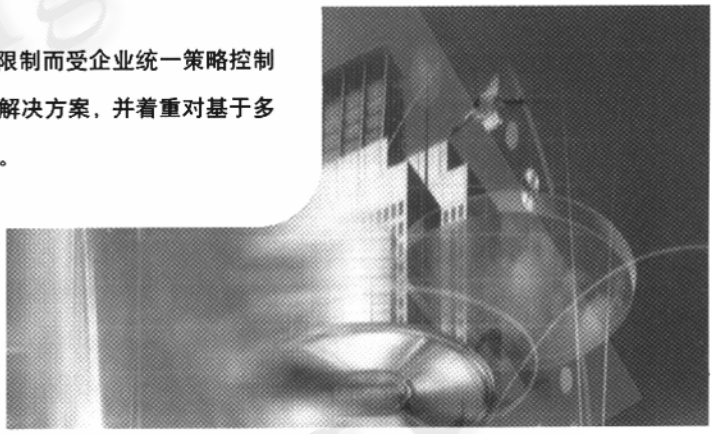
基于MPLS的VPN在城域网中的实现

李宏涛 彭涤 颜军 （深圳市宝安区信息中心 518101）



摘要： 利用VPN技术，可以在现有的公用网络平台上构筑不受地域限制而受企业统一策略控制和管理的企业网络。本文从VPN的基本概念出发，分析了其基本特征和解决方案，并着重对基于多协议标记交换（MPLS）技术的VPN进行了探讨，最后给出了一个实例。

关键词： VPN MPLS 隧道技术

随着Internet的普及和发展，虚拟专用网技术（Virtual Private Network,VPN）逐渐引起了人们的广泛关注，成为未来Internet应用和网络安全研究的一个重要方向。过去当企业需要把他们的信息网络扩展到远方而组成WAN时，通常的做法是租用PSTN、X.25、FR或DDN等线路，组成企业的专用网络。但随着Internet本身可靠性和可用性的增强，Internet已经为我们提供了最为廉价和普通的WAN通信；然而，Internet不能提供与专用网相比的安全性、带宽及服务质量（QoS）的保证。于是，一种新的企业通信模式——VPN应运而生。

1 VPN的基本概念及特征

所谓VPN，就是指在现有的公用网络平台上构筑不受地域限制而受企业统一策略控制和管理的企业网络。它与普通企业网不同的是其基础平台采用公用数据网，与其他用户共享网络资源而不是独占资源；它与普通互联网不同的是它受企业统一策略的网络管理，而不仅仅由网络服务商管理。

VPN的概念揭示了VPN的四个基本特征：

1.1 基于公用的网络平台

VPN所赖以运行的公网平台可以包括各种实际的网络，例如IP网、FR网、ATM网等，所以利用VPN技术组网，经济、便利、可靠、可用，同时组网灵活，具有良好的适应性和可扩展性。随着互联网的迅猛发展，TCP/IP已经成为应用最为广泛的网络协议体系，以下将主要针对基于IP的VPN（IP-VPN）进行讨论。

1.2 安全性

由于是构建在象Internet这样的网络环境之上，所以必须采用网络安全技术来保证信息的机密性、完整性、可鉴别性和可用性。开辟数据隧道、提供数据加密、建立专用连接、限制路由表分发等，都是安全性问题可能的解决方案，而这正是各种VPN技术的核心。

1.3 独占性

这是用户对构建在公用网络上的VPN的一种感觉，其实是在与其他用户或企业共享公用网络。

1.4 自成一体

VPN同专用网一样，可以拥有自己的地址空间，可以使用非IP协议，如IPX等。也就是说，VPN具有网络

地址翻译（NAT）和多协议支持的能力。

2 VPN的解决方案

一个有效的VPN必须满足以下基本要求：安全和保密性、高度的可管理性、灵活的可扩展能力，业务等级（CoS）及服务质量（QoS）的保证。为了满足上述需求，提供VPN业务的服务商所用的网络设备须具备提供这些技术的能力。事实上，由于网络技术的飞速发展，今天的许多网络设备已经具备了这些能力。一批公司，如Cisco、Bay、3Com、CheckPoint Software、Digital、IBM、Intel、Fortress Technologies、Microsoft、Extended Systems、Truested Information System、VP Net等，都先后开发并推出了各种VPN解决方案，包括IPSec安全协议、L2TP隧道技术、端到端的解决方案、CSM服务管理程序、CiscoAssure企业网络管理系统、IPQoS技术、MPLS技术等。从目前VPN的实际实施情况来看，主要基于以下两种技术：一是基于隧道技术，二是基于MPLS（多协议标记交换）。

2.1 传统的VPN技术——隧道技术

IP-VPN系统利用不可信任的公共IP网络通信，是通过安全的IP隧道来保证信息的机密性、完整性及可鉴别性，其核心是隧道技术。IP隧道替代了传统的WAN互联的“专线”，是组建“虚拟网络”的基础。在传统的隧道技术中，通常是不需要加密的，但在IP-VPN中必然要采用一定的安全协议，如IPSec（IP Secure）。

(1) IP隧道的“封装”机制：“封装”是构建隧道的基本手段，它使得IP隧道实现了隐蔽和抽象，为IP-VPN提供NAT、多协议支持等机制奠定了基础。当用一条隧道连接两个LAN时，只要申请两个Internet地址，而这两个LAN所组成的IP-VPN可以拥有自己的地址空间，通过NAT机制就实现了它们之间的透明的翻译转换。

(2) IP隧道的实现机制：IP隧道的实现机制主要涉及到两个方面，其一是第二层隧道与第三层隧道的问题，也就是说隧道所建立的连接是“虚拟”的链路层还是网络层。第二层隧道主要基于虚拟的PPP连接，如PPTP、L2TP等，它的主要优点是协议简单，易于加密，适合于为远程拨号用户接入IP-VPN提供虚拟PPP连接。但由于PPP会话贯穿整个隧道，并终止在用户网内的网关或RAS服务器上，所以需要维护大量的PPP会话连接状态，从而影响到系统的传输效率和系统的扩展性。而第三层隧道由于是IP in IP，如IP-Sec，其可靠性及可扩展性方面均优于第二层隧道，特别适合于LAN对LAN的互联，但对于移动用户就没有第二层隧道简单和直接了。

其二是在网络的什么层次上实现IP隧道，目前一般的做法是用IP协议实现IP隧道。

(3) IP隧道的安全协议：安全协议（隧道协议）是“专用网络”的保证，核心是加密、认证和密匙管理，目前用于IP隧道的有代表性的安全协议是：IPSec、PPTP、L2F、L2TP及SOCKs等。值得一提的是，IPSec是Internet工程任务组（IETF）为IP推荐的一个安全协议，它实际上是一个安全协议族，用于确保网络之间的安全通信。

(4) IP隧道技术的缺陷：基于传统IP方式的隧道技术具有以下一些先天的缺陷：一是扩展性，无论其隧道的建立是基于第二层或是第三层，当增加一个新节点时，每个节点必须与新增加的节点建立连接或是与其他路由器交换地址和链路以及设备状态信息，这在有成百上千个VPN的运营网络中是无法支持的；二是安全性，从目前看来许多协议的安全性不尽人意，如PPTP，无论是认证还是加密都还十分脆弱。三是服务质量，当用IPSec和通用路由封装（GRE）技术对VPN进行配置时，IPSec和GRE本身都不足以支持QoS。

2.2 新型的VPN技术——MPLS

MPLS（Multiprotocol Label Switch—多协议标签交换技术）是一种在开放的通信网上利用标签进行数据高速、高效传输的新技术。这里，标签（Label）是一个包头，标记交换路由器（Label Switch Router，LSR）根据事先算好的交换表，以此来转发数据包。图1为标签的格式示意图，标签的格式根据网络的属性而定。在IP网中，标签是独立的32位字段；在ATM网中，标签则位于VCI/VPI的信元头。

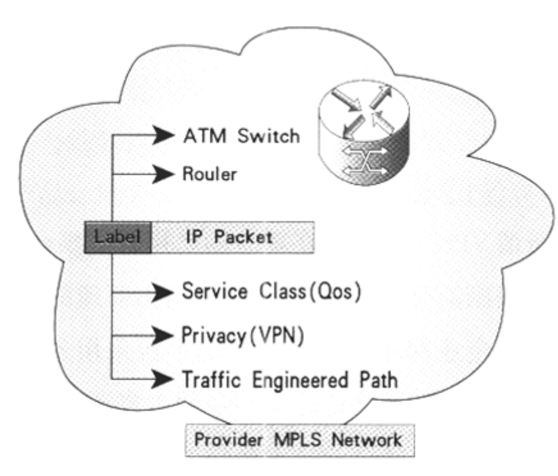


图1　标签格式示意图

MPLS的工作过程如图2所示。

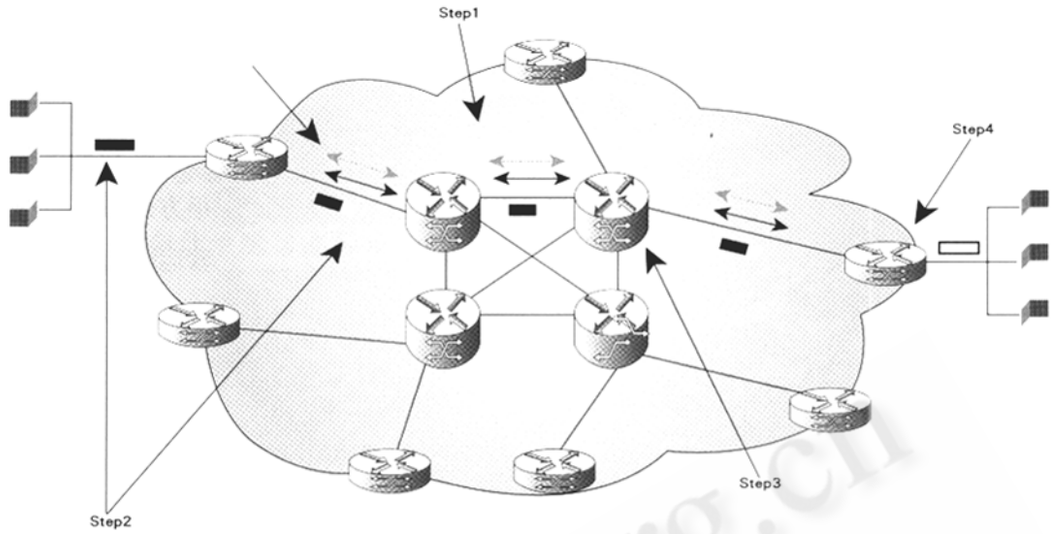


图 2 MPLS的工作过程

第1步，运营商网络的全部路由器使用IGP(如OSPF、IS-IS）路由协议自动建立路由表，然后通过标记分发协议（Label Distribution Protocol，LDP）使用路由表中的路由拓扑建立相邻设备的标签值(label value)，并建立标签交换路径（Label Switched Path，LSP)；第2步，一个入口数据包进入边缘标记交换路由器（Edge LSR)，在这里数据包经过处理，根据路由和所需要的L3服务（如QoS和带宽管理）在数据包头打标签并转发包；第3步，核心LSR读取每个数据包的标签，并将它替换成预先计算的交换表中所列的新标签，并转发包，这个操作在核心的每一跳中重复进行；第4步，出口Edge LSR去掉标签，读取数据包头，并转发到最终目的。

和基于传统隧道技术的VPN解决方案比较起来，MPLS的主要特点在于在一个无连接的IP网络中提供了面向连接的业务，由于网络中分组的转发是基于定长的标签，从而简化了网络的转发机制，降低了网络的复杂性和网络成本，使得转发路由器的容量很容易扩大到比特级。在提供IP业务的同时，能确保QoS和安全性，具有流量工程能力，并兼容现有的各种主流网络技术。由于解决了传统VPN网络中的扩展及维护成本等问题，MPLS技术必将成为下一代最具竞争力的通信网络技术之一。

通过以上对两种VPN技术的比较，可以看出MPLS技术将拥有更为广阔的前景。在深圳市宝安区信息网的建设中，我们选用的Cisco 12000交换机和7500路由器直接支持MPLS，这就为宝安信息网提供MPLS VPN业务建立了良好的运行平台。

3 MPLS VPN

3.1 MPLS VPN中的几个基本概念

(1) 提供者(Provider，P)路由器：P路由器是指运营商网络中的核心路由器，它就是LSR，只负责标签交换，并不理解具体的VPN。

(2) 提供者边缘(Provider Edge，PE)路由器：PE路由器是运营商网络的一部分，并与用户路由器相连。它是一个Edge LSR，提供MPLS运营商网络与不使用MPLS的用户网络的接口。

(3) 用户边缘 (Customer Edge,CE)路由器：CE路由器是用户网络的一部分，并连接PE路由器。CE路由器不使用MPLS，它只是一台普通IP路由器，不必支持任何VPN的特定路由协议或信令。

(4) 站点（Site)：站点是指这样一组网络或子网，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骨干网。

(5) 路径区别标志(Route Distinguisher，RD)：服务提供者将为每一条路径分配一个标志符(64位)，用于标识唯一一个VPN。

(6) VPN-IPv4地址：包括64位的RD和32位的IP地址。

(7) VPN路由/转发实例（VRF)：一个VRF由一个IP路由表,一个转发表，一套用于转发表的接口，一套规则和决定什么内容进入转发表的路由协议共同组成。一般情况下，VRF包括了定义客户VPN站点连接到PE路由器的路由信息。

3.2 MPLS IP-VPN的连接模型

MPLS IP-VPN的连接模型如图3所示。

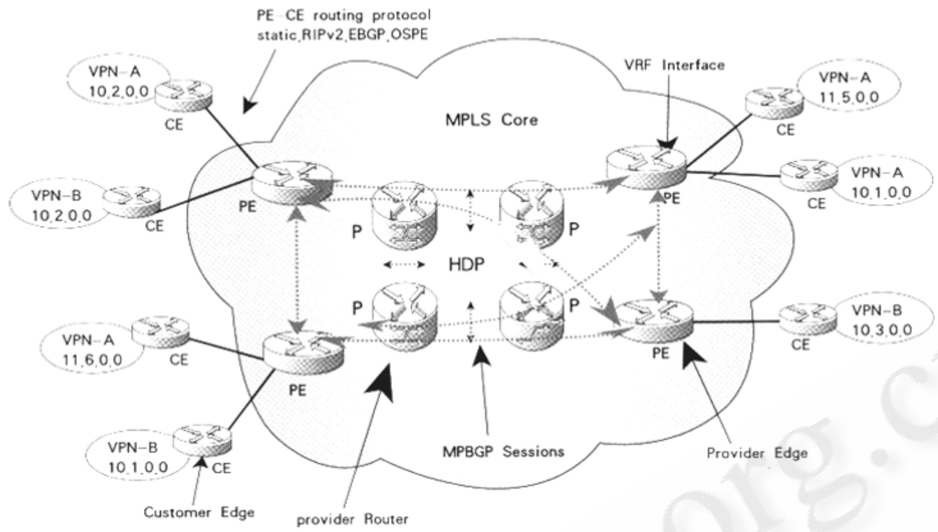


图3　MPLS IP-VPN的连接模型

MPLS IP-VPN连接模型的要点如下：

(1) 运营商全网要求IGP可达。

(2) PE路由器使用MP-iBGP（iBGP协议中的Community扩展属性）来实现彼此之间的通信，完成标记交换和每一个VPN策略。除非使用了路径映射路由器(route reflector)，否则PE之间是iBGP全网状连接。

(3) P路由器位于MPLS网络的核心，P路由器不使用iBGP协议而且对VPN一无所知，它们使用普通的MPLS协议与进程。P与PE路由器使用IGP来建立MPLS核心网络中的路径，并且使用LDP实现路由器之间的标记分发。

(4) CE路由器不必实现MPLS或对VPN有任何特别了解。PE路由器可以通过IP路由协议(RIPv2、EBGP)与CE路由器交换IP路径，也可以使用静态路径。在CE与PE路由器之间使用普通的路由进程，并且通过这一过程获得与之直接相连的用户网站IP地址前缀。

(5) VPN信息存放在PE路由器的VRF表中。PE之间的路由信息交换完成之后，每一个PE都将为每一个VPN建立一个转发表，该转发表将把VPN用户的特定地址前缀与下一跳PE路由器联系起来。当收到发自CE路由器的IP分组时，PE路由器将在转发表中查询该分组对应的VPN，以便决定对分组进行转发所要使用的接口。

(6) 在路径分发中，MP-iBGP使用VPN-IPv4地址（由RD和IPv4地址构成）。这样，不同的VPN可以使用重叠的IPv4地址空间而不会发生VPN-IP地址重复的情况。

4　一个实例

正在建设的深圳市宝安区信息网是一个覆盖全区733平方公里，以IP技术为核心的营运级宽带骨干网络信息服务平台。在骨干网的设备选型上，我们选择了支持MPLS的Cisco 12000交换机和7500路由器，在此基础上建立了教育、公安、卫生等系统的虚拟专用网络。拓扑简图如图4所示。■

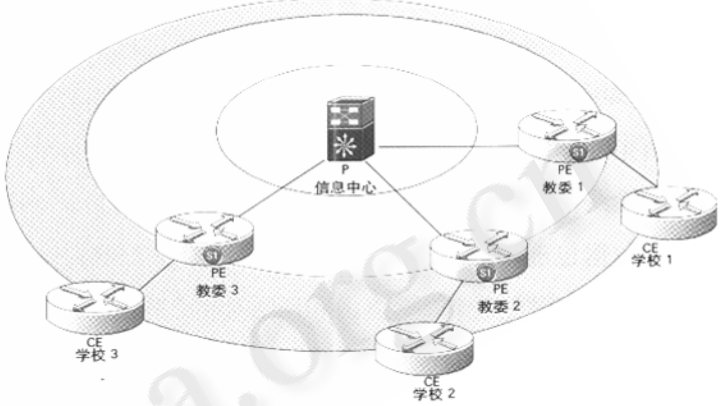


图4　教育系统拓扑简图

参考文献

1 Cisco, "Cisco MPLS Controller Software Configuration Guide", Release 9.3.0, April 2000。

2 Cisco White Paper, "Managing Virtual Private Networks—An Introduction to VPNs"。

3 Christopher Y.Metz, "IP Switching Protocols and Architectures", 机械工业出版社, 1999, 11。

4 李珂, 顾尚杰, 诸鸿文, "MPLS的研究发展及其关键技术综述", CHINA通信网, 2000, 4 。

5 毛小兵, "VPN演进之隧道交换", 计算机世界, 2000, 7。