BFD在IPv4_IPv6单跳_多跳环境应用方案 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/289/2021_2022_BFD_E5_9C_A8IPv4_c101_289628.htm 1. BFD应用于IPv4/IPv6单跳环境 在IPV4/V6的单跳环境中，部署BFD来检测转发路径的连通性，其基本工作原理相同，这里介绍和具体应用相关的几个问题，首先是如何区分一个会话，其次是BFD和Echo报文使用什么封装，最后介绍一下单跳环境下的安全机制。 1.1 会话区分 在单跳环境中，会话区分比较简单，这是因为BFD协议规定，对于同一个数据协议（如IPV4或IPV6），不管其中有多少应用（如BGP、OSPF、IS-IS等）需要使用BFD提供的检测服务，在同一个逻辑或物理接口，两个系统之间都只能建立一个BFD会话。这样一来，对于收到的BFD会话初始报文，虽然其“ Your Discirminator ”为0，但系统根据报文封装、接收报文的接口就可以区分出BFD报文属于哪个会话。 使用同一个会话的各种应用使用相同的参数，这样，如果各个应用要求的故障检测时间不一样，需要系统自身设计策略处理这种情况，一种可行的策略是：选取所有应用中检测时间最短的参数作为报文发送间隔，对于要求检测时间更长的应用，可以对来自BFD的通知滞后反应。 1.2 BFD报文封装 在IPV4单跳环境中，BFD控制报文必须使用UDP封装，目的端口必须是3784，源端口在49152和65535之间。虽然BFD会话并不由源端口区分，而是由“ Your Discriminator ”区分，但为了实现的高效，同一个会话必须使用相同的源端口。如果超过16384个会话同时激活，源端口可以重用，但应该均匀重用各个源端口（比如使用Hash）。某些BFD实现可能使用UDP源端口来

区分BFD会话，但最终的区分还是应该使用“ Your Discriminator ”。BFD报文的源IP地址和目的IP地址必须包含在发送BFD报文的接口的子网地址中。 IPV4单跳环境中，BFD的回声报文也必须使用UDP封装，目的端口为3785，源端口可由具体的应用来确定。Echo报文的目的地址的选择标准是必须使对端把报文沿原路回送，源地址的选择标准是不会导致对端发送ICMP重定向报文。Echo报文的其他内容不作具体要求，只要能区分出Echo属于哪个Session即可。 IPV6环境中，BFD报文和回声报文的封装和各种要求和IPV4环境中一样，唯一的不同是用IPV6封装替换了IPV4封装。 1.3 安全考虑 在单跳环境中，在不启用认证的情况下，BFD采用了一种简单的轻载安全机制：所有BFD控制报文在发送时，其TTL或Hop count必须为255.如果接收到的BFD控制报文，其TTL或Hop count不为255，那么必须丢弃，这种机制在一定程度上避免了跨网段的伪造BFD报文攻击，提供了一定安全性，同时避免了使用认证时对设备处理造成的负荷。 如果使用了认证，发送报文时TTL或Hop count也必须为255，不过接收报文时没有强制要求TTL或Hop count不为255必须丢弃。在IPV4和IPV6隧道情况下，如果隧道不改变TTL或Hop count，那么可使用不加认证的BFD来提供一定的安全性，否则应该使用认证机制。 2. BFD应用于IPv4/IPv6多跳环境 多跳环境和单跳环境相比，有一定不同。首先是单跳环境下的使用跳数来判断的轻载安全机制不能使用，保证安全性必须使用认证字段。 其次，在IPV4/IPV6多跳环境中，BFD报文的封装稍有不同，虽然也使用UDP封装，不过目的端口必须使用4784.最大的不同是区分会话的方式不一样。我们知道，一个会话

为检测一条转发路径的连通性而建立，在多跳环境中，不同转发路径之间可能有不同程度的重叠，包括第一跳接口和最后一跳接口都有可能重叠。因此，象单跳环境那样使用接口区分不太现实。BFD在多跳环境下有两种方式来区分会话：l一种是只关心源地址和目的地址之间的转发路径是否连通，不关心中间经过的节点。这种情况下，当收到BFD会话初始报文（“ Your Discirminator ”为0）时，使用源和目的地址来区分属于哪个会话。l另一种是使用带外方式来预先获取discriminator.这样在BFD会话初始报文中就会携带非0的“ Your Discirminator ”，使用“ Your Discirminator ”就可以直接区分会话。BFD for MPLS就使用这种方式，通过使用LSP-ping[RFC4379]来预先获取Discriminator.这种方式的缺点是需要额外的组件来预先获取discriminator. 另外，需要讨论一下单向链路上的BFD部署的问题。单向链路就象交通规则中“ 单行道 ”，在该链路上数据是单向流通的，不过可通过其他路径作回程。因为回程路径可能是多跳的，所以单向链路上BFD的部署也被纳入多跳范畴。单向路径可以用一种比较巧妙的方法解决会话区分问题，因为在单向链路上是单跳的，所以在该方向上是可以用接口区分会话的，因此，只要要避免在区分出会话之前使用可能为多跳的回程路径发送BFD报文，就可以解决单向链路及其回程路径的会话区分问题。这正好可以利用BFD的“ 角色 ”特性：设定单向链路的发送方工作在Active角色，接收方工作在Passive角色。那么对于接收方来说，收到发送方的BFD报文，通过接收报文的接口就可区分会话，同时也确认了“ Your Discirminator ”字段，这时才开始从回程路径发送BFD报文，因为这时已经确认

了“ Your Discirminator ”，所以对端也可以区分会话。 最后，需要说明一下BFD在MPLS网络中作多跳部署时，和FRR的共存问题。如果BFD的检测时间比FRR切换时间短，那么即使FRR成功切换到了备份路径，BFD还会报错，容易引起错误处理。所以BFD协议规定，在这种情况下BFD的检测时间应该比FRR切换时间长。 不过，BFD可代替RSVP Hello用于FRR时的邻居故障检测，这时BFD作单跳部署，不必把BFD检测时间设置为比FRR切换时间长。原因如下：对于链路down，BFD上报故障时能携带故障原因，所以设备对于BFD报的链路down和链路层上报的链路down不会重复处理；至于链路单通、节点故障则可用BFD检测到，并触发FRR. 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com