

运用 MPLS/VPN 技术构建集团化医院广域网信息平台

刘 谦 翁昌晶 陈加宜

(海南省人民医院信息中心 海口 570311)

〔摘要〕 结合海南省人民医院计算机广域网平台建设实际工作,在分析 MPLS/VPN 技术组网概念、原理和特点的基础上,提出基于 MPLS/VPN 技术的大型集团化综合医院计算机广域网平台建设方案,并对方案设计要点进行分析,为构建医院临床数据中心打下基础。

〔关键词〕 医院; MPLS; VPN; 广域网

Utilizing MPLS/VPN Technology to Construct WAN Information Platform for a Group of Hospitals LIU Qian, WENG Chang-jing, CHEN Jia-yi, the Information Center of Hainan Provincial People's Hospital, Haikou 570311, China

〔Abstract〕 Combining the experiences of constructing the Hainan Provincial People's Hospital WAN platform, analyzing the concept, the principle and the feature of MPLS/VPN technology networking, the paper proposes a WAN platform construction scheme based on MPLS/VPN technology for a group of general hospitals, and analyzes the critical points of this scheme, so as to lay a fundamental work for constructing a clinical data center in hospitals.

〔Keywords〕 Hospital; MPLS; VPN; Wide area network (WAN)

1 引言

近年来,随着医疗卫生体制的改革,我国综合医院的结构和规模发生很大变化。特别是加入了 WTO 以后,为了应对新形势下医疗市场的机遇与挑战,积极适应并参与国际医疗市场的竞争,国内开始出现了一些以设备先进、技术精湛、服务优质的大型综合医院为核心的医疗集团和医疗联合体。医院已经逐渐走出原来狭小的范围,开始形成集团

化、规模化的实体。与此同时,随着计算机信息处理技术的不断发展,医院信息化与数字化建设也取得了长足的进步,数字化医院的概念应运而生。数字化医院通过计算机网络把数字化医疗设备、医学影像系统和医疗信息系统等全部临床业务过程纳入到数字化网络中,从而实现管理和临床工作的无纸化运行。数字化医院的建立,将会使我国目前“以收费为中心”的医院信息系统走向“以病人为中心”的临床信息系统^[1]。继而医院计算机网络系统的建设又面临着新的挑战。一方面是医院规模和范围的不断扩大使得医院的计算机网络不能再局限于一种传统意义上的局域网系统;另一方面是医院的数字化建设要求医院计算机网络系统的传输速率要更加快捷。因此,探讨如何建立面向集团化医院的高速率、高效率计算机广域网平台,成为了医院信

〔收稿日期〕 2009-12-16

〔作者简介〕 刘谦,高级工程师,信息管理处处长,发表论文 60 余篇。

息化和数字化建设的热点。高速高效的计算机广域网平台的建设将为建设“以病人为中心”的临床信息系统打下一个坚实的基础^[2]。

2 MPLS/VPN 技术

2.1 MPLS/VPN 技术基本概念

近年来, 计算机网络与数字通信技术发展迅速, 特别是宽带互联网技术迅速崛起促进了计算机广域网技术革命性的飞跃发展。随着互联网及网络技术的发展, 虚拟专用网 (Virtual Private Network, VPN) 技术被广泛地应用。MPLS/VPN 是一种基于 MPLS 技术的 IP - VPN, 在网络路由和交换设备上应用 MPLS 技术, 从而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形成 IP 虚拟专用网络 (IP - VPN)^[3]。MPLS (Multi Protocols Label Switching) 即多协议标记交换, 是一项用绑定在包中的标记 (或叫标签) 通过网络进行数据包转发的技术。它将第 2 层的交换和第 3 层的路由技术很好地结合起来, 以简洁的方式完成了信息的传送, 把路由选择和数据转发分开, 由标签来规定通过网络的路径。VPN 是利用公共网络来传输私有信息而形成的逻辑网络, 用来在通用的网络结构上标识闭合的用户组^[4]。通过对网络数据的封包和加密传输, 在一个公用网络 (通常是因特网) 建立一个临时的、安全的连接, 从而在公网上完整、保密地传输私有数据^[5]。

2.2 MPLS/VPN 工作原理

MPLS/VPN 是指基于 MPLS 技术构建的虚拟专用网, 即采用 MPLS 技术在公共 IP 网络上构建企业的 IP 专网, 实现数据、语音、图像多业务宽带连接^[6]。MPLS/VPN 能够在提供原有 VPN 网络所有功能的同时, 提供强有力的 QoS (Quality of Service, 服务质量) 的能力, 具有可靠性高、安全性高、扩展能力强、控制策略灵活等特点。MPLS/VPN 的组网原理, 见图 1。

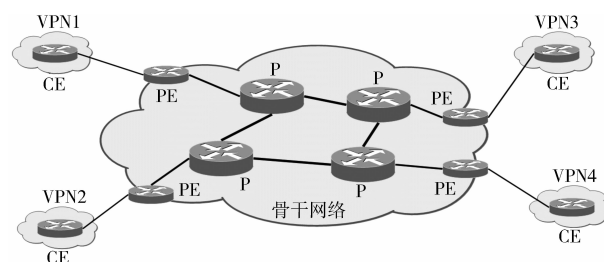


图 1 MPLS/VPN 组网原理

在 MPLS/VPN 中, 所有的路由器分为 3 类: 用户边缘路由器 (CE)、运营商边缘路由器 (PE) 和运营商骨干路由器 (P), 其中 PE 充当 IP - VPN 接入路由器。MPLS/VPN 的主要工作流程如下: 用户端的路由器 (CE) 首先通过静态路由和 BGP 将用户网络中的路由信息通知运营商路由器 (PE), 同时在 PE 之间采用 BGP 的 Extension 传送 VPN - IP 的信息以及相应的标记 (VPN 的标记, 以下简称为内层标记), 而在 PE 与 P 路由器之间则采用传统的 IGP 协议相互学习路由信息, 采用 LDP 协议进行路由信息与标记 (骨干网络中的标记, 以下称为外层标记) 的绑定。此时, CE、PE 以及 P 路由器基本的网络拓扑和路由信息已经形成, PE 路由器拥有了骨干网络的路由信息以及每一个 VPN 的路由信息。当属于某一个 VPN 的 CE 用户数据进入网络时, 在 CE 与 PE 连接的接口上可以识别出该 CE 属于哪一个 VPN, 进而到该 VPN 的路由表中去读取下一跳的地址信息, 同时在上传的数据包上打上 VPN 标记 (内层标记)。这时得到的下一跳地址为与该 PE 作 Peer 的 PE 的地址, 为了达到这个目的端的地址, 同时采用 LDP 在用户上传数据包中打上骨干网络中的标记 (外层标记)。在骨干网络中, 初始 PE 之后的 P 只读取外层标记的信息来决定下一跳, 因此骨干网络中只是简单的标记交换。在达到目的端 PE 之前的最后一个 P 路由器时, 将外层标记去掉, 读取内层标记, 找到 VPN 并送到相关的接口上, 进而将数据传送到 VPN 的目的地址处。从以上可见, MPLS/VPN 丝毫不改变 CE 和 PE 原有的配置, 有新的 CE 加入网络时, 只需在 PE 上作简单配置, 其余的改动信息由 IGP/BGP 自动通知 CE 和 PE。

2.3 MPLS/VPN 的特点

安全性: MPLS 可以将不同 VPN 的通信完全隔离,使得无关用户的通信不会混杂其中,从而提高了安全性。MPLS/VPN 借助 MPLS 技术,利用两层标记(Label),自动为不同用户的节点间建立不同的隧道,实现了用户流量的隔离,提供了逻辑上最大的安全性^[7]。

扩展性: MPLS/VPN 具有很好的网络扩展性,可建立任意的连接。同一个 VPN 中的用户节点数不受限制、容易扩充,特别是在实现用户节点间的全网状通信时不需要逐条配置用户节点间的电路。

可靠性: 网络的可靠性主要靠资源的冗余度实现。MPLS/VPN 依托互联网展开,因此设备、线路和路由都有冗余保护措施,保证网络的可靠性^[8]。

无连接的服务: MPLS/VPN 是“非面向连接的”,不需要通过建立许多点对点的隧道和加密技术来实现,这样可大大减少网络实现的复杂性^[9]。

易于实施: 由于 MPLS/VPN 是“非面向连接的”,且 VPN 信息只需要由 PE 来维护,对 CE 是透明的,网络的扩展和实施变得相对容易。增加 VPN 客户端站点时,只要简单地将 CE 设备接入 PE 即可,所有的配置只需在 PE 上进行,非常易于实现和管理^[10]。

3 基于 MPLS/VPN 的集团化医院广域网平台的建设方案

海南省人民医院是全省医疗设备先进、技术力量雄厚、建设规模最大、集医疗、急救、教学、科研、预防、保健、康复于一体的综合性三级甲等医院。除了在海府地区先后设立了 4 个门诊部之外,又新与省地矿局合作建立了医院的南沙路分院(眼科医院),与省洋浦管理局合作在洋浦经济开发区建立了洋浦分院。此外,医院还正在积极筹划建设海南省肿瘤医院,已经初步形成了集团化医院的总体结构。医院原有的广域网系统建设从 2003 年开始,主要租用海南电信公司的 2M 帧中继线路,之后又根据业务的发展租用了电信公司的 6M 数字电

路,实现龙华路门诊部与院本部的联网升级工作。显然,上述线路的带宽都十分有限,而且,随着近年来医院临床信息系统的建设,包括临床检验信息系统(LIS)、放射信息系统(RIS)、医学影像信息系统(PACS)、超声影像信息系统(USIS)在内的各种信息系统均在上述广域网平台上运行,网络的负荷十分繁重。随着 2009 年南沙和洋浦两分院的投入(或即将投入)使用,2003 年建设的医院广域网平台已经无法满足医院业务发展的需要,急需改造升级。

按照目前网络系统的拓扑结构,并充分考虑医疗业务快速增长的实际情况,利用 MPLS/VPN 技术构建广域网平台是恰当的选择。而且,目前海南电信正在全力推广基于 MPLS/VPN 的城域网业务,这也为医院利用 MPLS/VPN 技术提供一个有利的条件。实施改造后的医院广域网平台,见图 2。

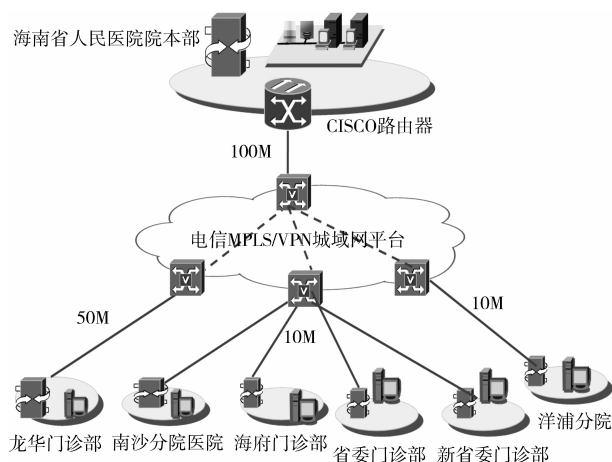


图 2 基于 MPLS/VPN 的医院广域网平台拓扑结构

4 方案设计要点

根据医院业务发展的需求,以院本部的信息大楼作为医院的数据中心。院本部作为广域网平台的主点通过一台 CISCOR 2811 的路由器作为 CE,以 100M 光纤电路接入电信城域网的 PE 路由器。考虑到各分点的业务量及网络经济性,其中龙华门诊部作为重要分点通过一台 CISCOR 2600 的路由器作为 CE,以 50M 光纤电路接入电信城域网的 PE 路由器;省委门诊部、海府路门诊部、新省委门诊部、

南沙路分院和洋浦分院等分别通过通过一台 CISCO 1711 的路由器作为 CE, 以 10M 光纤电路接入电信城域网的 PE 路由器。各个分支机构和主节点利用电信的骨干网络设备, 组建医院的 MPLS/VPN 网络, 实现各门诊部与秀英院本部的网络互联, 上述电路接口类型全部采用以太网技术标准。由于龙华路门诊部最大, 与院本部的信息交换最为频繁, 所以保证龙华路门诊部与院本部之间的通信畅通是整个系统的重要环节。在龙华路门诊部与院本部之间, 除了建立 MPLS/VPN 数据通道外, 还继续租用电信公司 6M 的数字电路作为备份电路, 两条线路相互配合, 互为备份, 较好地平衡了网络负载, 保证了与院本部之间的通信安全。

医院的局域网上有许多的信息资源, 包括患者的临床诊疗信息、医学文献及医学情报信息等。这些信息是医务人员在日常临床诊疗工作和业务学习中不可多得的宝贵资料。为了实现信息的检索能够不受地域的限制这一目标, 建立院本部的 VPN 访问服务器, 让临床医务人员可以在家里或其他医院局域网以外的任何地方, 通过 Internet 和 VPN 访问医院局域网上的数据资源。这样就大大地拓展了医院计算机网络系统的应用范围, 即使是出差在外的医务人员, 只要能进入互联网, 就可以通过 VPN 访问医院的网络, 处理患者的临床资料或查阅医学文献, 使医院的计算机网络系统和信息系统在更大的空间上发挥更大的作用。

上述网络组建后, 将实现海南省医院各种数据信息资源共享、信息资源统一调配, 今后随着医院业务的拓展, 网络带宽只需做相应的增加, 无需改变现有的网络架构, 最大限度地保障现有设备的可利用率。同时考虑到网络的安全性, 可同时采用数字电路或互联网 VPN 的方式来作为备用电路, 一旦主用电路出现故障, 可立即切换到备用电路, 以保证业务的不间断性。

采用上述网络体系结构, 系统平台网络可扩展性好, 充分利用电信公司城域网, 系统网络扩容方便, 不需要网络硬件投资。此外系统平台实用性

好, 组网灵活, 采用点对多点方式组网, 可任意增加系统网点, 系统平台结构不受影响, 并且安全可靠。备用电路可采用互联网 VPN 或数字电路传输方式保护, 保证业务的安全运行。

5 结语

目前上述广域网平台已经在海南省人民医院投入使用, 较好地满足了各个门诊部与院本部之间数据通信的需求。广域网平台的建设保证医院各种信息系统一体化的管理, 实现数据的集中存储和统一发布, 为构建医院的临床医学数据中心打下了坚实的基础。计算机广域网平台的建设是医院信息化建设和数字化建设的一项重要工作, 必须积极主动, 抓紧抓好这项工作。

参考文献

- 1 郝建东, 刘延洲. 基于 MPLS VPN 电子管理平台的大型医院战略管理 [J]. 中国医院管理, 2007, 21 (11): 70-71.
- 2 翟油华, 王晓艳. 医院管理信息系统的追求——“信息永不间断”和“数据绝对安全” [J]. 医疗装备, 2004, 17 (8): 28-30.
- 3 王昕. MPLS/VPN 的应用与分析 [J]. 软件世界, 2007, 27 (22): 61-63.
- 4 赵慧, 石永革. 广域网接入技术的发展与应用 [J]. 计算机与现代化, 2001, 7 (6): 44-47.
- 5 贾伟. 广域网高速接入与互连 [J]. 电脑开发与应用, 2001, 14 (12): 42-44.
- 6 沈继涛, 张君阳. 浅谈 MPLS/VPN 技术 [J]. 福建电脑, 2009, 11 (6): 66.
- 7 李文红. MPLS/VPN 安全性研究 [J]. 计算机与数字工程, 2006, 34 (8): 59-61.
- 8 李刚, 王果平. MPLS/VPN 技术浅析 [J]. 电脑与信息技术, 2006, 14 (1): 33-37.
- 9 肖海涛, 李之棠, 梅松. MPLS VPN 技术的研究 [J]. 计算机工程与应用, 2003, 22 (14): 173-175.
- 10 江晓峰, 高兴锁, 周海涛. 基于 MPLS 的 VPN 技术探究 [J]. 计算机技术与发展, 2006, 16 (3): 53-55.