VPLS 网络中的快速重路由机制①

胡建萍，杨军海

(杭州电子科技大学 电子信息学院，杭州 310018)

摘 要：VPLS 网络作为一种新型二层 VPN 技术，在大型城域网中的应用前景巨大。随着下一代网络（NGN）、网络电视(IPTV)等高质量业务在城域网中的流行，对网络可靠性的需求越来越高。介绍了 VPLS 网络的基本模型与技术特点，并提出结合 MPLS 流量工程的快速重路由（FRR）机制，对 VPLS 网络中关键链路或节点进行保护的方案，以提高服务质量，减少数据丢失，详细阐述了 FRR 的实现原理和在实际组网中的部署过程，并通过实验对方案进行了测试验证。

关键词：快速重路由；VPLS 网络；MPLS 流量工程

Implementation of Fast-Reroute in VPLS Networks

HU Jian-Ping, YANG Jun-Hai

(School of Electronics & Information, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: VPLS network as a new layer 2 VPN technology has huge prospect in large-scale MAN. With the popularity of high-quality services in MAN such as next generation network (NGN) and network TV (IPTV), it demand the increasing reliability in the network. This paper will introduce the basic model of VPLS network and its characteristic. Then an implementation of protecting VPLS network important link or node with the FRR of MPLS traffic engineering are presented to improve the quality of service, reduce the packet dropout. And also the principle of FRR and the process of traffic switching will be introduced in detail. At last, the result of experimentation is provided.

Keywords: fast reroute; VPLS network; MPLS traffic engineering

1 引言

近 20 年来，以太网技术以灵活、廉价、高速的特点在局域网中占据了统治地位。而随着各种新型以太网技术的不断涌现，以太网技术已将部署领域逐渐扩展到城域网，形成所谓城域以太网。VPLS(Virtual Private LAN Service，虚拟专用局域网服务)[1,2]作为新型以太网技术中的一种，在城域网中需求巨大，它结合了以太网与 MPLS(Multiprotocol Label Swit ching，多协议标签交换)技术的优点，在公共网络上提供点到多点的二层 VPN 服务，将分布在不同地域的用户网络相互连接起来。

目前，在国家大力推进三网融合的背景下，城域网中部署语音传输(VoIP)、网络电视(IPTV)等新型业务已成为必然。这些高质量的业务对网络可靠性保护能力提出更高要求，短暂的网络故障就足以导致业务中断，影响服务质量。这对于 VPLS 网络也是一个新的挑战，如何实现 VPLS 网络的故障快速处理，提高网络的安全性显得尤为关键。在电信级以太网中，故障恢复时间小于 50 ms 才能确保业务的正常运行。

2 VPLS网络技术

2.1 VPLS 网络模型

VPLS 网络的基本模型如图 1 所示，用户边界设备（CE）实现用户侧网络的汇聚，并通过接入链路与运营商边界设备（PE）之间相连。网络中所有 PE 设备由 MPLS 的标签转发路径（LSP，Label Switching Path）形成全网格连接。每条 LSP 隧道上承载了一条或多条虚链路（PW，Pseudo Wire），PW 用来仿真不

① 收稿时间:2010-09-06;收到修改稿时间:2010-10-13

同站点之间的以太网链路，其本质是两个 PE 之间通过协商建立的标签映射。VPLS 通过 PW 实现用户数据的二层透传，不仅如此，PE 还具有 MAC 学习能力，能建立 MAC 转发表，形成 MAC 地址与接入端口或 PW 的对应关系，实现单播报文的转发。

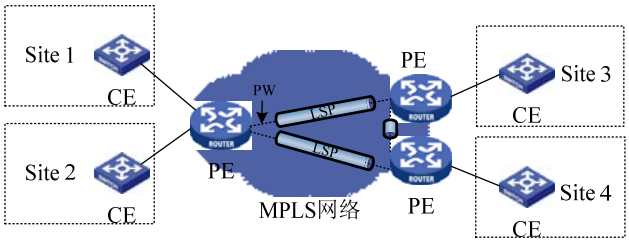


图 1　VPLS 网络基本模型

目前，IETF 发布的 RFC4761 和 RFC4762 分别定义了 VPLS 技术的两种实现方式：基于边界网关协议（BGP）的 Kompella 方式和基于标签分配协议（LDP）的 Martini 方式。两种方式的主要区别在于 PE 邻居发现和 PW 建立方式不同，VPLS 网络的数据转发是一样的。

1.2 VPLS 网络故障分析

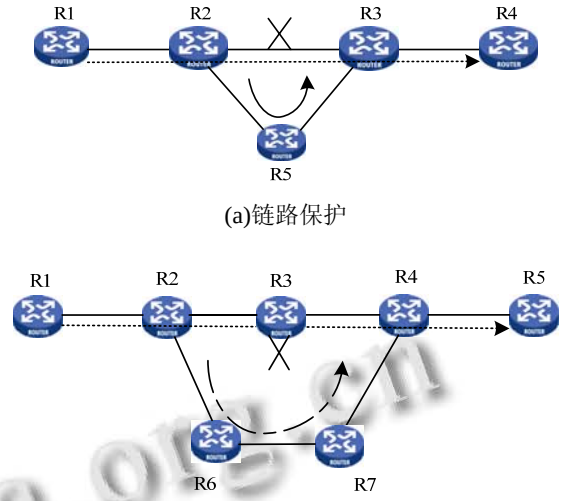
VPLS 网络中，经过 PE 设备封装的用户报文具有 MPLS 隧道标签和私网标签，隧道标签用于确定公网侧转发路径，私网标签指定了对端 PE 上相应 VPLS 实例的出端口。报文进入 PE 设备后，经过解析提取出目的 MAC 查找对应转发表项（FIB）。若查找成功，返回一组包含 Tunnel ID、VC ID 和 Port ID 的三元组，分别对应公网侧 LSP、PW 及出端口；若查找失败，VPLS 具有广播能力，可根据人报文所匹配的 VSI ID 和 VLAN 查找出该 VPLS 实例的所有三元组信息。PE 根据三元组进行报文的封装和转发。

由于三元组中的 PW 与公网隧道存在绑定关系，当公网 LSP 隧道发生变化时，Tunnel ID 值的变化引起 PW 连接超时重建，在新的绑定关系建立前的业务数据丢失。因此，等待网络路由收敛的方式是无法达到电信级要求的。VPLS 网络的保护需要解决如何实现 LSP 隧道快速切换，避免 PW 重建的问题。本文结合 MPLS 流量工程的 FRR(Fast Reroute，快速重路由)[3] 技术，预先建立备用隧道对网络中的关键链路或节点进行保护，利用隧道策略使 PW 与主隧道绑定。当故障发生后，主隧道保持 UP，流量切换到备用隧道转发。PE 上的 VPLS 转发表现不变，因此，PW 无需重建。

2　VPLS网络中FRR机制的实现

2.1 FRR 机制简介

基于 MPLS 流量工程的 FRR 机制分为 Detour 和 Bypass 两种方式[4]。前者为每一条 LSP 创建一条保护路径，网络开销较大。本文采用的 Bypass 方式，可以实现一条备用隧道对多条 LSP 的保护，在实际中应用广泛。如图 2 所示为 FRR 的两种模式：链路保护和节点保护。链路保护中，R2 与 R3 之间的链路受到保护，当链路故障时，业务流量切换到 R2--R5--R3 这条备用链路。节点保护与链路保护相似，但保护的对象是 R2、R3 之间的链路以及 R3 设备。两种模式中，备用隧道的首节点在故障发生时实现流量切换，被称为本地恢复节点(PLR)；备用隧道的尾节点在切换后将备用隧道的流量转发给主 LSP 的下游节点，称为汇聚节点(MP)。



(a)链路保护

(b)节点保护

图 2　链路保护与节点保护

2.2 FRR 机制的实现原理

当故障发生时，首先由检测机制快速发出切换指令，方案中采用 BFD(Bidirectional Forwarding Detec- tion，双向转发检测)来完成。BFD 部署在 PLR 与下一跳设备之间，通过周期性发送控制报文检测链路状态。如果 PLR 在定时器超时前未收到控制报文，则进入故障切换阶段。

故障切换主要在 PLR 节点上完成，如图 3 所示，PLR 节点上的入标签映射表（ILM）关联了主隧道下一跳标签转发表项 NHLFE1，还同时下发了备用隧道的下一跳标签转发表项 NHLFE2，并且把主隧道在 MP 节点的入标签保存在 ILM 的 FRRLabel 中。

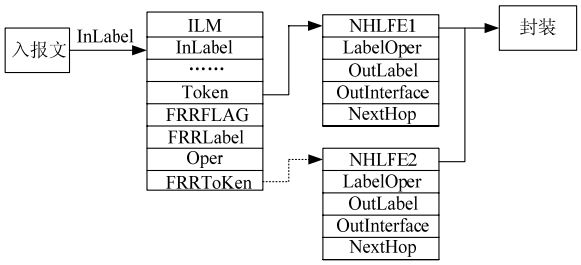


图 3 PLR 节点的标签转发表

报文进入PLR节点后，根据入标签查找ILM表项，关联对应的 NHLFE 表项，获得标签操作、出标签、出端口等信息进行报文转发。当主隧道正常时，关联主隧道 NHILFE1 表项进行转发；当 PLR 检测到保护链路或节点故障后，流量切换至备用隧道，报文先用FRRLabel 标签替换原有入标签，再关联 NHLFE2 表项压入 OutLabel 标签，封装后送出相应端口。报文到达 MP 节点时，备用隧道标签被弹出，根据原有 FRRLabel 标签进行转发，下游节点感知不到故障的发生。

切换完成后，PLR 向 LSP 头节点发送一个 PathErr 消息，其中的 ERROR_SPEC 对象包含用于 FRR 的错误码 25，错误值 3，表示下游节点已完成保护切换，当前流量沿备份隧道传输。主 LSP 头结点保持隧道 UP，并触发新的路由计算，尝试建立新的最优路径。如果是节点保护，MP 会向被保护节点发送 ResvTear 消息，通知其释放资源，被保护节点完成释放动作后回应 PathTear 消息。

3 VPLS流量转发

VPLS 的数据封装格式有两层标签，内层标签作为私有服务标签，用于区分不同 VPLS 实例，外层标签作为公网 LSP 上的转发标签。故障发生前的流量转发过程[5]如图 4 所示：

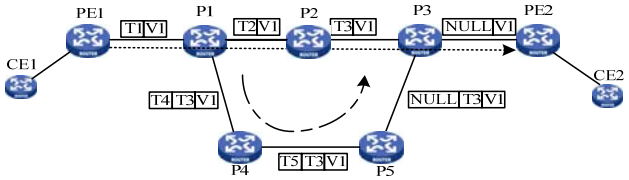


图 4 VPLS 网络中的数据转发过程

普通以太网报文从CE1到达PE1的私网接口，PE1把对应 VPLS 实例的私网标签（假设为 V1）压入到 IP 报文标签栈。

PE1 将 P1 分配的公网标签（假设为 T1）加入标签栈顶，并将报文发送到 P1，此时报文携带有两层 MPLS 标签。

P1 收到从 PE1 发送过来的报文，查找 T1 所对应的路由出标签为 T2，用 T2 交换原有外层标签 T1，并将报文发送到 P2。

P2 收到报文，处理过程与 P1 相同，外层标签更换成 T3 后发送给 P3。

P3 收到 P2 发送过来的报文，查看标签所对应的下一跳标签为 NULL，确定自己是倒数第二跳，去除报文中的外层标签 T3，将报文发送到 MPLS 网络边界路由器 PE2。此时报文只有一层 VPLS 私网标签。

PE2 收到 P3 发送过来的报文，根据私网标签查找出到 CE2 的私网接口，去除报文中的 MPLS 标签 V1，并将报文转发给 CE2，此时报文还原为普通以太网报文。

故障发生后，当报文到达 P1 节点，由于原来的下一跳失效，P1 将报文切换到备用隧道。首先用 MP 分配的主隧道标签 T3 交换报文外层标签 T1，再压入备用隧道的标签（假设为 T4），并将报文发送到备用隧道出接口，此时报文具有 3 层 MPLS 标签。在备用隧道上，报文的处理与主隧道相似，通过报文最外层标签进行下一跳查找并转发。报文到达 P3 节点后，由于 MP 使用全局标签，不检查报文的入端口，转发过程与主隧道失效前一致，下游节点对链路切换不感知。

4 网络的部署

城域网中的 VPLS 网络的基本模型[6]如图 5 所示。P2 与 P4 为核心层设备，完成数据的高速交换；P1 与 P3 为汇聚层设备，实现用户数据汇聚；PE1 与 PE2 为接入层设备，实现网络的全面覆盖和接入控制。核心层与汇聚层设备作为 VPLS 网络的服务提供商核心路由器（P 路由器），完成用户数据的 MPLS 转发。VPLS 网络中FRR机制的部署主要针对服务提供商的骨干网络，通过预先建立备用路径对重要链路或节点进行保护。当被保护链路和节点发生故障时，主链路上流量切换到备用链路，把网络故障对业务的影响降到最低，提高服务的保障能力。FRR 机制部署步骤如下：

1) 部署准备。FRR 机制基于 MPLS 流量工程实现的，部署 FRR 前需在骨干网设备全局及端口上启用 MPLS 流量工程。在 VPLS 网络中采用 IGP 路由协议

发布路由信息，需开启 OSPF 或 ISIS 的 TE 扩展属性，为隧道的建立提供必要的链路状态信息。

2) 建立主备隧道。VPLS 网络需要在 PE 设备之间建立双向 LSP 隧道，通过显示路径的方式指定隧道路径，在 PE1 上建立主隧道 Tunnel1 路径为 PE1--P1--P2--P3--PE2，P2 与 P1 作为 PLR 节点建立备用隧道 Tunnel2 与 Tunnel3 路径分别为 P2--P4--P3 与 P1--P4--P3。MPLS 流量工程建立的隧道是单向的，因此在 PE2 上建立主隧道 PE2--P3--P4--P1--PE1，在实现故障保护的同时，对 VPLS 业务流量进行链路分担。

3) 主备隧道绑定。主备隧道建立后，默认情况下不请求保护，在主隧道首节点上使能隧道 FRR 保护功能后，主隧道通过 PATH 消息通告下游节点。此外在 PLR 节点的主隧道出接口上配置与备用隧道对应关系。

4) 配置隧道策略。VPLS 网络中，业务流量默认不走 MPLS 流量工程建立的 LSP 隧道。在 VPLS 实例中绑定隧道策略，并在策略中指定实例关联的隧道类型和 ID，使流量走对应隧道转发。

5) 设置故障检测。利用 BFD 检测链路状态，分别在 P2 与 P3、P1 与 P4 之间建立关联 FRR 机制的 BFD 连接，设置 BFD 检测定时器时间为 10 ms，超时次数为 3 次，最慢可以在 30 ms 内检测到链路故障。

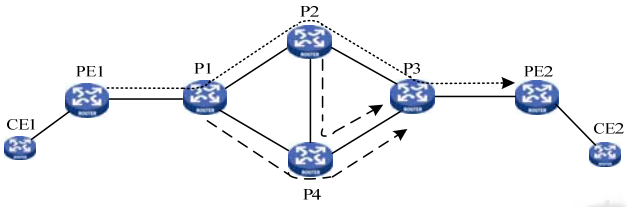


图 5　网络拓扑

5　结果验证

使用思博伦的 TestCenter 测试仪器模拟 CE 设备产生 VPLS 流量，同时在对端 CE 记录流量接收情况，测试故障切换所需的时间。

未部署 FRR 机制时，测试仪以 84459 个/秒的发包速度均匀的打入流量，人为切断 P2 与 P3 之间的链路，打流 30 s 后，测试仪记录发出报文数目为 2533770 个，收到报文数目为 2084958 个，丢包数为 448812 个，链路收敛时间 t = 448812（个）/ 84459（个/秒）= 5.31 s。

部署 FRR 机制后，通过人为切断 P2 与 P3 之间的链路模拟链路失效；关闭 P2 设备的电源模拟节点失效。测试结果如表 1 和表 2 所示。表明 VPLS 网络采用快速重路由机制，可以大大减少链路故障时的分组丢失，提高网络可靠性。

表 1　链路保护

测试次数	发包数目（个）	收包数目（个）	丢包个数（个）	倒换时间（ms）
1	2533770	2531022	2748	32.5
2	2533770	2531473	2297	27.2
3	2533770	2530975	2795	33.1

表 2　节点保护

测试次数	发包数目（个）	收包数目（个）	丢包个数（个）	倒换时间（ms）
1	2533770	2531015	2755	32.6
2	2533770	2530936	2834	33.6
3	2533770	2531257	2513	29.8

6　结语

本文提出结合 FRR 机制实现 VPLS 网络快速故障保护的方案，实现 50 ms 内的快速切换，降低链路或节点失效引起的数据丢失，保证 VPLS 网络中业务的正常运行。目前，在市场和技术的双重推动下，VPLS 网络在城域网中取得较大的进展，但相对于已广泛部署的三层 VPN 技术，尚缺乏大规模应用案例，需要在实践中进一步探索。结合 FRR 机制的 VPLS 网络具备快速保护恢复能力，能满足城域网中多媒体业务的运营需求，对 VPLS 网络的进一步发展具有重大的意义。

参考文献

1 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling. IETF RFC4761, 2007.

2 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling.IETF RFC4762, 2007.

3 RSVP-TE: Extensions to RSVP for LSP Tunnels. IETF RFC3209, 2001.

4 Fast Reroute Extensions to RSVP-TE for LSP Tunnels. IETF RFC4090, 2005.

5 Osborne E, Simbha A.基于 MPLS 的流量工程.北京:人民邮电出版社, 2003.231-272.

6 罗林,张博.基于 MPLS 网络的 LDP-VPLS 组网方案.电讯技术, 2005,45(2):125-129.