Computer Science and Application 计算机科学与应用, 2017, 7(8), 722-728
Published Online August 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.78083

Hans汉斯

Research on MPLS/BGP VPN Full Connection Network

Qinghua Gao, Shilin Li, Cunyu Liu, Xingyu Dong, Xiaochen Wang, Xiaoyu Liu

Beijing City University, Beijing
Email: qhuagqhuag@126.com

Received: Jul. 15th, 2017; accepted: Aug. 1st, 2017; published: Aug. 4th, 2017

Abstract

The normal networking of MPLS/BGP VPN consists of the client device GE, the provider border device PE providing the VPN service, and the internal switching device P device. However, the networking can result in a linear networking, easily causes the overall VPN network to be paralyzed phenomenon, and reduces network reliability. This paper introduces a networking mode to build a full connection network by switching the router between PEs and P devices, to improve reliability by achieving redundancy, based on the advantages and disadvantages of MPLS/BGP VPN technology.

Keywords

MPLS/BGP VPN, Full Connection, Networking Mode

MPLS/BGP VPN全连接组网研究

高清华，李士林，刘存钰，董行余，王笑尘，刘校瑜

北京城市学院，北京
Email: qhuagqhuag@126.com

收稿日期：2017年7月15日；录用日期：2017年8月1日；发布日期：2017年8月4日

摘　要

MPLS/BGP VPN正常组网由客户端设备GE、提供VPN服务的商端边界设备PE以及内部交换设备P设备组成，但这样组网会造成线性组网，很容易造成整体VPN网络瘫痪现象出现，降低网络可靠性。本文将基于MPLS/BGP VPN技术的优劣，介绍一种通过将路由器在PE与P设备之间进行切换使用，实现冗余工作提高可靠性的全连接式VPN组网方式。

文章引用: 高清华, 李士林, 刘存钰, 董行余, 王笑尘, 刘校瑜. MPLS/BGP VPN 全连接组网研究[J]. 计算机科学与应用, 2017, 7(8): 722-728. DOI: 10.12677/csa.2017.78083

关键词

MPLS/BGP VPN，全连接，组网方式

1. 引言

网络爆炸式发展的今天，人类越来越依赖于网络技术所带来的便利，小到个人生活娱乐；大到企业周转运营、城市国家各种设施正常工作全部与网络息息相关。网络的重要性不断被放大的今天，网络安全也变得越来越被个人、企业、国家所重视。网络数据想要跨大区域传输或通过公网访问局域网，就会增加网络信息被劫持被监听泄漏的危险。为了应对公网信息泄露的问题以及远程访问局域网的需要，VPN技术便孕育而生，在众多 VPN 技术中 MPLS/BGP VPN 凭借其众多闪光点占领了 VPN 领域的一席之地。

MPLS/BGP VPN 正常组网由客户端设备 GE，提供 VPN 服务商端边界设备 PE 以及内部交换设备 P 设备组成，但这样组网方式会造成线性组网网络故障，很容易造成整体 VPN 网络瘫痪现象出现，尤其对于网络敏感部门网络的可靠性尤为重要。老式设备由于硬实力有限，路由器与交换机之间相互替代情况难以真正实现。通常 P 设备只能由交换机来充当，而 PE 设备有路由器充当，若中间不连接 P 设备而是直接两台 PE 设备相连接，会造成由于路由器工作负荷过大问题，在充当交换机使用时更会出现路由器交换性能不佳，无法很好的完成大量数据交换问题，工作效率低，浪费网络资源。但科技不断发展的今天，设备不断地进步替换升级中，路由器与交换机之间的相互替代，在相对较高端的使用中已得到了实现，由于设备性能不断地蹿升，路由器执行交换功能和交换机执行路由功能所造成的性能浪费已经变得很低。那么通过将路由器在 PE 与 P 设备之间进行切换使用，实现冗余工作，提高网络可靠性的组网方式，随着设备的革新，已经能够很好地实现并投入使用。本文将基于 MPLS/BGP VPN 技术的优劣，介绍一种通过将路由器在 PE 与 P 设备之间进行切换使用，实现冗余工作提高可靠性的全链接式 VPN 组网方式。

2. MPLS/BGP VPN 技术

2.1. 技术简介

MPLS/BGP VPN 技术是大型运营商提供给客户的一种 VPN 业务，它由于其标签传输形式快于每一跳不断寻址查表的 IP 传输形式，并相对于传统网络有着优秀的 QOS 保证、流量工程实施等优点[1]，有着专线级别的带宽体验，最主要的是 VPN 并不需要由使用者投资搭建和维护，而是由运营商提供，只需要用户缴纳较少的租用费用即可放心使用。但相对长时间租用的花费会慢慢超过自己搭建一个 VPN 网络的费用，同时 MPLS/BGP VPN 传输过程中采用信息隔离来保证安全，信息并不会加密，这就产生了两种情况，如果用户完全信任运营商网络的安全，那么你的信息就是非常安全的，如果用户并不信任运营商网络的安全，那么你的信息有可能由于其不加密的特性而泄露。

其中 MPLS (Multi-Protocol Label Switching, MPLS)是新一代的 IP 高速骨干网络交换标准，由因特网工程任务组(Internet Engineering Task Force, IETF)提出。

MPLS 是利用标记(label)进行数据转发的。当分组进入网络时，要为其分配固定长度的短的标记，并

将标记与分组封装在一起，在整个转发过程中，交换节点仅根据标记进行转发。MPLS 独立于第二和第三层协议，诸如 ATM 和 IP。它提供了一种方式，将 IP 地址映射为简单的具有固定长度的标签，用于不同的包转发和包交换技术。它是现有路由和交换协议的接口，如 IP、ATM、帧中继、资源预留协议(RSVP)、开放最短路径优先(OSPF)等等。在 MPLS 中，数据传输发生在标签交换路径(LSP)上[2]。LSP 是每一个沿着从源端到终端的路径上的结点的标签序列。MPLS 主要设计来解决网路问题，如网路速度、可扩展性、服务质量(QOS)管理以及流量工程，同时也为下一代 IP 中枢网络解决宽带管理及服务请求等问题。多协议标签交换 MPLS 最初是为了提高转发速度而提出的。与传统 IP 路由方式相比，它在数据转发时，只在网络边缘分析 IP 报文头，而不用在每一跳都分析 IP 报文头，从而节约了处理时间[3]。简单的来说就是：传统 IP 数据包处理的方式是查找本地路由表，而且遵循最长匹配原则，有的需要进行多次的查表，从而浪费较多的时间和网络设备的性能，启用 MPLS 功能后，设备的本地数据库形成一张快速转发的标签表，启用 MPLS 的设备之间形成一个 MPLS 域，IP 数据包进入 MPLS 的域后查找的是一次标签表，为数据转发提供了更高的效率[4]，还有更重要的一点就是 MPLS 可以严格的控制报文的转发[5]，比如：报文的优先级，TTL 值，同时 MPLS 可以承载更多协议报文，例如：IPv4、IPv6、ATM 等。

2.2. 网络组成

MPLS/BGP VPN 主要由三部分组成[6]。

CE：用户网络边缘路由器，实际情况 CE 也可以是防火墙设备，并且 CE 端除了添加一条静态路由并不需要配置其他条目。

PE：运营商边缘路由设备，与 CE 设备相连接，负责 VPN 用户的入网接入，网络中非常重要的设备。

P：运营商核心路由设备，虽然叫做路由设备，其实主要进行标签交换的设备，同时为 PE 设备减轻压力。

2.3. 工作原理

用户接入 MPLS VPN 的方式是每个 site 提供一个或多个 CE，同骨干网的 PE 连接。在 PE 上为这个 site 配置 VRF，将连结 PE-CE 的物理接口、逻辑接口、甚至 L2TP/IPSEC 隧道绑定的 VRF 上，但不可以是多跳的 3 层连接。

BGP 扩展实现的 MPLS VPN 扩展的了 BGP NLRI 中的 IPv4 地址，在其前增加了一个 8 字节的 RD(Route Distinguisher)。RD 时用来标识 VPN 的成员---即 Site 的。VPN 的成员关系是通过路由所携带的 route target 属性来获得的，每个 VRF 配置了一些策略，规定一个 VPN 可以接收哪些 Site 来的路由信息，可以向外发布哪些 Site 的路由信息。每个 PE 根据 BGP 扩展发布的信息进行路由计算，生成每个相关 VPN 的路由表[7]。

PE-CE 之间要交换路由信息一般是通过静态路由，也可以通过 RIP、OSPF、BGP、IS-IS 等。PE-CE 之间采用静态路由的好处是可以减少 CE 设备可能会因为管理不善等原因造成对骨干网 BGP 路由产生震荡，影响骨干网的稳定性。

PE 与 PE 之间需要运行 IBGP 协议，存在可扩展性问题，但采用路由反射器 RR 可以显著地减少 IBGP 连接的数量。

MPLS/BGP VPN 提供了灵活的地址管理。由于采用了单独的路由表，允许每个 VPN 使用单独的地址空间中，称为 VPN-IPv4 地址空间，RD 加上 IPv4 地址就构成了 VPN-IPv4 地址。很多采用私有地址的用户不必再进行地址转换 NAT。NAT 只有在两个有冲突地址的用户需要建立 Extranet 进行通信时才需要。

在 MPLS/BGP VPN 中，属于同一的 VPN 的两个 site 之间转发报文使用两层标签来解决，在入口 PE

上为报文打上两层标签，第一层(外层)标签在骨干网内部进行交换，代表了从 PE 到对端 PE 的一条隧道，VPN 报文打上这层标签，就可以沿着 LSP 到达对端 PE，这时候就需要使用第二层(内层)标签，这层标签指示了报文应该到达哪个 site，或者更具体一些，可以到达其中哪一个 CE，这样，根据内层标签，就可以找到转发的接口。可以认为，内层标签代表了通过骨干网相连的两个 CE 之间的一个隧道。

L3 MPLS VPN 通过和 Internet 路由之间配置一些静态路由的方式，可以实现 VPN 的 Internet 上网服务，还可以为跨不同地域的、属于同一个 AS 但是没有自己的骨干网的运营商提供 VPN 互连，即提供“运营商的运营商”模式的 VPN 网络互连。(MPLS VPN 访问 Internet 及 Carrier’s Carrier 解决方案将在后面章节详细描述)。

MPLS/MBGP VPN 可以简化对用户端设备的需求和用户管理、维护 Intranet/Extranet 的复杂性，每个 CE 仅需要维持一个到 PE 的路由交换协议，CE 间的路由交换、传输控制、路由策略由运营商根据 VPN 用户的需求来实施。由于 BGP 的策略控制能力很强，随之而来的是 VPN 用户路由策略控制的灵活性。

2.4. 技术优劣

MPLS/BGP VPN 的优势：高带宽；高速度；高可靠；安全性相对较高；QOS 保障；强大扩展性；网络管理增值服务；提供一站式服务。

MPLS/BGP VPN 的劣势：对于运营商来说投资较大，对于用户来说，长期租赁花费较大；数据信息不加密。

3. 传统组网

3.1. 传统 MPLS VPN 组网

MPLS VPN 是一种基于 MPLS 技术的 IP-VPN，是在网络路由和交换设备上应用 MPLS 技术，简化核心路由器的路由选择方式，结合传统路由技术的标记交换来实现 IP 虚拟专用网络，满足灵活的业务需求。MPLS VPN 传统网络拓扑如图 1 所示。

3.2. 传统 MPLS VPN 组网解析

传统 MPLS VPN 组网，一般 PE 与 PE 之间并不会直接相连，同时一个客户端只会连接一个 PE 入网

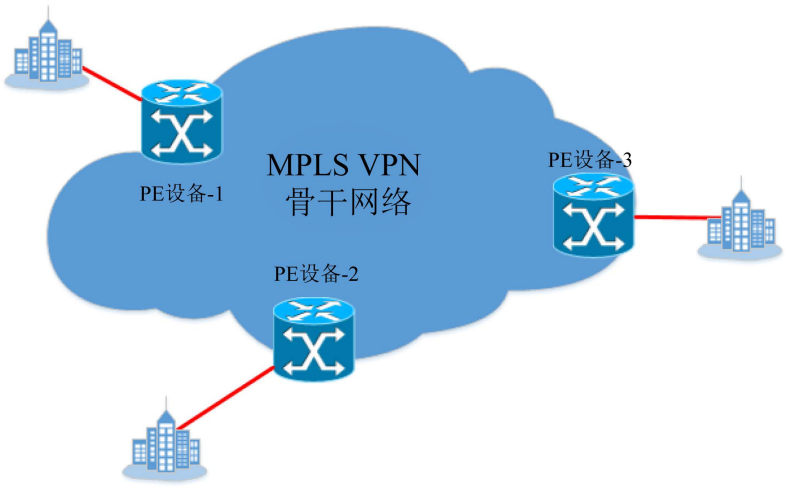

Figure 1. Traditional networking topology
图 1. 传统网络拓扑

点(POP)，当所连接线路出现故障，会造成如同运营商主光缆中断一样的断网危害，较为缺乏可靠性[8]，对于数据中心，灾备中心这种需要很高可靠性的网络来说，不能满足其可靠性要求。同时 P 设备的过多也会造成运营商运营开支增加，管理复杂化等问题。开支的增大固然会转嫁到用户租赁费用上，造成费用提高从而降低用户对 MPLS/BGP VPN 的优先级。但传统组网的优势也比较明显，长途线缆不需要过多架设，可减少高价 PE 设备的放置量，减少初期搭建开支，并且这种拓扑可以用在几乎所有地方，普适性很高，与其他网络相连时出现的问题较少[2]。

3.3. 传统 MPLS VPN 组网冗余方式

传统冗余方式一般使用平行冗余，机提供两台 PE 设备去连接一个区域，将其定义为主备冗余，中间的 P 设备一般也是如此，使 MPLS VPN 一直有两条路由路径来选择，其中断路立刻切换另一条链路，一个设备损坏立刻切换至后备设备继续运行 VPN 服务。

这种冗余方式效果优异，不仅仅 MPLS VPN 组网使用，几乎所有需要高可靠性网络，区域组网都会这样做，其缺点自然是增加了设备投入和设备维护人力成本投入，并且当两条路都出现中断的小概率事件依然会造成网络中断。

4. 全连接式 MPLSVPN 组网

4.1. 全连接式组网

由于 MPLS/BGP VPN 的三个组成部分是逻辑组成，在实际组网中 P 设备是可以舍弃或者由 PE 设备代替的。全链接式组网，在建设 MPLS/BGP VPN 时考虑放弃 P 设备，将所有 PE 设备进行一个全互连操作，如图 2 所示，这就会形成一个庞大的冗余链路，随着 PE 设备的添加，核心部分的冗余链路数量会越来越多，而对于接入用户来说，并不需要与所有 PE 设备都进行连接，而是仅仅连接多台就近的 PE 即可，从而减少线缆花费[9]。

在网络运行时，其中的设备会同时兼顾 PE 与 P 设备的功能，多台设备之间进行负载均衡，加上如今高端设备都是大型板卡式设备，这也就使得 PE 设备能有高扩展性和强大运行性能，同时负载均衡也会充分利用“空闲设备”不会由于缺乏 P 设备的减压(倒数第二跳弹出等为 PE 设备减轻工作压力的功能)造成 PE 设备压力过大。当客户与 PE 之间出现 Down 事件发生，用户数据会选择其他链路传输，并通过自动选路或人为选路在进行最优路径再选择，保证数据快速传至目的地。当核心内部出现 PE 设备故障或链路中断则会提供众多其他链路的选择，保证即使多台设备出现故障也能够网络正常工作[10]。

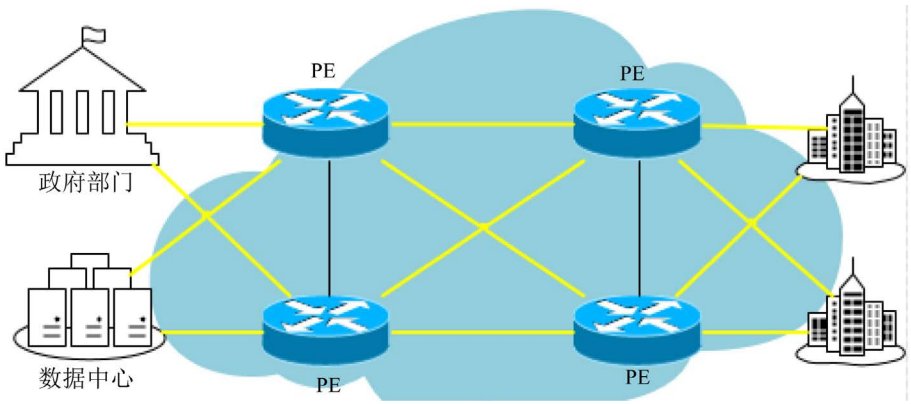

Figure 2. Full connection networking mode
图 2. 全连接式组网

4.2. MPLS/BGP VPN 组网优劣

通常 MPLS/BGP VPN 在具有传统组网的优点外，由于全连接式的组网方式，大量 PE 设备在核心区域会产生大量可选择链路，这些链路的出现使得网络拥有极高的可靠性，几乎不会出现网络中断现象，并且全链接也带来了 PE 和 P 设备的相互转化的可能性，使得多台设备进行负载分担成为可能，充分利用设备性能，降低性能浪费现象；并且省略了大量 P 设备的入网，设备整体数量大量减少，方面初级维护人员进行维护。MPLS/BGP VPN 组网具有极高可靠性；设备数量相对于传统组网大幅减少；设备性能利用率高。

但是，MPLS/BGP VPN 需要布置大量长途光纤；初期需要很多配置；需要专业人士维护；不适用于一般用户；大量长途光纤的布置，建成后线路故障会使工程队的工作量也会较大，工程费用相对于传统组网的费用会大幅增加；并且由于设备数量减少，大量的配置都要集中于 PE 设备上，并需要进行大量配置，并且较为复杂容易出错；维护方面，由于每个 PE 设备有大量配置，初级工程师很难进行维护操作，非物理故障，几乎必须专业人士才能进行排除。由于以上问题，这种组网方式更多的会使用于高可靠性要求的用户，如：数据中心、灾备中心、政府重要部门等。

5. 全连接与传统组网结合

由于全网连接组网需要大量物理线路，以及不适合一般用户使用的缺点，为了让该组网方式能够被更多的用户所选择，最根本的改变就是减少链路线路数量，也就是牺牲冗余性，于是就将原本客户端 CE 连接多个 PE 更改为之连接一个，缩减客户所需购买的专线数量，减少客户成本和运营商工程成本。

这样做将传统组网方式用于客户接入端，运营商核心内部依然使用正常全连接组网方式，削减了可靠性来换取对其他劣势的改进。这项改进对运营商核心内部也可使用此种做法，由于在实际工作中过多的备选链路并不会被用到，并且会加大路由器的路径条目，平添负担，通过减少链路数量来减少运营商线路开支，并降低搭建和维护人员的工作量，实现灵活组网。

5.1. 组合组网拓扑

组合组网方式下，核心网络并不采用全连接式组网，而是选择有选择性的进行组网连接，根据需要进行相关线路选择，连线思路主要依据于使用的用户和实际改变难度来进行选择搭建。如图 3 所示，针对于一般用户或者一般网络设施集群，使用传统的一条线路提供 VPN 连接服务，并且核心网络区域也会相对减少多台 PE 互联线路；而对于可靠性优先用户或政府重要部门、容灾数据中心则会增加链路数量，为其提供更高可靠性服务怎家灵活性、满足用户需求的同时降低价格从而获得更大的商业优势。

5.2. 全连接与传统组网结合优劣

全连接与传统组网结合相对于全连接式组网更加灵活，可根据用户和实际需要进行链路数量的选择减少维护难度和费用。由于链路减少相应配置也大幅减少(主要是控制路由的配置)。但是，全连接与传统组网结合省略了链路降低了可靠性，链路选择不当会出现环路问题。

6. 结论

本文是针对未来 MPLS VPN 建设的研究，主要对现有传统 MPLS VPN 组网拓扑进行一定的简化改进，结合网络设备功能和性能的不断强大，通过对传统 MPLS VPN 中 P 设备的简化和与 PE 设备的结合，减少不必要的 P 设备数量，从而简化拓扑结构，通过全连接，实现网络全冗余和极高的可靠性，并对特殊用户提供优势的 MPLSVPN 服务。同时通过与传统组网的结合实现物理线路的简化，减少不必要的链

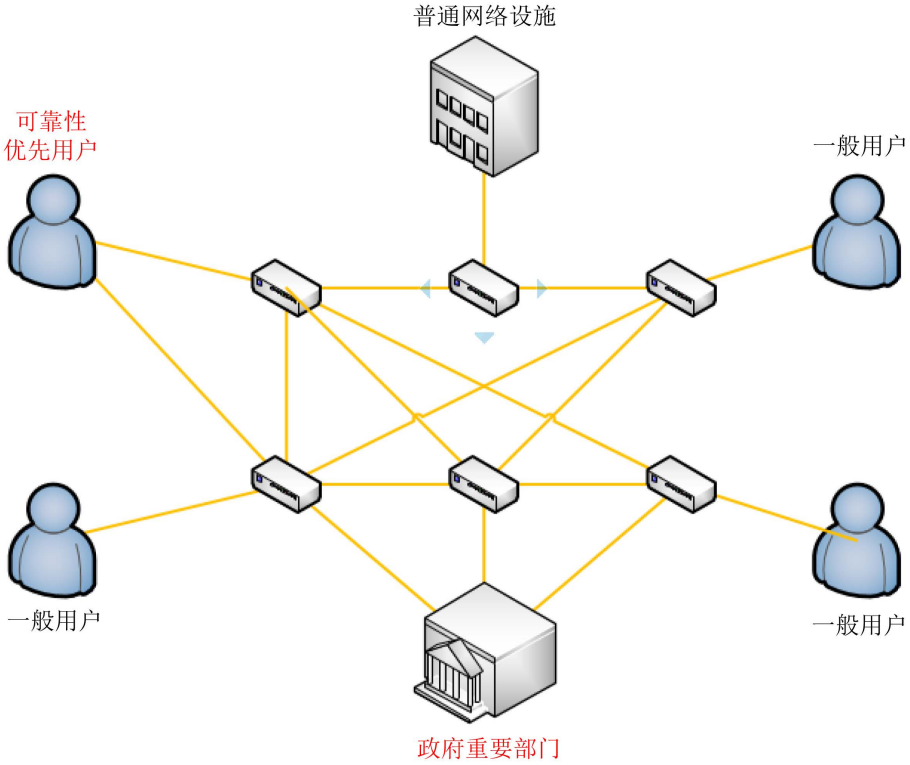

Figure 3. Topological diagram of combinational networking mode
图 3. 组合型组网拓扑示意图

路占用路由资源，降低搭建人员和维护人员的工作量。本文只是师生研究观点，可能有不当的地方，也请读者谅解并提出宝贵的改进意见。

基金项目

北京高等学校高水平人才交叉培养“实培计划”大学生科研训练计划深化项目。

参考文献 (References)

[1] 陈启美. 未来的 VPN-MPLS-VPN[J]. 电力自动化设备, 2002, 22(9): 85-88.

[2] 何璐茜. MPLS VPN 技术研究应用[J]. 现代电子技术, 2011, 34(15): 127-130.

[3] 符冰. MPLSVPN 技术在校园网的研究和实现[D]: [硕士学位论文]. 上海: 上海交通大学, 2012.

[4] 王华. MPLS 及 IP 网络流量工程的研究[D]: [博士学位论文]. 南京: 南京理工大学, 2003.

[5] 赵玉江. 基于 MPLS VPN 的 QOS 的研究与应用[D]: [硕士学位论文]. 杭州: 杭州电子科技大学, 2010.

[6] 蒋东毅. VPN 的关键技术分析[J]. 计算机工程与应用, 2003, 39(15): 173-177.

[7] 赵鹏. 基于 MPLS 骨干网络的 VPN 解决方案[J]. 电子学报, 2002, 30(s1): 2024-2026.

[8] 宋伟. 基于 MPLS VPN 技术的电子政务外网骨干网的设计与实现[D]: [硕士学位论文]. 内蒙古: 内蒙古大学, 2011.

[9] 李海华. BGPMPLSVPN 数据转发过程分析[J]. 计算机技术与发展, 2011, 21(6): 4-8.

[10] 邹昭源. MPLSVPN 技术的应用[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2015.