

HUAWEI 中低端路由器产品 MPLS 故障处理手册

声明

Copyright ©2006

华为技术有限公司

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、复制本书内容的部分或全部，并不得以任何形式传播。

、HUAWEI®、华为®、C&C08®、EAST8000®、HONET®、、视点®、ViewPoint®、INtess®、ETS®、DMC®、TELLIN®、InfoLink®、Netkey®、Quidway®、SYNLOCK®、Radium®、雷霆®、M900/M1800®、TELESIGHT®、Quidview®、Musa®、视点通®、Airbridge®、Tellwin®、Inmedia®、VRP®、DOPRA®、iTELLIN®、HUAWEI OptiX®、C&C08 iNET®、NETENGINE™、OptiX™、iSite™、U-SYS™、iMUSE™、OpenEye™、Lansway™、SmartAX™、边际网™、infoX™、TopEng™均为华为技术有限公司的商标。

对于本手册中出现的其它商标，由各自的所有人拥有。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

技术支持

技术支持网址：<http://support.huawei.com>

客户服务电话：8008302118 0755-28560000

地址：深圳市龙岗区坂田华为总部办公楼

客户服务邮箱：support@huawei.com

传真：0755-28560111

邮编：518129

目 录

声明.....	i
技术支持	i
HUAWEI 中低端路由器 MPLS 故障处理手册	1
1 MPLS 故障处理方法	1
1.1 MPLS 故障处理综述	1
1.1.1 MPLS 概述.....	1
1.1.2 MPLS 应用.....	1
1.1.3 MPLS 基本能力配置	3
1.1.4 MPLS VPN 故障通用诊断流程	4
1.2 案例分析.....	5
1.2.1 MPLS L2VPN 故障诊断与排除	5
1.2.2 MPLS VPN 业务时通时断.....	6

HUAWEI 中低端路由器 MPLS 故障处理手册

1 1 MPLS 故障处理方法

1.1 MPLS 故障处理综述

1. MPLS 概述

MPLS (Multiprotocol Label Switching) 是多协议标签交换的简称, 它用短而定长的标签来封装网络层分组。MPLS 从各种链路层 (如 PPP、ATM、帧中继、以太网等) 得到链路层服务, 又为网络层提供面向连接的服务。MPLS 能从 IP 路由协议和控制协议中得到支持, 同时, 还支持基于策略的约束路由, 它路由功能强大、灵活, 可以满足各种新应用对网络的要求。这种技术起源于 IPv4, 但其核心技术可扩展到多种网络协议 (IPv6、IPX 等)。

MPLS 最初是为提高路由器的转发速度而提出一个协议, 但是, 它的用途已不仅仅局限于此, 而是广泛地应用于流量工程 (Traffic Engineering)、VPN、QoS 等方面, 从而日益成为大规模 IP 网络的重要标准。

2. MPLS 应用

基于 MPLS 的 VPN

传统的 VPN 一般是通过 GRE、L2TP、PPTP 等隧道协议来实现私有网络间数据流在公网上的传送。LSP 本身就是公网上的隧道, 用 MPLS 来实现 VPN 有天然的优势。基于 MPLS 的 VPN 就是通过 LSP 将私有网络在地域上的不同分支联结起来, 形成一个统一的网络。基于 MPLS 的 VPN 还支持不同 VPN 间的互通。



表 1 基于 MPLS 的 VPN

图1 基于 MPLS 的 VPN

表 1 给出了基于 MPLS 的 VPN 的基本结构。CE (Customer Edge) 是用户边缘设备, 可以是路由器, 也可以是交换机, 甚至是一台主机; PE (Provider Edge) 是服务商边缘路由器, 位于骨干网络; PE 负责对 VPN 用户进行管理、建立各 PE 间 LSP 连接、同一 VPN 用户各分支间路由分派。

PE 间的私有网络路由分派通常是用扩展的 BGP 协议实现的。基于 MPLS 的 VPN 支持不同 VPN 间 IP 地址复用和不同 VPN 间互通, 和传统的路由相比, VPN 路由中需要增加分支和 VPN 的标识信息, 这就需要对 BGP 协议进行扩展才能携带 VPN 的路由信息。

基于 MPLS 的 QoS

为了能够在 IP 网络上支持语音, 视频等实时业务, 需要有 QoS 的支持, 以便保证重要的、敏感或者实时性较强的数据流在网络中得到优先处理。华为设备支持基于 MPLS 的 Diff-serv 特性, 在保证网络高效利用率的同时, 又能根据不同数据流的优先级实现差别服务, 从而为语音, 视频数据流提供有带宽保证的、低延时、低丢包率的服务。由于目前全网实施流量工程的难度比较大, 因此, 在实际的组网方案中, 往往倾向于使用差分服务模型来实施 QoS。

Diff-Serv 的基本机制是: 在网络边缘, 根据业务的服务质量要求, 将该业务映射到一定的业务类别中, 利用 IP 分组中的 DS 字段 (由 TOS 域而来) 唯一的标记该类业务, 然后, 骨干网络中的各节点根据该字段对各种业务采取预先设定的服务策略, 保证相应的服务质量。Diff-Serv 的这种对服务质量的分类和标签机制和 MPLS 的标签分配十分相似, 事实上, 基于 MPLS 的 Diff-Serv 就是通过将 DS 的分配融入 MPLS 的标签分配过程来实现的。

Diff-Serv 对不同的服务类别规定了一致的处理方法, 包括队列选择、排队、丢弃等操作, 这些处理组合就叫 PHB (Per Hop Behavior)。同时, 属于同一 PHB 的分组又可以有不同的丢弃优先级。PHB 和丢弃优先级信息通过为分组分配不同的 DS

编码来表示，这些 DS 编码又称 DSCP（Diff-Serv Code Point）。关于 Diff-Serv 的详细介绍，请参见本手册的 QoS 配置部分。

为了支持基于 Diff-Serv 模型的端到端的 QoS 服务，提供如下几种技术手段：

- 基于流量的 IP 优先级分类

IP 优先级分类在网络边缘进行，利用 IPv4 包头的 Type-of-Service 3 个比特对每一个 IP 包依据其地址进行优先级分类。在核心利用不同的队列技术对不同等级的流量进行不同的处理，使得不同的服务级别得到体现。为实现语音、图象、数据流的差分服务，对不同的业务流在进行标签交换时，即 PE 在给报文加 Label 时，会把 IP 报文携带的 TOS 值映射到标签的 CoS 域，这样，原来由 IP 携带的类型信息，现在由标签携带。在 PE 路由器之间，根据标签的 CoS 域，进行有差别的调度（PQ、CQ、WFQ、CBQ 等）。

- 用 TP 实现承诺带宽及限制带宽的功能

在 PE 上与 CE 相连的链路上配置 TP（Traffic Policing）可以实现该功能。同时，TP 还提供了承诺的带宽和限制带宽的功能。

- 用 WRED 进行拥塞避免

WRED 在网络的瓶颈处监视并缓解网络的拥塞。一般在接入层出现拥塞的概率比较大。WRED 监视网络的负载，当拥塞刚开始出现时，它就开始有选择地丢弃一些包以降低流量。WRED 丢包的策略为：低优先级的流先丢，以保证高优先级的流可以顺畅通过。在可能发生拥塞的端口运行 WRED，是避免拥塞的较好选择。

在具体实现中，为了达到最好的效率，需要对任务进行分工。因为 QoS 是一个需要消耗很多处理器资源的应用，所以，这一任务应分配在边缘和核心路由器上运行，以减少对单独路由器的压力。

综上所述，实现基于 CoS 的差分服务结构需要 4 个步骤：

- MPLS 边缘路由器上实现入口的带宽限制和完成入口流量的分类。
- 边缘设备也需要承担带宽管理的工作，采用 TP。
- MPLS 核心路由器完成 CoS 的管理工作，进行有差别的服务质量保证。
- 出口设备，像入口设备一样，完成带宽限制工作。入口、出口设备对带宽的限制保护了网络免于拥塞，使得网络具有很高的可扩展性。

3. MPLS 基本能力配置

MPLS 提供了比较完全的 MPLS 基本能力：

- 基本 MPLS 转发

VRP 支持基本 MPLS 转发功能。除标签报文的转发之外，还提供了 TTL 处理等功能。

- LDP 会话建立和 LSP 路径维护
支持 LDP 会话;支持最大跳数和路径向量两种方式的环路检测;提供静态 LSP 的建立、删除功能。

支持松散和严格的显式路由;可以人工指定 LSP 路径。

VRP 除提供 MPLS 基本功能外,还提供了性能监视和故障检测工具。

要使一台路由器具有基本的 MPLS 功能,一般的配置过程如下:

- (1) 配置 LSR 的标识 ID
- (2) 使能 MPLS
- (3) 使能 LDP 协议
- (4) 进入接口模式,使能接口的 LDP 功能。

经过上述的基本配置,路由器即可提供 MPLS 转发和 LDP 信令功能。

如果要修改一些缺省参数,或者实现一些特殊的 MPLS 功能,如手工建立 LSP、建立显式路由等,则可以根据配置列表提供的方法来配置。有些复杂的功能,可能需要多个配置的组合才能实现。

目前 MPLS 不支持的协议及接口如下:

- 封装了 X.25、MP 的串口
- Dialer 口
- 虚拟模板接口 (VT)

4. MPLS VPN 故障通用诊断流程

■ 检查基本路由协议运行是否正常

可在 LSP 的入节点 (ingress 节点) Ping 目的节点 (Egress 节点),查看能否 Ping 通:

如可以 Ping 通,排除路由协议错误的可能;

如不能 Ping 通,请检查路由协议的配置,如路由协议配置正确,建议重启路由协议。

■ 检查 LSP 是否建立成功

如采用 LDP 协议建立 LSP 不成功,注意检查以下方面:

检查环路检测配置,两端必须配置为一致,否则 LSP 无法建立。

建立会话时默认的传输地址一般是 MPLS LSR ID,本机必须将 LSR ID 的路由(一般为 loopback 地址)发布出去,同时,要学到对端的 LSR ID 的路由。

检查运行 MPLS 的路由器，其标签分配方式是否一致。不同厂家设备的标签分配方式可能不一致，在对接时需要注意。

■ 检查同一 VPN 各端的配置是否匹配

对于 BGP/MPLS VPN，应特别注意检查同一 VPN 各端配置的 RT 值是否一致。

对于 Martini 方式的 MPLS L2VPN，应特别注意检查同一 VPN 各端配置的 VC-ID 值是否一致。

对于 Kompella 方式的 MPLS L2VPN，应特别注意检查同一 VPN 各端配置的 RT 值是否一致，是否正确指定了对端 CE 的编号。

■ 检查同一 VPN 中各接口的 MTU 大小

由于大多数运行 MPLS 协议的设备不对 MPLS 报文进行分片，因此应注意检查接口的 MTU 值，查看通信报文的大小是否在接口 MTU 值范围内。假如通信报文的大小超过了接口的最大 MTU 值，不对 MPLS 报文进行分片的设备将丢弃该报文，试想，只要通信报文所经过的其中一台设备出现了该问题，通信都将受到影响。

1.2 案例分析

1. MPLS L2VPN 故障诊断与排除

现象描述

组网图：CE1—PE1—PE2—CE2

MPLS L2VPN 配置后，Ping 对端失败，查看 VC 状态，发现 VC 状态为 Down，Remote 值为无效值。

原因分析

VC 状态为 Down，注意检查本端和对端 PE 设备接口配置的封装类型和 MTU 是否一致，如果配置的封装能力不一样，连接将失败。

Remote 值为无效值，请检查两端是否已配置了 Remote 参数，并正确设置了对端的地址。

故障处理流程

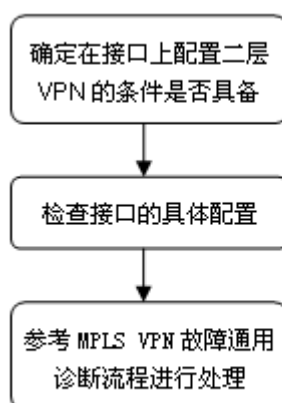


图2 1.2.1 故障处理流程

故障处理步骤

1) 步骤 1

确定在接口上配置二层 VPN 的条件是否具备。比如，若在 VLAN 接口上配置二层 VPN，必须满足下列条件：

若接口已经使能了 MPLS/BGP VPN、WebSwitch、组播或者 VLL 等业务，则不能再进行二层 VPN 配置。

Super-Vlan 或者是 Sub-Vlan 不能进行二层 VPN 配置，只有在正常的 VLAN 接口才能进行二层 VPN 配置。

2) 步骤 2

检查接口的具体配置。MPLS L2VPN 目前可支持多种链路层协议，但要求同一个 VPN 的各个节点使用统一的封装类型。

3) 步骤 3

参考 MPLS VPN 故障通用诊断流程进行处理。

2. MPLS VPN 业务时通时断

现象描述

MPLS VPN 配置好以后，业务通信出现时通时断的情况。

原因分析

造成 MPLS VPN 业务时通时断有如下可能：

专网内有病毒报文冲击服务器造成时通时断。

存在 IP 地址冲突问题。

专网服务器端处理报文能力不够导致网络不稳定。

设备之间物理连接有问题。
设备出现转发异常。

故障处理流程

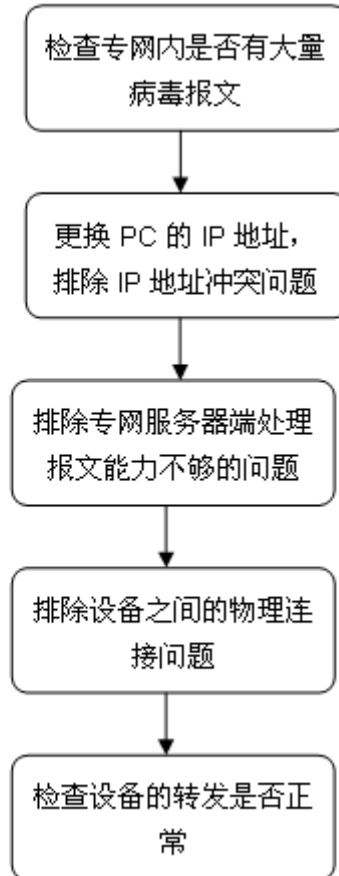


图3 1.2.2 故障处理流程

故障处理步骤

1) 步骤 1

检查专网内是否有大量病毒报文，若有，对专网内服务器和客户端 PC 进行查杀病毒。

2) 步骤 2

更换 PC 的 IP 地址，排除 IP 地址冲突问题。

3) 步骤 3

排除专网服务器端处理报文能力不够的问题。可在尽量靠近服务器的地方连接一台 PC，然后访问服务器，看是否出现时通时断的问题。

4) 步骤 4

排除设备之间的物理连接问题。比如检查设备之间的物理端口是否有问题，连接线缆是否有问题，设备接地、供电系统接地是否良好等等。

5) 步骤 5

检查设备的转发是否正常。比如检查设备的转发能力是否足够，检查设备的转发表项是否出现了异常等等。