基于 MPLS VPN 的电子政务外网构建技术

冯乃光[1] 曾黄麟[2]

(四川广播电视大学 成都 610073)[1] (四川理工学院 自贡 643000)[2]

摘 要 简要阐述了 MPLS VPN 技术及特点,分析了在公共网络基础设施上利用 MPLS VPN 技术构建电子政务专网的技术问题,提出了应用 MPLS VPN 技术实现电子政务专网的构建方案。通过四川省某市电子政务专网的建设,有效地实现了将市政府各部门的局域网连成一个整体,同时实现了信息的安全传输,取得了良好的社会效益。证明了基于 MPLS VPN 的电子政务外网构建技术具有应用流畅、涵盖范围宽、灵活实用等优点。

关键词 电子政务网,主干设计,组网配置

中图法分类号 TP393.02 **文献标识码** A

Techniques of Electronic Governmental Opening Network Construction Technique Based on MPLS VPN

FENG Nai-guang[1] ZENG Huang-lin[2]

(Teaching Office of Sichuan Radio and Television University, Chengdu 610073, China)[1]

(Sichuan University of Science & Engineering, Zigong 643000, China)[2]

Abstract The techniques and characteristics of MPLS VPN were introduced. Some of problems of an electronic governmental opening network built on the public network was analyzed based on MPLS VPN. A construction scheme of electronic governmental opening network was presented on MPLS VPN techniques. We accomplished one of sichuan province's electronic governmental opening network on the public network, which can connect all the local governmental networks as a whole network with safety information transmission effectively as well as a good social beneficial result. It is shown that electronic governmental opening network construction techniques based on MPLS VPN is of merits of easy and smooth use and flexible practice as well as wide application and so on.

Keywords Electronic governmental network, Main construction design, Network equipment

1 引言

随着计算机网络及政府信息化步伐的加快,电子政务网的构建已在全国上下迅速铺开,各地各级政府部门陆续都在进行着电子政务专网的规划设计、建设实施和运行管理。本文研究 MPLS/VPN 技术在地市和区县部门之间构建电子政务外网的技术实现,以确保网络上数据的安全传输。

2 MPLS VPN 的概念

MPLS(Multiprotocol Label Switching)即多协议标签交换,其兼有基于第二层交换的分组转发技术和第三层路由选择技术的优点,利用绑定在 IP 包中的标签通过网络进行数据包转发的技术。IP 包在进入第一个 MPLS 设备时,MPLS 边缘路由器就用标签封装起来。MPLS 边缘路由器分析 IP 包的内容并且为这些 IP 包选择合适的标签,尔后所有 MPLS 网络中节点都是依据这个简短标签来作为转发判决依据。在随后的转发过程中,数据包的网络层包头将不再被进一步分析。VPN(Virtual Private Network)即虚拟专用网络。顾名思义,可以把虚拟专用网络理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路,就好比是架设了一条专线一样,但是它并不需要真正地去铺设光缆之类的物理线路。一句话,VPN 的核心就是在利用公共网络建立虚拟私有网。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实现的 IP 虚拟专用网络(IP VPN),可用来构造宽带的 Intranet,Extranet,满足多种灵活的业务需求。

3 MPLS VPN 的基本模型及原理

MPLS VPN 的基本模型如图 1 所示,其构成包括以下组件:骨干路由器(P)、边缘路由器(PE)、用户边缘路由器(CE)以及站点(Site)。P 是核心路由器,作为标签交换路由器(LSR),它根据分组的外层标签对 VPN 数据进行透明转发,P 路由器只维护到 PE 路由器的路由信息而不维护 VPN 相关的路由信息。PE 作为标签边缘路由器(LER),它们为 VPN 成员保持着 VPN 路由,与 CE 以及连到 P 的接口对等交换路由。P 与 PE 路由器之间将使用 IP 路由协议,建立 MPLS 核

到稿日期:2008-12-23 返修日期:2009-03-23 本文受国家高技术研究发展计划(863 计划)第四批课题基金(2008AA11A134)资助。

冯乃光(1962-),女,副教授,主要研究领域为多媒体技术及多媒体通信技术等,E-mail:naigfeng730@163.com;曾黄麟(1955-),男,博士,教授,主要研究领域为神经网络、粗集理论、非线性系统理论、无线电及微电子技术等。

心网络中的路径，并且使用标签控制协议（如 LDP）实现路由器之间的标记分发。CE 使用传统的路由选择方法实现网络连接。CE 与 PE，PE 与 PE 之间使用 BGP 协议作为标签控制协议，这其中 CE 与 PE 之间属于 BGP 自治区域之间的会话，即 EBGP，PE 与 PE 之间属于 BGP 自治区域内的会话，即 IBGP。Site 是用户的一个连通的 IP 系统，每一个 Site 通过 CE 与 PE 相连，Site 是构成 VPN 的基本单元。一个 VPN 是由多个 Site 组成的，一个 Site 也可以同时属于不同的 VPN。每个 PE 都直接与属于相应 VPN 的 Site 相连，这些 VPN 都直接映射到每个 PE 的各自的虚拟路由中。通过使用 BGP 协议 PE 路由器之间自动的交换特定 VPN 的 MPLS 标记，并且自动地在内部 VPN 站点之间建立 MPLS 隧道，这些 MPLS 隧道能够传输一个或多个特定 VPN，每个 VPN 标签交换通道都直接与隧道两端点的站点连接。目前基于 MPLS 的 VPN 方案中，以 RFC2547 中规定的 MPLS VPN 得到了大多数厂家的支持，如 Cisco，Juniper 等。现在看看是如何转发用户数据的。属于同一的 VPN 的两个 Site 之间转发报文使用两层标签，在入口 PE 上为报文打上两层标签，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，然后再使用内层标签决定报文应该转发到哪个 Site 上。

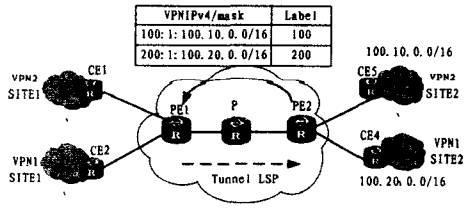

图 1　MPLS VPN 的基本模型

4　基于 MPLS VPN 构建电子政务外网技术的实现

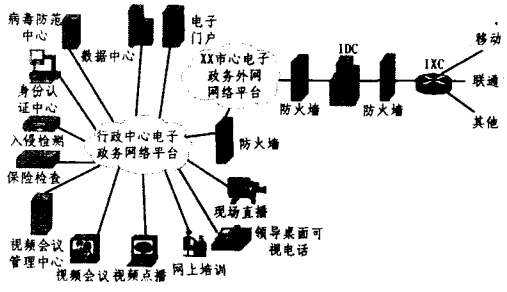

图 2　某市电子政务外网逻辑结构图

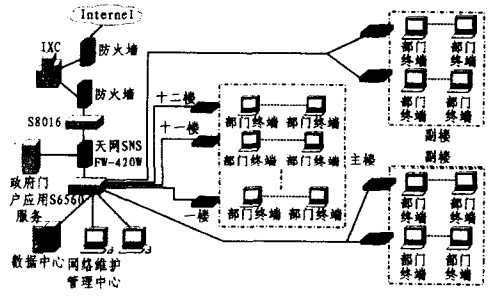

图 3　电子政务外网网络结构示意图

我省某市电子政务专网需要为该市近 200 个单位（包括党群口）建立市、区县二级横向网络，同时为省、市、区县三级党政部门建立纵向网络，满足各部门间资源共享的需要，其逻辑结构图如图 2 所示。图 3 为该电子政务外网网络结构示意图。

4.1　主干设计

该电子政务外网网络平台为该市网上办公提供统一的网络平台。在统一思想的网络平台上规范各部门业务流程和办事程序，统一资源规划、资源管理和网络建设。首先建立继往开来的信息发布机制，在网上发布各部门的职能、机构组成、办事章程、各项文件、资料、档案等，实现信息资源的共享。在网上建立该市办公自动化系统，实现公文流转、资料传递的网络化，实现无纸化办公；同时开发各种业务应用系统及各种管理系统，实现业务流程的网络化。随着网络应用于的深入，可以逐步在网上开展视频、声音等服务，如 IP 电话、视频会议等。

4.2　网络设计技术

4.2.1　网络结构

根据上级机构信息化办公室电子政务网络调整方案，该市电子政务外网依托广电光纤宽带，已覆盖至各镇及行政中心以外的部门并与上级电子政务外网相连，实现各种网络应用服务。

本着满足需求、节约经费的原则，该市政务中心大楼采用千兆光纤以太网作为网络系统主干，100 兆超五类线到桌面，使系统既具备了很好的扩展性，又拥有很高的性能价格比，能够为新业务的开展提供平滑的升级，保护投资。

系统使用一台华为 S6506 作为主干交换机，该交换机通过 1000M 光接口模块与电子政务外网骨干设备 S8016 直接连接。同时，该交换机连接实现线速的多层策略过滤，用以实现极为复杂的 VLAN 业务隔离，通过 VLAN 技术和二层交换技术，以达到隔离网络广播风暴、互通控制、流分类以及便于在楼内各部门之间进行分级权限管理等目的。边缘接入交换机选用华为 S3026，上行通过 1000M 光接口模块与 S6506 连接，下行 10/100M 到桌面，通过堆叠模块，可在不增加中心交换机端品及光纤的情况下，实现系统扩容，避免采用级联方式所带来的性能影响。

通过广电 S6506 交换机实现该所有政府部门 VLAN 透传至成都电子政务外网该核心节点华为 S8016，通过核心交换机华为 S8016 起用 MPLS/VPN，实现该市级各部门的互连和与成都电子政务外网、Internet 的互通。广电 S6506 交换机通过千兆单模光纤与成都电子政务外网该核心节点华为 S8016 相连。

4.2.2　IP 地址和路由设计

该市电子政务外网和政务中心大楼部门 IP 地址按照成都市电子政务外网地址规划方案实施。通过华为 S8016 实现该路由互连互通。

4.2.3　安全保障系统建设方案

该市电子政务外网接入成都市电子政务外网并通过逻辑隔离接入国际互联网，所以安全性显得尤其重要。该市电子政务外网的安全保密目标就是要解决以下安全问题：

- 防范国内外敌对势力的攻击。
- 防范网络攻击（即黑客）对网络可用性的攻击，保障网络的正常运行。
- 内部工作人员有意或无意的操作，导致网络出现安全

问题。

·满足今后网络发展所要求的网络用户身份鉴别、数字签名、安全审查、防止抵赖等。

4.3 采用 Q-in-Q 方式实现 CE 对 Internet 的访问

Q-in-Q(即 802.1Q-in-802.1Q)方式下,PE 的接入端一旦工作在 Q-in-Q 模式下,就只有缺省 Vlan 能起作用(用来作 VPLS 接入),进来的所有流量都认为是该 Vlan。在 Q-in-Q 端口下,该网络将某个 Vlan 接口指定为 Internet-access 接口,那么这个 Vlan 就可以和 Internet 连接,启动三层功能,而属于其它 Vlan 的流量则一律认为是 VPLS 流量。一个物理端口只能允许通过一个 Internet-access Vlan 接口。该电子政务外网组网配置示意图如图 4 所示。

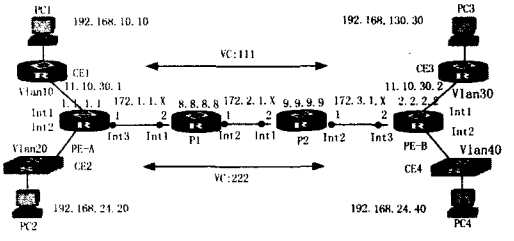

图 4 电子政务外网组网配置示意图

其中 PE-A 的主要配置

! MPLS 配置

[PE-A] mpls ldp

[PE-A-mpls-ldp] remote-peer local-ip 1.1.1.1 remote-ip 2.2.2.2

//建立 LDP Remote Session

[PE-A] int Int3

[PE-A-Int3] mpls ldp enable

! VPLS 的配置

[PE-A] mpls l2vpn //启动二层 VPN 功能

[PE-A] int vlan 10

[PE-A-Vlanif10] mpls vpls *encapsulation vlan mtu 1500*

//配置接口的 vpls 工作方式,封装模式为 vlan,mtu 为 1500。其中斜体字为可选配置

[PE-A-Vlanif10] mpls vpls vc 2.2.2.2 111

//和邻居 2.2.2.2 建立 VC,Vc 号为 111,不配封装模式和 mtu,则缺省为 vlan 接口的封装模式和 mtu

[PE-A] int vlan 20

[PE-A-Vlanif20] mpls vpls encapsulation ethernet

//配置接口的 VPLS 工作方式,封装为 Ethernet 模式

[PE-A-Vlanif20] mpls vpls vc 2.2.2.2 222 // 和邻居 2.2.2.2 建立 VC,VC号为 222

PE-B 的主要配置

! MPLS 配置

[PE-B] mpls ldp

[PE-B-mpls-ldp] remote-peer local-ip 2.2.2.2 remote-ip 1.1.1.1

//建立 LDP Remote Session

[PE-B] int Int3

[PE-B-Int3] mpls ldp enable

! VPLS 的配置

[PE-B] mpls l2vpn //启动二层 VPN 功能

[PE-B] int vlan 10

[PE-B-Vlanif10] mpls vpls *encapsulation vlan mtu 1500*

[PE-B-Vlanif10] mpls vpls vc 1.1.1.1 111

//和邻居 1.1.1.1 建立 VC,Vc 号为 111,不配封装模式和 mtu,则缺省为 vlan 接口的封装模式和 mtu

[PE-B] int vlan 20

[PE-B-Vlanif20] mpls vpls encapsulation ethernet

//配置接口的 VPLS 工作方式,封装为 Ethernet 模式

[PE-B-Vlanif20] mpls vpls vc 1.1.1.1 222 // 和邻居 1.1.1.1 建立 VC,VC 号为 222

结束语 本文主要以我省某市区电子政务外网为实例,讨论了基于 MPLS VPN 技术在该外网中的实际应用,并讨论了其技术实现方法。通过 MPLS VPN 技术在这个统一的网络平台上为各个行业和部门的应用系统划分各自独立的 VPN 隧道。该电子政务外网已投入使用,到目前为止运行稳定可靠。随着接入单位和用户的不断增加,带动了该市各单位的局域网建设和应用,取得了良好的社会效益。

参 考 文 献

[1] 王达,等. 虚拟专用网(VPN) 精解[M]. 北京:清华大学出版社,2005

[2] 纪辉进,魏华. VLAN 技术及其应用[J]. 软件导刊,2008,57(5)

[3] 王健全. 城域 MSTP 技术[M]. 北京:机械工业出版社,2005

[4] 杨红艳. MPLS/VPN 技术技术框架在大型企业网络中的应用[J]. 微型电脑应用,2007,10(57)

[5] Davie B,Rekhter Y. 多协议标签交换技术与应用[M]. 罗志祥,等译. 北京:机械工业出版社,2001

[6] 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

[7] 黄彦,梁京章,唐晓年. 基于 SNMP 的 VLAN 管理应用研究及其设计[J]. 微计算机信息,2008,237:11-13

[8] 赵霞,张黎军. 基于 MPLS 技术的网络仿真分析[J]. 重庆工学院学报:自然科学版,2007,21(4):112-114

(上接第 299 页)

[9] 王颖,李茂青. 基于一种新的评价指标的可重入生产系统调度[J]. 系统工程,2005,23(12):39-43

[10] Reeves C R. A Genetic Algorithm for Flow Shop Sequencing [J]. Computers Operations Research,1995,22(1):5-13

[11] Chen C L,Vempati V S,Aljaber N. An application of genetic algorithms for flow shop problems [J]. European Journal of Ops. Res.,1995,80:389-396

[12] 马玉敏,樊留群,张为民,等. 基于仿真的车间作业计划优化设计[J]. 系统仿真学报,2007,19(19):4548-4552

[13] 彭旺明,张晓川. Em-plant 在生产线作业仿真中的应用研究[J]. 武汉理工大学学报,2004,28(4):597-599

[14] 王仲君,程涤. 基于改进遗传算法的多维关联规则挖掘方法及应用[J]. 重庆工学院学报:自然科学版,2009,23(4):55-59