

目 录

1 MPLS OAM.....	1-1
1.1 MPLS OAM简介.....	1-1
1.1.1 MPLS Ping.....	1-1
1.1.2 MPLS Trace route.....	1-1
1.1.3 MPLS与BFD联动.....	1-1
1.1.4 周期性MPLS Trace route.....	1-2
1.1.5 协议规范.....	1-2
1.2 配置LSP隧道的MPLS OAM功能.....	1-2
1.2.1 配置MPLS Ping功能.....	1-2
1.2.2 配置MPLS Trace route功能.....	1-3
1.2.3 配置使用BFD检测LSP.....	1-3
1.2.4 使能LSP的周期性Trace route功能.....	1-4
1.3 配置MPLS TE隧道的MPLS OAM功能.....	1-4
1.3.1 配置MPLS Ping功能.....	1-4
1.3.2 配置MPLS Trace route功能.....	1-4
1.3.3 配置使用BFD检测MPLS TE隧道.....	1-5
1.4 配置PW的MPLS OAM功能.....	1-6
1.4.1 配置MPLS Ping功能.....	1-6
1.4.2 配置使用BFD检测PW.....	1-6
1.5 MPLS OAM显示和维护.....	1-10
1.6 MPLS OAM典型配置举例.....	1-10
1.6.1 BFD检测LSP配置举例.....	1-10

1 MPLS OAM

1.1 MPLS OAM简介

MPLS OAM (Operations, Administration and Maintenance, 操作、管理和维护) 功能为 MPLS 网络提供了数据平面连通性检测、数据平面与控制平面一致性校验、故障点定位等多种错误管理 (Fault Management) 工具。MPLS OAM 利用这些错误管理工具对 LSP、MPLS TE 隧道和 MPLS PW 进行检测和故障定位, 降低了 MPLS 网络的管理和维护的复杂度, 提高了 MPLS 网络的可用性。

MPLS OAM 提供的错误管理工具分为如下两类:

- 手工按需检测工具 (on-demand 工具): 根据需要手工触发的检测工具, 如 MPLS ping、MPLS Trace route。
- 系统主动检测工具 (proactive 工具): 系统主动启动、无需手工触发的检测工具, 如 MPLS 与 BFD 联动、周期性 MPLS Trace route。

1.1.1 MPLS Ping

用来对 LSP 隧道、MPLS TE 隧道或 PW 的连通性进行手工检测。MPLS Ping 的工作机制是: 在 Ingress 节点为 MPLS Echo Request 报文压入待检测隧道对应的标签; 经过隧道将该报文转发到 Egress 节点; Egress 节点处理该报文后, 回应 MPLS Echo Reply 报文; 如果 Ingress 节点接收到表示成功的 MPLS Echo Reply 报文, 则说明该隧道可以用于数据转发; 如果 Ingress 节点接收到带有错误码的 MPLS Echo Reply 报文, 则说明该隧道存在故障。

1.1.2 MPLS Trace route

用来查看 LSP 隧道或 MPLS TE 隧道从 Ingress 节点到 Egress 节点所经过的路径, 以便对 LSP 隧道或 MPLS TE 隧道的错误点进行定位。MPLS Trace route 功能通过沿着隧道连续发送 TTL 从 1 到某个值的 MPLS Echo Request 报文, 让隧道经过的每一跳收到该报文后, 返回 MPLS Echo Reply 报文。这样, Ingress 节点可以收集到隧道上每一跳的信息, 从而定位出故障节点。同时, MPLS Trace route 功能还可用于收集整条隧道上每个节点的重要信息, 如下游分配的标签等。

1.1.3 MPLS与BFD联动

MPLS 与 BFD 联动功能是指通过 BFD 会话来主动检测 LSP 隧道、MPLS TE 隧道或 PW 的连通性。当 BFD 检测到连通故障后, 触发设备及时进行相应地处理, 如快速重路由或路径保护倒换, 使得流量转发得以继续。

MPLS 与 BFD 联动功能的工作机制是: 在待检测隧道的 Ingress 节点和 Egress 节点之间建立 BFD 会话; 在 Ingress 节点为 BFD 控制报文压入隧道对应的标签; 沿着隧道转发 BFD 控制报文; 根据收到的 Egress 节点的 BFD 控制报文来判断隧道的状态。

可以通过两种方式建立检测 LSP 隧道、MPLS TE 隧道或 PW 的 BFD 会话:

- 静态方式: 通过命令行手工指定本地和远端的标识符, 根据指定的标识符建立 BFD 会话。
- 动态方式: 不需要手工指定本地和远端的标识符, 系统自动运行 MPLS Ping 来协商标识符, 并根据协商好的标识符建立 BFD 会话。

对于 LSP 隧道和 MPLS TE 隧道,采用静态方式时,Egress 节点通过反向隧道转发 BFD 控制报文;采用动态方式时,如果存在反向隧道,则 Egress 节点通过反向隧道转发 BFD 控制报文,否则,通过 IP 路由转发 BFD 控制报文。因此,静态方式用来检测两台设备间从本地到远端和从远端到本地的一对 LSP 隧道或 MPLS TE 隧道;动态方式用来检测两台设备间从本地到远端的一条单向 LSP 隧道或 MPLS TE 隧道。

由于 PW 是一条双向隧道,对于 PW,静态方式和动态方式的作用相同,都是用来检测一条 PW。

1.1.4 周期性MPLS Trace route

周期性 MPLS Trace route 功能,即周期性地对 LSP 隧道进行 Trace route 主动检测,用来对 LSP 隧道的错误点进行定位,对数据平面和控制平面一致性进行校验,并将发现的错误记录到系统日志(System Log Messages)中。管理员可以通过查看日志信息,了解 LSP 隧道是否出现故障。

如果同时配置了 BFD 自动检测 LSP 功能和周期性 MPLS Trace route 功能,则周期性 MPLS Trace route 检测到数据平面与控制平面不一致时,会拆除 BFD 会话,并基于控制平面重新建立 BFD 会话。

1.1.5 协议规范

与 MPLS OAM 相关的协议规范有:

- RFC 4379: Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 5085: Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- RFC 5885: Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)

1.2 配置LSP隧道的MPLS OAM功能

LSP 隧道的连通性检测方式分为以下两种:

- 按需方式: 执行 **ping mpls ipv4** 命令或 **tracert mpls ipv4** 命令手工触发 LSP 检测。
- 主动方式: 配置 BFD 检测 LSP 功能或 LSP 的周期性 Trace route 后,系统主动完成 LSP 检测。

1.2.1 配置MPLS Ping功能

表1-1 配置 MPLS ping 功能

操作	命令	说明
通过MPLS Ping功能检测IPv4地址前缀类型LSP的连通性	ping mpls [-a <i>source-ip</i> -c <i>count</i> -exp <i>exp-value</i> -h <i>ttl-value</i> -m <i>wait-time</i> -r <i>reply-mode</i> -rtos <i>tos-value</i> -s <i>packet-size</i> -t <i>time-out</i> -v] * ipv4 <i>dest-addr mask-length</i> [destination <i>start-address</i> [<i>end-address</i> [<i>address-increment</i>]]]	可在任意视图下配置本命令

1.2.2 配置MPLS Trace route功能

表1-2 配置 MPLS Trace route 功能

操作	命令	说明
通过MPLS Trace route功能查看IPv4地址前缀类型LSP从Ingress节点到Egress节点所经过的路径	tracert mpls [-a source-ip -exp exp-value -h ttl-value -r reply-mode -rtos tos-value -t time-out -v fec-check] * ipv4 dest-addr mask-length [destination start-address [end-address [address-increment]]]	可在任意视图下配置本命令

1.2.3 配置使用BFD检测LSP

要想在本地和远端设备之间建立检测LSP的BFD会话，本地和远端设备上需要进行的配置如 [表 1-3](#) 所示。

表1-3 本地和远端设备上的配置

BFD 会话建立方式	节点类型	是否需要执行 mpls bfd enable 命令	是否需要执行 mpls bfd 命令	是否需要通过 discriminator 参数指定标识符
静态方式	本地	是	是	是
	远端	是	是	是
动态方式	本地	是	是	否
	远端	是	否	-

配置使用 BFD 检测 LSP 时，需要注意：

- 配置静态方式 BFD 会话时，两端设备上配置的本地和远端标识符必须匹配，即本地设备上配置的本地标识符与远端设备上配置的远端标识符相同；本地设备上配置的远端标识符与远端设备上配置的本地标识符相同。
- BFD 会话的源地址为本端设备的 MPLS LSR ID。因此，配置 BFD 检测 LSP 功能前，需要先在本地设备上配置 MPLS LSR ID，并确保远端设备上存在到达 MPLS LSR ID 的路由。
- 为某一个 FEC 配置 BFD 检测时，要么指定下一跳创建会话，要么不指定下一跳自动为每个下一跳分别创建一个 BFD 会话，不能同时配置两种方式。
- 通过静态方式建立 BFD 会话时，Ingress 和 Egress 节点均工作在主动（Active）模式；通过动态方式建立 BFD 会话时，Ingress 节点工作在被动（Passive）模式，Egress 节点工作在主动（Active）模式。在 Ingress 节点和 Egress 节点上执行 **bfd session init-mode** 命令不会改变节点的工作模式。

表1-4 使用 BFD 检测 LSP

操作	命令	说明
进入系统视图	system-view	-
使能MPLS与BFD联动功能	mpls bfd enable	缺省情况下，MPLS与BFD联动功能处于关闭状态

操作	命令	说明
使用BFD检测指定FEC对应LSP的连通性	mpls bfd <i>dest-addr mask-length</i> [nexthop <i>nexthop-address</i> [discriminator local local-id remote remote-id]] [template <i>template-name</i>]	缺省情况下，未使用BFD检测FEC对应LSP的连通性

1.2.4 使能LSP的周期性Trace route功能

表1-5 使能 LSP 的周期性 Trace route 功能

操作	命令	说明
进入系统视图	system-view	-
使能MPLS与BFD联动功能	mpls bfd enable	缺省情况下，MPLS与BFD联动功能处于关闭状态
使能指定FEC对应LSP的周期性Trace route功能	mpls periodic-tracert <i>dest-addr mask-length</i> [-a <i>source-ip</i> -exp <i>exp-value</i> -h <i>ttl-value</i> -m <i>wait-time</i> -rtos <i>tos-value</i> -t <i>time-out</i> -u <i>retry-attempt</i> fec-check] *	缺省情况下，LSP的周期性Trace route功能处于关闭状态

1.3 配置MPLS TE隧道的MPLS OAM功能

MPLS TE 隧道的连通性检测方式分为以下两种：

- 按需方式：执行 **ping mpls te** 命令或 **tracert mpls te** 命令手工触发 MPLS TE 隧道检测。
- 主动方式：配置 BFD 检测 MPLS TE 隧道功能后，系统主动完成 MPLS TE 隧道检测。

1.3.1 配置MPLS Ping功能

表1-6 配置 MPLS ping 功能

操作	命令	说明
通过MPLS Ping功能检测MPLS TE隧道的连通性	ping mpls [-a <i>source-ip</i> -c <i>count</i> -exp <i>exp-value</i> -h <i>ttl-value</i> -m <i>wait-time</i> -r <i>reply-mode</i> -rtos <i>tos-value</i> -s <i>packet-size</i> -t <i>time-out</i> -v] * te <i>tunnel interface-number</i>	可在任意视图下配置本命令

1.3.2 配置MPLS Trace route功能

表1-7 配置 MPLS Trace route 功能

操作	命令	说明
通过MPLS Trace route功能查看MPLS TE隧道从Ingress节点到Egress节点所经过的路径	tracert mpls [-a <i>source-ip</i> -exp <i>exp-value</i> -h <i>ttl-value</i> -r <i>reply-mode</i> -rtos <i>tos-value</i> -t <i>time-out</i> -v fec-check] * te <i>tunnel interface-number</i>	可在任意视图下配置本命令

1.3.3 配置使用BFD检测MPLS TE隧道

要想在本地和远端设备之间建立检测MPLS TE隧道的BFD会话，本地和远端设备上需要进行的配置如表 1-8 所示。

表1-8 本地和远端设备上的配置

BFD 会话建立方式	节点类型	是否需要执行 mpls bfd enable 命令	是否需要执行 mpls bfd 命令	是否需要通过 discriminator 参数指定标识符
静态方式	本地	是	是	是
	远端	是	是	是
动态方式	本地	是	是	否
	远端	是	否	-

配置使用 BFD 检测 MPLS TE 隧道时，需要注意：

- 配置静态方式 BFD 会话时，两端设备上配置的本地和远端标识符必须匹配，即本地设备上配置的本地标识符与远端设备上配置的远端标识符相同；本地设备上配置的远端标识符与远端设备上配置的本地标识符相同。
- BFD 会话的源地址为本端设备的 MPLS LSR ID。因此，配置 BFD 检测 MPLS TE 隧道功能前，需要先在本地设备上配置 MPLS LSR ID，并确保远端设备上存在到达 MPLS LSR ID 的路由。
- 通过静态方式建立 BFD 会话时，Ingress 和 Egress 节点均工作在主动（Active）模式；通过动态方式建立 BFD 会话时，Ingress 节点工作在被动（Passive）模式，Egress 节点工作在主动（Active）模式。在 Ingress 节点和 Egress 节点上执行 **bfd session init-mode** 命令不会改变节点的工作模式。
- 如果在 MPLS TE 隧道上同时使用了 FRR 和 BFD 检测 TE 隧道功能，则为了保证 FRR 切换不会导致检测 TE 隧道的 BFD 会话 down，需要配置检测 TE 隧道的 BFD 会话的检测周期大于 FRR 触发机制（如 BFD 检测 RSVP 邻居）的检测周期。

表1-9 配置使用 BFD 检测 MPLS TE 隧道

操作	命令	说明
进入系统视图	system-view	-
使能MPLS与BFD联动功能	mpls bfd enable	缺省情况下，MPLS与BFD联动功能处于关闭状态
进入MPLS TE隧道对应的Tunnel接口视图	interface tunnel number	-
配置使用BFD检测当前隧道接口对应MPLS TE隧道的连通性	mpls bfd [discriminator local local-id remote remote-id] [template template-name]	缺省情况下，未使用BFD检测隧道接口对应MPLS TE隧道的连通性

1.4 配置PW的MPLS OAM功能

VCCV (Virtual Circuit Connectivity Verification, 虚电路连通性验证) 是一种 L2VPN PW OAM 功能, 用于确认 PW 数据平面的连通性。VCCV 有两种方式:

- 按需方式: 执行 **ping mpls pw** 命令手工触发 PW 检测。
- 主动方式: 配置通过 BFD 或 Raw-BFD 检测 PW 后, 系统主动完成 PW 检测。

用来检测 PW 连通性的报文统称为 VCCV 报文。PE 通过 CC (Control Channel, 控制通道) 来传送 VCCV 报文。

CC 有以下几种类型:

- **control-word** 类型: 通过控制字, 即 PW-ACH (PW Associated Channel Header, PW 随路通道首部), 标识 VCCV 报文。只有 PW 支持控制字时, 才能选择这种类型。控制字的详细介绍, 请参见“MPLS 配置指导”中的“MPLS L2VPN”。
- **router-alert** 类型: 通过在 PW 标签之前携带 MPLS 路由器告警标签来标识 VCCV 报文。
- **ttl** 类型: 通过将 PW 标签的 TTL 值设置为 1 来标识 VCCV 报文。

CV (Connectivity Verification, 连通性验证) 类型, 即检测工具类型, 分为如下几种:

- LSP Ping 类型: 采用 MPLS ping 检测 PW 的连通性。
- BFD 方式: 采用 BFD 检测 PW 的连通性, BFD 报文的封装方式为 IP/UDP Encapsulation (with IP/UDP Headers)。
- Raw-BFD 方式: 采用 BFD 检测 PW 的连通性, BFD 报文的封装方式为 PW-ACH Encapsulation (without IP/UDP Headers), 即封装在 VCCV 控制通道内的 BFD 控制报文不携带 IP 和 UDP 头。只有控制通道类型为 **control-word** 时, 指定本参数才会生效。

1.4.1 配置MPLS Ping功能

执行本配置前, 需要先:

- (1) 创建 PW 模板, 并在 PW 模板视图下通过 **vccv cc** 命令配置 VCCV 控制通道类型。
- (2) 创建 PW, 并指定该 PW 引用上述步骤中创建的 PW 模板。

表1-10 配置 MPLS ping 功能

操作	命令	说明
通过MPLS Ping功能检测PW的连通性	<pre>ping mpls [-a source-ip -c count -exp exp-value -h ttl-value -m wait-time -r reply-mode -rtos tos-value -s packet-size -t time-out -v] * pw ip-address pw-id pw-id</pre>	可在任意视图下配置本命令

1.4.2 配置使用BFD检测PW

使用 BFD 检测 PW 功能的配置步骤为:

- (1) 使能 MPLS 与 BFD 联动功能。
- (2) 创建 PW 模板, 并在 PW 模板视图下配置使用 BFD 检测 PW 的连通性。
- (3) 创建 PW, 并指定该 PW 引用上述步骤中创建的 PW 模板。

从上述步骤中可以看出，使用 BFD 检测 PW 功能并不是直接在 PW 上配置，而是通过引用 PW 模板间接来配置。

完成上述配置后，最终是否使用 BFD 检测 PW 的连通性、BFD 报文采用何种封装方式以及采用何种 VCCV 控制通道，由两端的配置共同决定：

- 如果两端 PE 上都配置了 BFD 检测 PW 且 BFD 报文封装方式相同，则采用该封装方式检测 PW；否则，不使用 BFD 检测 PW 的连通性。
- 如果两端 PE 上配置了相同的 VCCV 控制通道类型，则使用该 VCCV 控制通道；否则，不使用任何 VCCV 控制通道，这样会导致无法建立 BFD 会话。

1. 配置使用BFD检测MPLS L2VPN的PW

本配置可以用来检测 MPLS L2VPN 的静态 PW 和 LDP PW。

表1-11 配置使用 BFD 检测 MPLS L2VPN 的 PW

操作	命令	说明
进入系统视图	system-view	-
使能MPLS与BFD联动功能	mpls bfd enable	缺省情况下，MPLS与BFD联动功能处于关闭状态
创建PW模板，并进入PW模板视图	pw-class class-name	缺省情况下，设备上不存在任何PW模板
配置使用BFD检测PW的连通性	vccv bfd [raw-bfd] [template template-name]	缺省情况下，未使用BFD检测PW的连通性 执行本命令时如果指定了 raw-bfd 参数，则需要配置控制通道类型为 control-word
配置VCCV控制通道类型	vccv cc { control-word router-alert }	缺省情况下，没有指定VCCV控制通道类型
退回系统视图	quit	-
进入交叉连接组视图	xconnect-group group-name	-
进入交叉连接视图	connection connection-name	-
配置PW，引用已创建的PW模板，并进入PW视图	peer ip-address pw-id pw-id [in-label label-value out-label label-value] pw-class class-name [tunnel-policy tunnel-policy-name]	缺省情况下，未配置PW
（可选）配置检测PW的BFD会话的本地标识符和远端标识符	bfd discriminator local local-id remote remote-id	缺省情况下，没有指定检测PW的BFD会话的本地标识符和远端标识符 本端PE上配置的标识符需要和对端PE上配置的标识符相对应
（可选）配置备份PW，引用已创建的PW模板，并进入备份PW视图	backup-peer ip-address pw-id pw-id [in-label label-value out-label label-value] pw-class class-name [tunnel-policy tunnel-policy-name]	缺省情况下，未配置备份PW

操作	命令	说明
(可选) 配置检测备份PW的BFD会话的本地标识符和远端标识符	bfd discriminator local local-id remote remote-id	缺省情况下, 没有指定检测备份PW的BFD会话的本地标识符和远端标识符 本端PE上配置的标识符需要和对端PE上配置的标识符相对应

2. 配置使用BFD检测VPLS的静态PW

表1-12 配置使用 BFD 检测 VPLS 的静态 PW

操作	命令	说明
进入系统视图	system-view	-
使能MPLS与BFD联动功能	mpls bfd enable	缺省情况下, MPLS与BFD联动功能处于关闭状态
创建PW模板, 并进入PW模板视图	pw-class class-name	缺省情况下, 设备上不存在任何PW模板
配置使用BFD检测PW的连通性	vccv bfd [raw-bfd] [template template-name]	缺省情况下, 未使用BFD检测PW的连通性 执行本命令时如果指定了 raw-bfd 参数, 则需要配置控制通道类型为 control-word
配置VCCV控制通道类型	vccv cc { control-word router-alert }	缺省情况下, 没有指定VCCV控制通道类型
退回系统视图	quit	-
进入VSI视图	vsi vsi-name [hub-spoke]	-
指定VSI采用静态配置方式建立PW, 并进入VSI static视图	pwsignaling static	缺省情况下, 未指定VSI使用的PW信令协议
配置VPLS的PW, 引用已创建的PW模板, 并进入VSI static PW视图	peer ip-address pw-id pw-id in-label label-value out-label label-value pw-class class-name [hub no-split-horizon tunnel-policy tunnel-policy-name] *	缺省情况下, 未配置VPLS的PW
(可选) 配置检测PW的BFD会话的本地标识符和远端标识符	bfd discriminator local local-id remote remote-id	缺省情况下, 没有指定检测PW的BFD会话的本地标识符和远端标识符 本端PE上配置的标识符需要和对端PE上配置的标识符 相对应
(可选) 配置备份的静态PW, 引用已创建的PW模板, 并进入VSI static备份PW视图	backup-peer ip-address pw-id pw-id in-label label-value out-label label-value pw-class class-name [tunnel-policy tunnel-policy-name]	缺省情况下, 未配置VPLS的备份PW

操作	命令	说明
(可选) 配置检测备份PW的BFD会话的本地标识符和远端标识符	bfd discriminator local local-id remote remote-id	缺省情况下, 没有指定检测备份PW的BFD会话的本地标识符和远端标识符 本端PE上配置的标识符需要和对端PE上配置的标识符 相对应

3. 配置使用BFD检测VPLS的LDP PW

表1-13 配置使用 BFD 检测 VPLS 的 LDP PW

操作	命令	说明
进入系统视图	system-view	-
使能MPLS与BFD联动功能	mpls bfd enable	缺省情况下, MPLS与BFD联动功能处于关闭状态
创建PW模板, 并进入PW模板视图	pw-class class-name	缺省情况下, 设备上不存在任何PW模板
配置使用BFD检测PW的连通性	vccv bfd [raw-bfd] [template template-name]	缺省情况下, 未使用BFD检测PW的连通性 执行本命令时如果指定了 raw-bfd 参数, 则需要配置控制通道类型为 control-word
配置VCCV控制通道类型	vccv cc { control-word router-alert }	缺省情况下, 没有指定VCCV控制通道类型
退回系统视图	quit	-
进入VSI视图	vsi vsi-name [hub-spoke]	-
指定VSI使用LDP信令建立PW, 并进入VSI LDP视图	pwsignaling ldp	缺省情况下, 未指定VSI使用的PW信令协议
配置VPLS的PW, 引用已创建的PW模板, 并进入VSI LDP PW视图	peer ip-address pw-id pw-id pw-class class-name [hub no-split-horizon tnl-policy tunnel-policy-name] *	缺省情况下, 未配置VPLS的PW
(可选) 配置检测PW的BFD会话的本地标识符和远端标识符	bfd discriminator local local-id remote remote-id	缺省情况下, 没有指定检测PW的BFD会话的本地标识符和远端标识符 本端PE上配置的标识符需要和对端PE上配置的标识符相对应
(可选) 配置备份的LDP PW, 引用已创建的PW模板, 并进入VSI LDP备份PW视图	backup-peer ip-address pw-id pw-id pw-class class-name [tunnel-policy tunnel-policy-name]	缺省情况下, 未配置VPLS的备份PW
(可选) 配置检测备份PW的BFD会话的本地标识符和远端标识符	bfd discriminator local local-id remote remote-id	缺省情况下, 没有指定检测备份PW的BFD会话的本地标识符和远端标识符 本端PE上配置的标识符需要和对端PE上配置的标识符 相对应

1.5 MPLS OAM显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MPLS OAM 的运行情况，通过查看显示信息验证配置的效果。

表1-14 MPLS OAM 显示和维护

操作	命令
显示LSP隧道或MPLS TE隧道的BFD检测信息	display mpls bfd [ipv4 dest-addr mask-length te tunnel tunnel-number]
显示PW的BFD检测信息	display l2vpn pw bfd [peer peer-ip pw-id pw-id]

1.6 MPLS OAM典型配置举例

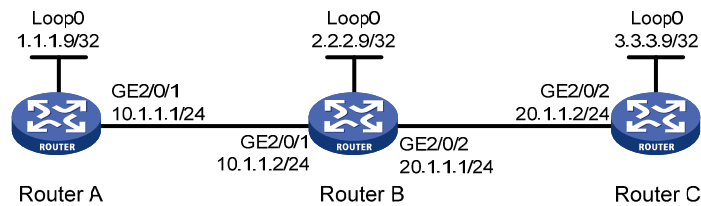
1.6.1 BFD检测LSP配置举例

1. 组网需求

利用 LDP 建立 1.1.1.9/32 到 3.3.3.9/32、3.3.3.9/32 到 1.1.1.9/32 两条 LSP 后，使用 BFD 检测 LSP 隧道的连通性。

2. 组网图

图1-1 BFD 检测 LSP 配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址

按照上图配置各接口 IP 地址和掩码，包括三层以太网接口和 Loopback 接口，具体配置过程略。

(2) 配置 OSPF，以保证各设备之间路由可达

配置 Router A。

```
<RouterA> system-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
<RouterB> system-view
[RouterB] ospf
```

```
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
<RouterC> system-view
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

(3) 使能 MPLS 和 LDP 功能

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.9
[RouterA] mpls ldp
[RouterA-ldp] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] mpls enable
[RouterA-GigabitEthernet2/0/1] mpls ldp enable
[RouterA-GigabitEthernet2/0/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.9
[RouterB] mpls ldp
[RouterB-ldp] quit
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] mpls enable
[RouterB-GigabitEthernet2/0/1] mpls ldp enable
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] mpls enable
[RouterB-GigabitEthernet2/0/2] mpls ldp enable
[RouterB-GigabitEthernet2/0/2] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.9
[RouterC] mpls ldp
[RouterC-ldp] quit
[RouterC] interface gigabitethernet 2/0/2
[RouterC-GigabitEthernet2/0/2] mpls enable
[RouterC-GigabitEthernet2/0/2] mpls ldp enable
[RouterC-GigabitEthernet2/0/2] quit
```

(4) 使能 MPLS 与 BFD 联动功能，并配置通过 BFD 检测 LSP 的连通性

配置 Router A。

```
[RouterA] mpls bfd enable
[RouterA] mpls bfd 3.3.3.9 32
```

配置 Router C。

```
[RouterC] mpls bfd enable  
[RouterC] mpls bfd 1.1.1.9 32
```

4. 验证配置

配置完成后，在设备 Router A 和 Router C 上执行 **display mpls bfd** 命令，可以看到检测 LSP 的 BFD 会话的建立情况。以 Router A 为例。

```
[RouterA] display mpls bfd  
Total number of sessions: 2, 2 up, 0 down, 0 init  
  
FEC Type: LSP  
FEC Info:  
  Destination: 1.1.1.9  
  Mask Length: 32  
NHLFE ID: -  
Local Discr: 513                Remote Discr: 513  
Source IP: 1.1.1.9             Destination IP: 3.3.3.9  
Session State: Up              Session Role: Active  
Template Name: -  
  
FEC Type: LSP  
FEC Info:  
  Destination: 3.3.3.9  
  Mask Length: 32  
NHLFE ID: 1042  
Local Discr: 514                Remote Discr: 514  
Source IP: 1.1.1.9             Destination IP: 127.0.0.1  
Session State: Up              Session Role: Passive  
Template Name: -
```

以上显示信息表示，Router A 和 Router C 之间建立了两个 BFD 会话，分别用来检测 3.3.3.9/32 到 1.1.1.9/32、1.1.1.9/32 到 3.3.3.9/32 两条 LSP。