基于多协议交换的虚拟专用网络应用

赵明生[1]，李爱梅[2]

(1. 南京森林公安高等专科学校信息技术系 南京 210046; 2. 钟山学院信息与电子工程系 南京 210049)

【摘要】基于MPLS VPN是一种应用在网络交换和路由设备上的MPLS技术，给出了应用这种技术构架宽带Internet和Intranet的命令配置设计，可以满足各行业的应用需要。

关 键 词 多协议交换; 多协议标记交换; 虚拟私有网络; 服务质量
中图分类号 TN393.04 文献标识码 A

Research for Application of Multi-Protocol Exchange on Virtual Dedicated Network

ZHAO Ming-sheng，LI Ai-mei

(1. Department of Information Technology, Nanjing Forestry Police College Nanjing 210046;
2. Department of Information and Electron Engineering, Zhong Shan College Nanjing 210049)

Abstract Multi-Protocol Label Switching(MPLS) has been applied to realize virtual private networks(VPN). This paper introduces a command configure of multi-protocal labe switching VPN. This kind of technology can construct the bandwidth of Internet & Intranet and satisfy every profession and trade.

Key words multi-protocol exchange; MPLS; virtual private network; quality of service

随着Internet 的快速普及，以IP网络为基础的应用发展十分迅速，企业采用IP网络来构建Intranet的需求也与日俱增。在传统的IP数据包传输过程中，每一个节点设备必须重复检查一次封包的表头并解析下一个路径，直到到达目的地为止。因此网络越庞大，传输的效率越低下，无法满足Internet高速度大容量传输的需求，多协议标记交换(Multi-Protocol Label Switching，MPLS)的出现解决了这一问题。

1 MPLS产生的背景

MPLS通过在每一个节点的标签(label)交换来实现数据包的转发。标签是一个短而固定的数值，由报文的头部携带，不包括拓扑信息，只有局部意义。在网络中，第一层的主要功能是进行数据的放大处理，MPLS技术结合第二层交换和第三层路由的特点，将第二层的基础设施和第三层的路由有机地结合起来。第三层的路由在网络的边缘实施，通过MPLS，第三层的路由可以得到第二层技术的很好补充，从而充分发挥第二层良好的流量设计管理以及第三层单跳(hop-by-hop)路由的灵活性。

2 MPLS VPN实现的基本原理

MPLS交换技术引入了基于标签的机制，把选路和转发分开，由标签来规定一个分组通过网络的路径。在数据转发时，在网络入口对报文分类，根据分类选择相应的标签交换路由器(Label Switch Router，LSP)，打上相应的标签。中间路由器在收到MPLS报文后，标签作为IP报文的报头在网络中的替代品而存在，在网络内部直接根据MPLS的报头标签来实现转发；当报文要退出MPLS网络时，报文被解开封装，继续按照IP包的路由方式到达目的地，如图1所示。MPLS网络包含一些基本的元素，在网络边缘的节点被称作标签边缘路由器(Label Edge Router，LER)，而网络的核心节点称为标签交换路由器。LER节点在MPLS网络中完成的是IP包的进入和退出过程。LSR节点在网络中提供高速交换功能，在MPLS节点之间的路径就是标签交换路径(Latel Switch Path，LSP)，一条LSP可以看作是一条贯穿网络的单向隧道。

收稿日期：2005 – 11 – 02
作者简介：赵明生(1957 –)，男，教授，主要从事网络与控制技术方面的研究.

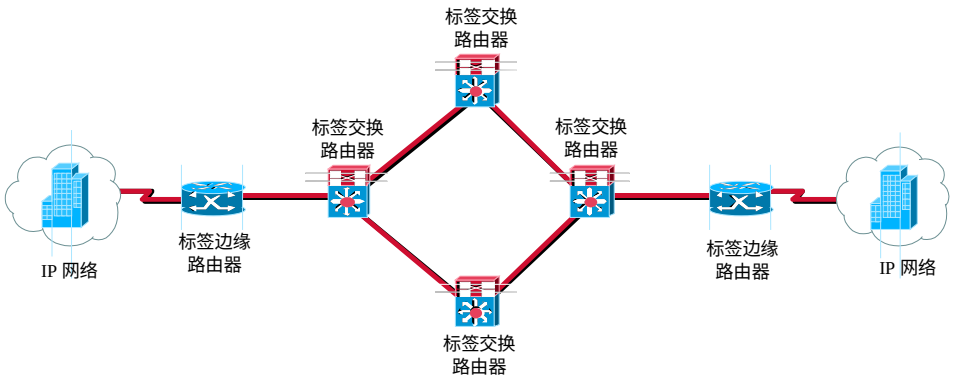

图1 MPLS的基本工作原理示意图

3 基于MPLS的IP VPN的结构[1]

MPLS为IP虚拟私有网络(Virtual Private Network，VPN)的实现提供了一种灵活的、具有可扩展性的技术基础。在MPLS网络中，一项IP VPN业务可以通过多种方式提供。一种方式是仿真第二层的IP VPN，如直接仿真帧中继；另一种方式是使用支持MPLS功能的用户设备来提供业务。无论哪一种方式都可以让业务提供者以一种集成的方式，在提供Internet服务的同一平台上提供这一流行业务。因此有多种支持IP VPN的方法，服务提供者可以根据内部网络以及用户的特定需求来决定自己的网络如何支持IP VPN。图2给出了使用MPLS和多协议边界网关协议来提供IP VPN业务的一种网络配置模型，该网络模型主要由提供者(provider)路由器、提供者边缘(provider edge)路由器、用户边缘(customer edge)路由器以及站点(site)组成。

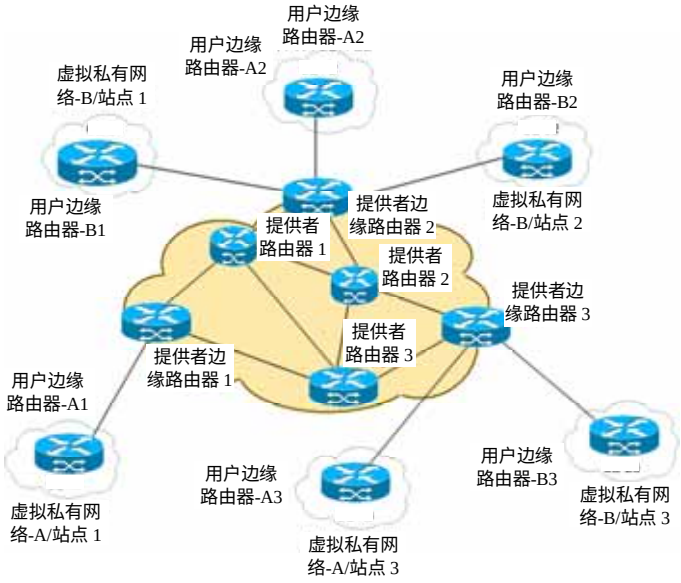

图2 基于MPLS的IP VPN网络组成模型示意图

P路由器相当于核心部分的标签交换路由器(LSR)，P路由器之间使用MPLS协议与进程，P与PE路由器使用IP路由协议(内部网关协议)来建立MPLS核心网络中的路径，并且使用标签分发协议(Label Distribution Protocol，LDP)实现路由器之间的标签分发。PE路由器相当于核心部分的标签边缘路由器(LER)。CE路由器的作用是将某个用户站点连接至PE路由器，它不使用MPLS，也不必支持任何VPN的特定路由协议和信令。站点(site)是一组网络或子网，它们是用户网络的一部分，通过一条或多条PE/CE链路接至VPN，而VPN是指一组共享相同路由信息的站点。一个站点可以同时位于不同的几个VPN之中。

图2中，每个PE(PE1－PE3)都直接和属于相应VPN的用户站点相连，这些VPN都直接映射到每个VPN各

自的虚拟路由中。通过使用边界网关协议(Border Gateway Protocol，BGP)，PE路由器之间自动地交换特定VPN的MPLS标签，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的VPN LSPs，每个VPN标签交换通道都直接与隧道两端点的站点连接。

4 MPLS IP VPN的工作过程[2]

CE路由器首先通过静态路由或BGP(MPLS/BGP VPN是指三层的VPN，而在MPLS的网络核心采用第二层交换)将用户网络中的路由信息通知PE路由器，同时在PE路由器之间采用BGP的Extension传送VPN-IP的信息以及相应的VPN标签；而在PE与P路由器之间则使用IGP协议的相互学习路由信息，采用标签分发协议(LDP)进行路由信息与骨干网络中的标签绑定。此时形成CE，PE以及P路由器中基本的网络拓扑以及路由信息。PE路由器拥有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VPN的CE数据进入网络时，在CE与PE路由器连接的接口上可以识别出该CE路由器属于那一个VPN，进而到该VPN的路由表中读取下一跳的地址信息；同时，在前传的数据包中打上VPN标签。为到达目的端PE路由器，在起始端PE路由器中读取骨干网络的路由信息，得到下一个P路由器的地址，同时采用LDP在用户前传数据包中打上骨干网络的标签。在骨干网络中，初始PE路由器之后的P路由器均只读取骨干网络中的标签的信息来决定下一跳，因此骨干网络中只是简单的标签交换。

在达到目的端PE路由器之前的最后一个P路由器时，将骨干网络中的标签去掉，读取VPN标签，找到VPN，并送到相关的接口，进而将数据传送到VPN的目的地址处。

5 MPLS VPN的命令配置设计

5.1 进入和退出各种命令模式的命令

```
rote >en
password:
rote #
rote #conf t
    rote (config)#interface fastethernet 0/0(配置路由器上面某个端口的IP地址)
    rote (config-if)#
    rote (config)#line con 0    (进入到console口的配置)
    rote (config-line)#
    rote (config)#line vty 0 4(进入到telnet的配置模式)
    rote (config-line)#
    rote (config)#router rip
    rote (config-router)#
```

5.2 配置路由器的主机名和进入特权模式的密码

```
    rote (config)#hostname rote
    rote(config)#
    rote(config)#enable secret rote
```

5.3 设定**console**口配置的登录密码

```
    rote(config)#line con 0
    rote(config-line)#exec-timeout 0 0
    rote(config-line)#login
    rote(config-line)#password rote
```

重新开启路由器进行console密码设定的验证，在rote(config)#reload重起路由器，开启时要求输入console登录密码。

5.4 为指定端口配置IP地址

```
    rote(config)#interface Ethernet 0/0
```

rote(config-if)#ip address 192.168.0.1 255.255.255.0

rote(config-if)#no shutdown

5.5 设定**telnet**登录密码并且使用远程主机进行登录配置

rote(config)#line vty 0 4

rote(config-line)#login

rote(config-line)#password rote

使用远程主机进行登录配置：(1) 用交叉线将路由器的ethernet口和pc的网卡接口连接；(2) 设置路由器的ethernet口的IP地址为同一网段，pc的ip设置为192.168.0.2；(3) 在运行里面键入“ telnet 192.168.0.1 ”回车；(4) 在虚拟终端里面输入telnet登录密码；(5) 在虚拟终端里用console进行配置。

5.6 使用**0×42**寄存器解决密码丢失问题

1) 开启路由器时，进入ROM检测模式。进入ROM有两种方法：(1) 开启路由器的时候按住<ctrl>+<break>；(2) 在全局模式下面键入rote(config)#config-register 0x0。

2) 设置路由器0x42引导系统，绕过正常时的0x2102寄存器，从而绕过NVROM中的enable口令，

rommon1>confreg 0x42

rommon2>reset

3) 重新启动路由器后将寄存器改为0x2102，

rote>enable

……

进入全局配置模式，将启动寄存器改为0x2102，

rote#config terminal

rote(config)#config-reg 0x2102

rote#reload

5.7 使用**show**命令查看路由器的配置

查看接口配置信息

show version

show process

show interface

show controllers

show buffers

show protocols

查看路由器内存中的配置及空间使用情况

show running-config

show startup-config

show flash

show mem

write terminal

show config

5.8 配置的保存和查看

(1) 将配置文件从RAM拷贝到NVRAM中，

rote# copy running-config startup-config

(2) 将NVRAM中的配置信息写入到RAM中，

rote#configure memory(路由器启动时这一过程是自动完成的)

(3)清除NVRAM中的配置文件，

rote#erase startup-config

(下转第92页)

4 结 束 语

已知目标求过程属于逆优化的范畴，它正在获得越来越多的学者的关注。网络扩充在现实生活中有着极其广泛的应用，出于现实的考虑，本文将时间约束加入到网络扩充问题中。通过网络变换，解决了给定时间限制和扩充目标容量求最小扩充费用的问题，并给出了网络容量的时间、费用Pareto扩充算法。本文的算法具有最一般化的形式，如果将时间约束放松至无穷，则问题便转化为仅考虑费用限制的网络容量扩充问题。事实上，网络规划是网络扩充的一个特例，只不过网络规划的现有网络为空。本文的研究同样适用于网络规划，可为决策者提供充足的信息，做出正确合理的决策。

参 考 文 献

[1] Zhang J, Yang C. A class of bottleneck expansion problems[J]. Computer Operation Research , 2001, 28(6): 505-519.
[2] Burkard R E, Klinz B, Zhang J. Bottleneck capacity expansion problems with general budget constraints[J]. Rairo Operation Research, 2001, 35(1): 1-20.
[3] Berman O, Einav D, Handler G. The constrained bottleneck problem in networks[J]. Operation Research, 1990, 38(2): 178-181.
[4] 王洪国, 马绍汉. 关于无向网络容量扩充的问题[J]. 山东大学学报, 2000, 35(4): 418-4.

编 辑 熊思亮

(上接第80页)

6 MPLS，QoS与宽带VPN业务

实现基于IP的VPN具有效率高、可扩展性好、管理配置简单等特点，适合超大规模的VPN应用。随着MPLS技术的完善和成熟，将保证全程全网端到端的高服务质量(Quality of Service，QoS)的互连互通，可满足不断增长的Internet业务对骨干网络设备的需求，其电信级可靠性、线速转发性能、完善的Diffserv/QoS机制和丰富的业务处理能力，适合于Internet骨干网和城域骨干网(Metropolitan Area Network，MAN)的建设需要；它支持MPLS交换，具有高速、宽带、智能、可靠、组网灵活等特点，并支持IP业务的QoS需求，为网络提供IP业务、VPN业务、智能路由，并对未来的MPLS网络业务提供良好的支持，可通过划分VPN网络来保障专业行业网络的安全性。

目前MPLS VPN技术已不断成熟，发展与应用也十分迅猛。MPLS VPN技术必将构建一个多业务的IP网络，为用户提供具有QoS保障、安全可靠，高速灵活的业务。

参 考 文 献

[1] 吴 江, 赵惠玲. 下一代的IP骨干网络技术—多协议标签交换[M]. 北京: 人民邮电出版社, 2001.
[2] 吴 伟. 下一代的IP网络技术保障—多协议标签交换[M]. 北京: 清华大学出版社, 2002.

编 辑 熊思亮