MPLS VPN 技术在电力企业广域网中的应用

苏雪娟，黄　玥，孙　宇
（滁州供电公司 科技信息部，安徽 滁州　239000）

摘　要　为实现电力企业双网隔离的要求，从 MPLS VPN 原理入手，结合滁州电力系统信息网络实际情况，构建了从网络核心层、汇聚层到接入层的安全管理体系。介绍了 MPLS VPN 技术的基本原理。实际应用表明，MPLS VPN 既可将现有网络划分成逻辑上隔离的网络，实现各个业务系统之间的隔离，又可以将企业信息外网与信息内网的灵活、高效、安全结合起来，为用户提供高质量的网络服务。

关键词　MPLS VPN；广域网；业务隔离
中图分类号　TP393.072　　**文献标识码**　A　　**文章编号**　1007－7820(2013)03－137－03

Application of MPLS VPN Technique in Power Enterprise Wide Area Network

SU Xuejuan, HUANG Yue, SUN Yu
(Department of Science and Technology Information, Chuzhou Power Supply Company, Chuzhou 239000, China)

Abstract　To meet the isolation requirements of power enterprise networks, a security management system including the network core, aggregation layer and the access layer is built based on the principles of MPLS VPN and the reality of Chuzhou power system networks. The basic principles of the MPLS VPN technology are introduced. Practical applications show that the MPLS VPN not only can divide the existing network into logically isolated networks for the separation of different business systems, but also combine the advantages of the outer network and inner network to provide the users with high-quality network services.

Keywords　MPLS VPN; WAN; business separation

随着电力信息化建设的快速发展，电力企业信息网络所承载的业务系统也越来越多，各个业务之间的互联互通与安全隔离就显得尤为重要，因此对于整个网络构架的良好性、可靠性以及扩展性都提出了更高的要求。于是 VPN 技术在企业组网中得到越来越多的运用。MPLS 由于其良好的网络拓展性并且支持大规模层次化的网络拓扑结构，所以 MPLS VPN 既可以把现有网络划分成逻辑上隔离的网络，实现各个业务系统之间的隔离，又可以将功能丰富、性能可靠、扩展性好的企业信息外网与信息内网的灵活、高效、安全结合起来。

1　MPLS VPN 原理

MPLS VPN 实际上是一种基于 MPLS 的 IP VPN。MPLS 技术是一种结合第 2 层交换和第 3 层路由功能的交换技术，即在网络路由和交换设备上运用 MPLS 技术，结合传统路由技术的标记交换实现的 IP VPN。它引入了基于标签的机制，把路由选路和数据转发分开，由标签通过网络的路径来规定一个分组。采用 MPLS VPN 技术可以把现有的网络划分为逻辑上隔离的网络，解决行业内部门之间的互联，同时也可以提供新的业务，如为电视电话视频系统专门开辟一个 VPN，以解决 IP 网络地址不足的问题。同时，基于 MPLS 技术的 VPN 还可与 QoS 保证结合，因为两者都是基于标记的技术，也可以用 MPLS VPN 为 IPv6 开展业务。基于 MPLS 的 VPN 适合应用在复杂的网络环境中，能够提供稳定并且有弹性的服务质量保证[1]。

在 MPLS VPN 的模型中，网络由骨干网和用户的各个 SITE 组成，所谓 VPN 就是对 SITE 集合的划分，一个 VPN 就对应一个由若干 SITE 组成的集合，MPLS VPN 主要由 CE、PE 和 P 共 3 部分组成[2]，如图 1所示。

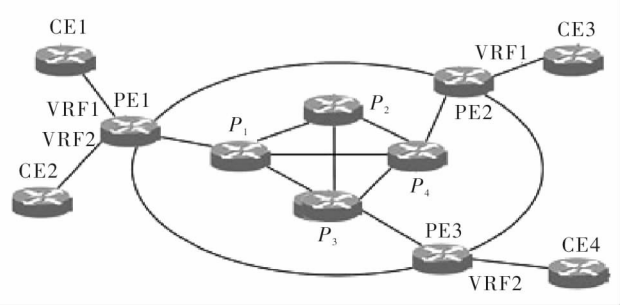

图 1　MPLS VPN 网络结构示意图

收稿日期：2012-10-18
作者简介：苏雪娟(1984—)，女，硕士，工程师。研究方向：无线通信与电磁兼容。E-mail：sue_3152@126.com

CE(Customer Edge Router),网络边缘路由器设备,直接与服务提供商网络相连。PE(Provider Edge Router),服务提供商边缘路由器设备,是 MPLS 三层 VPN 的主要实现者。P(Provider Router),服务提供商核心路由器设备,负责 MPLS 转发,不与 CE 直接相连。

PE 负责建立 LSP 连接,对 VPN 用户进行管理、同一 VPN 用户分支间路由分派;PE 间的路由分派通常是用扩展的 BGP 或 LDP 协议实现,支持不同 VPN 间互通和不同分支间 IP 地址复用,并且减化了寻址步骤,加快了报文转发,提高了设备性能。

2　基于 MPLS 的 VPN 广域网设计

企业中的广域网需要承载诸多业务系统,每个系统由于其功能不同,业务上要相互独立且在网络上逻辑分开,并且要求相互之间访问要在可控、可管理的方式下进行。由于各个业务系统的终端分布在不同的地理位置,企业不可能为各个业务系统单独建设一个物理网络,代价高而且不易统一管理。因此,在一个快速发展的骨干网络平台上实现各个业务系统网络的有力融合,并保障各个网络之间的相互独立和高效安全尤为必要。所以组网方案应方便各个业务系统的接入和扩展,并要求不对现有业务系统运行方式作任何改动。

2.1　网络架构设计

广域网采用3层结构,分别为:核心层、汇聚层和接入层。P 和 PE 设备采用千兆以太网组网,利用双链路环网通过接入到 PE 设备作为 CE 设备的通信通道。

2.2　路由设计

路由设计分为 IGP 的设计和 EGP 的设计,IGP 产生路由,EGP 传播路由。采用 BGP4 作为 MPLS VPN 路由协议,OSPF 作为内部路由协议。在汇聚层和接入层上同时运行 OSPF、BGP 和 MPLS BGP 完成全局选路和 VPN 选路。在 CE 设备上使用静态路由完成选路。

2.2.1　BGP 路由

文中的广域网是一个专网,没有和公网互连的需求,也不会和公网交互 BGP 路由信息,所以 AS 号可以自由地分配,为实现统一,将整个网络系统的 BGP 路由 AS 号暂定为65000。为解决 AS 内各节点需要IBGP 全连接的问题,可以采用 P 设备作为路由反射器,与 PE 设备建立 IBGP 对等关系,保持网络的扩展性和灵活性。

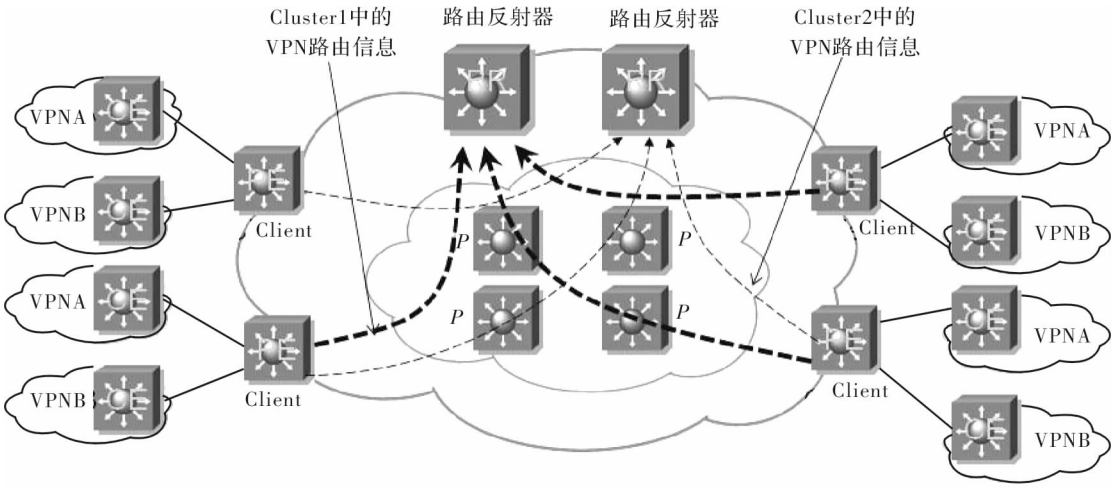

图2　路由反射器示意图

2.2.2　IGP 路由

IGP 对 MPLS 标签的建立有关键作用,并且通过全局路由表管理网络设备。在 IGP 中,OSPF 协议是应用于大型网络的链路状态的路由协议,因此在广域网中,为减少路由和网络带宽,将 P 设备和 PE 设备划分为 OSPF 骨干区域,而 CE 设备则根据其具体位置划分到不同的 OSPF 非骨干区域内,从而分散路由处理和减少网络带宽。

2.2.3　PE 设备和 CE 设备间的路由

对于 MPLS VPN,每个 VPN 都相当于一个专网,专网内的路由是通过 PE 设备与 CE 设备之间的路由实现的。采用 OSPF 协议,并针对不同的业务 VPN,启用不同 OSPF 进程号。为减少 CE 设备的路由条目,PE 设备学习 CE 设备所有路由条目的同时,由 PE 设备通过 OSPF 强制生成一条默认路由传递给 CE 设备,不将通过 BGP 学到的路由重新发布给 CE 设备,这样在 CE 设备上将只有默认路由和直连路由条目,大幅减少了路由条目的数量[3]。

2.2.4　PE 设备和 CE 设备间的互联

CE 设备采用支持 VRF 功能的 3 层交换机,可以为 VPN 内路由和全局路由提供各自独立的路由表,以达到各个 VPN 间逻辑隔离的目的。PE 设备和 CE 设

备间的互联,需考虑将 VPN 内路由和全局路由如何分别发布到 PE 设备上。可以在 PE 设备和 CE 设备上为 VPN 内路由和全局路由划分各自互联 VLAN,并将 PE 设备与 CE 设备互联的接口设置为 TRUNK 口。然后在 CE 设备上为各个 VPN 划分出业务 VLAN,且将 CE 设备上的同一组互联 VLAN 与业务 VLAN 放在同一个 VRF 内,这样 PE 设备便可以通过互联 VLAN 学习到 CE 设备上业务 VLAN 的路由条目。

3　MPLS VPN 在广域网中的实际应用

3.1　滁州供电广域网概况

滁州供电公司广域网网络规划主要按照物理位置进行划分,包括 6 个县级供电公司,24 个变电站、3 个集控站以及住宅小区,采用环网组网方式,变电站和县公司节点的接入均采用光纤接入的方式,以 100/1 000 Mbit·s^{-1}的速率相连。变电站和县公司新上设备作为全网中的 PE 设备,各县公司核心设备作为 CE 设备使用。县公司和变电站同时需要建立 2 个 VPN 实例[4],如图 3 和图 4 所示。

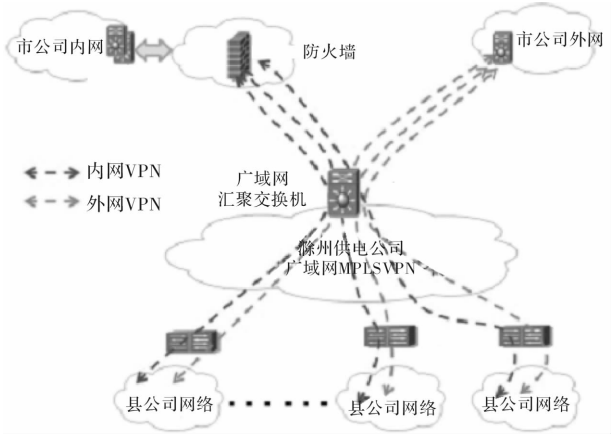

图 3　县公司 MPLS VPN 网络拓补图

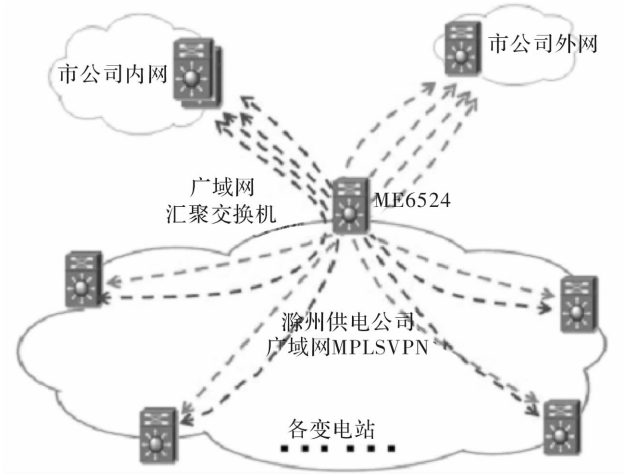

图 4　变电站 MPLS VPN 网络拓补图

3.2　MSLP VPN 在广域网中的应用

滁州供电公司网络承载有营销收费、生产 PMS、OA 办公、IP 电话等多种业务,这些业务系统分属不同的部门维护和管理。为满足企业业务支撑网络整体长期发展的需要,采用 MPLS VPN 技术对现有网络进行了改造升级。建立统一的 MPLS 骨干网络来承载公司所有内部业务,不同的业务系统通过划分 VPN 来实现互访与逻辑隔离。在市县公司都部署相应的 PE 设备,各县公司核心设备作为 CE 设备使用[5-6]。

在 VPN 规划上,针对不同的业务系统划分不同的 VPN。通过在 PE 上设置合理的 RT 对 VPN 间的互访与隔离实现了有效控制,相同的 VPN 间可以互相访问。

在网络的控制层面,把所有的 P 设备和 PE 设备都放在一个域内启用 OSPF 协议,用于 LDP 标签分发和建立 LSP。所有的 PE 设备也放在一个域内启用 MBGP,用于 VPN 路由的发布和处理。

由于采用基于 MPLS 的 VPN 技术组网,因此对于原来各业务系统的 IP 地址规划和各 CE 设备以下网络不需要做任何的改动。在 MPLS 骨干网络建设完成后,只需调整各系统的 CE 设备就可以实现各业务系统的平滑入网。

4　结束语

MPLS VPN 技术为电力企业的信息化建设提供了新的方向和技术支持。文中根据 MPLS VPN 技术的特点,探讨了其在信息网络中的实际应用,总结了改造后的 MPLS 的 VPN 网络有以下特点:(1)安全措施部署简单,各业务系统之间可以进行可控的互访和安全隔离。(2)统一骨干网络承载各个业务系统,网络结构清晰明了,维护简单。(3)可以根据各业务系统实际的流量分配带宽,网络资源利用率高。(4)网络扩展性好,当新增业务系统时,只需增加一个 VPN,不需要针对某个业务系统单独扩容网络带宽。

参考文献

[1] GUICHARD J. MPLS 网络设计权威指南[M]. 陈武,译. 北京:人民邮电出版社,2007.
[2] 陈雪非,黄河,李蓬. MPL8 VPN 关键技术研究[J]. 计算机工程与设计,2007,28(13):3138-3150.
[3] EL MGHAZLI. L3VPN operations and management framework [S]. USA:Stander of RFC4176,2005.
[4] 韩波,沈富可,刘莉. BGP/MPLS VPN 在 NS-2 中的实现[J]. 计算机应用,2006,26(4):980-982.
[5] 赖蔚蔚. 组播在电力 MPLS/VPN 城域网中的应用[J]. 电子科技,2007,20(5):45-48.
[6] 程彪,徐学洲. MPLS/BGP VPN 中组播的实现研究[J]. 电子科技,2007,20(3):53-57.