BFD 技术白皮书

Copyright © 2021 紫光恒越技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除紫光恒越技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。本文中的内容为通用性技术信息，某些信息可能不适用于您所购买的产品。

目 录

1 概述 ····· 1
1.1 产生背景 ····· 1
1.2 技术优点 ····· 1
2 BFD 技术实现 ····· 1
2.1 原理简介 ····· 1
2.2 echo 报文方式的 BFD 会话 ····· 2
2.2.1 BFD echo 报文 ····· 2
2.2.2 BFD 会话的建立 ····· 2
2.2.3 BFD 会话的检测机制 ····· 3
2.3 控制报文方式的 BFD 会话 ····· 3
2.3.1 BFD 控制报文 ····· 3
2.3.2 BFD 会话建立过程 ····· 4
2.3.3 定时器协商 ····· 5
2.3.4 BFD 会话的检测机制 ····· 7
3 SBFD 技术实现 ····· 7
3.1 原理简介 ····· 7
3.2 运行机制 ····· 8
3.3 应用限制 ····· 8
4 Comware 实现的技术特色—硬件 BFD 技术 ····· 8
4.1 产生背景 ····· 8
4.2 运行机制 ····· 9
4.3 应用限制 ····· 9
5 典型组网应用 ····· 10
5.1 路由协议与 BFD 联动典型组网应用 ····· 10
5.2 快速重路由与 BFD 联动典型组网应用 ····· 10
5.3 VRRP 与 BFD 联动典型组网应用 ····· 11
6 参考文献 ····· 12

1 概述

1.1 产生背景

网络设计时，通常使用冗余备份链路来保护关键应用。网络发生故障时，需要设备能够快速检测出故障，并将流量切换至备份链路以加快网络收敛速度。目前有些链路（如 POS）通过硬件检测机制来实现快速故障检测。但是某些链路（如以太网链路）不具备这样的检测机制。此时，应用就要依靠上层协议自身的机制来进行故障检测，上层协议的检测时间都在 1 秒以上，这样的故障检测时间对某些应用来说是不能容忍的。某些路由协议如 OSPF、IS-IS 虽然有 Fast Hello 功能来加快检测速度，但是检测时间也只能达到 1 秒的精度，而且 Fast Hello 功能只是针对本协议的，无法为其它协议提供快速故障检测。

1.2 技术优点

BFD 协议提供了一个通用的、标准化的、介质无关的、协议无关的快速故障检测机制。具有以下优点：

- 对网络设备间任意类型的双向转发路径进行故障检测，包括直连物理链路、虚电路、隧道、MPLS LSP、多跳路由路径以及单向链路等。
- 可以为不同的上层应用服务，提供一致的快速故障检测时间。
- 提供毫秒级的检测速度，从而加快网络收敛速度，减少应用中断时间，提高网络的可靠性。

2 BFD 技术实现

2.1 原理简介

BFD 在两台网络设备上建立会话，用来检测网络设备间的双向转发路径，为上层应用服务。BFD 本身并没有发现机制，而是靠被服务的上层协议通知来建立会话。上层协议在建立新的邻居关系后，将邻居的参数及检测参数（包括目的地址和源地址等）通告给 BFD；BFD 根据收到的参数建立 BFD 会话。会话建立后会周期性地快速发送 BFD 报文，如果在检测时间内没有收到 BFD 报文则认为该双向转发路径发生了故障，并通知该会话所服务的上层应用发生故障，由上层应用采取相应的措施。下面以 OSPF 与 BFD 联动为例，简单介绍会话工作流程。

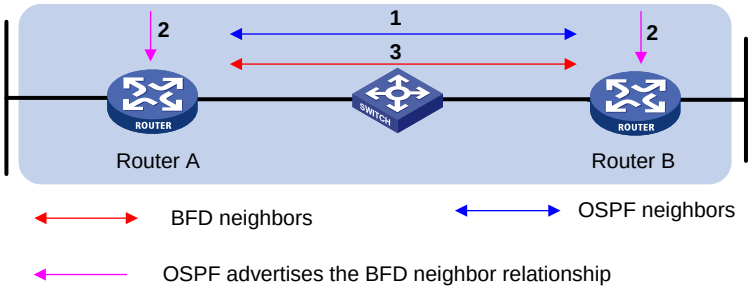
如(3)图 1 所示，上层应用与 BFD 联动触发建立会话的流程为：

(1) OSPF 通过自己的 Hello 机制发现邻居并建立连接；

(2) OSPF 在建立了新的邻居关系后，将邻居信息（包括目的地址和源地址等）通告给 BFD；

(3) BFD 根据收到的邻居信息建立会话。

图1 BFD 会话建立流程图



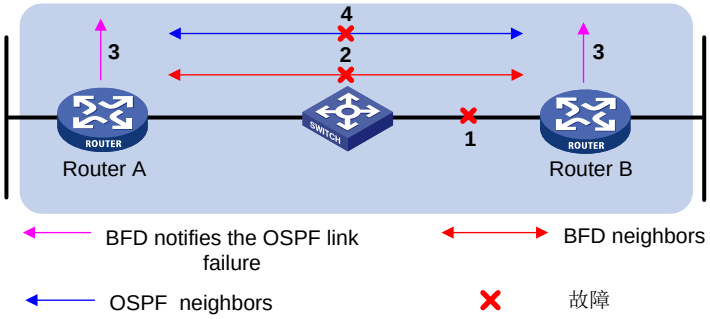
如图 2 所示，BFD 检测到链路故障通知上层应用的流程为：

(1) BFD 检测到链路故障，BFD 邻居不可达，BFD 会话状态变为 Down；

(2) BFD 通知本地 OSPF 进程 BFD 邻居不可达；

(3) 本地 OSPF 进程中断 OSPF 邻居关系。

图2 BFD 故障发现处理流程图



根据使用报文的不同，分为 echo 报文方式的 BFD 会话和控制报文方式的 BFD 会话，下面将分别对这两种方式进行介绍。

2.2 echo报文方式的BFD会话

2.2.1 BFD echo 报文

BFD echo 报文采用 UDP 封装，目的端口号为 3785，目的 IP 地址为发送接口的地址，源 IP 地址由配置产生（配置的源 IP 地址要避免产生 ICMP 重定向）。

BFD 协议并没有对 BFD echo 报文的格式进行定义，唯一的要求是发送方能够通过报文内容区分会话。

2.2.2 BFD 会话的建立

本端发送 echo 报文建立 BFD 会话，对链路进行检测。对端不建立 BFD 会话。

2.2.3 BFD 会话的检测机制

本端发送 echo 报文，对端只需把收到的 echo 报文转发回本端。如果本端在检测时间内没有收到对端转发回的 echo 报文，则认为会话 down。

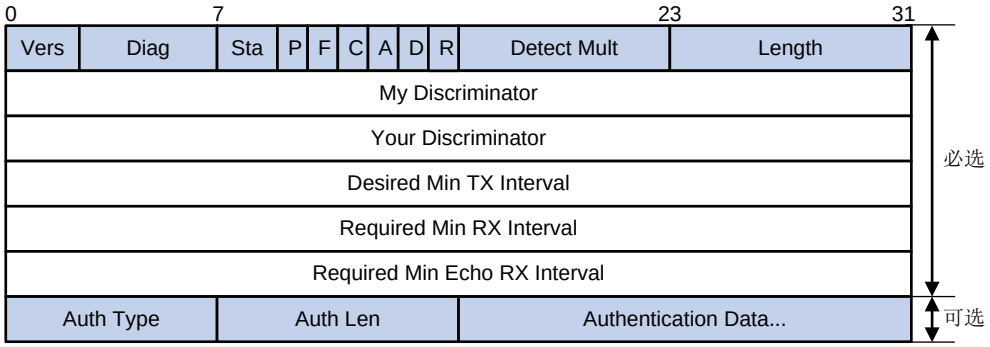
2.3 控制报文方式的BFD会话

2.3.1 BFD 控制报文

BFD 控制报文封装在 UDP 报文中，源端口号的范围为 49152 到 65535，对于单跳检测其 UDP 目的端口号为 3784，对于多跳检测其 UDP 目的端口号为 4784。

如图 3 所示，BFD 控制报文包括强制部分和可选认证部分。

图3 BFD 控制报文



BFD 控制报文各字段含义如表 1 所示。

表1 BFD 控制报文各字段含义

字段	含义
Vers	BFD协议版本号，目前版本号为1
Diag	诊断码，表明发送方最近一次会话Down的原因
Sta	发送方BFD会话当前状态，取值为：0代表AdminDown，1代表Down，2代表Init，3代表Up
P	会话参数变化时置位
F	如果收到的BFD控制报文P字段置位，则将下一个发送的BFD控制报文的F字段置位作为应答
C	该字段置位表明BFD的实现是独立于控制平面的
A	该字段置位表明报文包含认证部分，会话需要进行认证
D	该字段置位表明发送方希望以查询模式运行，不置位表明不希望以查询模式运行或不支持查询模式
R	保留位，发送时设为0，接收时忽略该字段
Detect Mult	检测时间倍数
Length	BFD控制报文长度，单位为字节

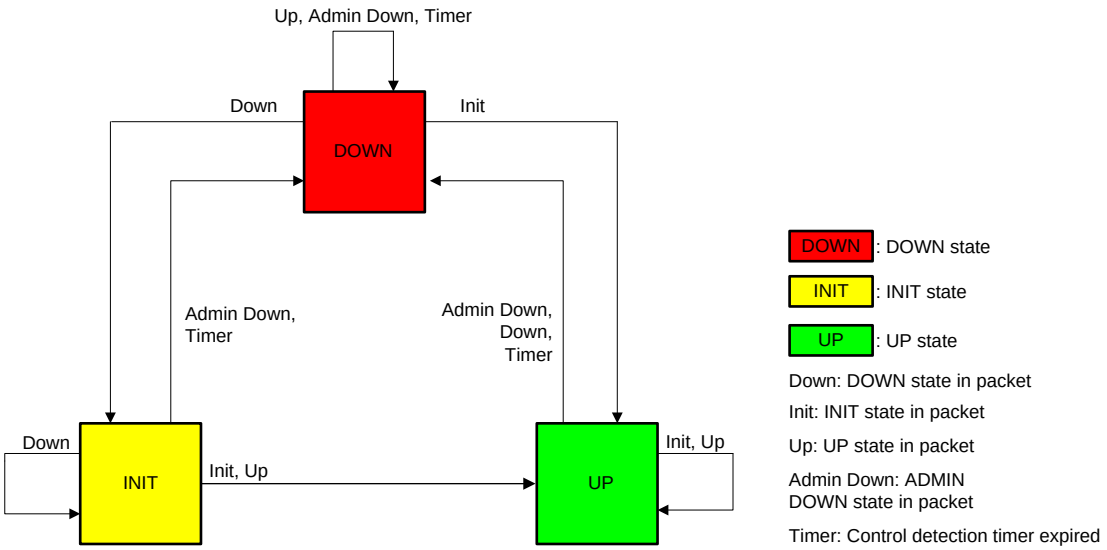
字段	含义
My Discriminator	发送方产生的一个唯一非0值，用来标识不同的BFD会话
Your Discriminator	如果已经收到会话邻居发送的BFD控制报文则该值为收到报文中的My Discriminator，否则为0
Desired Min TX Interval	发送方支持的最小BFD控制报文发送时间间隔，单位为微秒。
Required Min RX Interval	发送方支持的最小BFD控制报文接收时间间隔，单位为微秒
Required Min Echo RX Interval	发送方支持的最小BFD Echo报文接收时间间隔，单位为微秒。为0表示不支持BFD Echo报文
Auth Type	认证类型
Auth Len	可选认证部分长度，包括Auth Type和Auth Len字段，单位为字节
Authentication Data	认证数据区

2.3.2 BFD 会话建立过程

1. BFD 会话的状态机迁移机制

BFD 会话有三种状态，分别为：DOWN、INIT 和 UP。INIT 和 UP 用来建立会话，DOWN 用来断开会话。另外，还有一个特殊状态：ADMIN DOWN，通过管理手段使本端系统阻止建立 BFD 会话时，BFD 会话状态为 ADMIN DOWN。在状态机中 ADMIN DOWN 也是 DOWN 状态。状态机迁移机制如图 4 所示。

图4 BFD 会话状态机迁移机制



2. BFD 会话的建立

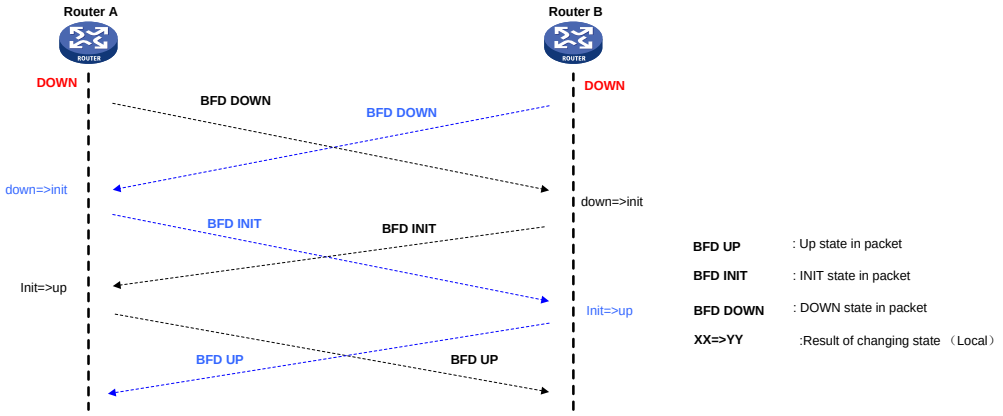
BFD 会话建立前，通过改变 BFD 会话的运行模式可以控制发送 BFD 控制报文的方式：

- 主动模式：在建立会话前不管是否收到对端发来的 BFD 控制报文，都会主动发送 BFD 控制报文；
- 被动模式：在建立会话前不会主动发送 BFD 控制报文，直到收到对端发送来的控制报文。

通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。

BFD 使用三次握手的机制来建立会话，发送方在发送 BFD 控制报文时会在 Sta 字段填入本地当前的会话状态，接收方根据收到的 BFD 控制报文的 Sta 字段以及本地当前会话状态来进行状态机的迁移，建立会话。

图5 BFD 会话建立过程



如图 5 所示，以两端均为主动模式的会话建立过程为例，说明 BFD 如何通过报文交互和状态机的变化建立会话，一端主动模式一端被动模式的会话建立过程基本相同：

(1) Router A 和 Router B 的 BFD 收到上层应用的通知后，发送状态为 DOWN 的 BFD 控制报文。

(2) Router B 收到对端状态为 DOWN 的 BFD 控制报文后，本地会话状态由 DOWN 迁移到 INIT，随后发送的 BFD 控制报文中将 Sta 字段填为 2 表明会话状态为 INIT。Router A 的 BFD 状态变化同 Router B。

(3) Router A 收到对端状态为 INIT 的 BFD 控制报文后，本地会话状态由 INIT 迁移到 UP，随后发送的 BFD 控制报文中将 Sta 字段填为 3 表明会话状态为 UP。Router B 的 BFD 状态变化同 Router A。

(4) BFD 双方状态都为 UP，会话成功建立并开始检测链路状态。

(5) 如果本端 BFD 会话 DOWN，将会向对端发送 Sta 字段填为 1 的 BFD 控制报文，通知对端会话 DOWN，对端的 BFD 会话也迁移到 DOWN 状态。

2.3.3 定时器协商

1. 定时器简介

在建立 BFD 会话的过程中，可以通过报文交互协商的定时器包括：

- BFD 控制报文的发送时间间隔：BFD 会话建立前，发送时间间隔至少为 1 秒，具体发送时间间隔与设备的型号有关，部分设备上会话数量越多发送的间隔越大。这样可以减小报文流量；在会话建立后，则以协商的时间间隔发送 BFD 控制报文，以实现快速检测。

- 检测时间：每当收到 BFD 控制报文时，就会重置检测时间定时器，保持会话 UP 状态。如果在检测时间内没有收到 BFD 控制报文，BFD 会话会迁移到 DOWN 状态，并通知该会话所服务的上层应用发生故障，由上层应用采取相应的措施。

2. 定时器协商机制

BFD 会话协商时，定时器值的选取原则为：

- BFD 控制报文发送时间间隔=MAX（本端 Desired Min TX Interval，对端 Required Min RX Interval），也就是说比较慢的一方决定了发送频率。
- 检测时间=对端 BFD 控制报文中的 Detect Mult×MAX（本端 Required Min RX Interval，对端 Desired Min TX Interval）。

BFD 会话不同方向的定时器协商是分别独立进行的，双向定时器时间可以不同。

在 BFD 会话有效期间，控制报文发送时间间隔和检测时间可以随时协商修改而不影响会话状态。修改原则为：

- 如果加大本端 Desired Min TX Interval，那么本端实际发送 BFD 控制报文的时间间隔必须要等收到对端 F 字段置位的报文后才能改变，这是为了确保在本端加大 BFD 控制报文发送时间间隔前对端已经加大了检测时间，否则可能导致对端检测定时器错误超时。
- 如果减小本端 Required Min RX Interval，那么本端检测时间必须要等收到对端 F 字段置位的报文后才能改变，这是为了确保在本端减小检测时间前对端已经减小了 BFD 控制报文发送间隔时间，否则可能导致本端检测定时器错误超时。
- 然而如果减小 Desired Min TX Interval，本端 BFD 控制报文发送时间间隔将会立即减小；加大 Required Min RX Interval，本端检测时间将会立即加大。

下面详细介绍参数改变后定时器的协商过程。如图 6 所示，Router A 与 Router B 建立 BFD 会话，双方的 Desired Min TX Interval 和 Required Min RX Interval（下面简称为 TX 和 RX）都为 100ms，Detect Mult 都为 3。根据定时器协商规则，Router A 的发送时间间隔为 Router A 的 TX 与 Router B 的 RX 中的最大值也就是 100ms，Router B 的发送时间间隔也是 100ms，双方的检测超时时间都为 300ms。

如果此时将 Router A 的 TX 和 RX 加大到 150 ms。

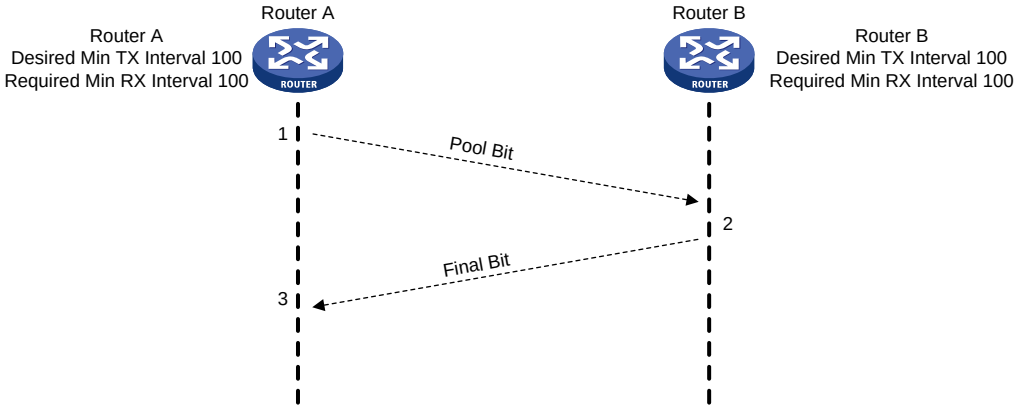
(1) Router A 比较本端的 RX（150ms）和 Router B 的 TX（100ms），从而将本端检测时间改为 450ms。同时向对端发送 P 字段置位的 BFD 控制报文（TX 和 RX 均为 150ms）。

(2) Router B 收到报文后，将收到报文中的 RX 与本端的 TX 进行比较，由于 RX 较大，故 Router B 的发送间隔改为 150ms。经过比较本端 RX 和对端的 TX，从而将检测时间也增大到 450ms。调整完成后给 Router A 回复 F 字段置位的 BFD 控制报文（TX 和 RX 均为 100ms）。

(3) Router A 收到对端发来 F 字段置位的控制报文。根据报文中的 RX 与本端的 TX 进行比较计算出新的时间间隔为 150ms。

(4) 定时器协商完成，双方的发送间隔和检测时间分别为 150ms 和 450ms。

图6 BFD 检测时间协商



2.3.4 BFD 会话的检测机制

BFD 会话建立后，两端通过周期性发送控制报文对链路进行检测。

BFD 支持两种检测模式：

- 异步模式：设备周期性发送 BFD 控制报文，如果在检测时间内没有收到对端发送的 BFD 控制报文，则认为会话 down。
- 查询模式：
  - 本端的 BFD 会话工作在查询模式时，本端设备会向对端发送 D 比特位置 1 的 BFD 控制报文，对端（缺省为异步模式）收到该报文后将停止周期性发送 BFD 控制报文。
  - 如果通信双方都是查询模式，则双方都停止周期性发送 BFD 控制报文。当需要验证连通性的时候，设备会以协商的周期连续发送几个 P 比特位置 1 的 BFD 控制报文。如果在检测时间内没有收到返回的报文，就认为会话 down；如果收到对方回应的 F 比特位置 1 的报文，就认为连通，停止发送报文，等待下一次触发查询。
  - 当系统中的 BFD 会话数量较多时，采用查询模式可防止周期性发送 BFD 控制报文的开销对系统的正常运行造成影响。

控制报文方式的 BFD 会话还可以通过回声功能辅助进行故障检测。回声功能启动后，会话的一端周期性地发送 BFD echo 报文，同时自动降低控制报文的接收速率，减少对带宽资源的消耗。对端不对 BFD echo 报文进行处理，而只将此报文转发回发送端。如果发送端连续几个 echo 报文都没有接收到，会话状态将变为 DOWN。

回声功能只可以检测直连网段故障，即 BFD echo 报文是单跳发送。

3 SBFD 技术实现

3.1 原理简介

SBFD（Seamless BFD，无缝 BFD）是一种单向的故障检测机制，其检测速度比 BFD 更快速，适用于仅一端需要进行链路状态检测的情况，如 MPLS TE 隧道和使用 LDP 动态建立 LSP 的场景。

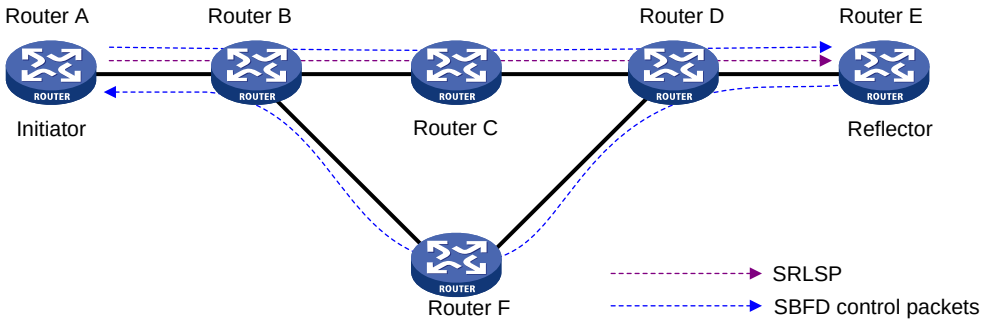
3.2 运行机制

SBFD 会话中，设备的角色分为 Initiator 和 Reflector：

- Initiator 通过周期性发送 SBFD 控制报文来检测网络节点到远端实体的链路是否可达。Initiator 将 SBFD 报文注入到 MPLS TE 隧道或 LDP LSP 中，由 Initiator 发起 SBFD 会话并维护 SBFD 会话的状态信息。
- Reflector 监听到达本地实体的 SBFD 控制报文，并发送 SBFD 控制报文类型的响应报文给 Initiator。

如图 7 所示，作为 Initiator 的 Router A 通过基于 SR（Segment Routing，段路由）建立的 MPLS TE 隧道，向作为 Reflector 的 Router E 发送 SBFD 控制报文。Router A 只要能够收到 Router E 发送的 SBFD 控制报文，即认为从 Router A 到 Router E 的 SRLSP 路径可达。

图7 SBFD 的 Initiator 和 Reflector



3.3 应用限制

Initiator 上指定的 SBFD 会话的远端标识符必须为 Reflector 上手工指定的 SBFD 会话本地标识符。否则，当 Reflector 收到 Initiator 发送的 SBFD 控制报文后，发现报文中携带的远端标识符不是自己的本地标识符时，不会发送响应报文给 Initiator。

4 Comware 实现的技术特色—硬件 BFD 技术

4.1 产生背景

软件 BFD 是指 BFD 检测过程中的报文收发、BFD 会话状态机的维护完全依赖 CPU 来处理。软件 BFD 会极大的消耗 CPU 能力。同时，受 CPU 性能影响，能够支持的 BFD 会话规格较小，无法用于大规格 BFD 会话需求的应用场景。

硬件 BFD 将发送报文、接收报文以及故障检测等消耗 CPU 性能的功能转移到硬件芯片上处理，从而提升 CPU 的利用率，以便支持大规格的 BFD 会话。

4.2 运行机制

对于 echo 报文方式的 BFD 会话，第一次收到转发回来的 echo 报文后，BFD 会话就会尝试转移到硬件芯片。如果检测到硬件芯片可以支持 BFD，系统会通知软件处理成功，软件不再维护 BFD 会话。如果检测到硬件芯片不支持 BFD，系统会通知软件处理失败，仍然由软件维护 BFD 会话。

控制报文方式的 BFD 会话状态需要通过控制报文进行协商，硬件芯片的功能比较简单，不能完成 BFD 会话协商功能。因此在会话状态 UP 之前，需要通过 CPU 维护。会话 UP 之后，会尝试转移到硬件芯片。如果系统检测到硬件芯片可以支持 BFD，会通知软件处理成功，软件不再维护 BFD 会话。如果系统检测到硬件芯片不支持 BFD，会通知软件处理失败，仍然由软件维护 BFD 会话。如果需要调整会话的各种参数，则由软件进行协商。

为了支持大规格 BFD 会话的并发协商能力，在协商定时器时，硬件 BFD 会话有一些特殊的处理：

(1) 本端在 DOWN 状态收到 INIT 报文，或者在 INIT 状态收到 UP 报文后，BFD 会话变成 UP 状态，并开始向对端发送 P 字段置位的报文。报文中携带的会话发送时间间隔、接收时间间隔和检测倍数都设置为设备支持的最大值。

(2) 对端收到 P 字段置位的报文时，回应 F 字段置位的报文。

(3) 当本端收到对端回应的 F 字段置位的报文，表明对端已经按照最大值调整好，此时开始尝试将发送时间间隔、接收时间间隔和检测倍数下调到配置的值，并向对端发送新的 P 字段置位的报文。报文中携带的发送时间间隔、接收时间间隔和检测倍数为配置的值。由于发送时间间隔变小，因此本端报文的发送时间间隔调整为 MAX（配置的发送时间间隔，上一次收到的对端发送时间间隔）；测时间调整为 MAX（最大接收时间间隔，对端接收时间间隔）×本端检测倍数。

(4) 对端收到新的 P 字段置位的报文时，回应 F 字段置位的报文。

(5) 当本端收到对端回应的新的 F 字段置位的报文，表明对端已经按照 P 字段置位的报文中携带的发送时间间隔、接收时间间隔和检测倍数调整好了实际发送时间间隔和检测时间。此时本端检测时间调整为 MAX（配置的接收时间间隔，对端接收时间间隔）×本端检测倍数。

(6) 如果本端未收到对端回应的 F 字段置位的报文，会持续向对端发送 P 字段置位的报文，在此期间定时器的值为发起协商前的值。直到收到对端回应的 F 字段置位的报文，协商过程才能结束，BFD 按照协商后的结果调整定时器的值。

4.3 应用限制

目前，硬件 BFD 存在如下限制：

- 硬件芯片对 BFD 会话的发送时间、接收时间和检测倍数有一定的限制，比如发送时间、接收时间可能要求必须是 10ms 的整数倍。
- 暂不支持对 BFD 报文进行认证。
- 硬件 BFD 的协商较普通 BFD 的协商流程复杂，因此耗时更久，如果在协商未完成之前链路发生故障，可能导致检测时间较长。

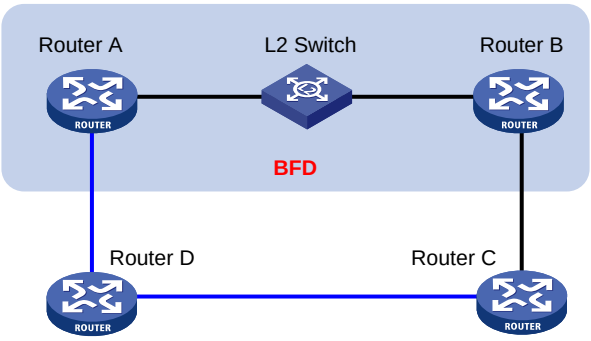
5 典型组网应用

5.1 路由协议与BFD联动典型组网应用

如图 8 所示，两台路由器 Router A、Router B 通过二层交换机互连，在设备上运行路由协议，网络层相互可达。

由于通过二层交换机相连，Router A 与 Router B 之间的链路故障可能不会导致接口 DOWN，只能通过协议握手去检测。通过在 Router A 与 Router B 之间使用 BFD 就能快速检测出故障，路由协议得到 BFD 通知后可以尽快计算新的路由，从而缩短收敛时间。

图8 路由协议与 BFD 联动组网图



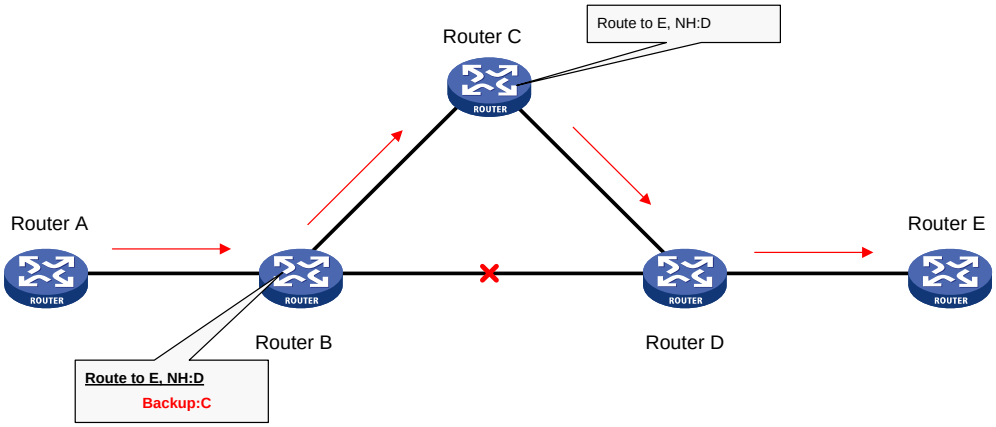
5.2 快速重路由与BFD联动典型组网应用

随着网络的快速发展，IP 网络越来越多的承载语音、视频等多种业务，这些业务对网络的高可靠性提出了更高的要求，从而运营商网络要求更快的收敛速度。

BFD 应用于路由协议以及路由协议快速收敛技术的使用虽然很大程度提高了收敛速度，但还是无法满足语音、视频等新业务对业务中断时间的要求。

而快速重路由和 BFD 联动技术可以很好的满足这种要求，如图 9 所示，通过提前计算备用路径，快速发现主用路径故障，并在主用路径故障时不依赖于控制平面的收敛而直接在转发平面切换至备用路径，极大的缩短了业务中断时间。

图9 快速重路由与 BFD 联动组网图

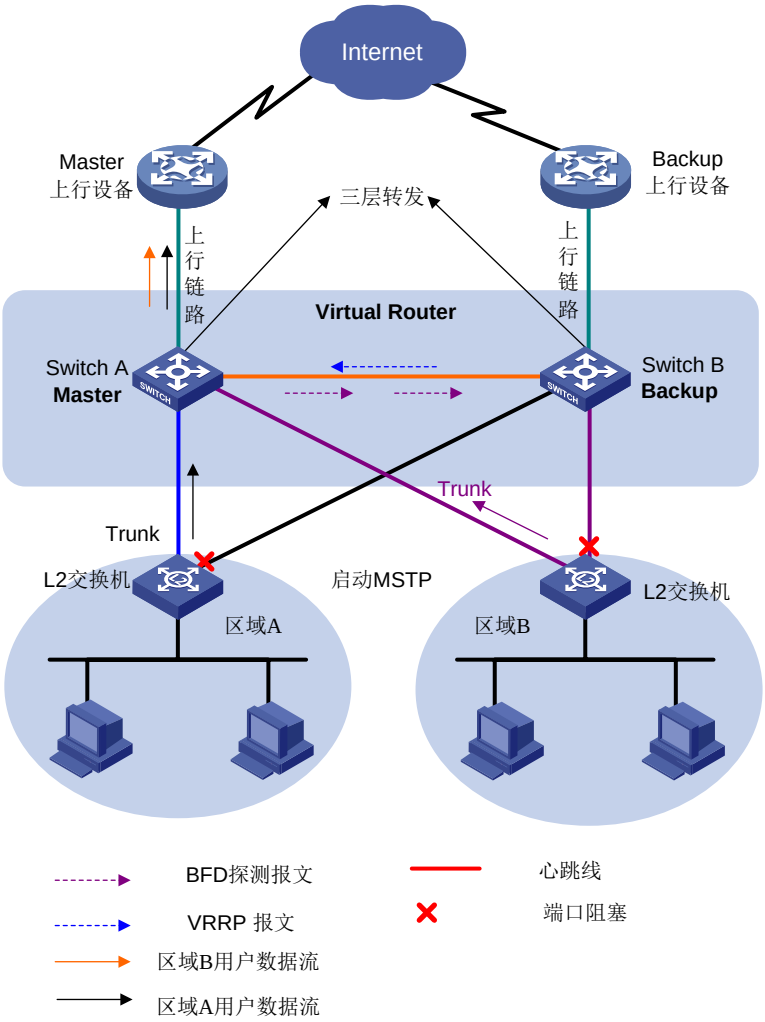


5.3 VRRP与BFD联动典型组网应用

VRRP 的协议关键点是当 Master 出现故障时，Backup 能够快速接替 Master 的转发工作，保证用户数据流的中断时间尽量短。当 Master 出现故障时，VRRP 依靠 Backup 设置的超时时间来判断是否应该抢占，切换速度在 1 秒以上。如图 10 所示，将 BFD 应用于 Backup 对 Master 的检测，可以实现对 Master 故障的快速检测，缩短用户流量中断时间。

VRRP 还会监视 Master 的上行链路能否正常工作，Master 即使正常工作，但是如果其上行链路出现了故障，用户报文实际上也是无法正常转发的。VRRP 是依靠监视接口状态来判断上行链路是否正常工作的，当被监视的接口 DOWN 掉时，Master 主动降低优先级，引起切换。这种监视接口的处理方式依赖于接口的协议状态，如果上行链路出现故障而接口不 DOWN 则无法感知到。将 BFD 应用于 VRRP 上行链路的检测可以有效解决问题。

图10 VRRP 与 BFD 联动典型组网图



6 参考文献

- RFC 5880：Bidirectional Forwarding Detection (BFD)
- RFC 5881：Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)
- RFC 5882：Generic Application of Bidirectional Forwarding Detection (BFD)
- RFC 5883：Bidirectional Forwarding Detection (BFD) for Multihop Paths