BFD

双向转发检测 BFD（Bidirectional Forwarding Detection）是一种全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况，具有以下优点：（UDP 3784）

1 对相邻转发引擎之间的通道提供轻负荷、快速故障检测。这些故障包括接口、数据链路，甚至有可能是转发引擎本身

2 用单一的机制对任何介质、任何协议层进行实时检测

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 本身并没有邻居发现机制，而是靠被服务的上层应用通知其邻居信息以建立会话。会话建立后会周期性地快速发送 BFD 报文，如果在检测时间(3s)内没有收到 BFD 报文则认为该双向转发路径发生了故障，通知被服务的上层应用进行相应的处理

具体工作过程

（1）BFD 会话建立方式

BFD 会话的建立有两种方式，即静态建立 BFD 会话和动态建立 BFD 会话。静态和动态创建 BFD 会话的主要区别在于本地标识符（Local Discriminator）和远端标识符（Remote Discriminator）的配置方式不同。BFD 通过控制报文中的 LocalDiscriminator 和 Remote Discriminator 区分不同的会话

1 静态建立 BFD 会话（VRRP、静态路由）

静态建立 BFD 会话是指通过命令行手工配置 BFD 会话参数，包括配置本地标识符和远端标识符等，然后手工下发 BFD 会话建立请求

2 动态建立 BFD 会话（OSPF、BGP、RIP、ISIS、PIM、MPLS LDP）
动态建立 BFD 会话时，系统对本地标识符和远端标识符的处理方式如下：

3 动态分配本地标识符
当应用程序触发动态创建 BFD 会话时，系统分配属于动态会话标识符区域的值作为 BFD 会话的本地标识符。然后向对端发送 Remote Discriminator 的值为 0 的 BFD 控制报文，进行会话协商

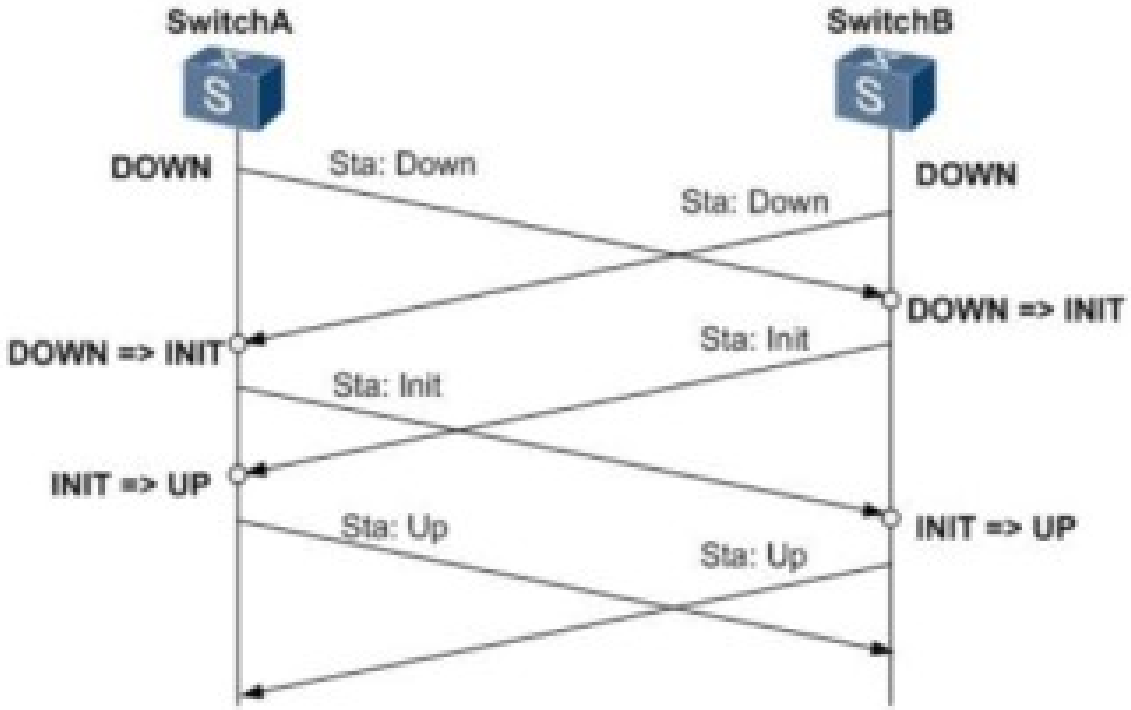
4 自学习远端标识符
当 BFD 会话的一端收到 Remote Discriminator 的值为 0 的 BFD 控制报文时，判断该报文是否与本地 BFD 会话匹配，如果匹配，则学习接收到的 BFD 报文中 LocalDiscriminator 的值，获取远端标识符

BFD 检测机制

BFD 的检测机制是两个系统建立 BFD 会话，并沿它们之间的路径周期性发送 BFD 控制报文，如果一方在既定的时间内没有收到 BFD 控制报文，则认为路径上发生了故障。
BFD 提供异步检测模式。在这种模式下，系统之间相互周期性地发送 BFD 控制报文，如果某个系统连续几个报文都没有接收到，就认为此 BFD 会话的状态是 Down。

BFD 会话管理

BFD 会话有四种状态：Down、Init、Up 和 AdminDown。会话状态变化通过 BFD 报文的 State 字段传递，系统根据自己本地的会话状态和接收到的对端 BFD 报文驱动状态改变。BFD 状态机的建立和拆除都采用三次握手机制，以确保两端系统都能知道状态的变化



1 SwitchA 和 SwitchB 各自启动 BFD 状态机，初始状态为 Down，发送状态为 Down 的 BFD 报文。对于静态配置 BFD 会话，报文中的 Remote Discriminator 的值是用户指定的；对于动态创建 BFD 会话，Remote Discriminator 的值是 0
2 SwitchB 收到状态为 Down 的 BFD 报文后，状态切换至 Init，并发送状态为 Init 的 BFD 报文
3 SwitchA 收到状态为 Down 的 BFD 报文后，状态切换至 Init，并发送状态为 Init 的 BFD 报文
4 SwitchB 本地 BFD 状态为 Init 后，不再处理接收到的状态为 Down 的报文
5 SwitchA 本地 BFD 状态为 Init 后，不再处理接收到的状态为 Down 的报文
6 SwitchB 收到状态为 Init 的 BFD 报文后，本地状态切换至 Up
7 SwitchA 收到状态为 Init 的 BFD 报文后，本地状态切换至 Up

扩展追问 1：可以和哪些协议联动？
答：可以和静态路由、OSPF、IS-IS、BGP、MPLS、VRRP、PI

M 等协议进行联动。

扩展追问 2：BFD 与 OSPF 怎样联动？

BFD 会话建立过程如下所示：
<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
<4>会话建立以后，BFD 开始检测链路故障，并做出快速反应

发现故障处理流程：
<1>被检测链路出现故障
<2>BFD 快速检测到链路故障，BFD 会话状态变为 Down
<3>BFD 通知本地 OSPF 进程 BFD 邻居不可达
<4>本地 OSPF 进程中断 OSPF 邻居关系

SNMP

SNMP 的定义与组成

通过网络管理软件可以集中式对多台设备进行统一管理，并且可以直观的看到网络设备的运行情况。而且可以通过网管软件对设备进行相应的配置 SNMP 系统包括网络管理系统 NMS（Network Management System）、代理进程 Agent、被管对象 Management object 和管理信息库 MIB（Management Information Base）四部分组成：

NMS 作为整个网络的网管中心，对设备进行管理。每个被管理设备中都包含驻留在设备上的 Agent 进程、MIB 和多个被管对象。NMS 通过与运行在被管理设备上的 Agent 交互，由 Agent 通过对设备端的

MIB 的操作，完成 NMS 的指令

各版本间操作的差异：

SNMPv1：包括 Get、GetNext、Set、Response 和 Trap

SNMPv2c：包括 Get、GetNext、Set、Response 、Trap、Getbulk、inform

SMMPv3：包括 Get、GetNext、Set、Response 、Trap、Getbulk、inform

SNMP v1、v2c、v3 各自的特点？

（1）各个版本间的差异：

1 SNMPv1 基于团体名认证，安全性较差，且返回报文的错误码也较少。读取效率慢

2 SNMPv2c 中引入了 GetBulk 和 Inform 操作，支持更多的标准错误码信息，支持更多的数据类型提高读取效率

3 SNMPv3 版本提供了基于 USM（User Security Module）的基于 VACM（View-based Access Control Model）的访问控制

a）基于用户认证（针对不同的用户分配密码，访问权限），提高

安全性对报文传输过程中进行可选加密
b）USM：提供身份验证和数据加密服务（新加入了用户名和对数据进行加密，防止数据被窃取）
c）VACM：对用户组或者团体名实现基于视图的访问控制

扩展问题 1：现网中常用的是 SNMPv2c，但是还一直使用 SNMPv1 的 trap 报文，而不常用 inform 报文？
因为现网中丢包的情况很少出现，所以使用 trap 报文即可实现被管理设备的告警，而使用 inform 报文的话虽然也能实现告警，但是会增加报文的交互数量、消耗设备的处理性能；
因为 infrom-request 报文会重复的发送给到 NMS，直到重传时间超时或者 NMS 发送 infrom-response 报文给到 Agent 时，infrom 报文才会停止发送；

扩展问题 2：Agent 是什么？代理一台设备还是还几台设备？
Agent 是一台运行了 Agent 进程的设备（路由器或者交换机等），主要是管理本台设备上的接口、CPU、内存等；代理的其实是本台设备；