目的 mac 或者源 mac 等方式，具体可以参见 AP 和 ECMP 的配置手册。在本配置手册中，可以配置本地优先转发，本设备收到的报文优先在本设备转发，这样报文可以不通过 VSL 链路转发到其他设备中。

9.3.5 系统管理

工作原理

▾ 控制台访问

VSU 系统主设备的控制台同时管理系统内的多台设备。从设备、候选设备的控制台不支持命令行输入。但用户可以在主机上对指定成员设备进行 VSU 相关的配置，也可以通过从机的串口登录到主机的控制台。可以利用 session 重定向到某个设备的主管理板。

▾ 线卡命名

对于机箱式设备，在 VSU 模式下，线卡的编号命名中加入了设备编号(Switch ID)，即线卡的编号由一维变两维，如线卡 1/1，表示编号为 1 的成员设备上的 1 槽位的线卡。

▾ 接口命名

VSU 工作模式下，由于同一个插槽号可能分别出现在多台设备内，所以接口的命名方式中加入了设备编号(Switch ID)。

例如：interface gigabitEthernet 1/1/1 表示 ID 为 1 的设备插槽 0 上的千兆端口 1；interface gigabitEthernet 2/1/2 表示 ID 为 2 的设备插槽 0 的千兆端口 2。

访问文件系统

VSU 工作模式下，可以从主设备上访问其他成员设备上的文件系统。具体方式和访问本地文件系统相同。唯一不同的是使用不同的 URL 前缀。

系统升级

VSU 系统通常情况下要求成员设备主程序版本号一致,然而成员设备众多,按照单机模式逐一升级，不仅费时费力，而且容易出错.锐捷交换机提供了完善的系统升级方案,使您能够使用如下两种方法轻松完成系统升级。

- VSU 系统建立时：系统会自动匹配所有成员设备的主程序版本号,当发现主程序版本不一致时，其会选择主设备上的主程序同步到所有成员设备。
- VSU 系统建立后：可以通过 TFTP 下载的文件将自动的同步到所有成员设备。

SYSLOG

VSU 系统的所有成员设备都可以打印 SYSLOG。主机产生的 SYSLOG 直接在主机控制台上打印，且格式和单机情况下是完全一样的；其它成员设备的 SYSLOG 也在主机控制台上打印，但消息格式与单机不同，相比之下增加了设备编号信息。

例如：单机产生的 SYSLOG 信息是：“%VSU-5-DTM_TOPO_CVG: Node discovery done. Topology converged.” 那么由编号为 3 的成员设备产生的 SYSLOG 信息应该就是：“%VSU-5-DTM_TOPO_CVG:(3) Node discovery done. Topology converged.”

9.3.6 快闪搜索功能

在网络布线环境中，常常存在交换机所在的机房与操作的控制台不在一处的情况。当环境中设备较多时，网络管理人员对设备具体位置的定位就存在了困难。

快闪搜索功能给网络管理人员提供了一种闪烁定位设备的方法。在控制台上操作指定设备的 status 灯快闪，再到机房中就可以很方便地找到对应的设备。



快闪搜索功能打开期间，原 status 灯状态无法显示。直至快闪搜索被关闭，才可以显示 status 灯状态。

9.4 产品说明



每台设备至少指定一个万兆口作为 VSL 链路的成员端口。

两台设备的 VSL 成员端口之间的连接方式：通过 SFP+模块+光纤线缆或者铜缆的方式进行连接。

配置 VSL 口的时候，不需要配置 VSL AP，VSL AP 自动协商。

VSL 心跳检测不允许配置。

千兆以下端口不能作为 VSL 口。

产品名称	堆叠模块	普通端口	线性拓扑	环形拓扑	成员设备最大数量
------	------	------	------	------	----------

S6000E 系列	不支持	支持	支持	支持	8
-----------	-----	----	----	----	---



在 S6000E 设备上，为了防止在多条 BFD 检测线时候，用户连接错误，BFD 检测口检测配置，不需要配置成一对，只需要单个配置。



采用聚合口进行双主机检测是，上游设备必须为锐捷设备，该设备需要支持双主机检测报文的转发。目前 S6000E 设备支持转发功能。

9.5 配置详解

配置项		配置建议 & 相关命令	
单机模式下配置 VSU 参数		 必选。用于配置单机模式下的 VSU 参数。	
		switch virtual domain	配置域 ID
		switch	配置设备在虚拟设备中的编号
		switch priority	配置设备的优先级
		vsl-port	进入 VSL 端口配置模式
		port-member interface	把普通口配置到 VSL 端口池中
		switch convert mode virtual	单机模式切换到 VSU 模式
		 可选。用于配置 VSU 模式下的设备属性。	
		switch description	配置设备的别名
		switch crc	错帧配置
VSU 模式下配置 VSU 参数	配置 VSU 属性	 可选。用于配置 VSU 模式下的设备属性。	
		switch domain	更改机箱域 ID
		switch renumber	更改设备编号
		switch description	配置设备别名
		switch crc	错帧配置
	配置 VSL 链路	 可选。用于配置虚拟交换链路。	
		vsl-port	进入 VSL-PORT 模式
		port-member interface	配置 VSL-AP 成员口
	配置双主机检测	 必选。用于配置双主机检测功能。	
		dual-active detection	配置双主机检测
		dual-active bfd interface	配置 BFD 检测接口
		dual-active interface	将聚合口配置为双主机检测口
		dual-active exclude interface	配置例外端口
	配置流量平衡	 可选。用于配置 VSU 模式下的流量平衡功能。	

		switch virtual aggregateport-lff enable	配置 AP 本地转发优先模式
		switch virtual ecmp-lff enable	配置 ECMP 本地转发优先模式
	配置 recovery 模式的恢复方式	⚠ 可选。用于配置 recovery 模式下的设备恢复方式。	
		recovery auto-restart enable	开启 recovery 模式下自动重启恢复
	配置从 VSU 模式切换到单机模式	⚠ 可选。用于将设备从 VSU 模式切换到单机模式。	
		switch convert mode standalone	从 VSU 模式切换到单机模式
快闪搜索	⚠ 可选。用于快速定位设备。		
	led-blink	开启/关闭快闪搜索功能	

9.5.1 单机模式下配置 VSU 参数

配置效果

将设备在单机模式下启动，配置 VSU 相关的参数。以用于组建 VSU 系统。

注意事项

-

配置方法

配置方法配置 VSU 属性

- 交换设备缺省以单机模式启动，用户需要构建 VSU 系统的两台机箱上配置相同的域 ID(domain ID)，虚拟设备号取值范围在局域网内域 ID 必须是唯一的。用户还需要配置每台机箱在虚拟设备中的编号。
- 首先使用命令 **switch virtual domain domain_id**，配置域 ID，该命令必选；
- 使用 **switch switch_id** 命令配置设备在虚拟设备中的编号，该命令必选；设备在 VSU 系统内编号越大，则在相同的设备优先级情况下，编号越小的优先选为全局主设备。
- 使用 **switch switch_id priority priority_num** 命令配置设备的优先级，该命令必选。
- 取值范围为 1 到 255，数值越大优先级越高。
- 使用 **switch switch_id description switch1** 命令配置设备的别名，该命令可选。默认名字为 Ruijie，为便于网络环境中设备的区分，希望标示设备别名的可选择此配置项。
- 最大 32 个字符。

【命令格式】 **switch virtual domain number**


【参数说明】 **number** : VSU 的虚拟域编号。

- 【缺省配置】 缺省域编号为 100。
- 【命令模式】 全局配置模式
- 【使用指导】 域编号相同的两台设备才能组合成一台虚拟设备，域编号在局域网内必须唯一。

- 【命令格式】 **switch** *switch_id*
- 【参数说明】 *switch_id*：设备在 VSU 内的编号，取值范围根据不同的产品而定。
- 【缺省配置】 缺省设备编号是 1。
- 【配置模式】 config-vs-domain 配置模式
- 【使用指导】 设备编号用来在虚拟设备中标识每个成员，在 VSU 模式下，接口名称的格式从 “slot/port” 转换为 “switch/slot/port”，其中 “switch” 就是接口所属交换机的编号。
- 在选举主设备的过程中，如果两台设备都已经是主设备，或者都是刚启动还没有确定角色，并且两台交换机的优先级相同，那么编号小的设备成为主设备。
- 该命令只能在单机模式下修改交换机编号，VSU 模式下需要通过 **switch** *switch_id* **renumber** *new_switch_id* 修改交换机编号。无论是单机模式，还是 VSU 模式，修改的编号需要重新启动才能生效。

- 【命令格式】 **switch** *switch_id* **priority** *priority_num*
- 【参数说明】 *switch_id*：需要配置优先级的交换机编号。
- priority_num*：对应交换机的优先级，取值范围是 1 到 255。
- 【缺省配置】 *priority_num*：缺省的优先级是 100。
- 【配置模式】 config-vs-domain 配置模式
- 【使用指导】 优先级的数值越大，表示优先级越高。在选举主设备的过程中，优先级高的设备成为主设备。
- 该命令在单机模式和 VSU 模式都可以使用。修改的优先级必须重启以后才会生效。
- 该命令不会修改 *switch_id*。单机模式下如果配置了 *switch_id* 为 1，再执行 **switch** 2 **priority** 200，则命令不会生效，除非先将设备的 *switch_id* 修改为 2，再执行 **switch** 2 **priority** 200 才会生效。VSU 模式下，*switch_id* 表示当前运行的交换机编号，如果当前不存在该编号，则配置也不生效。

- 【命令格式】 **switch** *switch_id* **description** *dev-name*
- 【参数说明】 *switch_id*：需要配置别名的交换机编号。
- 【缺省配置】 -
- 【配置模式】 config-vs-domain 配置模式
- 【使用指导】 配置设备的别名，最大为 32 个字符（可选）。
- 该命令在单机模式和 VSU 模式都可以使用，VSU 模式下配置立即生效。

 配置优先级与别名的命令只会修改优先级，不会修改交换机编号。所以在配置时必须正确输入当前设备的编号。例如，当前已经配置交换机编号为 1，如果输入 **switch** 2 **priority** 100，则优先级配置不生效。

📌 配置 VSL 链路

- 为了组成 VSU 系统，还需要配置一些端口作为 VSL 成员端口。

- 使用 **vsl-port** 命令进入 vsl 端口配置模式，该命令必选。
- 使用 **port-member interface** *interface-name* [**copper** | **fiber**] 命令添加 VSL 端口，该命令必选。
- 当设备进入到 VSL-PORT 的配置模式时，可以配置或删除 VSL 口。

【命令格式】 **vsl-port**

【参数说明】 -

【缺省配置】 -

【配置模式】 config 配置模式

【使用指导】 该命令在单机模式和 VSU 模式都可以使用。

【命令格式】 **port-member interface** *interface-name* [**copper** | **fiber**]

【参数说明】 *interface-name*：二维接口名，如 Tengigabitethernet 1/1, Tengigabitethernet 1/3。

copper：电口属性。


fiber：光口属性。

【缺省配置】 -

【配置模式】 config-vsl-port 配置模式

【使用指导】 添加 VSL-AP 链路的成员端口。*interface-name* 为单机模式下的二维端口名称，可以为万兆口，也可以为千兆口（千兆口可以为光电复用口，如果不指定介质类型，则默认为千兆电口）。对于光电复用口，必须指定其光电属性。箱式设备 VSL 口必须是万兆口。

该命令可以在 VSU 模式下，也可以在单机模式下。命令配置后需要保存配置，并重启 VSL 成员端口所在设备才能生效。

 单机模式下，VSL 端口的配置不能立即生效，需要转化为 VSU 模式重新启动后才能生效。

错帧配置

- 使用 **switch crc** 配置错帧，该命令可选。选择此命令可以修改错帧的默认检查方式。
- VSL 口上会有错帧，需要进行错帧校正。默认每 5 秒检查一次 vsl 口，如果和上次比较，错帧个数大于 3 则认为是一次错帧，连续 10 次的话，则认为端口异常。在存在多条 vsl 链路的时候，如果发生错帧，vsl 链路会切换。最后一条 vsl 链路，为了防止拓扑分裂，链路不进行切换。

【命令格式】 **switch crc errors** *error_num* **times** *time_num*


【参数说明】 *error_num*：用于配置两次检查错帧递增个数（当大于这个数认为是一次错帧）

time_num：连续多少次后，采取的动作（动作为提示或关闭端口）

【缺省配置】 errors 缺省值为 3；times 缺省值为 10

【配置模式】 config-vs-domain 配置模式

【使用指导】 默认每 5 秒检查一次 vsl 口，如果和上次比较，错帧个数大于 3 认为一次错帧，连续 10 次，可以认为端口异常。对端口异常的处理是，默认是 log 提示，可以配置成关闭端口处理，如果关闭端口，需要插拔恢复。

 不同的产品对错帧检查要求不一样，对 vsl 口的处理也不一样。11.0 版本，错帧作为可以配置。

单机模式切换到 VSU 模式

- 使用 **switch convert mode virtual** 命令，将设备从单机模式切换到 VSU 模式。
- 单机模式下，执行以上命令后，软件自动进行如下动作：
 - 将单机模式下的各个 VSD 的全局配置文件 “config.text” 备份为 “vsd.standalone.text.vsd 序号”；
 - 清除各个 VSD 的全局配置文件 “config.text” 的内容；
 - 把 VSU 相关的配置写到特殊配置文件 “config_vsu.dat” 中。
- 如果交换设备上存在 “vsd.virtual_switch.text vsd 序号” 备份文件，则提示用户是否将备份文件的内容覆盖到对应 VSD 下 “config.text” (“vsd.virtual_switch.text.vsd 序号” 文件是交换设备从 VSU 模式切换到单机模式时对各 vsd 下的 “config.text” 的备份文件)，用户可选择 “yes” 或 “no”。选择 “yes” 使用 “vsd.virtual_switch.text.vsd 序号” 文件，替换对应 vsd 的 “config.text” 文件，如果选择 “no”，清空对应 vsd 的 “config.text” 文件。最后交换设备进行重启，读取 “config_vsu.dat” 中的 VSU 参数，以 VSU 模式进行启动。


【命令格式】 **switch convert mode virtual**

【参数说明】 -

【缺省配置】 缺省时设备处于单机模式。

【配置模式】 特权模式

【使用指导】 将设备从单机模式切换到 VSU 模式。

 如果当前交换设备已经在 VSU 模式，则不允许再次切换到 VSU 模式，即以上命令无效。

检验方法

通过 **show switch virtual config [switch_id]** 命令查看单机模式下当前交换设备的 VSU 配置。

【命令格式】 **show switch virtual config [switch_id]**

【参数说明】 *switch_id* : 设备编号，指定这个参数可以只显示特定设备的 VSU 配置信息。

【配置模式】 特权模式

【使用指导】 显示单机或 VSU 模式下的 VSU 配置信息

 由于 VSU 相关的配置是针对单个物理设备的，其配置信息存储在特殊配置文件 config_vsu.dat 中，因此 **show running config** 看不到 VSU 相关的配置信息，只能通过 **show switch virtual config** 来查看当前 VSU 的配置。

 单机模式下，VSU 运行信息全部空，用户敲入 **show switch virtual** 等命令时，则提示当前为单机模式，无 VSU 系统运行信息。

配置举例

❏ 单机配置举例

【网络环境】

图 9-16



Switch-1 及 Switch-2 组成 VSU，domain 域为 100，左边机箱配置成机箱号 1，优先级 200，别名 switch-1，上面有端口 1/1、1/2 为 VSL 口。右边机箱配置成机箱号 2，别名 switch-2，优先级 100，上面有端口 1/1、1/2 为 VSL 口。

【配置方法】

5. 在 Switch-1 机箱上配置：
 - 配置 VSU 属性、VSL 口。
 - 将单机模式转换成 VSU 模式。
6. Switch-2 机箱上配置：
 - 配置 VSU 属性、VSL 口。
 - 将单机模式转换成 VSU 模式。

Switch-1

```
Ruijie# configure terminal
Ruijie(config)# switch virtual domain 100
Ruijie(config-vs-domain)#switch 1
Ruijie(config-vs-domain)#switch 1 priority 200
Ruijie(config-vs-domain)#switch 1 description switch-1
Ruijie(config-vs-domain)# switch crc errors 10 times 20
Ruijie(config-vs-domain))#exit
Ruijie(config)#vsl-port
Ruijie(config-vsl-port)#port-member interface Tengigabitethernet 1/1
Ruijie(config-vsl-port)#port-member interface Tengigabitethernet 1/2
Ruijie(config)#exit
Ruijie#switch convert mode virtual
```

Switch-2

```
Ruijie# configure terminal
Ruijie(config)# switch virtual domain 100
Ruijie(config-vs-domain)# switch 2
Ruijie(config-vs-domain)# switch 2 priority 200
Ruijie(config-vs-domain)# switch 2 description switch-2
Ruijie(config-vs-domain)# switch crc errors 10 times 20
Ruijie(config-vs-domain))#exit
Ruijie(config)#vsl-port
Ruijie(config-vsl-port)#port-member interface Tengigabitethernet 1/1
Ruijie(config-vsl-port)#port-member interface Tengigabitethernet 1/2
Ruijie(config-vsl-port)#exit
Ruijie#switch convert mode virtual
```

【检验方法】

- 使用 **show switch virtual config** 命令查看 Switch-1、Switch-2 的 VSU 属性。

Switch-1

```
Ruijie#show switch virtual config
switch_id: 1 (mac: 0x1201aeda0M)
!
switch virtual domain 100
!
switch 1
switch 1 priority 100
!
switch convert mode virtual
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/2
!
switch crc errors 10 times 20
!
```

Switch-2

```
Ruijie#show switch virtual config
switch_id: 2 (mac: 0x1201aeda0E)
!
switch virtual domain 100
!
switch 2
switch 2 priority 100
!
switch convert mode virtual
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/2
!
switch crc errors 10 times 20
!
```

常见错误



在箱式设备中，VSL 口必须是万兆口以上的端口。

9.5.2 配置 VSU 模式下的功能

9.5.2.1 配置 VSU 属性

配置效果

设备组成 VSU 或 VSU 系统运行过程中，如果需要修改一些参数，用户可以登录到 VSU 系统的主机控制台上进行修改，从机控制台禁止进入全局配置模式。

注意事项

- 除 **switch switch_id description switch1** 命令立即生效外，其他配置命令只有在交换设备重启后才能生效。

配置方法

进入 domain 配置模式

- 可选配置。
- VSU 模式下使用该命令进入 domain 配置模式。只有相同域编号的交换机组成 VSU。VSU 模式下，只有进入 domain 配置模式，才能修改或配置域编号、设备优先级、交换机编号。

【命令格式】 **switch virtual domain domain_id**

【参数说明】 *domain_id*：VSU 的虚拟域编号。

【缺省配置】 缺省域编号为 100。

【命令模式】 全局配置模式

【使用指导】 域编号相同的两台设备才能组合成一台虚拟设备，域编号在局域网内必须唯一。

更改机箱域 ID

- 可选配置。
- 如果需要修改某设备的 *domain_id*，可在 VSU 系统的主机控制台上执行此配置项。

【命令格式】 **switch switch_id domain new_domain_id**

【参数说明】 *switch_id*：VSU 模式下当前运行的设备编号，取值范围为 1-8。

new_domain_id：修改后的 domain id，范围为 1-255。

【缺省配置】 *domain id* 缺省值为 100。

【命令模式】 config-vs-domain 配置模式

【使用指导】 该命令只能在 VSU 模式下使用，不能在单机模式下使用，且重启后才能生效。

更改设备编号

- 可选配置

- 如果需要修改某设备的 `switch_id`，可在 VSU 系统的主机控制台上执行此配置项。

【命令格式】 **switch** *switch_id* **renumber** *new_switch_id*

【参数说明】 *switch_id*：VSU 取值范围为盒式设备 1-16，箱式设备为 1-4。

new_switch_id：修改后的设备编号。

【缺省配置】 -

【命令模式】 config-vs-domain 配置模式

【使用指导】 该命令只能在 VSU 模式下使用，不能在单机模式下使用，且重启后才能生效。

✎ 更改设备优先级

- 可选配置。
- 如果需要修改某设备的优先级，可在 VSU 系统的主机控制台上执行此配置项。
- 优先级的数值越大，表示优先级越高。在选举主设备的过程中，优先级高的设备成为主设备。

【命令格式】 **switch** *switch_id* **priority** *priority_num*

【参数说明】 *switch_id*：需要配置优先级的交换机编号。

priority_num：对应交换机的优先级，取值范围为盒式设备 1-255。

【缺省配置】 缺省的优先级是 100。

【命令模式】 config-vs-domain 配置模式

【使用指导】 优先级的数值越大，表示优先级越高。在选举主设备的过程中，优先级高的设备成为主设备。

该命令在单机模式和 VSU 模式都可以使用。修改的优先级必须重启以后才会生效。

该命令不会修改 *switch_id*。单机模式下如果配置了 *switch_id* 为 1，再执行 `switch 2 priority 200`，则命令不会生效，除非先将 *switch_id* 修改为 2，再执行 `switch 2 priority 200` 才会生效。VSU 模式下，*switch_id* 表示当前运行的交换机编号，如果当前不存在该编号，则配置也不生效。

✎ 配置设备别名

- 可选配置。
- 如果需要配置某设备的别名，可在 VSU 系统的主机控制台上执行此配置项。
- 使用 **switch** *switch_id* **description** *switch1* 命令配置设备的别名，最大为 32 个字符。

【命令格式】 **switch** *switch_id* **description** *dev-name*

【参数说明】 *switch_id*：需要配置优先级的交换机编号。

dev_name：设备名称描述

【缺省配置】 -

【命令模式】 config-vs-domain 配置模式

【使用指导】 该命令在单机模式和 VSU 模式都可以使用，VSU 模式下配置立即生效。

✎ 错帧配置

- 可选配置。
- 使用 **switch** **crc errors** *error_num* **times** *time_num* 命令配置错帧触发的条件。

【命令格式】 **switch** **crc errors** *error_num* **times** *time_num*

【参数说明】	<i>error_num</i> ：用于配置两次检查错帧递增个数（当大于这个数认为是一次错帧） <i>time_num</i> ：连续多少次后，采取的动作（动作为提示或关闭端口）
【缺省配置】	errors 缺省值为 3；times 缺省值为 10
【命令模式】	config-vs-domain 配置模式
【缺省级别】	14
【使用指导】	-

保存配置文件

使用 **exit** 命令退出虚拟设备配置模式，并使用 **write** 命令保存配置到文件 config_vsu.dat 中。

检验方法

使用 **show switch virtual [topology | config]** 命令显示当前运行的 VSU 信息，拓扑形状，或当前配置的 VSU 参数。

【命令格式】	show switch virtual [topology config]
【参数说明】	Topology-拓扑信息，config-VSU 配置信息
【命令模式】	特权模式
【使用指导】	查看域 ID，以及每台设备的编号、状态和角色。

配置举例

配置 VSU 属性

【网络环境】
图 9-47



Switch-1 和 Switch-2 组成 VSU，把 Switch-2 的机箱号修改为 3，优先级修改为 150。假设 Switch1 是全局主交换机，在全局主交换机上配置。

【配置方法】	● 修改 Switch-2 的配置
Switch-1	<pre>Ruijie#config Ruijie(config)# switch virtual domain 100 Ruijie(config-vs-domain)# switch 2 renumber 3 Ruijie(config-vs-domain)# switch 2 priority 150 Ruijie(config-vs-domain)# switch 2 description switch-3</pre>
【检验方法】	● 使用命令 show switch virtual config 查看。
Switch-1	<pre>Ruijie#show switch virtual config switch_id: 1 (mac: 0x1201aeda0M)</pre>

```
!  
switch virtual domain 100  
!  
switch 1  
switch 1 priority 100  
!  
switch convert mode virtual  
!  
port-member interface Tengigabitethernet 1/1  
!  
port-member interface Tengigabitethernet 1/2  
!  
switch_id: 3 (mac: 0x1201aeda0E)  
!  
switch virtual domain 100  
!  
switch 3  
switch 3 priority 150  
!  
switch convert mode virtual  
!  
port-member interface Tengigabitethernet 1/1  
!  
port-member interface Tengigabitethernet 1/2  
!  
switch 3 description switch-3  
!
```

常见错误

-

9.5.2.2 配置 VSL 链路

配置效果

设备组成 VSU 或 VSU 系统运行过程中，如果需要在普通口和 VSL 端口之间互相转换，用户可以登录到 VSU 系统的主机控制台上进行修改，从机控制台禁止进入全局配置模式。

注意事项

- 可以通过串口或 telnet 登录到 VSU 系统控制台进行添加或删除 VSL 成员端口的配置。
- 为了防止实际场景连错，VSL AP 采用动态协商。先配置 vsl 口池，协商成功后，加到同一个 AP 中。和同一台设备相连的端口在同一个 AP 中。

配置方法

进入 VSL-PORT 模式

- 使用 **vsl-port** 命令进入 VSL-PORT 配置模式。该命令可选。
- 当设备进入到 VSL-PORT 的配置模式时，可以配置或删除 VSL 口。

【命令格式】 **vsl-port**

【参数说明】 -

【缺省配置】 -

【命令模式】 config 配置模式

【使用指导】 该命令在单机模式和 VSU 模式都可以使用

配置 VSL-AP 成员口

- **port-member interface** *interface-name* [**copper** | **fiber**] 命令配置 VSL 口。该命令可选。
- 使用 **port-member interface** 命令配置或删除 VSL 口。

【命令格式】 **port-member interface** *interface-name* [**copper** | **fiber**]

【参数说明】 *interface-name* : 二维接口名，如 GigabitEthernet 0/1, GigabitEthernet 0/3。


copper : 电口属性。


fiber : 光口属性。


【缺省配置】 -


【命令模式】 config-vsl-port 配置模式

【使用指导】 该命令可以在 VSU 模式下，也可以在单机模式下。命令配置后需要保存配置，并重启 VSL 成员端口所在设备才能生效。


 VSU 系统运行过程中，配置的 VSL 成员链路即刻生效。所有设备上都要配置 vsl 口


 箱式设备只能万兆以上光口做 vsl 口，盒式设备上千兆以上光口和电口，都可以做 vsl 口。

 箱式设备上模块也必须使用万兆以上的模块。

 40G 一分四端口不能做成 VSL 口。

 对于 40G 端口（无论该端口是否执行了拆分操作），其成员口（即 4 个 10G 口）不允许进行转换为 VSL 成员口的操作。

 如果端口被用户配置为 NLB 反射口必须将该配置删除，才能进行转换为 VSL 成员口的操作。

 为了防止 VSL 成员口退出 VSL 聚合端口的瞬间发生环路，在执行命令将 VSL 成员口退出 VSL 聚合端口时，系统自动将该成员口设置为 shutdown 状态。在退出 VSL 聚合端口操作完成以后，用户可以重新连接链路并通过 no shutdown 命令重新启用该端口。配置 VSL 口时候，系统会将端口先 shutdown，如果配置失败，如果想作为普口继续使用，可以通过 no shutdown 命令重新启用该端口。添加某个成员端口编号，必须是三维端口号。比如进入 VSL-PORT 配置模式，执行 **port-member interface** Tengigabitethernet 1/1/1 命令，则表示将全局三维端口 1/1/1 配置成 VSL 口。

❗ 从 VSL 口变为普通口，如果导致 VSU 拓扑断裂，不允许删除，可以先断掉物理口，再删除 VSL 口。

检验方法

使用 **show switch virtual link [port]** 命令查看当前的 VSL-AP 运行信息。

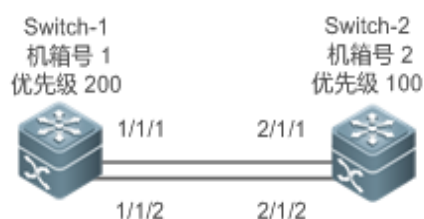
- 【命令格式】 **show switch virtual link [port]**
- 【参数说明】 **port** : 显示 VSL 子接口的状态信息。
- 【命令模式】 特权模式
- 【使用指导】 -

配置举例

配置 VSL 链路

【网络环境】

图 9-58



【配置方法】 ● 在 Switch-1 中，增加端口 1/1/3 作为 VSL 口，将 1/1/2 从 vsl 口中移除。

Switch-1

```
Ruijie#config
Ruijie(config)# vsl-port
Ruijie(config-vsl-port)# port-member interface Tengigabitethernet 1/1/3
Ruijie(config-vsl-port)# no port-member interface Tengigabitethernet 1/1/2
```

【检验方法】 ● 使用 **show switch virtual config** 命令查看 VSL 链路的情况。假设是 Switch-1 是全局主交换机，在全局主交换机上执行命令。

Switch-1

```
Ruijie#show switch virtual config
switch_id: 1 (mac: 0x1201aeda0M)
!
switch virtual domain 100
!
switch 1
switch 1 priority 100
!
switch convert mode virtual
!
port-member interface Tengigabitethernet 1/1
```

```
!  
port-member interface Tengigabitethernet 1/3  
!  
switch_id: 3 (mac: 0x1201aeda0E)  
!  
switch virtual domain 100  
!  
switch 3  
switch 3 priority 150  
!  
switch convert mode virtual  
!  
port-member interface Tengigabitethernet 1/1  
!  
port-member interface Tengigabitethernet 1/2  
!  
switch 3 description switch-3  
!
```

常见错误

-

9.5.2.3 配置双主机检测

配置效果

配置相关的检测机制以防止产生双主机。

注意事项

- 双主机检测只能在 VSU 模式下进行配置，单机模式下不允许配置双主机检测机制。
- 所有双主机检测配置在主从机上立即生效，且属于全局配置，**show running-config** 可以查看。
- BFD 检测的配置信息不能通过 BFD 的显示命令进行显示，只能通过双主机检测显示命令进行显示。

配置方法

📌 配置 BFD 双主机检测

- 基于 BFD 的双主机检测，要求在两台机箱之间建立一条直连链路，链路两端的端口必须是物理路由端口。以下配置在两台机箱上均需配置。
- 首先进入检测接口的接口配置模式，将检测接口配置为路由口。
- 退出接口配置模式后通过命令 **switch virtual domain *domain_id*** 进入 config-vs-domain 配置模式。
- 在模式 config-vs-domain 下，通过命令 **dual-active detection bfd** 打开 BFD 开关。该命令可选，当需要配置 BFD 双主机检测功能时选用此命令。
- 在模式 config-vs-domain 下，通过 **dual-active bfd interface *interface-name*** 配置 BFD 检测接口。该命令可选，当配置 BFD 双主机检测功能时需使用此命令配置 BFD 检测接口。
- 删除 BFD 检测接口，如果没有剩余的 BFD 检测口，会导致 BFD 检测无法使用。

【命令格式】 **switch virtual domain *domain_id***

【参数说明】 *domain_id* : VSU 的虚拟域编号

【缺省配置】 域编号缺省为 100

【命令模式】 全局配置模式

【使用指导】 域编号相同的两台设备才能组合成一台虚拟设备，域编号在局域网内必须唯一。

【命令格式】 **dual-active detection { aggregateport | bfd }**

【参数说明】 **aggregateport** : 指定聚合口探测方式。

Bfd : 定 BFD 探测方式。

【缺省配置】 检测双主设备状态的功能是关闭的。

【命令模式】 config-vs-domain 配置模式

【使用指导】 该命令只能在 VSU 模式下进行配置。

【命令格式】 **dual-active bfd interface *interface-name***

【参数说明】 *interface-name* : 检测接口类型和编号

【缺省配置】 -

【命令模式】 config-vs-domain 配置模式

【使用指导】 BFD 检测接口必须是路由端口，且在不同的设备上。

- ❗ BFD 检测接口必须是直连的物理路由端口，检测端口必须在不同的设备上。
- ❗ 配置的接口类型没有限制，由于双主机检测链路只用于传输 BFD 报文，流量不大，建议使用千兆口或百兆口作为双主机检测端口。
- ❗ 当配置为双主机的三层路由口被转换为二层交换口(在该接口下执行 **switchport** 命令)后，BFD 双主机配置将自动清除。
- ❗ BFD 建议使用在直连方式，只能连接主从两台设备。
- ❗ 当 VSU 系统检测出双主机冲突并让其中一堆 VSU 进入 recovery 状态后，用户应该通过修复 VSL 故障方式来解决，而不能直接复位那堆进入 recovery 状态的 VSU，否则可能会引起网络上出现双主机冲突。

📌 配置聚合口双主机检测

- 要配置基于聚合口检测方式，必须先配置一个 AP 聚合口，然后指定 AP 聚合口为检测口。
- 使用 **port-group ap-num** 命令将物理成员口加入到 AP 聚合口中。
- 进入 config-vs-domain 配置模式后，使用 **dual-active detection aggregateport** 命令打开聚合口方式检测开关。该命令可选。当需要配置聚合口检测功能时选用此命令。
- 使用 **dual-active interface interface-name** 命令将聚合口配置为双主机检测口。该命令可选，配置聚合口检测功能时需使用此命令将聚合口配置为双主机检测口。
- 使用 **dad relay enable** 命令打开上下游设备接口的双主机检测报文中转功能。该命令可选，当配置基于聚合口检测双主机时，需使用此命令转发 dad 报文（双主机检查报文）。
- 关闭聚合口双主机检测功能，会使聚合口双主机检测失效。
- 删除检测口，如果没有剩余的聚合口检测口，会导致聚合口检测无法使用。
- 缺省关闭基于聚合口检测双主机的转发特性。

【命令格式】 **dual-active detection { aggregateport | bfd }**

【参数说明】 **aggregateport**：指定聚合口探测方式。

bfd：定 BFD 探测方式。

【缺省配置】 检测双主设备状态的功能是关闭的。

【命令模式】 config-vs-domain 配置模式

【使用指导】 该命令只能在 VSU 模式下进行配置。

【命令格式】 **dual-active interface interface-name**

【参数说明】 **interface-name**：接口类型和接口编号，必须为 AP 类型的接口。

【缺省配置】 -

【命令模式】 config-vs-domain 配置模式

【使用指导】 基于聚合口的双主机检测口只能配置一个，在设置 AP 口为检测接口前要先创建该接口，后配置的检测口会覆盖前一次配置的检测口。


【命令格式】 **dad relay enable**

【参数说明】 -

【缺省配置】 缺省关闭基于聚合口检测双主机的转发特性。

【命令模式】 接口配置模式

【使用指导】 该命令只能在 AP 接口上使用。

 建议加入到聚合检测口的物理接口尽量分布在不同设备上。

配置 recovery 模式的例外端口列表

- 当检测到双主机，其中一台主机必须进入 recovery 模式。Recovery 模式下，需要将所有业务口进行关闭。为了某些特殊用途业务口的正常使用（如配置一个端口远程登陆管理设备），用户可以将某些端口配置为在 recovery 模式不关闭的例外端口。

- 进入 config-vs-domain 配置模式后，通过 **dual-active exclude interface** *interface-name* 命令指定在 recovery 模式不关闭的例外端口。该命令可选。

【命令格式】 **dual-active exclude interface** *interface-name*

【参数说明】 *interface-name*：接口类型和接口编号。

【缺省配置】 -

【命令模式】 config-vs-domain 配置模式

【使用指导】 该命令只能在 VSU 模式下进行配置。例外端口必须是路由端口，不能是 VSL 端口。用户可以配置多个例外端口。

⚠ 例外端口必须是路由端口，不能是 VSL 端口。

⚠ 当例外端口由路由口被转换为交换口(在该接口下执行 switchport 命令)后，该接口关联的例外端口配置将被自动清除。

检验方法

通过命令 **show switch virtual dual-active { aggregateport | bfd | summary }** 查看当前双主机配置信息。

【命令格式】 **show switch virtual dual-active { aggregateport | bfd | summary }**

【参数说明】 **aggregateport**：查看基于聚合口检测信息。

bfd：查看基于 BFD 检测信息。

summary：显示 DAD 概要信息。

【命令模式】 特权模式

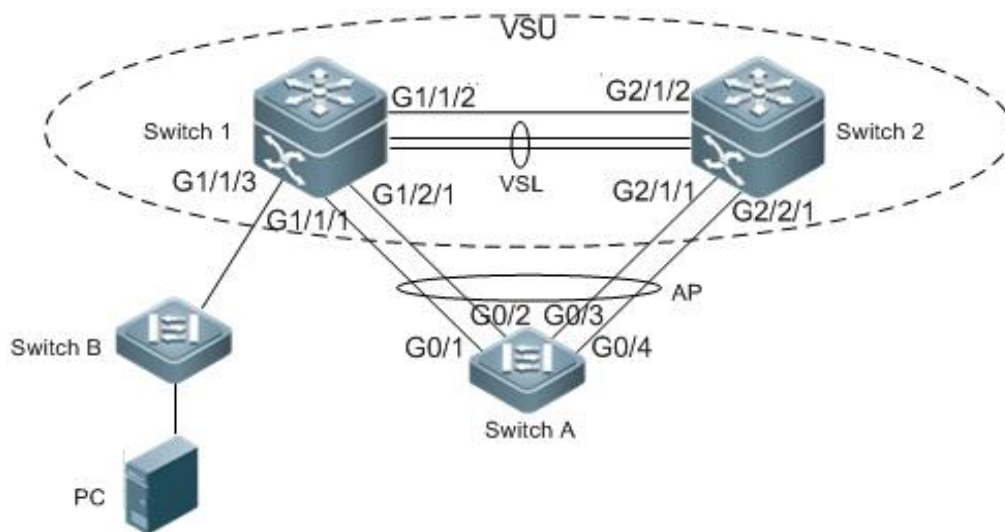
【使用指导】 -

配置举例

采用基于 BFD 来检测双主机

【网络环境】

图 9-19




- Switch 1 和 Switch 2 组成虚拟设备 VSU(domain ID 为 1)，Switch 1 的优先级是 200，Switch 2 的优先级是 150。Switch 1 的 Te1/3/1，Te1/3/2 与 Switch 2 的 Te2/3/1,Te2/3/2 分别建立链接，组成 Switch 1

和 Switch 2 之间的 VSL 链路。Switch A 的端口 G0/1，G0/2，G0/3 和 G0/4 等 4 个端口分别与 Switch 1 的 G1/1/1 和 G1/2/1，以及 Switch 2 的 G2/1/1 和 G2/2/1 建立连接，并构成一个包含 4 个成员链路的聚合端口组，聚合端口组的 ID 是 1。聚合端口组 1 的所有成员均为千兆光口。G1/1/2 和 G2/1/2 均为路由口。

- G1/1/2 和 G2/1/2 是一对 BFD 双主机接口。

【配置方法】

- 将 G1/1/2 和 G2/1/2 口配置为路由口
- 开启 BFD 双主机检测功能
- 配置 G1/1/2 和 G2/1/2 为 BFD 检测接口

 因为 Switch 1 和 Switch 2 组成虚拟设备 VSU，所以以上配置可在 Switch 1 及 Switch 2 中任意一台设备上配置。此处以在 Switch 1 上配置为例。

Switch 1

```
Ruijie(config)# interface GigabitEthernet 1/1/2
Ruijie(config-if-GigabitEthernet 1/1/2)# no switchport
Ruijie(config)# interface GigabitEthernet 2/1/2
Ruijie(config-if-GigabitEthernet 2/1/2)# no switchport
Ruijie(config-if)# switch virtual domain 1
Ruijie(c config-vs-domain)# dual-active detection bfd
Ruijie(config-vs-domain)# dual-active bfd interface GigabitEthernet 1/1/2
Ruijie(config-vs-domain)# dual-active bfd interface GigabitEthernet 2/1/2
```

Switch A

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface aggregategateport 1
Ruijie(config-if-aggregategateport 1)# interface range GigabitEthernet 0/1-4
Ruijie(config-if-aggregategateport 1)# port-group 1
Ruijie(config)# interface vlan 1
Ruijie(config-if-vlan 1)#ip address 1.1.1.2 255.255.255.0
Ruijie(config-if-vlan 1)#exit
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)# dad relay enable
Ruijie(config-if-AggregatePort 1)# exit
```

【检验方法】

- 查看双主机箱配置状态
- 查看 BFD 双主机箱检测配置

Switch 1

```
Ruijie# show switch virtual dual-active summary
BFD dual-active detection enabled: No
Aggregateport dual-active detection enabled: Yes
Interfaces excluded from shutdown in recovery mode:
In dual-active recovery mode: NO
Ruijie# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
```

```
BFD dual-active interface configured:
GigabitEthernet 1/1/2: UP
GigabitEthernet 2/1/2: UP
```

常见错误

- 作为 BFD 检测口，必须为路由口。
- BFD 检测和聚合口检测只能激活其中的一种。

9.5.2.4 配置流量平衡

配置效果

在 VSU 系统中，如果出口分布在多台设备中，通过该配置，优先在本台设备上转发。

注意事项

默认都是本地优先转发

配置方法

📌 配置 AP 本地转发优先模式

- 进入 config-vs-domain 配置模式后，使用 **switch virtual aggregateport-lff enable** 命令打开 AP 本地转发优先 LFF(Local Forward First)。该命令可选。
- AP 成员口可以分布在 VSU 系统的两个机箱上。用户可以根据实际流量情况，配置 AP 的出口流量是否优先从本地成员口进行转发。
- 该功能若关闭，则流量转发根据 AP 配置规则转发流量。具体配置见 ap 配置。

【命令格式】 **switch virtual aggregateport-lff enable**

【参数说明】 -

【缺省配置】 缺省时该功能是打开的。

【命令模式】 config-vs-domain 配置模式

【使用指导】 打开 VSU 模式下 AP 口的本地优先转发特性。

📌 配置 ECMP 本地转发优先模式

- 进入 config-vs-domain 配置模式后，使用 **switch virtual ecmp-lff enable** 命令打开 ecmp 本地转发优先 LFF(Local Forward First)。该命令可选。

- ECMP 路由出口可以分布在 VSU 系统的两个机箱上。用户可以根据实际流量情况，配置 ECMP 的出口流量是否优先从本地成员口进行转发。
- 该功能若关闭，则转发模式根据 ecmp 配置规则转发。具体配置见 ecmp 配置。

【命令格式】 **switch virtual ecmp-lff enable**

【参数说明】 -

【缺省配置】 缺省时该功能是打开的。

【命令模式】 config-vs-domain 配置模式

【使用指导】 打开 VSU 模式下 ecmp 本地成员优先转发。

⚠ VSU 模式下，默认关闭跨机箱 AP 本地转发优先模式及 EMCP 路由口本地转发优先模式。

⚠ 三层设备若部署 VSU，建议用户配置基于 IP 的 AP 负载均衡模式（src-ip，dst-ip，src-dst-ip 等）。

检验方法

使用 **show switch virtual balance** 命令查看当前 VSU 系统流量均衡模式。

【命令格式】 **show switch virtual balance**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 显示 VSU 模式下的流量均衡模式配置。

配置举例

配置本地优先转发

【网络环境】

图 9-20



上图中 Switch-1 和 Switch-2 组成 VSU，假设 Switch-1 是全局主交换机，在 Switch-1 执行配置。

【配置方法】 ● AP 本地优先转发

Switch-1

```
Ruijie#config
Ruijie(config)# switch virtual domain 100
Ruijie(config-vs-domain)# switch virtual aggregateport-lff enable
```

【检验方法】 ● 使用 **show switch virtual balance** 命令查看。

Switch-1

```
Ruijie#show switch virtual balance
Aggregate port LFF : enable
Ecmp lff enable
```

常见错误

-

9.5.2.5 配置从 VSU 模式切换到单机模式

配置效果

将 VSU 系统转换成独立的设备，以单机模式进行工作。

注意事项

-

配置方法；

- 使用 **switch convert mode standalone** [switch_id]命令将设备切换为单机模式。该命令可选。
- 用户执行切换命令后，系统将进行以下提示：“是否将配置文件恢复为之前备份的“standalone.text” 如果选 “yes”，则将配置文件恢复；如果选 “no”，则清除虚拟设备模式的配置。”

【命令格式】 **switch convert mode standalone** [switch_id]

【参数说明】 switch_id 设备号

【缺省配置】 缺省时设备处于单机模式。

【命令模式】 特权模式

【使用指导】 用户执行 **switch convert mode standalone** 切换命令后，主机箱把 VSU 模式下的各个 VSD 全局配置文件备份为“vsd.virtual_switch.text.vsd 序号”，然后清除清除 VSU 模式下的各个 VSD 全局配置文件 “config.text”，并提示用户是否将文件“vsd.standalone.text.vsd 序号” 内容覆盖到各个 VSD 的全局配置文件 “config.text”，用户选择 “yes”，把“vsd.standalone.text.vsd 序号”内容覆盖到各个 VSD 的全局配置文件 “config.text”；否则不恢复 “config.text”。最后重启交换机。

该命令既可以在单机模式下使用，也可以在 VSU 模式下使用。如果在单机模式下使用，则切换的对象为本机；如果在 VSU 模式下使用，且加上 sw_id 参数，切换的交换机编号为 sw_id，如果没有加上 sw_id 参数，则切换的对象为主机。建议先切换从机，再切换主机。

检验方法

-

配置举例

➤ 将设备从 VSU 模式转化成单机模式

【网络环境】

图 9-21



上图中，假设 Switch-1 和 Switch-2 组成 VSU，Switch-1 是全局主设备。

【配置方法】

- 把交换设备 1 转化成单机模式
- 把交换设备 2 转化成单机模式

Switch-1

```
Ruijie# switch convert mode standalone 1
Ruijie# switch convert mode standalone 2
```

【检验方法】

使用命令 **show switch virtual config** 查看设备的状态。

Switch-1

```
Ruijie#show switch virtual config
switch_id: 1 (mac: 0x1201aeda0M)
!
switch virtual domain 100
!
switch 1
switch 1 priority 100
!
switch convert mode standalone
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/3
!
switch_id: 2 (mac: 0x1201aeda0E)
!
switch virtual domain 100
!
switch 2
switch 2 priority 150
!
switch convert mode standalone
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/2
!
```

```
switch 2 description switch-2
!
```

常见错误

-

9.5.3 快闪搜索配置

配置效果

打开快闪搜索功能，设备 status 灯快闪。

注意事项

如果未主动关闭快闪搜索功能，在开启 30 分钟后，会自动关闭。

配置方法

📌 开启/关闭快闪搜索

- 必选。在需要被查找的设备上使用此功能。
- 在特权模式下，使用 `led-blink` 命令开启/关闭快闪搜索功能。

【命令格式】 **led-blink** { **enable** | **disable** } [**device** *device_id*]

【参数说明】 enable：开启快闪搜索功能
disable：关闭快闪搜索功能
device_id：设备 id

【缺省配置】 关闭快闪搜索功能

【命令模式】 特权模式

【使用指导】 在单机模式下，仅可以开启/关闭本设备的快闪搜索功能，无 `device` 关键字。
在 VSU 模式下，可以通过指定 `device_id`，对指定设备开启/关闭快闪搜索功能，如果忽略 `device` 选项，则表示 VSU 中所有设备的快闪搜索功能开启/关闭。
如果未主动关闭快闪搜索功能，在开启 30 分钟后，会自动关闭。
此配置不可保存，一旦重启，或发生主备切换，快闪搜索将被关闭。

检验方法

查看设备的 status 灯，是否快闪。

配置举例

使用 VSU 环境中 2 设备的快闪搜索功能

- 【网络环境】 假设 Switch-1 和 Switch-2 组成 VSU，Switch-1 是全局主设备。
- 【配置方法】
- 在 Switch-1 控制台上输入 led-blink enable device 2，打开快闪搜索。
 - 在 Switch-1 控制台上输入 led-blink disable device 2，关闭快闪搜索。
- 【检验方法】 在快闪搜索打开期间，观察 device 2 上的 status 灯状态是否为快闪。

常见错误

-

9.5.4 Recovery 模式下设备在 VSL 恢复正常后的恢复方式配置

配置效果

关闭 recovery 模式下自动重启恢复。

注意事项

如果关闭了该功能，recovery 模式下的设备恢复需要重新打开该功能或者手动重启设备。

配置方法

开启/关闭 recovery 模式下的自动重启功能

- 必选。在需要开启、关闭该功能的设备上执行。
- 在 config-vs-domain 模式下，使用[no] recovery auto-restart enable 命令开启/关闭 recovery 模式自动重启功能。

【命令格式】 **recovery auto-restart enable**

【参数说明】 -

【缺省配置】 打开 recovery 模式下自动重启恢复功能

【命令模式】 config-vs-domain 模式

【使用指导】 该命令只能在 vsu 模式下执行，命令配置后需要保存配置，立即生效。

检验方法

执行 show run 命令查看配置。

配置举例

使用 VSU 环境中关闭 recovery 模式下自动重启恢复功能

【网络环境】

图 8-22



假设 Switch-1 和 Switch-2 组成 VSU，Switch-1 是全局主设备。开启双主机检测功能。

- 【配置方法】
- 在 Switch-1 控制台上输入 switch virtual domain 100，进入 config-vs-domain 模式下。
 - 在 Switch-1 控制台上输入 no recovery auto-restart enable，关闭自动重启恢复功能

【检验方法】 断开 vsl 链路，双主机检测完成后，switch-2 将进入 recovery 模式；
重新连上 vsl 链路，switch-2 将不会重启；
在 switch-2 控制台上输入 recovery auto-restart enable，开启自动重启恢复功能，switch-2 将自动复位。

常见错误

-

9.6 监视与维护

查看运行情况

作用	命令
显示当前运行的 VSU 信息，拓扑形状，或当前配置的 VSU 参数	show switch virtual [topology config role]
查看当前双主机配置信息	show switch virtual dual-active { bfd aggregateport summary }
VSU 模式下查看当前的 VSL-AP 运行信息	show switch virtual link [port]
显示本设备的交换机编号	show switch id

10 RNS

10.1 概述

RNS 是 Reliable Network Service 的缩写，RNS 通过探测对端设备提供的特定服务，来监控服务的可用性，端到端连接的完整性和服务的质量。利用 RNS 探测结果，用户可以：

- 及时了解网络的性能状况，针对不同的网络性能进行相应处理。
- 对网络故障进行诊断和定位。

 下文仅介绍 RNS 的相关内容。

协议规范

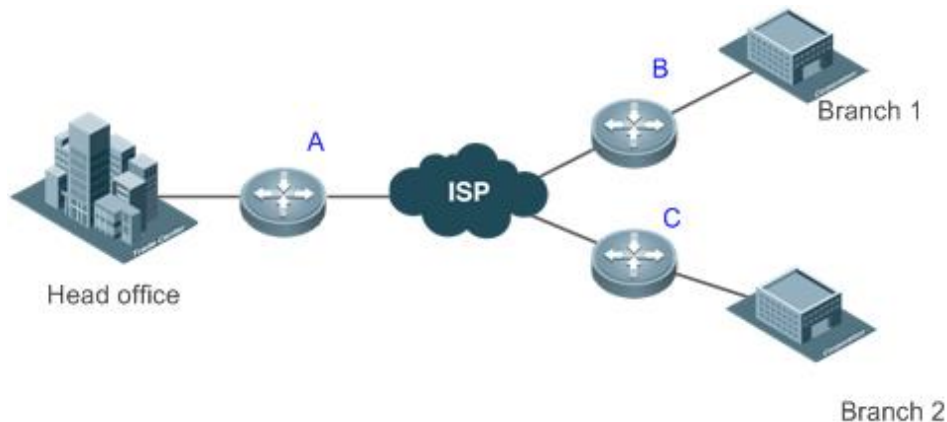
无

10.2 典型应用

10.2.1 对业务性能进行探测评估

应用场景

如下图，某公司打算在总部和分支结构之间部署视频会议系统，并已经进行了相关的 Qos 配置。在正式部署之前，要先检测在公司现有的业务压力下，该新业务是否能正常的运作。由于视频会议系统对于网络的 UDP 延迟和 UDP 传输抖动性能比较敏感，传统的 ping 工具仅仅能检测 ICMP 的性能，对于 UDP 传输性能没法有效的衡量，而且也无法满足抖动性能的测量。



【注释】 A,B,C 均为交换机设备

功能部署

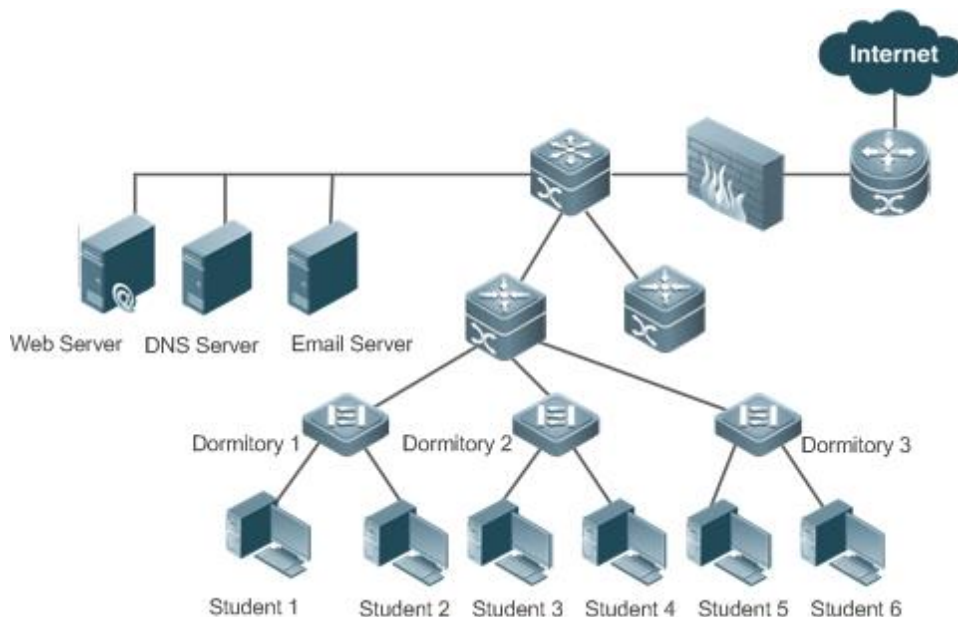
- 在分支机构的出口交换设备/交换机上配置 RNS 探测，能进行 UDP 抖动检测，UDP 延迟检测；
- 用户只需要在交换机 A 上指定好总部的出口交换设备/交换机的 IP 地址，UDP 端口，就能主动发送 UDP 报文，总部的出口交换设备/交换机能通过配置，自动应答该 UDP 报文，通过在分支机构的出口交换设备/交换机上对发送和接收报文的处理，计算 UDP 抖动值。为了了解在各个时段的情况，RNS 探测还应开启定时启动/停止，重复运行等时间调度功能。

10.2.2 定位网络故障

应用场景

如下园区中，学生 1 报告无法访问 Web 服务器，学生 3 报告无法访问 Internet，学生 6 报告邮件无法正常收发。

图 10-1



功能部署

- 管理员直接在该学生宿舍的接入交换机上开启 DNS 功能的探测，检测是否是域名服务器解析问题；若 DNS 探测失败，则自动触发 ICMP-Echo 探测以检测 Web 服务器网络是否可达。
- 当出现故障时，仅需要启动一个探测，后续的都能自动触发，然后查看结果就可以分析大致的问题点，大大简化管理员的工作。

10.3 功能详解

基本概念

📌 RNS 探测实例

RNS探测实例，可看作是一个RNS进程。进行RNS探测前，需要创建RNS探测实例。在RNS探测实例中配置RNS探测的参数，如探测类型，探测目的地址，探测频率等。探测实例ID全局唯一。

功能特性	作用
RNS 探测	主要用于监控网络的连通性，服务的可用性，端到端连接的完整性和服务的质量。
track 联动功能	Track 可跟踪探测结果，并将结果通告给相应的模块。

10.3.1 RNS 探测

主要用于监控网络的连通性，服务的可用性，端到端连接的完整性和服务的质量，如探测该设备 DNS 功能是否正常，目前 RNS 支持的探测类型包括 ICMP-Echo，DNS 和 TCP 类型的探测。

工作原理

📌 ICMP-Echo 探测

ICMP-Echo 探测是 RNS 最基本的功能，遵循 RFC 2925 来实现。其实现原理是通过发送 ICMP 报文来判断目的地的可达性、计算网络响应时间及丢包率。

ICMP-Echo 探测根据设置的探测时间及频率向探测的目的 IP 地址发 ICMP 回显请求报文，目的地址收到 ICMP 回显请求报文后，回复 ICMP 回显应答报文。ICMP-Echo 探测根据 ICMP 回显应答报文的接收情况，如接收时间和报文个数，计算出到目的 IP 地址的响应时间及丢包率，从而反映当前的网络性能及网络情况。ICMP-Echo 探测的结果和历史记录将被记录，可以通过命令行来查看。

⚠ ICMP-Echo 探测成功的前提条件是目的设备要能够正确响应 ICMP 回显请求报文。

📌 DNS 探测

DNS 探测通过模拟 DNS 客户端向指定的 DNS 服务器发送域名解析请求，根据域名解析是否成功及域名解析需要的时间，来判断 DNS 服务器是否可用，及域名解析速度。DNS 探测只是模拟域名解析的过程，不保存解析的域名与 IP 地址的对应关系。DNS 探测的结果和历史记录将被记录，可以通过命令行来查看。

📌 RNS 探测的配置过程

32. 创建特定类型的探测实例，根据探测类型进行相应探测参数的配置。
33. 启动 RNS 探测实例。
34. RNS 探测实例构造指定探测类型的报文，并发送给对端。
35. 对端收到探测报文后，回复相应类型的应答报文。

36. RNS 探测实例根据是否收到应答报文，以及接收应答报文的时间，计算报文丢失率、往返时间等。

37. 通过显示命令或调试命令查看探测结果。



以上配置过程介绍的是 RNS 实例探测通用的流程，不同类型的探测具体配置步骤，参看下文配置详解。

相关配置

配置探测的重复时间间隔

缺省情况下，探测的重复时间间隔为 60 秒。

在 RNS 探测类型对应的模式下，使用 **frequency** *millisecond* 命令可以配置探测重复时间间隔。

配置 **frequency** 应当满足下面的公式，以保证探测的计算正确。

$$(\text{frequency milliseconds}) > (\text{timeout milliseconds}) \geq (\text{threshold milliseconds})$$

配置探测超时时间

不同探测类型的缺省超时时间不同，可以通过 **show ip rns configuration** 查看

在 RNS 探测类型对应的模式下，使用 **timeout** *millisecond* 命令可以配置探测实例超时时间间隔。

配置 **timeout** 应当满足一定的计算关系，请参见 **frequency** 的使用指导。

配置探测的时间阈值

缺省情况下，探测的时间阈值为 5000ms。

在 RNS 探测类型对应的模式下，使用 **threshold** *milliseconds* 命令可以配置实例探测的时间阈值。

配置 **threshold** 应当满足一定的计算关系，请参见 **frequency** 的使用指导。

探测设置一个标签

无缺省配置

在 RNS 探测类型对应的模式下，使用 **tag** *text* 命令可以配置探测标签。

tag 可以为探测指定一个标签，通常用于标识这个探测的作用。

配置探测实例的协议载荷大小

不同探测类型的缺省值不同，默认为对应探测类型协议报文必须的最小值或适合值。

在对应 RNS 探测类型配置模式下，使用 **request-data-size** *bytes* 命令可以配置协议载荷大小。

配置探测的报文的 TOS 字段

缺省配置为 0。

在 RNS 探测类型对应的模式下，使用 **tos** *number* 命令配置 RNS 探测报文中 IPv4 首部 TOS 字段。

配置探测的 VRF

无缺省配置。

在 RNS 探测类型对应的模式下，使用 **vrf vrf-name** 命令可以配置 RNS 探测实例所处的 VRF。

10.3.2 track 联动功能

track 支持跟踪的对象类型包括：跟踪一个 RNS 探测结果、跟踪一个 RNS 列表的状态、跟踪一个接口的链路状态以及跟踪一个 track 列表的状态。同时当 track 的状态发生变化时，可以触发其他模块进行联动。

工作原理

以 track 跟踪 RNS 探测结果为例，说明 track 的工作原理。

- 配置一个 track 对象，用来跟踪一个 RNS 探测结果。
- 当 RNS 探测结果发生变化时，RNS 模块发送状态变化的消息给 track 模块。
- track 模块接收到 RNS 探测结果的消息，经过设置的延迟时间后，若该 RNS 探测结果未发生变化，则修改该 track 对象的状态，通告关注该 track 对象的模块。若在这段时间内，该 RNS 探测结果又恢复原有状态，则不修改 track 状态和通告相应的模块。

相关配置

配置用于跟踪接口链路状态的 track 对象

缺省情况下，跟踪接口的链路状态功能不生效。

使用 **track interface line-protocol** 命令可以配置一个 track 对象，用于跟踪一个接口的链路状态。

该接口的链路状态为 up，则 track 对象的状态为 up；该接口的链路状态为 down，则 track 对象的状态为 down。

配置用于跟踪 RNS 探测结果的 track 对象

缺省情况下，跟踪 RNS 探测结果功能不生效。

使用 **track rns** 命令可以配置一个 track 对象，用于跟踪一个 RNS 探测结果。其中，RNS 探测编号范围为 1-500。

若该 RNS 探测结果为成功，则 track 对象的状态为 up；若该 RNS 探测结果为失败，则 track 对象的状态为 down。

配置用于跟踪 track 列表状态的 track 对象

缺省情况下，跟踪 track 列表状态的功能不生效。

使用 **track list** 命令可以配置一个 track 对象，用于跟踪一个 track 列表的状态，其结果可以是所有成员状态取“与”或者“或”的结果。

配置 track 对象的结果取所有成员状态“与”的结果，则当所有成员的状态“与”的结果为 up 时，该 track 对象的状态为 up；当所有成员的状态“与”的结果为 down 时，该 track 对象的状态为 down。“或”情况类似。

配置 track 列表成员

缺省情况下，track 列表成员为空。

使用 **object** 命令可以配置一个 track 列表成员，该列表成员的状态可配置为与对应 track 对象相同或相反。

📌 调整 track 的延迟通告时间

缺省情况下，track 的延迟通告时间为 0，即无通告延迟。

使用 **delay** 命令可以调整 track 的延迟通告时间，包括 track 状态由 up 变为 down 的延迟通告时间和由 down 变为 up 的延迟通告时间，取值范围是 0-180，单位为秒。

track 延迟通告的时间越大，则需要等待越长的时间，才会将该状态通告给关注该 track 对象的模块。track 延迟通告的时间越小，则需要等待越短的时间，便会将该状态通告给关注该 track 对象的模块。

10.4 配置详解

配置项	配置建议 & 相关命令	
配置 RNS 基本功能	⚠️ 必选配置，用于设置 RNS 基本功能参数。	
	ip rns	支持详细配置与简洁配置。其中， 详细配置：定义一个 RNS 操作对象。用于后续具体探测及参数的配置标识 简洁配置：无需进行后续配置，可以一步启动探测。目前支持 ICMP-Echo、DNS、TCP 类型的 RNS 探测一步启动。
	ip rns reaction-configuration	配置 RNS 探测实例的主动阈值监控和触发机制。
	ip rns reaction-trigger	配置一个 RNS 探测实例在发生监控阈值超过预期时，触发另一个处于 pending 状态的 RNS 探测实例激活探测。
	ip rns schedule	配置 RNS 探测实例的调度方法、启动时间、生存时间。
	ip rns restart	重新启动一个 RNS 探测实例。
	ip rns reset	清除所有 ip rns 的配置。
配置 icmp-echo 探测	⚠️ 可选配置，用于实现 ICMP-Echo 类型的 RNS 探测。	
	icmp-echo	创建一个 ICMP-Echo 类型的 RNS 探测实例。
	request-data-size	配置探测的协议载荷大小。
	frequency	设置探测的重复时间间隔。
	tag	设置标签。
	threshold	配置探测的时间阈值。
	timeout	配置探测的超时时间。
	tos	配置探测报文的 IPv4 首部 TOS 字段。
	vrf	配置探测所处的 VRF。
配置 dns 探测	⚠️ 可选配置，用于实现 DNS 类型的 RNS 探测。	
	dns	创建一个 DNS 类型的 RNS 探测实例。
	frequency	设置探测的重复时间间隔。

	tag	设置标签。
	threshold	配置探测的时间阈值。
	timeout	配置探测的超时时间。
	tos	配置探测报文 IPv4 首部的 TOS 字段。
	vrf	配置探测所处的 VRF。
配置 track 联动功能	 可选配置，用于与其他模块进行联动。	
	track rns	配置 track 对象，跟踪一个 RNS 探测的探测结果。
	track interface line-protocol	配置 track 对象，跟踪一个接口的链路状态。
	track list	配置 track 对象，跟踪一个 track 列表的状态。
	object	设置一个 track 跟踪的 list 对象的成员对象。
	delay	设置 track 状态变化的通告延迟时间。

10.4.1 配置 RNS 基本功能

配置效果

- 详细配置：配置 RNS 探测实例，完成 RNS 探测实例基本配置。
- 简洁配置：一步配置并启动具体的 RNS 探测实例（可选）。

注意事项

- 详细配置下，在通过命令进入 IP-RNS 模式后，若没有进一步配置探测类型，那么这个 RNS 探测实例不会被创建。
- 详细配置下，在配置完一个 RNS 探测实例后，应当通过 **ip rns schedule** 命令配置它的启动策略，否则该探测不会被执行。

配置方法

📌 定义 RNS 操作对象

- 必须配置。
- 若无特殊要求，应在每台交换设备上定义 RNS 操作对象。
- 简洁配置属于可选配置项。

📌 配置 RNS 探测实例的主动阈值监控和触发机制

- 如果要求配置探测的主动阈值监控和触发机制，则必须配置。
- 若无特殊要求，应在每台交换设备上配置探测的主动阈值监控和触发机制。

📌 配置一个 RNS 探测实例触发另一个 RNS 探测实例

- 如果要求一个 RNS 探测实例在发生监控阈值超过预期时，触发另一个处于 pending 状态的 RNS 探测实例开始运行，则必须配置。
- 如果被触发运行的 RNS 探测实例未配置调度参数，则以默认的调度参数运行。
- 若无特殊要求，应在每台交换设备上配置一个 RNS 探测实例触发另一个 RNS 探测实例。

配置 RNS 探测实例的调度参数

- 若无特殊要求，应在每台交换设备上配置 RNS 探测的调度参数。
- 简洁配置下，已使用默认参数自动配置了该命令，无需手动配置。

配置 ip rns restart 重新启动一个 RNS 探测实例

- 如果要求重新启动一个调度处于 pending 状态的探测实例，则可以使用该命令（或者直接配置调度启动 ip rns schedule X start-time now）。

配置 ip rns reset 清空 RNS 探测配置

- 如果要求清除所有配置实例的探测（如配置了大量探测实例，发现配置有误时），则可以使用该命令。

检验方法

- 通过命令 **show ip rns configuration** 查看 RNS 探测实例配置。

相关命令

定义 ip rns 操作对象

【命令格式】 **ip rns operation-number**

【参数说明】 *operation-number* : RNS 探测实例编号，取值范围<1-500>。

【命令模式】 全局模式

【使用指导】 目前 RNS 探测仅支持 IPv4 的相关探测，暂不支持 IPv6。目前最多支持配置的探测数量为 500 个。根据不同设备的性能情况，可能无法达到该最大值。由于探测功能只是一个增值功能，当配置了大量的探测，导致消耗掉系统过多的资源时，探测功能会被暂时的禁止，以保证核心业务（如路由转发等）的正常运行。

详细配置（执行 ip rns operation-number 必选项）：执行该命令后，进入 IP-RNS 配置模式。在这个模式内可以定义各种探测类型，若没有进一步配置探测类型，那么这个 RNS 探测不会被创建；在配置完一个 RNS 探测后，还应当通过 **ip rns schedule** 命令配置它的调度参数，否则该探测不会被执行。

一个 RNS 探测配置完探测类型后，下一次再通过 **ip rns** 命令将直接进入对应探测类型的模式，如果要修改一个 RNS 探测实例的探测类型，应当先删除该 RNS 探测实例（通过全局模式下输入 **no ip rns** 命令），再重新进行配置。

配置探测的主动阈值监控和触发机制

【命令格式】 **ip rns reaction-configuration operation-number react monitored-element [action-type option] [threshold-type { average [number-of-measurements] | consecutive [occurrences] | immediate | never | xofy [x-value y-value] }] [threshold-value upper-threshold lower-threshold]**

- 【参数说明】 *operation-number* : RNS 探测实例编号, 取值范围<1-500>。
monitored-element : 指定被监视的探测信息元素。
action-type option : 触发后联动的动作。
average [*number-of-measurements*] : 被监视元素以 *number-of-measurements* 次数的平均值超出阈值则触发。
consecutive [*occurrences*] 被监视元素连续 *occurrences* 次超出阈值范围则触发, *occurrences* 缺省值为 5, 可选范围 1-16。
immediate : 被监视元素一超出阈值范围就触发。
never : 从不触发。
xofy [*x-value y-value*] : 在最后 Y 次探测中, 有 X 次探测结果超出阈值范围, x 和 y 默认值均为 5, 可选范围 1-16。
threshold-value upper-threshold lower-threshold : 该参数用于配置阈值上下限, 具体含义如下:
- 当 *monitored-element* 为 *rtt* 时, 解释为时间, 默认值参见 “使用指导”。可选范围均为 0-60000ms。
 - 需要注意的是: 当 *react* 类型为 *timeout* 时, *threshold-value* 值无需配置。

【命令模式】 全局模式

【使用指导】 对于同一个 RNS 探测, 可以配置多个阈值监控, 每一个监控不同的元素。不同的探测类型, 支持的监控对象对应关系见下表:

monitored-element	icmp-echo	dns
timeout	✓	✓
rtt	✓	✓

各监控元素的默认阈值如下表:

Monitored Element	Upper Threshold	Lower Threshold
timeout	-	-
rtt	5000ms	0ms

配置一个 RNS 探测实例触发另一个 RNS 探测实例

- 【命令格式】 **ip rns reaction-trigger operation-number target-operation**
【参数说明】 *operation-number* : 触发动作的源 RNS 探测实例编号, 取值范围<1-500>。
target-operation : 被触发的目的 RNS 探测实例编号, 取值范围<1-500>。
【命令模式】 全局模式
【使用指导】 *trigger* 功能通常用在网络故障诊断场景, 普通场景下不需要配置 *trigger* 功能。

配置 RNS 探测实例的调度参数

- 【命令格式】 **ip rns schedule operation-number [life { forever | seconds }] [start-time { hh:mm [:ss] [month day | day month] | pending | now | after hh:mm:ss }] [recurring]**
【参数说明】 *operation-number* : RNS 操作索引, 取值范围<1-500>。
life forever : RNS 探测实例启动后一直运行。
life seconds : RNS 探测实例的运行时间秒数。
hh:mm [:ss] : RNS 探测实例启动时刻, 24 小时制。
month : RNS 探测实例启动的月份, 默认是本月。

day : RNS 探测实例启动的日期，默认是当日。
pending : RNS 探测实例启动时间未定，默认值。
now : RNS 探测实例立即启动。
after hh:mm:ss : RNS 探测实例延迟 hh:mm:ss 的时间后启动。
recurring : RNS 探测实例是否在每天的相同时间启动。

- 【命令模式】 全局模式
- 【使用指导】 已经通过 **ip rns schedule** 命令配置了调度参数的 RNS 探测实例，其配置参数在运行期间无法进行修改，如果要修改该配置，应当先通过 **no ip rns schedule** 命令删除调度参数，然后再进行修改。
life { seconds } 是指 RNS 探测运行时间，即在启动探测后，经过 seconds 时间后将停止探测。

配置 ip rns restart 重新启动一个 RNS 探测

- 【命令格式】 **ip rns restart operation-number**
- 【参数说明】 **operation-number** : RNS 探测实例编号，取值范围<1-500>。
- 【命令模式】 全局模式
- 【使用指导】 该命令将一个已经配置了调度，并调度已停止后(调度状态为 pending)的 RNS 探测重新启动。对于未配置调度的 RNS 探测，该命令无效。

配置 ip rns reset 清空 RNS 探测配置

- 【命令格式】 **ip rns reset**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 该命令清除所有 ip rns 的所有配置信息。只有在极端情况下，才需要使用该命令（例如配置了大量 RNS 探测实例，但发现配置有误）。

配置举例

配置 RNS 基本功能

【网络环境】
图 10-2



- 【配置方法】
- 在交换机 A 上配置探测实例 1
 - 配置探测实例 1 的探测的调度方法、启动时间、生存时间
 - 配置探测实例 1 的主动阈值监控和触发机制
 - 配置探测实例 1 在发生监控阈值超过预期时，触发另一个处于 pending 状态的探测实例 2 探测

```
Switch A
A# configure terminal
A(config)# ip rns 1
A(config-ip-rns)#icmp-echo 10.1.1.1
A(config-ip-rns-icmp-echo)#exit
A(config)#ip rns schedule 1 start-time now life forever
```

```
A(config)#ip rns reaction-configuration 1 react timeout threshold-type immediate action-type trigger
A(config)#ip rns reaction-trigger 1 2
```

【检验方法】 通过 **show ip rns configuration** 命令显示实例配置信息

```
Router#show ip rns configuration 1
Entry number: 1
Tag: ruijie555
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): 3500
Next Scheduled Start Time:Start Time already passed
Target address/Source address: 2.2.2.3/0.0.0.0
Request size (ARR data portion): 36
```

常见错误

无

10.4.2 配置 icmp-echo 探测

配置效果

创建一个 ICMP-Echo 类型的 RNS 探测实例。

注意事项

- 必须先配置 RNS 基本功能。

配置方法

📌 创建 ICMP-Echo 类型的 RNS 探测实例

- 必须配置。
- 若无特殊要求，应在每台交换设备上创建 ICMP-Echo 类型的 RNS 探测实例。

📌 配置探测通用可选参数

- 如果要求改变探测通用可选参数（重复时间间隔、标签、时间阈值、超时时间、TOS 字段等），则必须配置。

- 若无特殊要求，应在每台交换设备上配置探测通用可选参数。

配置探测的协议载荷大小

- 如果要求改变探测的协议载荷大小，则必须配置。
- 若无特殊要求，应在每台交换设备上配置探测的协议载荷大小。

检验方法

- 通过 **show ip rns configuration** 命令查看。

相关命令

创建一个 ICMP-Echo 类型的 RNS 探测实例

【命令格式】 **icmp-echo** { **oob** { *destination-ip-address* | *destination-hostname* [**name-server** *ip-address*] } [**source-ipaddr** *ip-address*] **via** *type num* **next-hop** *ip-address* } | { { *destination-ip-address* | *destination-hostname* [**name-server** *ip-address*] } [**source-ipaddr** *ip-address*] [**out-interface** *type num*] [**next-hop** *ip-address*]] }

【参数说明】 **oob** : MGMT 口探测。

destination-ip-address : 目的 IP。

destination-hostname : 目的主机名。

name-server *ip-address* : 配置目的主机名时，指定域名服务器，默认使用设备上通过 **ip name-server** 配置的域名服务器进行解析。

source-ipaddr *ip-address* : 源 ip 地址。

out-interface *type num* : 指定探测报文的出接口（非 MGMT 口）。

via *type num* : 指定 MGMT 口为探测报文的出接口。

next-hop *A.B.C.D* : 下一跳 ip 地址

【命令模式】 IP RNS 配置模式(config-ip-rns)

【使用指导】 ICMP-Echo 类型的 RNS 探测启动后将发送 ICMP 回显请求报文以探测本机到目标主机网络是否连通。创建 ICMP-Echo 类型的 RNS 探测后将进入 IP RNS ICMP-Echo 模式。默认 ICMP 回显请求报文的协议载荷大小是 36 字节。通过 **request-data-size** 命令，可以修改报文大小。应当先配置 RNS 探测的类型（如 icmp-echo 探测，dns 探测），然后再配置该探测类型的具体参数。如果要修改一个 RNS 探测实例的探测类型，必须先删除该 RNS 探测（通过全局模式下输入 **no ip rns** 命令），再重新进行配置。

配置 RNS 探测实例的协议载荷大小

【命令格式】 **request-data-size** *bytes*

【参数说明】 *bytes* : 探测报文的字节数，不同探测类型的最小/最大字节数不同，依据对应探测类型配置模式下的命令提示进行配置。

【命令模式】 IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)

【使用指导】 该命令主要用来在探测数据包中填充一些字节，以进行较大数据包的探测。

配置探测的重复时间间隔

- 【命令格式】 **frequency** *milliseconds*
- 【参数说明】 *milliseconds* : 报文的发送时间间隔 (毫秒), 默认值 60000 毫秒, 范围<10-604800000>, 最长一周时间。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 在一个 RNS 探测实例启动后, 会进行周期性的探测。通过配置 **frequency** 命令, 可以指定该重复间隔。配置 **frequency** 应当满足下面的公式, 以保证探测的计算正确。
$$(\text{frequency } milliseconds) > (\text{timeout } milliseconds) \geq (\text{threshold } milliseconds)$$

▮ 为 RNS 探测实例设置一个标签

- 【命令格式】 **tag** *text*
- 【参数说明】 *text* : 设置探测的标签, tag 由可打印字符组成, 最长允许输入 79 个字符。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 tag 可以为探测指定一个标签, 通常用于标识这个探测的作用。

▮ 配置 RNS 探测实例的时间阈值

- 【命令格式】 **threshold** *milliseconds*
- 【参数说明】 *milliseconds* : 探测的时间阈值, 取值范围为 0-60000, 单位 ms, 默认值 5000。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 配置 **threshold** 应当满足下面的公式, 以保证探测的计算正确。
$$(\text{frequency } milliseconds) > (\text{timeout } milliseconds) \geq (\text{threshold } milliseconds)$$

▮ 配置 RNS 探测实例的超时时间

- 【命令格式】 **timeout** *millisecond*
- 【参数说明】 *millisecond* : 探测超时时间, 取值范围为 10-604800000, 单位 ms, 不同探测类型, 其超时默认值不同。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 配置 **timeout** 应当满足下面的公式, 以保证探测的计算正确。
$$(\text{frequency } milliseconds) > (\text{timeout } milliseconds) \geq (\text{threshold } milliseconds)$$

▮ 配置 RNS 探测的 IPv4 报文 TOS 字段

- 【命令格式】 **tos** *number*
- 【参数说明】 *number* : 设置探测报文 IPv4 头部的 TOS 字段, 取值范围 0-255。默认为 0。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 TOS 是 IPv4 报文首部中的一个 8bit 字段。通过设置 TOS, 可以控制探测报文的优先级。不同的 TOS, 中间路由器的处理优先程度不同。

▮ 配置 RNS 探测所处的 VRF

- 【命令格式】 **vrf** *vrf-name*

- 【参数说明】 *vrf-name* : 指定 VRF 名称。
- 【命令模式】 IP RNS DNS 配置模式 (*config-ip-rns-dns*)
IP RNS ICMP-Echo 配置模式 (*config-ip-rns-icmp-echo*)
- 【使用指导】 *vrf* 命令将探测报文限定在指定 VRF 中。

配置举例

i 以下配置举例，仅介绍与 *icmp-echo* 相关的配置。

【网络环境】

图 10-3



【配置方法】 在 switch A 上配置 RNS 探测实例 1 及相应参数

Switch A

```
A# configure terminal
A(config)# ip rns 1
A(config-ip-rns)#icmp-echo 10.2.2.2
A(config-ip-rns-icmp-echo)#exit
A(config)#ip rns schedule 1 start-time now life forever
```

【检验方法】 通过 **show ip rns configuration** 命令显示实例配置信息

Switch A

```
A#show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): foerver
Next Scheduled Start Time:Start Time already passed
Target address/Source address: 10.2.2.2/0.0.0.0
Request size (ARR data portion): 36
```

常见错误

无

10.4.3 配置 dns 探测

配置效果

创建一个 DNS 类型的 RNS 探测实例，进行 dns 探测。

注意事项

- 必须先配置 RNS 基本功能。

配置方法

创建 DNS 类型的 RNS 探测实例

- 必须配置。
- 若无特殊要求，应在每台交换设备上创建 DNS 类型的 RNS 探测实例。

配置探测通用可选参数

- 如果要求改变探测通用可选参数（重复时间间隔、标签、时间阈值、超时时间、TOS 字段等），则必须配置。
- 若无特殊要求，应在每台交换设备上配置探测通用可选参数。

检验方法

- 通过 **show ip rns configuration** 命令查看

相关命令

创建一个 DNS 类型的 RNS 探测实例

- 【命令格式】 **dns destination-hostname name-server ip-address [source-ipaddr ip-address] via type num next-hop ip-address }**
- 【参数说明】 **destination-hostname**：目的主机域名。
name-server ip-address：DNS 服务器 IP 地址。
- 【命令模式】 IP RNS 配置模式(config-ip-rns)
- 【使用指导】 DNS 类型的 RNS 探测启动后将发送 DNS 解析请求报文以探测本机到目标主机网络是否连通。创建 DNS 类型的 RNS 探测后将进入 IP RNS DNS 模式。
您必须先配置 RNS 探测的类型，然后再配置该探测类型的具体参数。如果要修改一个 RNS 探测的探测类型，必须先删除该 RNS 探测（通过全局模式下输入 **no ip rns** 命令），再重新进行配置。

配置探测的重复时间间隔

- 【命令格式】 **frequency milliseconds**
- 【参数说明】 **milliseconds**：报文的发送时间间隔（毫秒），默认值 60000 毫秒，范围<10-604800000>，最长一周时间。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 在一个 RNS 探测实例启动后，会进行周期性的探测。通过配置 **frequency** 命令，可以指定该重复间隔。配置

frequency 应当满足下面的公式，以保证探测的计算正确。

$$(\text{frequency milliseconds}) > (\text{timeout milliseconds}) \geq (\text{threshold milliseconds})$$

▾ 为 RNS 探测实例设置一个标签

- 【命令格式】 **tag** *text*
- 【参数说明】 *text*：设置探测的标签，tag 由可打印字符组成，最长允许输入 79 个字符。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 tag 可以为探测指定一个标签，通常用于标识这个探测的作用。

▾ 配置 RNS 探测实例的时间阈值

- 【命令格式】 **threshold** *milliseconds*
- 【参数说明】 *milliseconds*：探测的时间阈值，取值范围为 0-60000，单位 ms，默认值 5000。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 配置 **threshold** 应当满足下面的公式，以保证探测的计算正确。
$$(\text{frequency milliseconds}) > (\text{timeout milliseconds}) \geq (\text{threshold milliseconds})$$

▾ 配置 RNS 探测实例的超时时间

- 【命令格式】 **timeout** *millisecond*
- 【参数说明】 *millisecond*：探测超时时间，取值范围为 10-604800000，单位 ms，不同探测类型，其超时默认值不同。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 配置 **timeout** 应当满足下面的公式，以保证探测的计算正确。
$$(\text{frequency milliseconds}) > (\text{timeout milliseconds}) \geq (\text{threshold milliseconds})$$

▾ 配置 RNS 探测的 IPv4 报文 TOS 字段

- 【命令格式】 **tos** *number*
- 【参数说明】 *number*：设置探测报文 IPv4 首部的 TOS 字段，取值范围 0-255。默认为 0。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 TOS 是 IPv4 报文首部中的一个 8bit 字段。通过设置 TOS，可以控制探测报文的优先级。不同的 TOS，中间路由器的处理优先程度不同。

▾ 配置 RNS 探测所处的 VRF

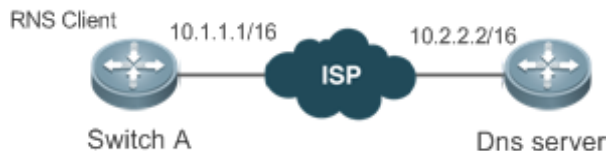
- 【命令格式】 **vrf** *vrf-name*
- 【参数说明】 *vrf-name*：指定 vrf 名称。
- 【命令模式】 IP RNS DNS 配置模式 (config-ip-rns-dns)
IP RNS ICMP-Echo 配置模式 (config-ip-rns-icmp-echo)
- 【使用指导】 vrf 命令将探测报文限定在指定 VRF 中。

配置举例

i 以下配置举例，仅介绍与 dns 相关的配置。

【网络环境】

图 10-4



【配置方法】

在 switch A 上配置 RNS 探测实例 1 及相应参数

Switch A

```
A# configure terminal
A(config)# ip rns 1
A(config-ip-rns)# dns www.ruijie.com.cn name-server 10.2.2.2
A(config-ip-rns-dns)#exit
A(config)#ip rns schedule 1 start-time now life forever
```

【检验方法】

通过 **show ip rns configuration** 命令显示实例配置信息

Switch A

```
A#show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: dns
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): foerver
Next Scheduled Start Time:Start Time already passed
Target host name: www.ruijie.com.cn
Name Server: 10.2.2.2
```

常见错误

- 域名解析服务器 IP 地址错误

10.4.4 配置 track 联动功能

配置效果

- 配置 track 与 rns 联动，track 能跟踪一个 RNS 探测的探测结果。
- 配置 track 跟踪一个接口的链路状态。
- 配置 track 跟踪一个 track 列表的状态。

- 跟踪一个 RNS 探测列表的状态。

注意事项

- 如果配置 track 跟踪一个 RNS 探测的探测结果，则需要配置相应的 RNS 探测。
- 如果配置 track 跟踪一个接口的链路状态，则需要配置相应的接口。
- 如果配置 track 跟踪一个 track 列表的状态，则需要配置相应的 track 列表成员。
- 如果配置 track 跟踪一个 RNS 探测列表的状态，则需要配置相应的 RNS 探测列表成员。

配置方法

配置 track 对象

- 如果要求创建 track 对象，则必须配置。
- 配置 track 对象的四种方法：配置跟踪 RNS 探测的探测结果，配置跟踪接口的链路状态，配置跟踪一个 track 列表的状态，配置跟踪一个 RNS 探测列表的状态。
- 配置跟踪 RNS 探测的探测结果：若无特殊要求，应在每台交换设备上配置跟踪 RNS 探测的探测结果的 track 对象。
- 配置跟踪接口的链路状态：若无特殊要求，应在每台交换设备上配置跟踪接口的链路状态的 track 对象。
- 配置跟踪 track 列表的状态：若无特殊要求，应在每台交换设备上配置跟踪 track 列表状态的 track 对象。
- 配置跟踪 RNS 探测列表的状态：若无特殊要求，应在每台交换设备上配置跟踪 RNS 探测列表状态的 track 对象。

配置 track 对象的延迟通告时间

- 若需要延迟通告 track 对象的状态，则必须设置 track 的延迟通告时间。。
- track 状态的延迟通告时间包括两种：track 状态由 up 变为 down 的延迟通告时间、track 状态由 down 变为 up 的延迟通告时间。可设置其中一种，也可两者都进行设置。
- 若无特殊要求，应在每台交换设备上配置 track 对象的延迟通告时间。

配置 track 成员

- 如果配置 track 对象用于跟踪一个 track 列表的状态，必须配置。
- 配置 track 成员，可配置其满足条件时的状态为 up 或 down。
- 若无特殊要求，应在每台交换设备上配置 track 成员。

检验方法

使 track 跟踪的对象（如 RNS 探测的探测结果、接口的链路状态、track 列表的状态）状态发生变化，观察相应的 track 对象的状态。

- 经过设置的延迟时间后，通过 **show track** 命令查看当前 track 的状态是否发生变化。

相关命令

配置跟踪接口链路状态的 track 对象

- 【命令格式】 **track** *object-number* **interface** *interface-type* *interface-number* **line-protocol**
- 【参数说明】 *object-number* : track 对象的编号, 取值范围为 1-700。
Interface-type interface-number : 接口类型及接口编号。
- 【命令模式】 全局模式
- 【使用指导】 使用该命令配置一个 track 对象, 用来跟踪一个接口的链路状态。当接口链路状态为 up 时, 相应的 track 对象状态为 up。

配置跟踪 RNS 探测的探测结果的 track 对象

- 【命令格式】 **track** *object-number* **rns** *entry-number*
- 【参数说明】 *object-number* : track 对象的编号, 取值范围为 1-700。
entry-number : RNS 探测实例编号, 取值范围为 1-500。
- 【命令模式】 全局模式
- 【使用指导】 使用该命令配置一个 track 对象, 用来跟踪一个 RNS 探测的探测结果。当 RNS 探测的探测结果成功时, 则相应的 track 对象状态为 up。

配置跟踪 track 列表状态的 track 对象

- 【命令格式】 **track** *object-number* **list boolean { and | or }**
- 【参数说明】 *object-number* : track 对象的编号, 取值范围为 1-700。
- 【命令模式】 全局模式
- 【使用指导】 该命令配置一个 track 对象, 用来跟踪一个 track 列表的状态。其结果可以是所有成员状态取 “与” 或者 “或” 的结果。

配置 track 成员

- 【命令格式】 **object** *object-number* [**not**]
- 【参数说明】 *object-number* : track 对象的编号, 取值范围为 1-700。
- 【命令模式】 track 配置模式
- 【使用指导】 该命令配置一个 track 跟踪的 list 对象的成员对象, 可以配置的对象个数仅受 track 对象容量的限制。

配置 track 的延迟时间

- 【命令格式】 **delay { up seconds [down seconds] | [up seconds] down seconds }**
- 【参数说明】 **up seconds** : 指定 track 状态由 down 变为 up 的延迟时间, 取值范围为 0-180, 单位为秒。缺省为 0。
down seconds : 指定 track 状态由 up 变为 down 的延迟时间, 取值范围为 0-180, 单位为秒。缺省为 0。
- 【命令模式】 track 配置模式
- 【使用指导】 当 track 对象的状态不停的震荡, 会使得使用该 track 对象的客户端状态也跟着不停变化。
使用该命令可以延迟通告 track 对象状态的变化。比如某一个 track 对象的状态由 up 变为 down, 如果用户配置了 **delay down 10**, 则 track 对象的 down 状态在 10 秒后才会通告。如果在这段时间内, track 对象的状态又变为 up, 那就不会通告。在使用该 track 对象的客户端看来, track 对象的状态一直是 up 的。

显示 track 的统计信息

- 【命令格式】 **show track** [*object-number*]
- 【参数说明】 *object-number* : 指定 track 对象的编号, 取值范围 1-700。缺省为所有 track 对象。
- 【命令模式】 特权模式
- 【使用指导】 使用该命令可以查看 track 对象的统计信息。

配置举例

配置 track 对象(编号为 3), 跟踪一个接口 (FastEthernet 1/0) 的链路状态。

- 【配置方法】
- 配置 track 对象, 跟踪一个接口的链路状态。
 - 配置状态由 up 变为 down 的延迟时间。

```
Ruijie# configure terminal
Ruijie(config)# track 3 interface FastEthernet 1/0 line-protocol
Ruijie(config-track)# delay down 10
Ruijie(config-track)# exit
```

- 【检验方法】 使接口 FastEthernet 1/0 的链路状态变为 down。
- 立即检查 track 的状态, 确认仍旧为 up。
 - 过 10s 后, 再次检查 track 的状态, 确认 track 的状态变为 down

```
Ruijie# show track 3

Track 3

  Interface FastEthernet 1/0

  The state is Up, delayed Down (5 secs remaining)

    1 change, current state last: 300 secs

  Delay up 0 secs, down 10 secs
```

配置一个 track 对象编号 3, 当 track 对象 1 为 up, 2 为 down 同时满足时, track 对象 3 为 up。

- 【配置方法】
- 配置 track 1 和 track 2 ;
 - 配置 track 3, 其成员为 track 1 和 track 2。

```

Ruijie # config
Ruijie(config)#track 1 interface gigabitEthernet 0/0 line-protocol
Ruijie(config-track)#delay up 20 down 40
Ruijie(config-track)#exit
Ruijie(config)#
Ruijie(config)#track 2 interface gigabitEthernet 0/1 line-protocol
Ruijie(config-track)#delay down 30
Ruijie(config-track)#exit
Ruijie(config)# track 3 list Boolean and
Ruijie(config-track)#object 1
Ruijie(config-track)#object 2 not
Ruijie(config-track)# exit

```

【检验方法】 使 track 1 和 track 2 的状态发生变化，查看 track 3 的状态。

- track 1 的状态由 down 变为 up，track 2 状态保持 down 不变，确认 track 3 的状态由 down 变为 up。
- track 1 的状态保持 up 不变，track 2 状态由 down 变为 up，确认 track 3 的状态由 up 变为 down。

```

Ruijie# show track 3

Track 3
  List boolean and
  Object 1
  Object 2 not
  The state is Down
    1 change,current state last:10 secs
  Delay up 0 secs,down 0 secs

```

🔗 配置 track 对象(编号为 5)，跟踪一个 RNS 探测 (编号为 7) 的探测结果。

- 【配置方法】**
- 配置一个 RNS 探测
 - 配置 track 对象，跟踪一个 RNS 探测的探测结果。
 - 配置探测结果由 up 变为 down、由 down 变为 up 的延迟通告时间。

```

Ruijie# configure terminal
Ruijie (config)#ip rns 7
Ruijie (config-ip-rns)#icmp-echo 2.2.2.2
Ruijie (config-ip-rns-icmp-echo)#exit
Ruijie (config)#ip rns schedule 7 start-time now life forever
Ruijie(config)# track 5 rns 7
Ruijie (config-track)# delay up 20 down 30
Ruijie (config-track)# exit

```

【检验方法】 使编号为 7 的 RNS 探测结果由成功变为失败。

- 探测结果变为失败时立即检查 track 的状态，确认仍旧为 up。
- 过 30s 后，再次检查 track 的状态，确认 track 的状态变为 down。

```
Ruijie# show track 5

Track 5

    Reliable Network Service 7

    The state is Down

        2 change, current state last: 10 secs

    Delay up 20 secs, down 30 secs
```

配置 track 对象(编号为 5)，跟踪一个 RNS 探测列表（编号分别为 1,2-5,8）的探测结果。

- 【配置方法】
- 配置并启动 RNS 探测（参见 RNS 配置）
 - 配置 track 对象，跟踪一个 RNS 探测列表的探测结果。
 - 配置探测结果由 up 变为 down、由 down 变为 up 的延迟通告时间。

```
Ruijie(config)# track 5 rns-list 1,2-5,8 and
Ruijie (config-track)# delay up 20 down 30
Ruijie (config-track)# exit
```

【检验方法】 使编号为 1,2,-5,8 的 RNS 探测中的一个结果由成功变为失败。

- 探测结果变为失败时立即检查 track 的状态，确认仍旧为 up。
- 过 30s 后，再次检查 track 的状态，确认 track 的状态变为 down。

```
Ruijie# show track 5

Track 5

    rns-list 1,2-5,8 and

    The state is Down

        2 change, current state last: 10 secs

    Delay up 20 secs, down 30 secs
```

常见配置错误

- 配置了跟踪 RNS 探测的 track，但未配置相应的 RNS 探测。
- 配置了跟踪接口链路状态的 track，但未配置相应的接口。
- 配置了跟踪 track 列表的 track 对象，但未配置相应的 track 成员。
- 配置了跟踪 RNS 探测列表的 track，但未配置相应的 RNS 探测。

10.5 监视与维护

查看运行情况

作用	命令
查看 rns 对象的配置信息。	show ip rns configuration [<i>operation-number</i>]
查看 rns 对象探测的详细统计信息。	show ip rns collection-statistics [<i>operation-number</i>]
查看 rns 对象探测的当前状态信息。	show ip rns operational-state [<i>operation-number</i>]
查看 rns 对象探测的主动阈值监控信息。	show ip rns reaction-configuration [<i>operation-number</i>]
查看 rns 对象探测的触发探测信息。	show ip rns reaction-trigger [<i>operation-number</i>]
查看 rns 对象的简单统计信息。	show ip rns statistics [<i>operation-number</i>]
查看 track 对象的统计信息。	show track [<i>object-number</i>]
查看 track 客户端的统计信息。	show track client

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 track 模块相关的调试开关。	debug track { <i>all</i> <i>proc-event</i> <i>rdnd-event</i> <i>client</i> }
打开 rns 模块相关的调试开关。	debug rns { <i>all</i> <i>interface</i> <i>lib</i> <i>rdnd-event</i> <i>restart</i> <i>rns_id</i> [<i>0, 500</i>] }

