基于 MPLS 的 VPN 网络设计与工程应用

计算机应用技术专业

研究生 朱　斌　　**指导老师** 徐　林

随着网络规模不断扩大，构建具有更高扩展性、更易于维护管理的 VPN 成为 VPN 网络发展的必然趋势。传统 VPN 网络在扩展性、维护管理性等方面已经不能满足 ISP（Internet 服务提供商）和企业对 VPN 网络的需求。MPLS（多协议标签交换）是一种将数据链路层交换技术与网络层路由技术结合起来的集成数据传输技术。利用 MPLS 在 VPN 方面的特点，采用 MPLS 来构建 VPN 网络可以很好地解决上述问题。本文设计并实现了这么一种基于 MPLS 的 VPN 网络。

首先，本文分析并指出了传统的采用隧道技术实现的 VPN 网络在扩展性、可维护管理性以及拓扑灵活性等方面的不足之处,提出了采用 MPLS 来构建 VPN 网络，并详细论述了采用 MPLS 来实现 VPN 的工作过程以及 MPLS/VPN 网络的特点和优势。

其次，本文设计了成都电信数据支撑中心 VPN 网络改造方案，根据该方案构建了 MPLS 的 VPN 网络，对构建 MPLS/VPN 网络的几个主要方面：IGP 协议、BGP 协议、路由反射以及 VPN 网络结构等方面进行了详细的规划与设计，并将该设计思想在路由设备上进行了具体实现。

最后，本文根据该设计模型，对实验网络进行了规划和设计并在具体的路由设备上配置实现,从安全性、扩展性等方面对该 VPN 试验网络进行了测试，通过获得的实验数据论证并详细分析了基于 MPLS 的 VPN 网络除了可以提供传统 VPN 网络的安全保障外，在扩展性、拓扑灵活性、以及可维护管理性等方面优于传统的 VPN 实现技术，为 ISP 和企业构建 VPN 提供了很好参考模型和解决方案。

关键词：多协议标签交换；虚拟专用网络；边界网关协议；网络性能分析；网络工程

MPLS Oriented VPN Network Design and Its Engineering

Major: Computer Application Technology

Postgraduate: Bin Zhu **Advisor:** Lin Xu

Due to enormous network expansion, it becomes an inevitable tendency to construct highly extensional and highly manageable VPN networks. But the traditional VPN network can not meet the demands of ISP and Enterprises in expansion and management. MPLS (Multi-Protocol Label Switching) combines the transmission technology of L2/L3 (Data-link-layer and IP-layer) .Using the characters of MPLS to construct VPN, It can solve totally these problems. This paper designs and implements a model of MPLS/VPN.

Firstly, this paper analyzes and points out the disadvantages of VPN that use traditional tunnel technology. Putting forward the model of MPLS/VPN and demonstrating the realization procession of MPLS/VPN and its characters and advantages in detail.

Secondly, this paper designs VPN reconstruction project of transaction supporting network of CHENGDU telecom, constructing the model of MPLS/VPN. Demonstrating the design and implementation of VPN network in main facets, as follow, IGP protocol 、BGP protocol and router-reflect in detail. In addition, applying these ideas in routers.

Finally, According to this VPN model, this paper designs and constructs the experimental network and realizes in routers. Testing this VPN in security 、extension and management. By way of the acquired experimental data , It is demonstrated that MPLS/VPN has high security In addition, operation、flexibility and expansion of MPLS/VPN . It is the better than traditional technology of VPN. The model of MPLS/VPN provides a good reference model and project for ISP and Enterprises.

Keywords: MPLS; VPN; BGP; Network performance Analysis; Network Engineering

第一章 序言

1.1 论文的课题来源

成都电信现有的业务支撑网络是构建在基于ATM技术的网络上，由于建立时间较长，随着电信业务的发展现有的ATM网络上支撑的业务也越来越多，这些业务是通过在ATM网络上构建不同的VPN来实现不同业务的隔离。

随着IP网络的不断发展，已经逐渐取代ATM成为网络互连的主流技术，因此成都电信不但需要构建安全的VPN还需要构建扩展性强、稳定性好、易维护和管理并且和现有的IP技术有很好的兼容性的VPN网络，需要对原有的基于ATM的VPN网络进行升级改造。本文的课题就是来源于成都电信计费网络升级改造方案的设计。

1.2 本人所做的工作

我在成都电信实习期间，结合该公司现有业务支撑网络的一些问题，提出了将原有的基于ATM的VPN网络改造到基于IP的MPLS/VPN网络，设计了基于MPLS的VPN网络模型，并搭建了MPLS/VPN实验网络，通过对该实验网络的测试，分析了MPLS/VPN网络在安全性、扩展性、拓扑灵活性、网络可靠性、QoS/CoS、网络维护管理等方面优于传统的VPN实现技术，为ISP以及其它企业在构建高效、易维护、扩展性强的VPN网络提供了有价值的参考。

1.3 MPLS概述

MPLS是多协议标签交换的简称，它是将第二层交换技术与第三层路由技术结合起来的一种L2/L3集成的数据传输技术，它界于网络层与数据链路层的2.5层，它是用短且定长的标签来封装网络层分组。MPLS由于

它是多协议的，所以它支持多种链路层（如 PPP、ATM、帧中继、以太网等）协议，又为网络层提供面向连接的服务。MPLS 能从 IP 路由协议和控制协议中得到支持，同时还支持基于策略的约束路由，路由功能强大、灵活，可以满足各种新应用对网络的要求。这种技术早期起源于 IPv4，但其核心技术可扩展到多种网络协议（IPv6、IPX 等）。

MPLS 实现了将第二层的交换技术和第三层的路由技术很好的结合。它以十分简洁的方式完成信息的传送。MPLS 首先根据某种特定的映射规则在网络入口 LER 处将数据流分组头和固定长度的标签对应起来，这种映射不但考虑到数据流的目的信息而且也考虑到了有关 QoS 的信息，然后在数据流的分组头中插入标签信息。在以后的网络转发过程中，MPLS LSR 就只是根据数据流所携带的标签进行交换和转发。相对于传统的“逐跳”的路由方式，MPLS 极大的提高了路由器的转发效率，同时 MPLS 在解决网络的扩展性、实施流量工程、同时支持多种要求特定 QoS 保障的 IP 业务等诸多方面具备得天独厚的技术优势。通过 MPLS 实现的宽带网络有效地结合了 L2 层快速交换与 L3 层灵活路由的技术优势，同时确保了 ISP 对网络原有设备的投资，MPLS 像其它宽带技术一样，会不断发展，不断完善，最终将成为下一带 Internet 的核心技术。

1.4 MPLS 出现的技术背景

1.4.1 Internet 的发展与变化

随着 Internet 与人们的生活关系越来越密切，Internet 在最近几年的发展速度是 Internet 出现时发展的几倍甚至几十倍，对 Internet 的发展用“爆炸式”来形容一点也不过分，Internet 在用户数目以及对带宽的需求这两个方面的增长，已经对 Internet 服务提供商的网络提出了越来越多的需求。为了满足对带宽不断增长的要求，ISP 需要更高性能的交换与路由产品。除了要让路由器变的更快以外，网络还要能处理更加丰富的业务，就需要路由器必须有一些新的功能来满足不断增长用户的新的需求，因此对路由协议也提出了新的要求。由于原有的路由算法在路由和转发之间的紧密耦

合，路由功能很难得到提高，这就需要一个新的转发算法而且这种算法不需要对原有路由硬件设备做任何改动就可以采用。

1.4.2 价格与性能

在 Internet 上最关键的器件是路由器，路由器的基本任务是转发 IP 分组穿越网络，路由器除了转发数据分组外还要执行非常广泛的功能，比如在网络的不同部分过滤数据包，对于很多应用场合，路由器的重要的特点不是它可以多快地转发分组，而是它可以提供一组多丰富的功能，另外一个重要的网络器件是交换机，路由器是三层设备，而交换机是二层设备。与路由器相比交换机更简单一些，它不能提供丰富的功能，但能提供对二层数据包的高速速转发。随着 Internet 的成功，IP 成为路由器需要处理的唯一一个协议的情况增加，我们在比较交换机和路由器的性能/价格比时，发现交换机的的性能/价格比高于路由器，这就让我们设想能否制造一台设备像交换机使用硬件的设备来完成路由器的功能，在一个交换机的价格/性能的水平上提供 IP 转发的期望。

1.4.3 扩展路由功能

采用标签交换不仅仅用来提高路由器的转发效率，标签交换也能提供新的功能如 QoS、流量工程和 VPN 等，而有现有的 IP 路由器来提供这些功能是很困难的，扩展路由功能也成为 MPLS 发展的一个推动因素。

第二章 MPLS体系结构

2.1 基本概念

2.1.1 MPLS标签结构

标签位于数据链路层包头和网络层分组之间，长度为4个字节，标签共有4个域。标签的封装结构如图2-1所示。

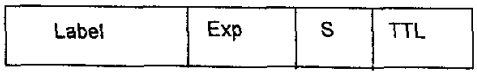

图2-1 标签的封装结构

Label：标签值字段，长度为20bits，用于转发的指针。

Exp：3bits，保留，用于试验。

S：1bit，MPLS支持标签的分层结构，即多重标签。值为1时表明为最底层标签。

TTL：8bits，和IP分组中的TTL意义相同。

2.1.2 标签在分组中的封装位置

标签在数据分组中的位置如图2-2所示：

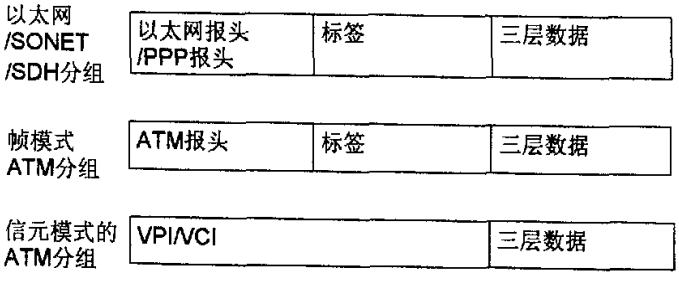

图2-2 标签在分组中的封装位置

2.1.3 标签分发方式

MPLS中使用的标签分发方式有两种：(1)下游自主标签分发方式(DU，Downstream Unsolicited)。(2)下游按需标签分发方式(DoD，Downstream On Demand)。

下游自主标签分配：对于一个特定的FEC（转发等价类），LSR（标签交换路由器）无须从上游获得标签请求消息即进行标签分配与分发的方式。

下游按需标签分配：对于一个特定的FEC，LSR获得标签请求消息之后才进行标签分配与分发的方式。

具有标签分发邻接关系的上游LSR和下游LSR之间必须对使用哪种标签分发方式达成一致。

在MPLS体系中，将特定标签分配给特定FEC的决定由下游LSR作出，下游LSR随后通知上游LSR。即标签由下游指定，分配的标签按照从下游到上游的方向分发。

2.1.4 标签控制方式

标签控制方式分为两种：（1）独立（Independent）标签控制方式和（2）有序（ordered）标签控制方式。

当使用独立标签控制方式时，每个LSR可以在任意时间向和它连接的LSR通告标签映射。

当使用有序标签控制方式时，只有当LSR收到某一特定FEC下一跳的特定标签映射消息或者LSR是LSP的出口节点时，LSR才可以向上游发送标签映射消息。

2.1.5 标签保留方式

标签保留方式分为两种：（1）自由标签保留方式和（2）保守标签保留方式。

在LSP路径上的相邻的两台路由器，对于特定的一个FEC，如果上游

LSR收到了来自下游LSR的标签绑定：当该下游路由器不是该上游LSR的下一跳时，如果该上游LSR保存该绑定，则称该LSR使用的是自由标签保留方式；如果上游LSR丢弃该绑定，则称该LSR使用的是保守标签保留方式。

当要求LSR能够迅速适应路由变化时可使用自由标签保留方式；当要求LSR中保存较少的标签数量时可使用保守标签保留方式。

2.1.6 LSP（标签交换路径）建立

LSP的建立过程其实就是将FEC和标签进行绑定，并将这种绑定通告LSP上相邻LSR的过程。这个过程是通过标签分发协议LDP（Label Distribution Protocol）来实现的。LDP规定了LSR间的消息交互过程和消息结构，以及路由选择方式。

2.1.6.1 LDP工作过程

LSR通过周期性地发送Hello消息来发现LSR邻居，然后与新发现的相邻LSR间建立LDP会话。通过LDP会话，相邻LSR间通告标签交换方式、标签空间、会话保持定时器值等信息。LDP会话是TCP连接，需通过LDP消息来维护，如果在会话保持定时器值规定的时间内没有其它LDP消息，那么必须发送会话保持消息来维持LDP会话的存在。图2-3为LDP标签分发示意图。

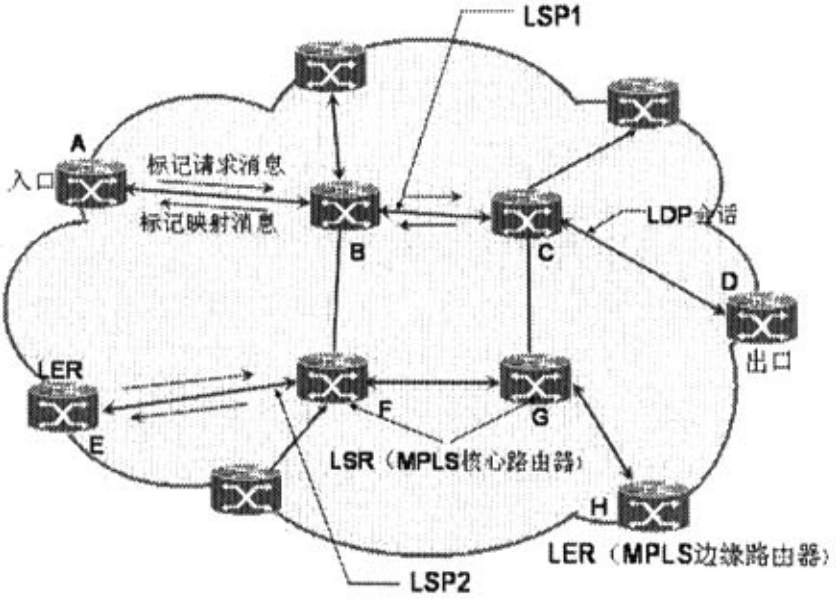

图 2-3 标签分发过程

在一条 LSP 上，沿数据传送的方向，相邻的 LSR 分别叫上游 LSR 和下游 LSR。如在图 2-3 中的 LSP1 上，LSR B 为 LSR C 的上游 LSR。

前面提到，标签的分发过程有两种模式：DoD（downstream-on-demand）模式和 DU（downstream unsolicited）模式。这两种模式的主要区别在于标签映射的发布是上游请求还是下游主动发布。

DoD（downstream-on-downstream）模式下标签的分发过程是这样：上游 LSR 向下游 LSR 发送标签请求消息（包含 FEC 的描述信息），下游 LSR 为此 FEC 分配标签，并将绑定的标签通过标签映射消息反馈给上游 LSR。下游 LSR 在何时反馈标签映射消息，取决于该 LSR 采用独立标签控制方式还是有序标签控制方式。当下游 LSR 采用有序标签控制方式时，只有收到它的下游返回的标签映射消息后才向其上游发送标签映射消息；当下游 LSR 采用独立标签控制方式时，则不管有没有收到它的下游返回的标签映

射消息都立即向其上游发送标签映射消息。上游LSR一般是根据其路由表中信息来选择下游LSR的。图2-3中LSP1沿途的LSR都采用有序标签控制方式，LSP2上LSR F采用独立标签控制方式。

DU（downstream unsolicited）模式下分发标签的过程：下游LSR在LDP会话建立成功，主动向其上游LSR发布标签映射消息。上游LSR保存标签映射信息，并根据路由表信息来处理收到的标签映射信息。

2.1.6.2 基于约束路由的LDP

MPLS还支持基于约束路由的LDP机制（CR-LDP，Constrain-based Routing LDP）。所谓CR-LDP，就是入口节点在发起建立LSP时，在标签请求消息中对LSP路由附加了一定的约束信息。这些约束信息可以是对沿途LSR的精确指定，此时叫严格的显式路由；也可以是对选择下游LSR时的模糊限制，此时叫松散的显式路由。

2.1.6.3 LSP环路控制

在MPLS域中建立LSP也要防止路径循环。防止LSP的路径循环有最大跳数和路径向量两种方式。

最大跳数方式是在传递标签绑定的消息中包含跳数信息，每经过一跳该值就加一，当该值超过规定的最大值时就认为出现了环路，从而终止LSP的建立过程。

路径向量方式是在传递标签绑定的消息中记录路径信息，每经过一跳，相应的路由器就检查自己的ID是否在此记录中，如果没有就将自己的ID添加到该记录中，若有就说明出现了环路，终止LSP的建立过程。

2.2 标签交换的转发功能主件

2.2.1 标签交换算法

2.2.1.1 标签交换算法流程

标签交换算法的工作过程是：当一个LSR接收到一个分组的时候，判

断该分组是否是标签分组，如果不是标签分组就交给传统的路由控制功能器件来进行处理，如果是标签分组就从分组中提取该标签，并用此标签作为查找转发表的一个索引，然后对该转发表进行查找，一旦由此标签检索的表目被查找出来，路由器就利用此表目的输出标签替代分组中的标签，并通过此表目指定的输出接口将这个分组传送到此表目指定的下一跳。如果此表目指定了一个特定的输出队列，那么路由器就将此分组放置于此特定的队列中。流程图如图 2-4 所示：

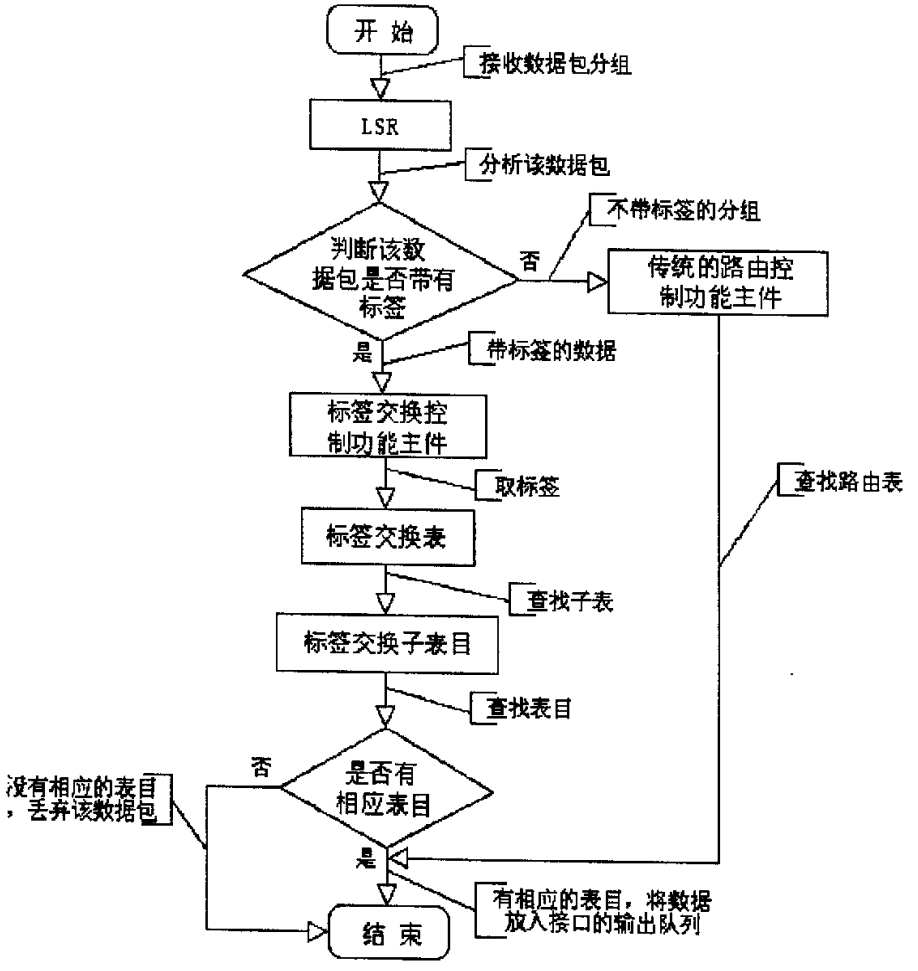

图 2-4 标签交换算法流程图

2.2.1.2 标签交换转发算法与传统路由算法的区别

标签交换算法是多协议标签交换技术（MPLS）得以实现的基础，也是它区别于传统的 IP 路由技术的最长匹配算法而成为一种高效的转发算法的一个重要方面。

传统的路由体系结构中，路由器的控制功能器件对不同的路由需要不同的转发算法，如：单播路由、组播和有服务类型的单播路由，都需要不同的路由算法。如表 2-1 所示：

表 2-1 传统的路由体系结构

寻址方式	单播数据分组	带 QoS 的单播数据分组	组播数据分组
转发算法	用目的地址来进行最长的匹配	用目的地址的最长匹配+服务类型上的精确匹配	用源地址的最长匹配+源地址和目的地址以及输入接口上的精确匹配

标签交换的的一个显著的特点是在标签交换路由器（LSR）中的转发功能器件不需要多种转发算法，仅仅使用一种转发算法就可以支持非常广泛的路由功能和支持非常丰富的路由服务。如表 2-2 所示：

表 2-2 标签交换的体系结构

寻径方式	单播数据分组	带 QoS 的数据分组	组播数据分组
转发算法	共同的转发算法（标签交换算法）		

2.2.2 标签交换转发表

标签交换转发表是由标签交换路由器（LSR）维护的一系列的表目组成，每个表目是由输入标签和多个子表目组成，而每个子表目有由一个输出标签、一个输出接口和下一跳地址组成（如表 2-3 所示），同时为了处

理多播分组，单个表目中不同子表目可能具有不同的输出标签，这样使到达一个输入接口的分组可以被转发到多个输出接口上。

表 2-3　转发表表目

输入标签	子表目		
	输出标签	输出标签接口	输出标签的下一跳地址

转发表根据输入标签来进行索引，通过索引找到相应的表目，然后对分组进行转发。标签交换转发表除了包含控制分组将转发到什么地方的信息外，还可以包含与分组可能使用的资源相关的信息。

一个 LSR 可以维护一个单一的转发表，在这种方式下对分组的处理由分组携带的标签来决定，同时也可以根据情况在每一个接口上维护一个转发表，在这种方式下对一个分组的处理不仅仅根据分组中携带的标签还要由分组到达的接口来共同决定。

2.2.3 转发粒度

转发粒度是 FEC（转发等价类）的一个重要特征。FEC 是指在 LSR（标签交换路由器）中以相同的方式来处理的分组的集合。FEC 可以提供的转发粒度是很丰富的，它可以用包括网络层目的地地址与一特定地址前缀相匹配的所有分组来提供粗糙的转发粒度，也可以用仅仅包括网络层源地址和目的地地址都相同且传输层端口也相同的分组来提供非常精细的转发粒度。

标签交换的转发功能主件对转发粒度没有任何限制，该转发粒度与一个特定的 FEC 相关联从而与一个标签相关联。可以与 FEC 相关联的进而与标签相关联的转发粒度以及与不同转发粒度相混合的能力都仅由标签交换的控制功能主件来决定。但合适的转发粒度对网络的影响很大的，粗糙的转发粒度有利于网络的扩展，但仅仅支持粗糙的转发粒度却使网络控制

变得不够灵活，因为它不能够区别不同类型的业务流，如：它不能对属于不同应用的业务流采用不同的转发和资源预留，所以要建立功能丰富的转发系统需要支持广泛的转发粒度。

2.3 标签交换的控制功能主件

标签交换控制功能主件（如表2-4所示）是LSR（标签交换路由器）的重要组成部分，它主要负责：（1）在LSR间分布路由信息 。（2）利用FEC与标签的绑定信息来构造转发功能主件中的转发表。

表2-4 标签交换的控制功能主件的组成

网络层路由协议	建立标签和FEC之间绑定的程序	发布标签绑定的程序
转发表的维护程序		

2.3.1 标签绑定

标签交换控制功能主件的一个重要的功能就是要建立标签交换转发表，由LSR维护的转发表的表目包含了一个输入标签以及一个或多个输出标签，在LSR的控制功能主件提供了两种类型的标签绑定：

- 本地绑定：标签绑定由本地的路由器选择的标签来实现与FEC的绑定。
- 远程绑定：标签绑定由该路由器接收来自与其他某个LSR分布的标签绑定信息，此信息与另外一个路由器建立的标签绑定是一致的。

本地绑定和远程绑定之间的一个重要区别是，本地绑定中与绑定有关的标签是本地LSR自己选择的，而远程绑定的标签是由其他LSR来选择的。

2.3.2 标签驱动

在 LSR 中要建立标签与 FEC 的绑定关系，必须要有一种方式来触发 LSR 建立或者撤消与 FEC 之间的绑定，通常有以下两种方式：

- 控制驱动标签绑定：标签绑定的建立或者撤消是由 LSR 的控制信息（路由信息）触发。
- 数据驱动标签绑定：标签绑定的建立或者撤消是由 LSR 必须转发的分组触发。

2.4 MPLS 网络结构

如图 2-5 所示，MPLS 网络的主要构成单元是：标签交换路由器 LSR（Label Switching Router)。由 LSR 构成的网络叫做 MPLS 域，位于区域边缘和其它用户网络相连的 LSR 称为边缘 LSR（也称 LER，Labeled Switching Edge Router ），位于区域内部的 LSR 则称为核心 LSR。核心 LSR 可以是支持 MPLS 的路由器，也可以是由 ATM 交换机等升级而成的 ATM-LSR。被标签的分组沿着由一系列 LSR 构成的标签交换路径 LSP(Label Switched Path) 传送。

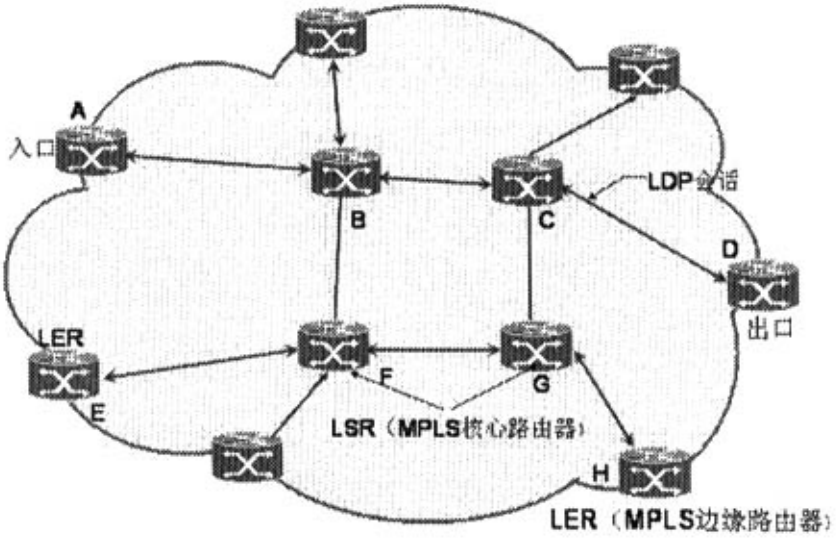

图 2-5　MPLS 网络结构

2.5　MPLS 与其他协议的关系

2.5.1　MPLS 与路由协议的关系

LDP 通过逐跳方式建立 LSP 时要利用沿途各 LSR 路由转发表中信息来确定下一跳，而路由转发表中的信息一般是通过 IGP、BGP 等路由协议收集的。但是 LDP 并不直接和各种路由协议有关联，只是间接使用路由信息。

另一方面，虽然 LDP 是专门用来实现标签分发的协议，但 LDP 并不是唯一的标签分发协议。对 BGP、RSVP 等已有协议进行扩展也可以支持 MPLS 标签的分发。MPLS 的一些应用也需要对某些路由协议进行扩展。例如，基于 MPLS 的 VPN 应用就需要对 BGP 协议进行扩展，以便 BGP 协议能传播 VPN 的路由信息；基于 MPLS 的流量工程（TE，Traffic Engineering）需

要对OSPF或IS-IS协议进行扩展，以便携带链路状态信息。

2.5.2 RSVP对MPLS的扩展

资源预留协议RSVP（Resource Reservation Protocol）经扩展后可以支持MPLS标签的分发，同时，在传送标签绑定消息时还能携带资源预留的信息。通过这种方法建立的LSP可以具有资源预留功能，即沿途的LSR可以为该LSP分配一定的资源，使在此LSP上传送的业务得到保证。

RSVP协议的扩展主要是在其Path消息和Resv消息中增加新的对象，这些新对象除了可以携带标签绑定信息外，还可以携带对沿途LSR寻径时的限制信息，从而支持LSP约束路由的功能。扩展的RSVP协议还支持快速重路由，即在一定条件下LSP需要改变时，可以在不中断用户业务的同时，将原来的业务流重新路由到新建立的LSP上。

2.6 MPLS环路处理

2.6.1 环路处理的必要性

MPLS使用基于分布式的传统IP路由协议。在网络拓扑结构发生变化的瞬间，由这些协议计算得到的路由可能会产生瞬间环路。分组进入有环路的LSP传送时，可能会导致两个问题：（1）分组无法转发到正确的目的地址。（2） 拥塞，即使采用了TTL值来丢弃产生环路的分组，但分组仍可能在环路中存活很长时间，并占用大量的网络资源，这对没有产生环路的数据包的正确传输产生了很大的影响，产生环路的数据包造成的拥塞可能导致非环路数据包延迟加长或丢弃，严重时还能导致网络瘫痪。

由于环路的发生会导致网络性能的下降，因此MPLS网络中应有相应的机制以防止环路的形成或是保证在出现环路的情况下，网络的性能不致下降很多。

2.6.2 环路处理方法

在MPLS网络中处理环路的方法有很多，通常可以分为两大类：（1）防止环路的形成。（2）允许环路的形成但将环路对网络的影响减到最小。在环路的处理方法上，一般要考虑使用该方法后环路可能发生的数量以及使用该方法对路由计算收敛的影响，减少环路的发生意味着路由计算的收敛时间更长，所以，网络采用的环路防止方法是路由收敛与环路发生概率的折中。

由于要保证网络的冗余性，在网络物理结构中就会存在产生逻辑环路的可能，IP网络通常的处理办法是基于对转发时对IP分组TTL域的递减操作、以及TTL为0后丢弃分组的办法来实现。IP网络所采用的动态路由协议也在一定程度上缩短了环路存在的时间。

我们通常使用的环路处置方法可以分为三类：

•**环路幸存**（Loop Survial）：这种方法通过诸如限制环路所能使用的网络资源的大小来最小化环路对网络服务性能的影响。

环路幸存是指即使在网络出现了短暂的环路的情况下，仍然能够正常运做的方法。环路幸存采用的基本方法是限制发生环路的的数据包消耗的网络资源，并最小化环路对其他非环路业务量的影响，如传统的TTL域的方法。

•**环路检测**：允许环路的产生，但在随后的检测中发现环路时就删除它们。

环路检测指在第二层允许建立环路，但随后环路就被检测出来。发现环路后，可以通过去掉标签与LSP的映射关系，而在第二层去除环路，然后再根据分组头在第三层转发。

•**环路防止**：避免在LSP建立的时候发生环路。

环路防止是利用一定的办法来保证在第二层不出现环路，通过给出口交换机分配和分发标签，出口交换机通知相邻交换机到特定目的地址应使用的标签。那个交换机又给它的相邻上游交换机通知另一个相关的标签，如此直至每个入口。与此同时，含有转发标签的控制消息里还包括到达出口所经历的路径上各个节点的标识，这样来避免环路的发生。

2.7 MPLS其它应用

2.7.1 基于MPLS的流量工程

流量工程是指在网络的物理拓扑结构上映射通信流量的过程，以及为这些通信流量的资源定位。

- **流量工程的作用**

网络拥塞是影响骨干网络性能的主要问题。拥塞的原因一般是网络资源不足，或者网络资源的负载不均衡，导致局部拥塞。流量工程用来解决由负载不均衡导致的拥塞。流量工程通过动态监控网络的流量和网络单元的负载，实时调整流量管理参数、路由参数和资源约束参数等，使网络运行状态迁移到理想状态，优化网络资源的使用，从而避免由于负载不均衡引起的拥塞

- **用MPLS来实现流量工程的优点**

现有的IGP协议都是拓扑驱动的，只考虑网络静态的连接情况，不能反映带宽和流量特性等动态状况，这正是导致网络负载不均衡的主要原因。而MPLS具有的一系列不同于IGP的特性，正是实现流量工程所需要的：MPLS支持异于路由协议路径的显式LSP路由；LSP较传统单个IP分组转发更便于管理和维护；基于约束路由的LDP可以实现流量工程的各种策略；基于MPLS的流量工程的系统开销较其它实现方式更低等等。

- **基于MPLS的流量工程的实现**

理想的流量工程解决方案是根据业务需要分配网络资源，它应该具有将通信流量映射到特殊路径和专用资源上以实现负载均衡的方法。一个具有流量工程的网络可以利用面向连接的技术来实现。将多种技术混合起来的网络，需要各自的网管系统来管理，操作上带来很大的不便。MPLS多协议标记交换融合了IP路由技术、ATM的QoS及第二层的交换技术，使得以上的流量工程模式可以部署在基于IP的网络，用MPLS实现流量工程允许为网络的数据流预先建立一条路径。这些预留的路径占用特殊的网络资源，既可被手工设定为显式路径，也可根据需要自动生成最佳的路径。

2.7.2 基于 MPLS 的 QoS

随着网络的不断发展，新业务的不断引入，用户迫切需要 ISP 将保证特定 QoS 的业务引入到目前没有明确划分业务类型的 IP 网络中。由于网络实际传输带宽有限，当特定链路传输的业务流量超过有效带宽时，即使具备相同的输入和输出节点的业务流，由于对 QoS 的要求不同，也无法使用相同的路径。解决该问题的理想方法是根据特定的 QoS 要求，网络逐一为每个业务流建立特定的传输路径。但是因为不同用户对于 QoS 的要求千差万别，而当前的 IP 网络又没有 QoS 的概念，如果要求网络中的路由器或交换机根据特定算法预先为每年不同服务等级的业务流预留带宽是不现实的。

所谓 QoS 路由是指根据特定业务流要求的 QoS，在网络中建立相应路径的方法。MPLS 技术通过使用约束路由机制，根据用户的特定要求仅在边缘节点处计算特定的标签交换路径，随后利用显式路由技术以及支持 QoS 的标签交换分配信令（如 CR-LDP）在网络内部构成此 LSP 的 LSR 之间传递相应的建路信息。

MPLS 的 QoS 路由机制与流量工程十分相似，二者都需要利用显式路由技术建立特定 LSP。其不同点是 QoS 路由机制对网络中业务流的区分粒度更为精细。

第三章 基于MPLS的VPN

3.1 VPN体系结构

3.1.1 VPN简介

VPN（Virtual Private Network）是虚拟专用网络的简称，它是利用现有的Internet网络提供专有网络的服务，随着Internet的迅猛发展也给VPN的发展提供了一个发展的网络平台，随着经济全球化的发展，许多企业都在努力在全球范围内开展业务，因此企业的办公地点在地理位置上也是相对分散的，VPN作为一种新的技术使企业利用Internet构建自己的专有网络已经成为一种必然的、首选的方式。

3.1.1.1 VPN特点

- VPN是利用Internet来构建企业所需要的专有网络，它是逻辑上的专有网络，通过对网络进行配置，来为用户提供专有网络相同的安全级别，但比传统的专有网络费用低很多。

VPN只为特定的企业或用户群体所专用。从VPN用户角度看来，

- 用VPN与传统专网没有区别。VPN作为私有专网，一方面与底层承载网络之间保持资源独立性，即在一般情况下，VPN资源不会被承载网络中的其它VPN或非该VPN用户的网络成员所使用；另一方面，VPN提供足够安全性，确保VPN内部信息不受外部的侵扰。
- VPN不是一种简单的高层业务。该业务建立专网用户之间的网络互联，包括建立VPN内部的网络拓扑、路由计算、成员的加入与退出等，因此VPN技术就比各种普通的点对点的应用机制要复杂得多。

3.1.1.2 VPN优势

- VPN为企业的分散机构、外出工作人员、商业合作伙伴与总部之间提供了可靠安全的连接，保证了他们之间数据传输的安全性，VPN的这一特

点对于实现电子商务或金融网络与通讯网络的融合将有特别重要的意义。

- VPN 利用 Internet 这种公共的网络平台来实现的，它就能以很低的价格实现 VPN 服务的接入，大大降低了企业信息成本，同时更加有效的使用了 Internet 资源为 ISP 带来了新的业务增长点。
- VPN 的配置也比以前的专有网络要简单得多，增加和删除用户也非常简单，不需要对硬件设备做很大的改动，只需要进行软件的配置即可，增加了 VPN 的灵活性。

支持驻外 VPN 用户在任何时间、任何地点的移动接入，这将满足不断增长的移动业务需求。

3.1.2 VPN 基本技术

隧道技术是在 Internet 实现 VPN 的核心技术，而隧道是靠隧道协议来实现的，VPN 的隧道可以建立在 OSI 模型的第二层（数据链路层）和第三层（网络层），那么就有相应的第二层隧道协议和第三层隧道协议，目前常用的隧道协议有：

3.1.2.1 第二层隧道协议

第二层隧道协议是将整个 PPP 帧封装在内部隧道中。现有的第二层隧道协议有：

- PPTP (Point-to-Point Tunneling Protocol)：点到点隧道协议，由微软、Ascend 和 3COM 等公司支持，在 Windows NT 4.0 以上版本中支持。该协议支持点到点 PPP 协议在 IP 网络上的隧道封装，PPTP 作为一个呼叫控制和管理协议，使用一种增强的 GRE (Generic Routing Encapsulation，通用路由封装）技术为传输的 PPP 报文提供流控和拥塞控制的封装服务。
- L2F (Layer 2 Forwarding) 协议：二层转发协议，由北方电信等公司支持。L2F 协议支持对更高级协议链路层的隧道封装，实现了拨号服务器和拨号协议连接在物理位置上的分离。
- L2TP (Layer 2 Tunneling Protocol)：二层隧道协议，由 IETF 起草，微软等公司参与，结合了上述两个协议的优点，为众多公司所接受，并且

已经成为标准RFC。L2TP既可用于实现拨号VPN业务，也可用于实现专线VPN业务。

3.1.2.2 第三层隧道协议

第三层隧道协议的起点与终点均在ISP内，PPP会话终止在NAS处，隧道内只携带第三层报文。现有的第三层隧道协议主要有：

- GRE（Generic Routing Encapsulation）协议：这是通用路由封装协议，用于实现任意一种网络层协议在另一种网络层协议上的封装。
- IPSec（IP Security）协议：IPSec协议不是一个单独的协议，它给出了IP网络上数据安全的一整套体系结构，包括AH（Authentication Header）、ESP（Encapsulating Security Payload）、IKE（Internet Key Exchange）等协议。

GRE和IPSec主要用于实现专线VPN业务。

3.1.3 VPN分类

VPN的分类方式有很多，按照不同的标准有不同分类方法，目前主要有以下几种分类方法：

3.1.3.1 按实现模型划分

覆盖VPN（Overlay-VPN）

在这种模型中，服务提供商给客户提供的仿真的租用线路，由于这种方式与传统的专线服务比较类似，所以这种模型也是最容易理解的，在这种模型中客户和服务提供商的职责是非常清晰的。

覆盖VPN特点

- 由服务提供商来为用户提供一条仿真的租用线路，这些仿真的线路我们成为VC，这种线路在逻辑上和专线是相同的。根据VC的建立方式分为PVC（永久虚电路）和SVC（交换虚电路），其中PVC是一直可用的，适合线路使用率较高的用户。SVC适合数据比较少且使用时间比较固定的用户
- 客户通过服务提供商提供的VC在客户前端设备（CPE）之间建立路由

器到路由器的通信。路由协议总是在客护设备之间交换，客户网络内部结构对服务提供商来说是透明的。

- **覆盖 VPN 实现方式**

覆盖 VPN 的实现可以在 ISO 模型的数据链路层或网络层来实现。在数据链路层可以用交换式的第二层技术，如：X.25、帧中继、ATM 或 SMDS 来实现覆盖 VPN 网络。但近年来也出现了在 IP 层上使用 IP-OVER-IP 隧道技术通过专用 IP 主干或公用的互联网来实现覆盖 VPN 网络，如：GRE（Generic Route Encapsulation）和 IPSec。

- **覆盖 VPN 缺点**

覆盖 VPN 属于静态的 VPN，这种模型非常适合包括的中央站点不多，而远程站点非常多的非冗余配置，但对连接性更为复杂的配置，这非常难于管理。

覆盖 VPN 的 QOS 保证通常是通过 VC 的带宽来保证的，但要正确的提供 VC 的容量必须要详细的了解站点间流量情况，而要获得站点间流量也是十分困难的，还必须手动的对网络中的设备进行配置，增加了网络技术人员的工作量，而且具有 N 平方问题：即如果某个客户的 VPN 中新增了一个结点，则需要完成如下工作（必须手工对所有的需要与该节点建立连接的节点设备进行配置，以建立新增加的这个节点和网络中其它节点的隧道连接）。由于 “静态” VPN 的静态性无法对网络的变化作出及时的反映。

使用第二层技术实现 VPN 模型时，将在新的服务提供商网络中引入另一层不必要的复杂性，因此会增加获得网络的成本以及运行成本。

对等 VPN(Peer-to-Peer VPN)

为了克服覆盖 VPN 的不足之处产生了对等 VPN，在对等 VPN 中用户设备（CE）和提供商设备（PE）之间交换路由信息，然后由提供商的网络将用户的私有路由传递到对端的 CE 设备，这种方式减少了用户配置的复杂程度。

对等VPN实现方式

- **共享路由器方式**

所有VPN用户的CE都连到同一台PE上，PE与不同的CE之间运行不同的路由协议（或者是相同路由协议的不同进程，比如OSPF）。
由路由始发PE将这些路由发布到公网上，在接收端的PE上将这些路由过滤后再发给相应的CE设备。

缺点：为了防止连接在同一台PE上的不同CE之间互通，必须在PE上配置大量的ACL。

- **专用路由器方式**

为每一个VPN单独准备一台PE路由器，PE和CE之间可以运行任意的路由协议，与其他VPN无关。PE与P之间运行BGP，并使用路由属性进行过滤。优点：无需配置任何的ACL了。缺点：每一个VPN用户都有新增一台专用的PE，代价过于昂贵了。

对等VPN缺点：

由于没有采用隧道技术，私网路由信息就暴露在公网上，安全不能得到保证。

传统的VPN的安全特性完全靠路由控制来保证，导致在CE设备上无法配置缺省路由，同时还不能解决不同VPN共享相同的地址空间的问题。

3.1.3.2 按业务用途划分

- **企业内部虚拟专网**（Intranet VPN）

企业内部VPN（Intranet VPN）通过公用网络进行企业内部各个分布点互联，是传统的专线网或其它企业网的扩展或替代形式。

- **扩展的企业内部虚拟专网**（Extranet VPN）

扩展的企业内部（Extranet VPN）是指利用VPN将企业网延伸至供应

商、合作伙伴与客户处，使不同企业间通过公网来构筑VPN。

- **远程访问虚拟专网**（ Access VPN ）

远程访问VPN（ Access VPN ）向出差流动员工、远程办公人员和远程小办公室提供了通过公用网络与企业的Intranet和Extranet建立私有的网络连接。远程访问 VPN 的结构有两种类型，一种是用户发起（Client-initiated）的 VPN 连接，另一种是接入服务器发起（NAS-initiated）的VPN连接。

3.1.3.3 按拓扑结构来划分

企业或者提供商构建VPN的时候，会根据企业不同的需求和和自身的信息点的分布情况来选择不同的VPN拓扑结构，目前主要的拓扑结构有以下几种：

- **星型拓扑结构**

这种拓扑结构由于在搭建网络的时候比较容易，成本也比较低，所以是用得比较多的一种VPN实现方式。在这种拓扑方式中，各个分支站点都与中心站点交换数据，对那些采用集中数据管理的用户来说这种结构是非常有效的。由于星型结构在冗余性方面的先天不足所以必须采用必要的冗余措施，通常采用双中心节点的方式。中心节点互为备份通过高速链路连接起来，降低了中心节点障碍对全网的影响。

虽然星型拓扑结构在构建VPN的时候是用的最为普遍的，但由于其在结构上的特点，也使这种结构有它的一些缺陷：

- 这种结构只适合具有严格层次结构的企业，如：银行、政府部门、连锁企业等。
- 不适合各分支节点有大量数据交互的企业，因为这样会增加中心节点的负担，在数据量很大的时候甚至回造成中心节点崩溃。

- **网状拓扑结构**

由于星型拓扑结构在应用上的一些局限性，所以有必要引入新的VPN拓扑结构—网状拓扑结构。引入网状拓扑结构的原因：

- 企业的组织结构的层次性不是很强，需要在各个用户站点之间交换数据。
- 各个用户之间的一些应用程序需要对等的通信（如：OA、ERP）。
- 对于一些跨国公司，由于国际链路非常昂贵，采用星型拓扑结构的成本可能很高。

网状拓扑结构又可以分为：部分网状拓扑结构和全网状拓扑结构。全网状结构的所有用户站点都有直接的连接，这种结构的冗余性是最好的，但网络成本很高。部分网状结构中只有部分站点之间有直接的连接，冗余性没有全网状拓扑结构高，但组网成本要低于全网状结构。

- **混合拓扑结构**

在这种结构中既有星型拓扑结构也有网状拓扑结构，这种拓扑结构适合各个用户站点之间有大量的数据流量，同时和中心站点之间也有大量的数据交互。混合拓扑结构具有星型拓扑和网状拓扑的优点，同时有克服了它们的一些缺点，给用户构建VPN提供了更加有效和灵活的方式。混合拓扑结构的优点：

- 在混合拓扑结构中采用了模块化的思想，将网络分为：核心网络、接入网络、分发网络，使网络层次更加清晰，便于设计和维护。
- 可以将核心网络和接入网络隔离开，通过分发网络连接起来，这样有助于将用户故障本地化，减少用户故障对核心网络的影响。

3.2 MPLS/VPN体系结构

基于MPLS的VPN就是通过LSP将私有网络在地域上的不同分支联结起来，形成一个统一的网络。

3.2.1 MPLS/VPN网络结构

图3-1给出了基于MPLS的VPN的基本结构。CE是用户边缘设备，可以是路由器，也可以是交换机，甚至是一台主机；PE是服务商边缘路由器，位于骨干网络；PE负责对VPN用户进行管理、建立各PE间LSP

连接、在同一 VPN 用户各分支间进行路由分派。

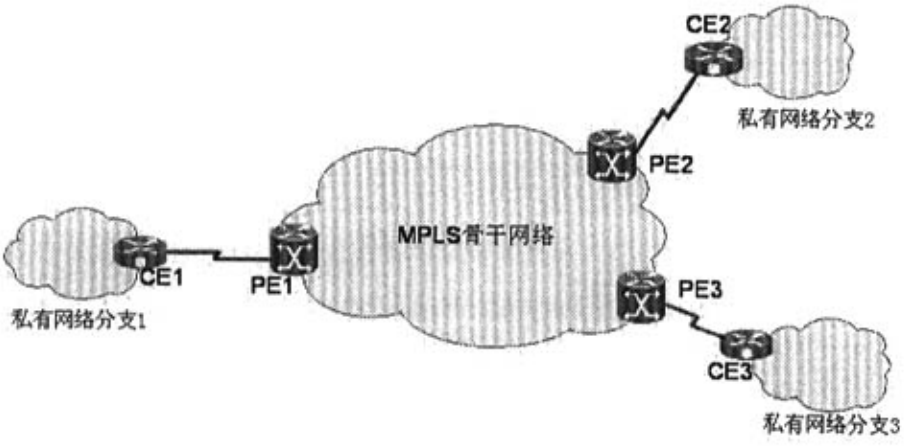

图 3-1 MPLS/VPN 的网络结构

3.2.2 MPLS/VPN 实现过程

和其它的 VPN 一样，用 MPLS 来实现的 VPN 也必须采用隧道技术来保证 VPN 的安全性和与其它业务的隔离。

3.2.2.1 MPLS/VPN 隧道建立

在前面我们论述了传统的 VPN 一般是通过 GRE、L2TP、PPTP 等隧道协议来建立隧道，从而实现私有网络间数据流在公网上的传送，不管是建立第二层的 VPN 还是建立第三层的 VPN 都需要额外的隧道协议来实现，

但用 MPLS 来实现 VPN 不需要额外的使用这些隧道协议，因为通过 LDP 协议建立起来的 LSP 本身就是公网上的隧道，用 MPLS 来实现 VPN 有天然的优势。

在基于 MPLS 的 VPN 中隧道的建立过程就是 LSP 建立的过程，PE 对进入的数据包打上标签，VPN 转发表中包括与 VPNIP 地址相对应的标签。通过这个标签将数据传送到相应地点。这就保证了数据包按照建立的 LSP 进行转发，LSP 就好像是建立的一个隧道一样，保证了标签数据与其它数据的隔离从而保证了数据的安全，而且这种隧道是动态建立的，它是在最优路由的前提下建立起来的，比传统的 VPN 实现方式采用的静态隧道方式更灵活，当网络出现故障的时候能动态的建立新的隧道，从而保证了 VPN 网络的可靠性既然标签代替了 IP 地址，用户可以保持他们的专用地址结构，无需进行网络地址翻译（NAT）来传送数据。因为数据是通过使用 LSPs 来转发的，LSP 定义一条特定的路径，再路由收敛的情况下不可以被改变，这样对安全性也有保证。这种基于标签的模式可与帧中继和 ATM 一样提供保密性。服务提供商，而不是用户，应用 VPN 时将一个特定的 VPN 与接口联系起来，数据包的转发是由用于入口的标签决定的。

3.2.2.2 MP-BGP 协议

PE 间的路由分派通常是用 LDP 或扩展的 BGP 协议实现的。基于 MPLS 的 VPN 支持不同分支间 IP 地址复用和不同 VPN 间互通，为了保证在基于 MPLS 的 VPN 中，不同 VPN 使用相同的 IP 地址时发生路由混乱，服务提供商为每个 VPN 分配了一个标识符，称作路由标识符（RD），这个标识符在服务提供商的网络中是独一无二的。转发表中包括一个独一无二的地址，叫作 VPNIP 地址，是由 RD 和用户的 IP 地址连接形成。VPN-IP 地址在网络中是独一无二的，地址表存储在转发表中和传统的路由相比，VPN 路由中需要增加分支和 VPN 的标识信息，这就需要对 BGP 协议进行扩展才能携带 VPN 的路由信息。BGP 是一个路由信息分布协议，它利用多协议扩展和共有属性来定义 VPN 的连接性。在基于 MPLS 的 VPN 中，BGP 只对同一个 VPN 的成员发布信息，通过流量分离来提供基本的安全性。

第四章 基于MPLS的VPN网络设计与实现

本章首先分析了成都电信现有的基于ATM的VPN网络的一些不足之处，然后根据前面论述的MPLS/VPN的工作过程，设计了基于MPLS的VPN网络模型，并为后面搭建实验网络平台和对MPLS/VPN网络的性能进行测试，以及为以后的在具体的应用环境中实现基于MPLS的VPN网络做准备。

4.1 需求分析及设计目标

需求分析：

成都电信的业务支撑网络是基于IBM的ATM技术构建的，因此其VPN网络也是构建在该技术上的，这种VPN采用的传统的基于封装（隧道）技术以及加密模块技术，可在两个位置间安全地传输数据。由于它属于覆盖VPN的一种，在每个VPN站点之间必须建立一个隧道，这就导致了网络的低效，最大的缺点是可扩充性差。随着VPN网络中接入站点的增加，需要支持的隧道的数量随着站点的数目呈几何级数增加对于VPN的维护人员来说，配置将成为问题，技术人员必须配置好每个隧道，配置单一的一个隧道不成问题，但网络结点数量增大时，工作量就非常大。另外一个缺点就是这种VPN对设备的兼容性很差，需要确保所有的CPE（客户前端设备）之间能够兼容。但在每个位置使用同一种CPE设备并不总是可行的，ATM就是由于其技术过于复杂与其它技术的兼容性差，才逐渐被IP技术所取代逐渐的淡出主流技术市场的， 随着成都电信的发展原有的VPN实现技术已经远远不能满足业务对该技术的要求，必须寻求一种新的基于IP技术的VPN网络。

设计目标：

- 与主流的IP技术兼容性好
- 安全性高
- 扩展性强

- 高可靠性
- 容易维护和实现

4.2 基于 MPLS 的 VPN 网络设计

4.2.1 IGP 规划

在设计 MPLS/VPN 网络的时候我们首先对 IGP 协议进行规划，因为 IGP 协议在 MPLS/VPN 网络中起着连通骨干、选径和自动迂回的作用。IGP 通过计算每条路径的权值来寻找最佳路径。IGP 并不承载外界路由，但所有外界路由在 BGP4 中都有“下一跳”(next-hop) 这个属性，IGP 通过对 next-hop 的选径来控制到外界的数据流。在 MPLS/VPN 网络中可以使用的 IGP 协议有很多种，如：RIP、OSPF、IS-IS 等，但考虑到设计的 MPLS/VPN 模型要具有普适性，OSPF 协议在 ISP 的网络中被普遍使用，所以我们在设计该模型的时候决定采用 OSPF 协议做为整个网络的 IGP 协议。由于 OSPF 协议需要层次性的网络设计，所以需要对该网络进行层次化的设计，具体的设计如下：

- 两级层次设计

其中骨干节点与分支节点路由器形成 OSPF 的 Area 0（即 Backbone）；每一个分支包括的所有路由器构成第二个层次的 OSPF 域；分支节点的路由器做为 ABR，交换 Area 0 和其它子域的 LSAs（Link-State Advertisements）。网络拓扑和 OSPF 协议必须是连续的；一个 Area 的网络节点数不超过 100 个。

由于 OSPF 骨干域是整个网络路由的核心，必须维持骨干区域的稳定性和冗余性。设计中应该尽量减少骨干区域路由器的个数，如骨干区域只包括 20 多个 Area 0 骨干域路由器。骨干域中路由器的连接应采用稳定线路冗余联接，避免骨干区域的路由震荡和分离。建议不要在骨干区域连接服务器，工作站等共享资源，从而避免对骨干区域的影响。

4.2.2 MP-IBGP 规划

PE 路由器通过 IGP 路由协议（我们采用的 OSPF）从 CE 路由器那里学到了与之相连的客户 VPN 路由，在我们的模型中都认为企业的所有的路由器在同一个 AS 内，所以所有的 BGP 会话都是内部的 BGP 会话。MPLS/VPN 优于其他 VPN 实现模型的一个特点就是它有很强的扩展性，体现在具体上就是增加、删除一个 VPN 用户是很容易的，甚至允许不同的 VPN 客户有相同的 IP 地址，既可以节约宝贵的 IP 地址也方便 VPN 客户的维护。所以在 BGP 更新消息中要包括 VPN-IPV4 地址、MPLS 标签信息、扩展 BGP 共同体、还可能包含标准的 BGP 共同体。未了使 BGP 能携带除 IPV4 地址以外的其他信息，需要对 BGP 协议进行扩展，在两个对等体建立 BGP 会话的时候，使用 OPEN Message 来交换 Initial BGP 参数。OPEN 消息可以包含可选参数，其中的 Capability 就表明该对等体能理解和支持哪些功能，其中的多协议扩展参数就使得 BGP 能够携带除标准 IPV4 地址以外的其他地址。所以为了在基于 MPLS 的 VPN 网中全面实现 MPLS/VPN 功能，在全网中各 PE 节点之间要运行 MP-IBGP,。由于这些 PE 节点均处在同一个 AS 之中，它们之间实际上是运行 MP-IBGP 协议。

在 MPLS/VPN 的骨干网络中只要求 PE 设备上要运行 BGP 协议，利用 BGP 能实现跨路由器建立 TCP 连接，从而保证 PE 之间能交换 VPN 的路由信息，实现 VPN 的内部互通。

4.2.3 路由反射设计

由于在 MPLS/VPN 网络中必须运行 BGP 协议，而 BGP 的 Split-Horizon 规则，要求运行 IBGP 的路由器必须进行 Fully Meshed 连接。随着 VPN 网络的用户会越来越多，网络中运行 IBGP 协议的路由器（所有 PE）会越来越多，BGP 会话也会越来越多，考虑到以后的可扩展性，采用 Fully Meshed 的方式是不可行的，举例来说，如果运行 IBGP 有 n 个路由器，则必须维护的 IBGP Sessions 将会有：

$$n\times (n-1) /2$$

如此巨大的会话数，对于 ISP 来说是不可想象的，因此，必须采用 BGP

Route Reflector（RR）技术。

路由反射器的详细设计如图4-1所示：

- 两层结构

采用两层结构的层次化设计，不仅可以极大地提高扩展性，还能够进一步降低IBGP的会话数目，减轻路由器处理会话的负担。具体说来，第一级将地市中心两台路由器做为RR，所有县级节点做为它们的路由反射器客户端；第二级由省级骨干网中的RR形成Fully Meshed连接。

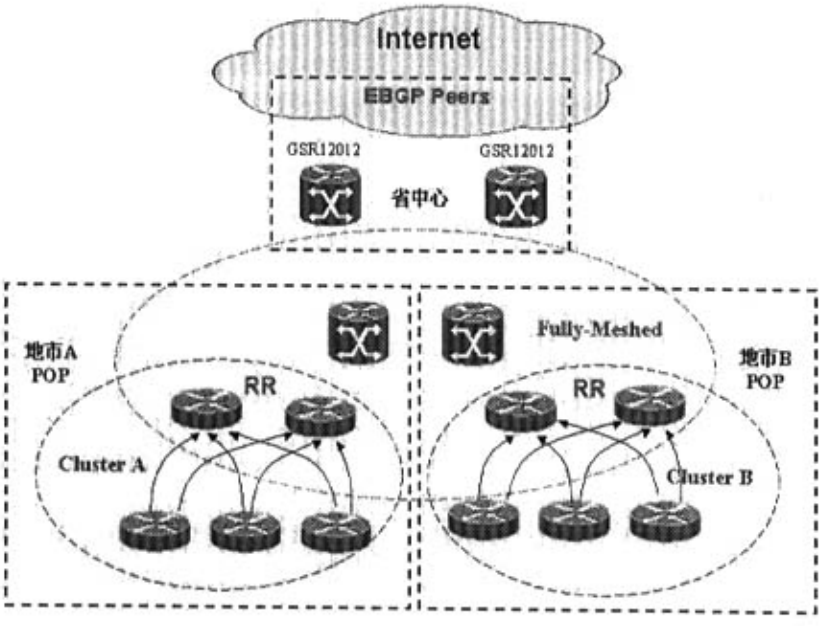

图4-1 路由反射器设计

冗余备份

为避免因路由反射器发生故障而导致IBGP的Full-Mesh产生Partition-Meshed，从而使BGP产生不正确的信息，我们在每一级都设置2台路由反射器，与该级别的路由反射器客户形成一个Cluster；同时，这2台路由反射器通过IGP形成Fully Meshed。

当一个Cluster有2个或者以上的路由反射器时，必须设置Cluster ID保证同 一Cluster内的路由反射器可以相互识别。Cluster ID是32bit的值。当每收到 一条路由信息后，BGP会检查该路由的cluster_list。cluster_list是BGP的路由属性（Attribute），cluster_list指该路由每经过一个cluster，该路由的cluster_list就会增加这个cluster的Cluster ID。如果该路由的cluster_list中已含有所在Cluster的Cluster ID，则丢弃该路由。反之，则进行反射，并把自己的Cluster ID增加在该路由cluster_list中。

4.3 基于MPLS的VPN网络实现

在对MPLS/VPN网络模型进行设计完成后，必须将这些设计思想通过对网络设备（路由器）的配置来实现。

4.3.1 配置VRF

VRF是指VPN路由转发实例（VPN Routing & Forwarding Instance）每一个VRF可以看作虚拟的路由器，好像是一台专用的PE设备。该虚拟路由器包括如下元素：

- 一张独立的路由表，当然也包括了独立的地址空间。
- 一组归属于这个VRF的接口的集合。
- 一组只用于本VRF的路由协议。

对于每个PE，可以维护一个或多个VRF，同时维护一个公网的路由表（也叫全局路由表），多个VRF实例相互分离独立。

在MPLS VPN网络中每一个VPN客户需要配置一个VRF。可以使用命令ip vrf vrfname来配置如：

```
router (config) ip vrf vrfname
```

4.3.2 配置路由区分符与导入导出策略

在MPLS VPN网络中，每个VRF都只包含属于自己的VPN的路由信息，

由于在MPLS VPN网络中不同的VPN可以使用相同的IP地址，那么就会产生属于不同VPN的相同的路由信息，为了不使路由信息产生混乱，在VRF中为不同的VPN设置一个路由区分符RD。RD通常有两中结构：1. ASN：nn 2.IP-地址：nn。RD的配置通常使用如下命令来实现：

router (config) ip vrf vrfname

router (config-vrf) rd ASN：nn 或者

router (config-vrf) rd IP-地址：nn

配置VRF的最后一步是添加每个VRF使用的导入导出策略。这些策略用于将路由添加到 VRF 中以及通告来自该 VRF 的路由。在 VRF 中使用route-target命令来控制这些策略，在route-target命令中使用import和export来分别指定每个VRF的导入和导出策略。具体命令如下：

router (config) ip vrf vrfname

router (config-vrf) rd ASN：nn

router (config-vrf) route-target import ASN：nn

router (config-vrf) route-target export ASN：nn

4.3.3 PE到CE链路配置

为了使CE设备能与PE设备交换路由信息，可以在采用如下两种方式：

- 采用静态路由协议：在CE和PE设备上配置静态路由，静态路由方式的优点是简单，不消耗路由器和链路资源，缺点是维护和管理不便，不适应VPN站点、路由的动态变化，不能适应CE站点内较复杂的IP地址划分；
- 采用动态路由（RIP V2、OSPF、EBGP等）协议：通过PE和CE上的动态路由协议配置，能够适应VPN站点、路由的动态变化，维护量小，缺点是消耗了路由器和链路的资源。

下面分别介绍两种方式：

静态路由协议

在CE设备上配置静态路由或缺省路由：

router(config)#ip route x.x.x.x x.x.x.x s0/0

x.x.x.x—其他CE站点子网

router (config)#ip route 0.0.0.0 0.0.0.0 s0/0

在PE设备上配置：

配置VPN静态路由

router(config)#ip route vrf vrfname x.x.x.x x.x.x.x s0—该PE设备直接连接的CE站点子网

将静态路由通过MP-IBGP分发到其他VPN站点

router (config)#router bgp xxxx

router (config-router)#address-family ipv4 vrf MYbilling

router (config-router-af)#redistribute static

动态路由（RIP V2、OSPF、EBGP等）协议，以OSPF为例

在CE设备上配置：

router(config)#router ospf 1

router(config-router)#network x.x.x.x x.x.x.x area 0.0.0.0

在PE设备上配置：

router (config)#router ospf 100 vrf vrfname

router (config-router)#network x.x.x.x x.x.x.x area 0.0.0.0

router (config-router)#network x.x.x.x x.x.x.x area 0.0.0.0

router (config)#router bgp xxxx

router (config-router)#address-family ipv4 vrf vrfname

router (config-router-af)#redistribute ospf 101 match internal external 1 external 2

4.3.4 接口与VRF关联性

在PE路由器上定义相关的VRF后，必须将路由器上的端口与特定的VRF相关联，可以有多个接口属于同一个VRF。通常使用接口模式命令来完成接口与VRF的关联，同时在VRF中，既可以定义主接口，也可以定义子接口。其接口定义如下：

router(config) interface serial 0

router(config-interface) ip vrf vrfname

```
router(config-interface)ip address x.x.x.x x.x.x.x
!
```

4.3.5 配置IGP

IGP在MPLS/VPN网络中保证了主干的连通性，这样才能保证BGP协议能运行起来，下面以OSPF为例来说明：

```
router(config)router ospf 1
router(config-router)network x.x.x.x x.x.x.x
```

4.3.6 配置多协议BGP

在MPLS/VPN网络中配置的BGP协议与在普通的IP网络中配置BGP是不相同的，在MPLS/VPN网络中BGP协议除了要携带IPV4地址以外还要能携带VPN-IPV4地址，所以在PE之间的BGP会话中一些会话携带VPN-IPV4地址，一些只携带IPV4路由，另一些携带VPN-IPV4和IPV4路由，对于注入BGP或者从BGP中导出的路由以及从VRF导入导出的路由，通过在BGP配置中使用地址家族进行控制，对于属于全局路由表的路由，则通过常规的BGP配置流程进行控制。

通常使用如下命令来实现：

```
(config)#router bgp ASN
(config-router)#no bgp default ipv4-unicast
(config-router)#neighbor xx.xx.xx.xx remote-as ASN
(config-router)#address-family ipv4 vrfname
…
!
exit-address-family 或者
(config-router)#address-family ipv4 vrfname
!exit-address-family
```

第五章 MPLS/VPN网络性能分析

本章主要是通过组建实验网络，从中获得的实验数据验证并分析MPLS/VPN在安全性、扩展性、拓扑灵活性、可靠性、COS/QOS、网络维护管理等方面优于传统的VPN实现技术。

5.1 MPLS/VPN实验网络组建及测试

为了进一步的验证和分析 MPLS/VPN 的安全性、扩展性、可靠性、COS/QOS、和网络易维护管理性，根据前面的MPLS/VPN设计模型，我们搭建一个实验网络，对它的一些主要的性能进行测试。

实验目的

通过实验数据进一步论证基于MPLS的VPN网络在安全性、可扩展性、以及可维护管理性等方面的优点,为以后的具体网络建设做准备。

实验项目

- 搭建实验网络平台，对不同VPN的IP地址进行规划。
- 对P、PE以及CE设备进行配置。
- 查看配置，测试相同以及不同VPN之间的安全性。

5.1.1 实验网络的设计与实现

在实验网络中我们使用3台Quidway的AR28-40路由器来充当VPN网络的PE路由器，用一台Quidway的AR28-40充当P路由器，用3台Cisco的3620来充当VPN网络的CE路由器，在PE和CE之间设置Loopback地址，专门用于VPN应用，以使VPN应用和其它应用区分开来，通过配置PE路由器，使其只对由Loopback转发的数据包Tag，对其他数据报按普通的数据包路由处理，以便对VPN进行维护和管理。

如图5-1所示，整个网络由一台一台Quidway的AR28-40路由器来担任骨干网的P路由器，由3台Quidway的AR28-40路由器来担任PE路由

器，整个MPLS骨干域有两VPN：OA和JF(计费)，这两个VPN在不同的地方设有接入点，其中计费在新都、龙泉以及温江设有接入点，OA在新都和温江设有接入点。这两个VPN在不同的接入点都只有一条CE到PE的链路，MPLS骨干域为这两个VPN提供自己VPN内任何站点之间的非冗余的企业内部网VPN服务。

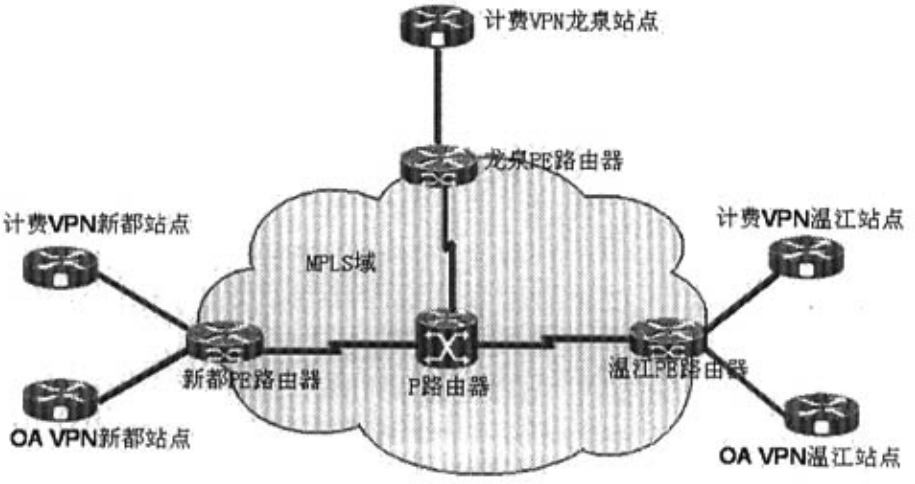

图 5-1 MPLS VPN的实验拓扑

在这个实验环境中IGP采用了OSPF路由协议，EGP采用的是M-BGP协议。其中OSPF是用于保证PE路由器之间能互通，为了减少路由的再发布，我们在PE与CE路由器之间也采用BGP。EBGP使PE路由器从CE获取不同的客户的路由，IBGP用于不同PE之间传递路由信息。

由于基于MPLS的VPN支持地址重叠，所以在OA和计费VPN的不同站点之间的IP地址分配可以非常灵活，允许使用相同的IP地址，在实验中我们在该实验网络的PE、P、以及CE路由器IP地址分配如6-2表所示。

表 5-1 实验网络 IP 地址分配

	CE 站　点	子　网
计费 VPN	新　都	168.1.1.2/24
	龙　泉	168.2.1.2/24
	温　江	168.3.1.2/24
OA VPN	新　都	10. 2. 1. 2/24
	温　江	10. 2. 2. 2/24
主　干	新　都（环路 0）	202.100.1.1/32
	龙　泉（环路 0）	202.100.1.2/32
	温　江（环路 0）	202.100.1.3/32

路由器配置

为了构建基于 MPLS 的 VPN 网络必须对网络设备进行有效的配置，包括构建 MPLS 骨干的 PE 设备和 P 设备，以及对用户的接入设备（CE）的配置。

(1) 配置新都 PE-XD

在 PE-XD 上创建 VPN-JF 的 VPN-instance，并配置相关属性以控制 VPN 路由信息的发布。

```
[PE-XD] ip vpn-instance vpn-JF
[PE-XD-vpn-vpn-jf] route-distinguisher 100:1
[PE-XD-vpn- vpn-jf] vpn-target 100:1 export-extcommunity
[PE-XD-vpn- vpn-jf]vpn-target 100:1 import-extcommunity
```

```
[PE-XD-vpn- vpn-jf] quit
[PE-XD] ip vpn-instance vpn-OA
[PE-XD-vpn-vpn-jf] route-distinguisher 100:2
[PE-XD-vpn- vpn-jf] vpn-target 100:2 export-extcommunity
[PE-XD-vpn- vpn-jf]vpn-target 100:2 import-extcommunity
[PE-XD-vpn- vpn-jf] quit
```

PE-XD 分别与 CE-JF 和 CE-OA 间建立 EBGP 邻居，并将学到的 CE-JF 和 CE-OA 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族。

```
[PE-XD] bgp 100
[PE-XD-bgp] ipv4-family vpn-instance vpn-JF
[PE-XD-bgp-af-vpn-instance] group 168 external
[PE-XD-bgp-af-vpn-instance] peer 168.1.1.1 group 168 as-number
65410
[PE-XD-bgp-af-vpn-instance] import-route direct
[PE-XD-bgp-af-vpn-instance] quit
[PE-XD-bgp] ipv4-family vpn-instance vpn-OA
[PE-XD-bgp-af-vpn-instance] group 10 external
[PE-XD-bgp-af-vpn-instance] peer 10.2.1.1 group 10 as-number 65410
[PE-XD-bgp-af-vpn-instance] import-route direct
[PE-XD-bgp-af-vpn-instance] quit
[PE-XD-bgp] quit
```

#将 PE-XD 上的 ethernet 1/1 绑定到 VPN-JF

```
[PE-XD] interface ethernet 1/1
[PE-XD- ethernet 1/1] ip binding vpn-instance vpn-JF
[PE-XD- ethernet 1/1] ip address 168.1.1.2 255.255.0.0
[PE-XD- ethernet 1/1] quit
```

#将 PE-XD 上的 ethernet 1/2 绑定到 VPN-OA

```
[PE-XD] interface ethernet 1/2
[PE-XD- ethernet 1/2] ip binding vpn-instance vpn-OA
[PE-XD- ethernet 1/2] ip address 10.2.1.2 255.255.0.0
```

[PE-XD- ethernet 1/2] quit

配置LoopBack接口（对PE路由器，配置LoopBack接口地址时，必须使用32位掩码的主机地址，以防止此路由被聚合，导致LSP不能正确处理内层标签）。

[PE-XD] interface loopback0

[PE-XD-LoopBack 0] ip address 202.100.1.1 255.255.255.255

[PE-XD-LoopBack 0] quit

配置MPLS基本能力，并在PE1与P路由器相连的接口上使能MPLS及LDP。建立LSP和实现MPLS报文转发。

[PE-XD] mpls lsr-id 202.100.1.1

[PE-XD] mpls

[PE-XD] mpls ldp

[PE-XD] interface ethernet1/0

[PE-XD- ethernet1/0] ip address 172.1.1.1 255.255.0.0

[PE-XD- ethernet1/0] mpls

[PE-XD- ethernet1/0] mpls ldp enable

[PE-XD- ethernet1/0] quit

在PE-CD与P路由器相连的接口及loopback接口上启用OSPF，并引入直连路由。实现PE内部的互通。

[PE-XD] ospf

[PE-XD-ospf-1] area 0

[PE-XD-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255

[PE-XD-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0

[PE-XD-ospf-1-area-0.0.0.0] quit

[PE-XD-ospf-1] import-route direct

[PE-XD-ospf-1] quit

在PE与PE之间建立MP-IBGP邻居，进行PE内部的VPN路由信息交换。并在VPNv4地址族视图下激活MP-IBGP对等体。

[PE-XD] bgp 100

[PE-XD-bgp] group 202 internal

```
[PE-XD-bgp] peer 202.100.1.2 group 202
[PE1-bgp] peer 202.100.1.2 connect-interface loopback0
[PE-XD-bgp] peer 202.100.1.3 group 202
[PE-XD-bgp] peer 202.100.1.3 connect-interface loopback0
[PE-XD-bgp] ipv4-family vpnv4
[PE-XD-bgp-af-vpn] peer 202 enable
[PE-XD-bgp-af-vpn] peer 202.100.1.2 group 202
[PE-XD-bgp-af-vpn] peer 202 enable
[PE-XD-bgp-af-vpn] peer 202.100.1.3 group 202
[PE-XD-bgp-af-vpn] quit
[PE-XD-bgp] quit
```

(2) 配置P

配置P路由器的MPLS基本能力，并在P与PE相连的各接口上使能LDP，以转发MPLS报文。

```
[P] mpls lsr-id 172.1.1.3
[P] mpls
[P] mpls ldp
[P] interface ethernet1/1
[P-Serial1/0/0] ip address 172.1.1.2 255.255.0.0
[P-Serial1/0/0] mpls
[P-Serial1/0/0] mpls ldp enable
[P-Serial1/0/0] interface ethernet 1/0
[P-Serial2/0/0] ip address 172.2.1.2 255.255.0.0
[P-Serial2/0/0] mpls
[P-Serial2/0/0] mpls ldp enable
[P-Serial1/0/0] interface ethernet 1/2
[P-Serial2/0/0] ip address 172.3.1.2 255.255.0.0
[P-Serial2/0/0] mpls
[P-Serial2/0/0] mpls ldp enable
```

在P与PE相连的各接口上启动OSPF协议，并引入直连路由，实现PE

内部的互通。

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.255.255
[P-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.255.255
[P-ospf-1-area-0.0.0.0] network 172.3.1.0 0.0.255.255
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] import-route direct
```

(3) 配置PE-WJ

其它PE的配置过程与PE-CD相似，不相同的是其它PE上对于VPN路由属性的设置。

在PE-WJ上创建VPN-JF的VPN-instance，并配置相关属性以控制VPN路由信息的发布。

```
[PE-WJ] ip vpn-instance vpn-JF
[PE-WJ-vpn-vpn-jf] route-distinguisher 100:1
[PE-WJ-vpn- vpn-jf] vpn-target 100:1 export-extcommunity
[PE-WJ-vpn- vpn-jf] vpn-target 100:1 import-extcommunity
[PE-WJ-vpn- vpn-jf] quit
[PE-WJ] ip vpn-instance vpn-OA
[PE-WJ-vpn-vpn-OA] route-distinguisher 100:2
[PE-WJ-vpn- vpn-OA] vpn-target 100:2 export-extcommunity
[PE-WJ-vpn- vpn-OA]vpn-target 100:2 import-extcommunity
[PE-WJ-vpn- vpn-OA] quit
```

#PE-WJ分别与CE-JF和CE-OA间建立EBGP邻居，并将学到的CE内部VPN路由引入MBGP的VPN-instance地址族。

```
[PE-WJ] bgp 100
[PE-WJ-bgp] ipv4-family vpn-instance vpn-JF
[PE-WJ-bgp-af-vpn-instance] group 168 external
[PE-WJ-bgp-af-vpn-instance] peer 168.1.1.1 group 168 as-number
65430
```

```
[PE-WJ-bgp-af-vpn-instance] import-route direct
[PE-WJ-bgp-af-vpn-instance] quit
[PE-WJ-bgp] quit
[PE-WJ-bgp] ipv4-family vpn-instance vpn-OA
[PE-WJ-bgp-af-vpn-instance] group 10 external
[PE-WJ-bgp-af-vpn-instance] peer 10.2.1.1 group 10 as-number 65430
[PE-WJ-bgp-af-vpn-instance] import-route direct
[PE-WJ-bgp-af-vpn-instance] quit
[PE-WJ-bgp] quit
```

将PE-WJ与CE-JF相连的接口Ethernet1/0绑定到VPN-JF。

```
[PE-WJ] interface ethernet 1/0
[PE-WJ-Ethernet1/0] ip binding vpn-instance vpn-JF
[PE-WJ-Ethernet1/0] ip address 168.3.1.2 255.255.0.0
[PE-WJ-Ethernet1/0] quit
```

配置LoopBack接口。

```
[PE-WJ] interface loopback0
[PE-WJ-LoopBack 0] ip address 202.100.1.3 255.255.255.255
[PE-WJ-LoopBack 0] quit
```

配置MPLS基本能力，并在PE-WJ与P路由器相连的接口上使能MPLS及LDP。建立LSP和实现MPLS报文转发。

```
[PE-WJ] mpls lsr-id 202.100.1.3
[PE-WJ] mpls
[PE-WJ] mpls ldp
[PE-WJ] interface Ethernet1/1
[PE-WJ- Ethernet1/1] ip address 172.3.1.1 255.255.0.0
[PE-WJ- Ethernet1/1] mpls
[PE-WJ- Ethernet1/1] mpls ldp enable
[PE-WJ- Ethernet1/1] quit
```

在PE-WJ与P路由器相连的接口及loopback接口上启用OSPF，并引入直连路由。

```
[PE-WJ] ospf
[PE-WJ-ospf-1] area 0
[PE-WJ-ospf-1-area-0.0.0.0] network 172.2.0.0 0.0.255.255
[PE-WJ-ospf-1-area-0.0.0.0] network 202.100.1.3 0.0.0.0
[PE-WJ-ospf-1-area-0.0.0.0] import-route direct
# 在PE与PE之间建立MP-IBGP邻居，进行PE内部的VPN路由信息交换。
[PE-WJ] bgp 100
[PE-WJ-bgp] group 202 internal
[PE-WJ-bgp] peer 202.100.1.1 group 202
[PE-WJ-bgp] peer 202.100.1.1 connect-interface loopback0
[PE-WJ-bgp] ipv4-family vpnv4
[PE-WJ-bgp-af-vpn] peer 202 enable
[PE3-bgp-af-vpn] peer 202.100.1.1 group 202
[PE3-bgp-af-vpn] quit
[PE-WJ-bgp] peer 202.100.1.3 group 202
[PE-WJ-bgp] peer 202.100.1.3 connect-interface loopback0
[PE-WJ-bgp] ipv4-family vpnv4
[PE-WJ-bgp-af-vpn] peer 202 enable
[PE3-bgp-af-vpn] peer 202.100.1.3 group 202
[PE-WJ-bgp-af-vpn] quit
```

PE-LQ的配置过程与前面的PE配置类似，就不在赘述。

(5) 配置温江的CE-JF

```
[CE-JF] interface ethernet 0/0/0
[CE-JF-Ethernet0/0/0] ip address 168.3.1.1 255.255.0.0
[CE-JF-Ethernet0/0/0] quit
[CE-JF] bgp 65410
[CE-JF-bgp]  neighbor 168.3.1.2 255.255.0.0 remote-as 100
[CE-JF-bgp]  network 168.3.0.0 mask 255.255.0.0
```

其它各个站点的CE设备的配置也和CE-JF类似，就不再重复。从上面的配置来看VPN的创建和维护全部在PE设备上完成，增加和减少一个

VPN将是非常方便的，不像其他的VPN实现方式都存在N平方的问题（增加一个VPN用户就必须建立这个用户与其它用户的隧道连接），不利于VPN的大规模部署，扩展性很差。采用MPLS来实现的VPN网络对接入用户来说也很容易维护，甚至只需要将CE设备连到相应的VPN接口上即可，这是其它的VPN实现方式无法达到的，这就极大的简化企业技术人员对VPN的维护的工作，使MPLS/VPN成为企业或者ISP首选的且容易实现的VPN实现方式。

5.1.2 MPLS/VPN网络测试

5.1.2.1 VPN安全性测试

VPN的安全性是通过不同VPN之间的路由隔离来实现的，MPLS/VPN作为VPN的一种实现方式也必须具备路由隔离的特点，为了达到安全性的要求不同的VPN之间是不能互相通信，为了测试基于MPLS的VPN网络的安全性，我们在实验网络中采取通常的容易实现的Ping指令来测试VPN的连通性来验证VPN的安全性。

• 在CE设备上用Ping命令测试VPN安全性：

在新都CE-JF上Ping温江的CE-JF

```
CE-JF# ping 168.3.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 168.3.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8
ms
```

在温江CE-JF上Ping新都的CE-JF

```
CE-JF# ping 168.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 168.1.1.1, timeout is 2 seconds:
!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

在新都CE-JF上Ping温江的CE-OA

CE-JF# ping 10.2.2.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

在温江CE-JF上Ping新都的CE-OA

CE-JF# ping 10.2.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.1.2, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

在新都CE-JF上Ping骨干网的端口

CE-JF# ping 172.1.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.1.1.2, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

CE-JF# ping 202.1.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 202.1.1.2, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

上面的测试表明：相同的VPN之间可以互通，而不同的VPN之间是不能通讯的，VPN与主干路由器之间也是不能Ping通的这样就能保证VPN的内部数据不会外泄。

5.1.2.2 查看配置信息

- **分别查看PE、P和CE设备的路由表**

先查看P设备的路由表

```
[Quidway-P]dis ip routing-table
 Routing Table: public net
Destination/Mask    Protocol  Pre  Cost      Nexthop
Interface
127.0.0.0/8         DIRECT    0    0         127.0.0.1
InLoopBack0
127.0.0.1/32        DIRECT    0    0         127.0.0.1
InLoopBack0
172.1.0.0/16        DIRECT    0    0         172.1.1.2
Ethernet1/1
172.1.1.2/32        DIRECT    0    0         127.0.0.1
InLoopBack0
172.2.0.0/16        DIRECT    0    0         172.2.1.2
Ethernet1/0
172.2.1.2/32        DIRECT    0    0         127.0.0.1
InLoopBack0
172.3.0.0/16        DIRECT    0    0         172.3.1.2
Ethernet1/2
172.3.1.2/32        DIRECT    0    0         127.0.0.1
InLoopBack0
202.100.1.1/32      OSPF      10   2         172.1.1.1
Ethernet1/1
202.100.1.2/32      OSPF      10   2         172.2.1.1
```

Ethernet1/0

202.100.1.2/32 OSPF 10 2 172.3.1.1

Ethernet1/2

从上面的路由信息我们可以看到：在P路由器上有整个MPLS骨干的全局路由，这个路由信息保证了骨干网络的通讯，但没有VPN-JF和VPN-OA的路由信息，VPN路由信息通过公网透明的传递VPN路由信息，而公网上的路由器无法获得VPN的路由信息，这也保证了VPN的安全性。

• 查看PE设备上的路由表

以成都PE设备为例来说明•

[PE-CD]dis ip routing-table

Routing Table: public net

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
172.1.0.0/16	DIRECT	0	0	172.1.1.1	Ethernet1/0
172.1.1.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
172.2.0.0/16	OSPF	10	2	172.1.1.2	Ethernet1/0
172.3.0.0/16	OSPF	10	2	172.1.1.2	Ethernet1/0
202.100.1.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
202.100.1.2/32	OSPF	10	3	172.1.1.2	Ethernet1/0

```
202.100.1.3/32        OSPF        10      3                  172.1.1.2
Ethernet1/0

[PE-CD]dis ip vpn-instance vpn-JF
VPN-Instance : vpn-JF
   No description
   Route-Distinguisher :    100:1
   Interfaces :
    Ethernet1/1

[PE-CD]dis ip vpn-instance vpn-OA
VPN-Instance : vpn-OA
   No description
   Route-Distinguisher :    100:2
   Interfaces :
    Ethernet1/2
```

从上面的路由调试信息可以看出：在PE设备上有两种路由信息一个是MPLS骨干的全局路由信息，另一个是PE上不同VPN自己的路由信息，这就论证了我们前面提到的PE设备从不同的CE那里学到不同VPN的路由信息，然后将该路由信息通过MPLS骨干传递到对端的PE设备。

• 查看CE设备路由表

我们以温江的CE为例

```
CE-WJ#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
```

```
EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
Gateway of last resort is not set
     168.1.0.0/32 is subnetted, 1 subnets
B       168.1.1.2 [20/0] via 168.3.1.2, 00:03:38
168.2.0.0/32 is subnetted, 1 subnets
B       168.2.1.2 [20/0] via 168.3.1.2, 00:03:38
C    168.3.0.0/16 is directly connected, FastEthernet1/0
```

从CE的路由信息我们可以看出：在CE设备上我们只能获得相同的VPN的路由信息，甚至连公网的路由信息我们也无法获得，这也证明了前面为什么不能Ping通骨干网的那些端口，公网只是透明的传递VPN路由信息，对VPN的不同CE站点来说，公网逻辑上是透明的，这就从根本上保证了VPN数据的安全性。

前面我们提到VPN的路由信息是通过BGP透明的传输的，通过下面的调试信息我们可以清楚的看到：

```
[PE1-CD]dis bgp vpnv4 all routing-table
Flags:  # - valid       ^ - active      I - internal
        D - damped      H - history     S - aggregate suppressed

In/out     As
   Dest/mask            Next-hop         Med          Local-pref
label     path
------------------------------------------------------------------
----
Route Distinguisher:100:1 (VPN instance:vpn-JF)
#^     168.1.1.2/32                0.0.0.0                        0
1024/-
```

```
#^I  168.3.0.0          202.100.1.2      0          100
-/1024
Route Distinguisher:100:2 (VPN instance:vpn-OA)
#^     10.2.1.2/32            0.0.0.0                0
1024/-
#^I  10.2.2.0           202.100.1.2      0          100
-/1024
Routes total: 2
```

• BGP信息测试

BGP路由协议在实现MPLS/VPN中起着重要的作用，它透明的传输VPN路由信息，既保证了VPN的安全性，同时又保证了VPN网络的通讯。我们都以新都PE设备为例来 测试BGP信息。

```
[PE1-CD]dis bgp routing-table
Flags:  # - valid       ^ - active      I - internal
        D - damped      H - history     S - aggregate suppressed
    Dest/Mask           Next-hop        Med         Local-pref
Origin As-path
------------------------------------------------------------------
------------
# I  172.2.0.0            202.100.1.2      0          100
INC
  I  172.3.0.0            202.100.1.2      0          100
INC
  I  202.100.1.2/32       202.100.1.2      0          100
INC
  I  202.100.1.3/32       202.100.1.2      0          100
INC
  Routes total: 2
```

```
[PE1-CD]dis bgp peer
 Peer        AS-num Ver Queued-Tx     Msg-Rx     Msg-Tx     Up/Down
State
------------------------------------------------------------------------
----
202.100.1.2          100   4            0          35          35
00:33:05 Establishe
202.100.1.3          100   4            0          35          35
00:33:05 Establishe
```

• **MPLS信息测试**:

MPLS是构建VPN隧道的基础，也是实现MPLS/VPN网络的核心技术，通过对它的测试来验证隧道的建立情况。

```
[PE1-CD]dis mpls interface
  MPLS interface information:
  Interface Ethernet1/0 ( Label Range : 16-204799 )
 [PE1-CD]dis mpls lsp
------------------------------------------------------------------------
----
                LSP Information: Ldp Lsp
------------------------------------------------------------------------
----
TOTAL:  2 Record(s) Found.
NO      FEC                          NEXTHOP              I/O-LABEL
OUT-INTERFACE
1       202.100.1.1/32       127.0.0.1       3/-----      -------
2       202.100.1.2/32       172.1.1.2       -----/1025   Eth1/1
3       202.100.1.3/32       172.1.1.2       -----/1026   Eth1/0

[Quidway-PE1]dis mpls ldp interface
```

```
Displaying information about all Ldp interface:
     Interface Ethernet1/0(address=172.1.1.1):
     Label distributing enabled,bound to entity:202.100.1.1:0
     Generic label range configured:16 - 204799
     Label Advertisement Mode: Downstream-Unsolicited
     Configured KeepAlive hold time:60, Configured Hello hold
time:15
     Negotiated Hello hold time:15
     Hello packets sent/rcv:472/467

[Quidway-PE1]dis mpls ldp peer
Displaying information about all peers:
   Local LDP ID: 202.100.1.1:0
   Peer LDP ID: 172.1.1.2:0
   Internetwork Address Type: IPv4
   Internetwork Address: 172.1.1.2
   Maximum Peer PDU length: 4096
   Peer KeepAlive hold time: 60
   Peer Distribution Method: Downstream Unsolicited
   Peer Type: Local
   Peer RowStatus: Active
```

从上面的实验结果可以看出：基于MPLS的VPN不但能满足VPN安全性的要求，而且用LDP建立的LSP还能满足最优路由的要求,因为LSP是根据最优的路由建立起来动态的隧道。用MPLS来实现的VPN扩展性非常的好，增加一个或者减少一个VPN客户是非常容易，只需要在PE设备上进行配置就可以了，对提供商来说是非常容易管理的，而用户要接入VPN也是十分的简单，比传统的VPN实现技术来说扩展性要强很多，而且用MPLS来实现的VPN也继承了MPLS在流量工程和QOS上天然优势，也是其它VPN实现技术无法比拟的。

5.2 MPLS/VPN 网络的性能分析

通过理论分析以及对 MPLS/VPN 实验网络的配置与测试，我们从扩展性、拓扑灵活性、可靠性、网络维护管理、安全性等方面的对比来分析传统 VPN 网络与 MPLS/VPN 网络性能差别：

- **扩展性**

传统的专网是在运营商网络之上构建的覆盖型网络，因此在实现用户节点间的全网状通信时，会存在 N 平方的扩展性问题。

我们以在不同节点数的 VPN 网络中增加一个节点来分析，如图 5-2 所示：

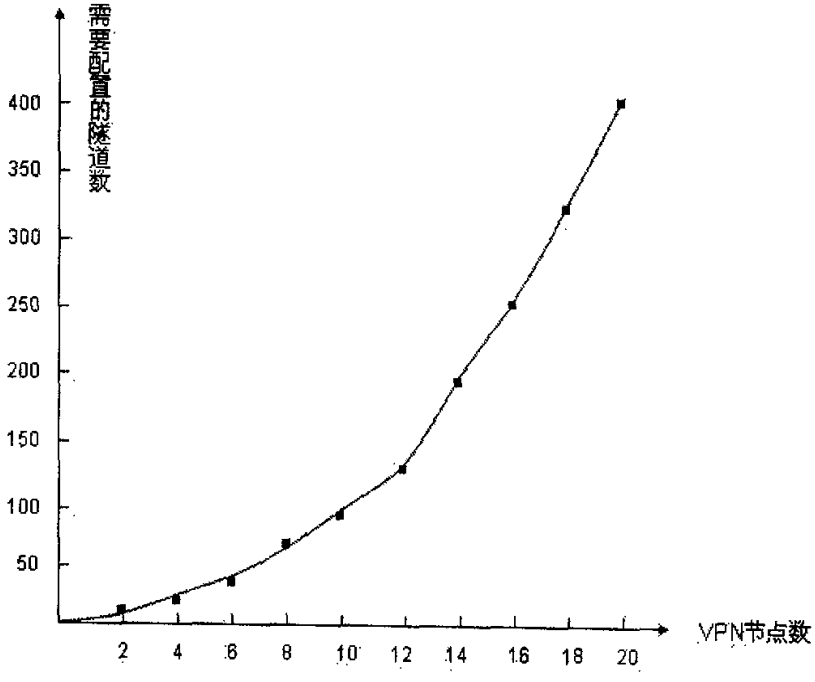

图 5-2 传统的基于隧道技术的 VPN 网络的扩展性

在有 2 个节点的传统的基于隧道技术的 VPN 网络中，每增加一个节点，该节点要与其他节点建立 VPN 连接，需要建立的隧道数为 4 个。当有 10 个

节点的网络，每增加一个节点，该节点要与其他节点建立VPN连接，需要建立的隧道数为100个，当有20个节点的网络，每增加一个节点，该节点要与其他节点建立VPN连接，需要建立的隧道数为400个，对于ISP来说节点数远远大于20个节点，在这样的环境中每增加一个节点需要建立的隧道数是非常大的，随着VPN网络规模的不断扩大，VPN中随时都有可能增加新的用户节点，如果采用传统的VPN实现技术，扩展性就成为制约VPN网络发展的重要因素。

但基于MPLS的VPN网络，由于借助于BGP协议进行成员的分配和管理，同一个VPN中的用户节点数不受限制，容易扩充，并可以实现相同VPN内不同分支节点间的直接通信，所以MPLS/VPN网络则具有很强的扩展性。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，用户侧只需要对接入的PE设备进行配置即可，不需要对每个VPN接点进行配置，避免了N平方的扩展性问题。

- **拓扑灵活性**

由于是点对点连接，传统专网的逻辑拓扑调整起来相对比较复杂。对于用户来说可能需要新增、删除电路，修改路由配置。运营商也要在网络侧对电路相应地新增、删除并需要逐条配置，维护工作量较大。

MPLS/VPN可以通过网络侧参数的调整，很容易实现用户节点间的星形、全网状以及其它任何形式的逻辑拓扑，以满足用户对内部节点间管理上的要求。这一逻辑拓扑调整不需要用户侧新增任何线路或修改任何配置，完全可在网络侧完成，对用户完全透明，有效地减少了用户的维护工作量。

- **网络可靠性**

网络的可靠性主要靠资源的冗余度来实现。由于在前几年ATM建设热潮中全球绝大部分大型电信运营商都建成了自己比较完备的ATM网，因此ATM网多路由、富余的传输资源基本上都可以满足专线网络的可靠性要求。通过ATM网的信令和路由体系，在ATM网内部中继线中断时，现在ATM/FR PVC和基于电路仿真的DDN都可以通过自动切换/迂回路由保护业务电路。但由于ATM产品种类特别多，至少在目前还无法很好地实现异种ATM网络之间的电路自动切换/迂回路由。而传统的基于电路交叉连接的DDN电路

则一般不具备电路自动切换/迂回路由能力，它可以依靠 SDH 环提供线路保护，但无法摆脱 DDN 设备出故障时带来的网络设备单点故障。

由于全球基于互联网的 IP 基础设施非常发达，因此依托它来开展 MPLS/VPN 业务，自然就具有大带宽、多节点、多路由、充裕的网络和传输资源来保证网络的可靠性。当互联网内部中继线中断时，MPLS VPN 的流量与普通互联网流量一起依据 IGP 迂回到其它电路上，这一过程完全依靠 IGP 的收敛自动完成，对用户完全透明，在广域网传输中不存在单点故障。

- **网络维护管理**

从用户自身网络的维护管理来看，传统专网要求用户维护一个广域网，较高档次的设备和多而复杂的线路也可能会增加维护管理的复杂性和难度，而且工作量大，对技术人员的要求也非常高。我们根据图 5-3 所示：

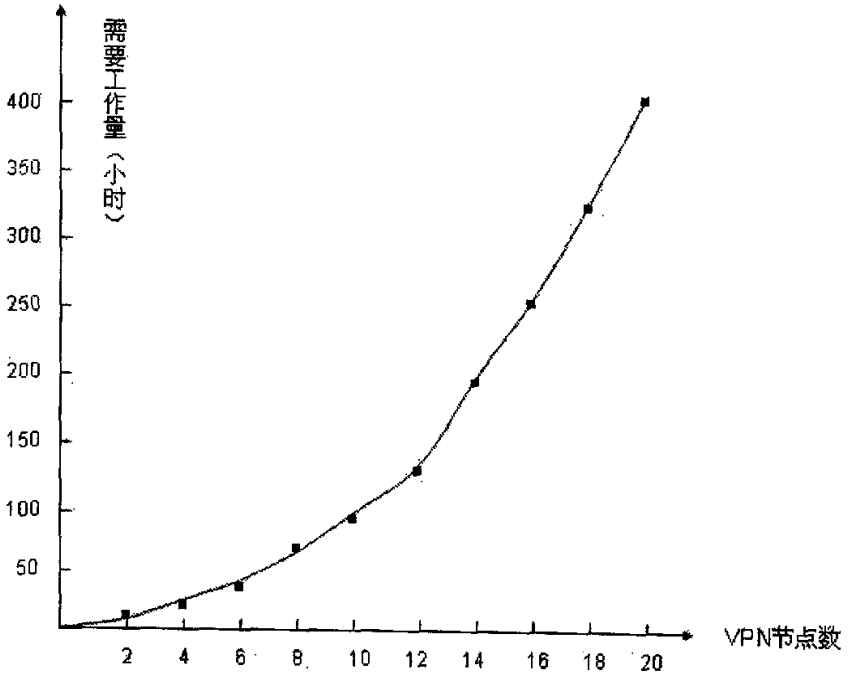

图 5-3 传统 VPN 网络维护管理工作量

在VPN网络中每增加一个节点，需要配置N^2个（N为VPN网络中的节点数）隧道，而隧道需要在隧道两端都要进行配置，这个工作量就是非常大的，传统的VPN网络的隧道技术基本是采用软件加密技术来实现的，其配置过程也比较复杂，需要专业的工程师才能完成。一般来说一个熟悉工程师配置一个隧道需要1个小时来计算，那么随着节点的增加，工作量也是按N^2增加的。对采用MPLS/VPN进行组网，只需要对PE设备进行维护和管理就可以了，把VPN站点的管理分散给介入用户，对ISP来说所需要的工作量就小，配置20个节点需要2个小时左右，而传统的需要400个小时，随着节点的增加这种优势更明显，而且对技术人员的要求也低，用户可以把大部分精力放在局域网的建设、维护上。可以说MPLS/VPN与传统专线组网方式最大的区别就在于它在极大地提高了用户网络管理效率的同时，大大降低了用户在网络管理方面投入的人力和物力。而且由于MPLS/VPN还可以向用户提供集成的互联网接入能力，这特别适合于缺乏专门技术人员而想尽量节省资金的那些以接入互联网为主，其次才是通过互联网访问公司内部网络的中小企业用户。

- **安全性**

传统专网的安全性保证主要来自其"闭合用户群（CUG）"特性。它不向用户暴露运营商的网络结构，提供的是透明传输，因此可限制来自用户侧的DoS等攻击。MPLS/VPN由于采用了路由隔离、地址隔离和信息隐藏等多种手段，提供了抗攻击和标记欺骗的手段，因此MPLS/VPN完全能够提供与ATM/FR VPN相类似的安全保证。

从以上几个方面的对比分析可以看出基于MPLS技术的VPN网络，在许多性能指标上都优于传统的VPN网络，这也是构建新的VPN网络的必然要求，也代表了VPN网络的发展趋势。

第六章 结论

通过设计基于MPLS的VPN模型，并按照该模型搭建的实验网络获得的测试结果表明，基于MPLS的VPN网络除了具有传统VPN实现技术在安全性上的基本保证外，但在扩展性、灵活性、可操作性以及流量工程和QOS方面是其它传统VPN实现技术无法比拟的，基于MPLS的VPN技术也代表了未来VPN发展的方向。

基于MPLS的VPN解决方案的优势在于服务提供商可以通过相同的网络结构来支持许多种VPN，并不需要为每一个用户建立单独的网络。而且，这种方案将IPVPN的能力内置于网络本身，所以，服务提供商可以为所有租用者配置一个网络来提供专用的IP网服务，如Intranet和Extranet，而无需复杂的管理，隧道或VC Mesh。QoS可为每个VPN提供特有的业务政策，QoS服务可与基于MPLS的VPN无缝结合，因为两者都是基于标记的技术。

基于MPLS的VPN网络可以很容易地与基于IP的用户网络结合起来。租用者可与供应商提供的服务无缝结合，不必改变Intranet应用，因为这些网络具有应用通晓性、保密性和QoS内置于网络中。用户能够使用他们专有的IP地址而无需NAT。

同一种网络结构目前可支持许多种VPN，可减轻为每一个新网络实施工程的负担。这种方案易于进行VPN的添加、移动和改变。如果某个公司需要在自己的VPN中增加一站点，服务提供商只需告诉客户端设备的路由器如何与网络连接，并配置LSR来识别来自于CPE的VPN成员。BGP会自动更新VPN成员。与增加一台设备需要大量操作的Overlay VPN相比，这种方案要简单、迅速和便宜的多。在一个Overlay VPN中增加一台新设备要涉及到更新流量Matrix，从新站点建立VC到所有现存的站点，更新每个站点的OSPF设计，针对新的拓扑结构图重新配置每台CPE设备。

对于ISP来说构建的VPN网络必须能够通过应用类型得知数据类型，如语音、重要的应用或电子邮件。网络可以很容易地根据VPN区分数据类型，而不用配置复杂的、点到点的连接。进一步来说，网络需要具有通晓

VPN的能力，使得服务提供商能够很容易地将用户和服务分组，提供用户所需的服务。这是VPN具备的最基本功能。MPLS是一项将VPN通晓性带入交换式或路由式网络的技术，它使得服务提供商能够迅速、有效地在同一个网络结构中建立各种大小的VPN。与Overlay VPN相比，基于MPLS的网络能够将数据流分开，无需人工的建立隧道或加密即可提供保密性，基于MPLS的VPN网络以网络到网络的方式提供保密性，如同传统的VPN实现技术是以连接到连接的方式提供保密性。基于MPLS的VPN网络为用户提供服务，而传统的VPN实现技术提供数据的传输，这将支持服务提供商实现从面向传输的模式到面向服务的模的转变。

基于MPLS的VPN网络是下一代增值IP服务的基础，如多媒体/组播应用、VoIP、Intranet content hosting，而这些服务都需要特殊的服务质量和安全性。既然QoS和安全性已内置于网络中，对于每种服务我们就无需单独实施工程。可从某个角度看，我们可设计多个VPN，每个VPN具有不同的服务。这种灵活的方案可以以更低的耗费提供更快更新的服务。

构建一个网络并对它多次销售，服务提供商可为更多的用户提供经济、可扩展的专用IP服务，增加市场份额和利润。在过去，由于对花费的限制以及缺少内部的专用技术，小型企业无法利用广域网（WAN）的优势。而且，由于网络服务是基于第二层的结构，这种管理的复杂性不能为用户提供好的解决方案。基于MPLS的IPVPN网络降低了运行耗费，使得服务提供商以可担负的价格，为小型企业提供可被管理的服务。缺少网络和路由专门技术的用户可以选择被管理的IP服务，将Plug&Play的简易性用于Intranet和Extranet。

总之，基于MPLS的VPN网络，不但具有很强扩展性、拓扑灵活性和网络可靠性而且还具有流量工程和QoS能力，它为ISP和企业构建高扩展性、易维护管理的VPN提供了有价值的参考，同时MPLS/VPN也代表了VPN网络的发展趋势。

参考文献

(1)(美) Ivan Pepelnjak, Jim Guichard. MPLS and VPN Architectures [M]. 北京：人民邮电出版社，2001. 89～109，129～155

(2)(美) Ivan Pepelnjak, Jim Guichard. MPLS and VPN Architectures [M]. 北京：人民邮电出版社，2004.

(3)(美) Bruce Davie, Yakov Rekhter. MPLS：Technology and Applications [M]. 北京：机械工业出版社，2001. 2～35

(4)(美) Eric W. Gray. MPLS: Implementing the Technology [M]. 北京：电子工业出版社，2003. 119～122

(5)(美)Cstherine Paquet, Diane Teare. Building Scalable Cisco Internetworks [M]. 北京：人民邮电出版社，2003.

(6)(美) Douglas E. Comer. 用TCP/IP进行网际互连：第三版 第一卷 原理协议和体系结构 [M]. 北京：电子工业出版社，98.

(7)(美) W. Richard. stevens. TCP/IP 详解：第一卷 协议 [M]. 北京：机械工业出版社，2000.

(8)(美) Jeff Doyle. Routing TCP/IP volume 1 [M]. 北京：人民邮电出版社，2003.

(9)(美) Thomas M. Thomas II. OSPF Network Design Solutions Second Edition [M]. 北京：人民邮电出版社，2004.

(10)(美) Eric Osborne, Ajay Simha. Traffic Engineering With MPLS [M]. 北京：人民邮电出版社，2003.

(11) 石晶林，丁炜等. MPLS 宽带网络互联技术 [M]. 北京：人民邮电出版社，2001. 158～166

(12) 王达等. 虚拟专用网（VPN）精解 [M]. 北京：清华大学出版社，2004.

(13) 黎连业，张维，向东明等. 路由器及其应用技术 [M]. 北京：清华大学出版社，2004.

(14) 高海英，薛元星，辛阳等. VPN 技术 [M]. 北京：机械工业出版社，2004.

(15)(美) Vivek Alwayn. Advanced MPLS Design And Implementation [M]. 北京：

人民邮电出版社，2003.

（16）彭晖.新型的骨干网路由平台-MPLS. 北京：人民邮电出版社，2002.

（17）（美）Parkhurst.CISCO BGP-4 命令与配置手册［M］.北京：中国电力出版社，2002.

（18）（美）Carlton R .Davis. IPsec：VPN的安全实施［M］. 北京：清华大学出版社，2002.

（19）（美）Mark Norris，Steve Pretty.全域网设计-Intranet、VPN及企业 网［M］.北京：人民邮电出版社，2001.

（20）戴宗坤.VPN与网络安全［M］.北京：电子工业出版社，2002.

（21）思科系统（中国）网络技术有限公司.基于多协议标记交换的虚拟专用网［S］.

（22）孙云清.基于MPLS的VPN技术研究实现［D］.成都：电子科技大学，2002.

（23）韦云凯.基于Ipsec的BGP/MPLS VPN研究与设计［D］. 成都：电子科技大学，2004.

（24）徐正福，陈文元，张卫平.基于协议标记交换的虚拟专用网［J］.电子工程师，2001.

（25）张蓉.多协议标记交换VPN的加密与封装技术［D］.湖南大学，2004.

（26）肖慧.MPLS技术实现流量工程及服务质量等问题的研究［D］.广东工业大学，2002.

（27）刘冲霄.MPLS/VPN在广域网中的应用［D］.哈尔滨工业大学，2003.

（29）彭燕妮.MPLS及其网络优化算法的研究［D］.重庆大学，2004.

（30）郭兰.BGP/MPLS VPN网络中基于CE-CE路由认证机制［D］.天津大学，2004.

作者在读期间科技成果简介

1. 参加成都电信数据支撑中心 MPLS/VPN 网络的设计以及实验 MPLS/VPN 网络的设计、实施和测试工作。

2. 撰写的论文《Web 安全性分析》被核心期刊计算机应用研究收录。

3. 撰写的论文《MPLS 技术在 VPN 中的研究与实现》发表于计算机与数字工程，2005 年第 4 期。

声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得四川大学或其他教育机构的学位或证书而使用过的材料。与本人一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

本学位论文成果是本人在四川大学读书期间在导师的指导下完成的。论文成果归四川大学所有，特此声明。

学生：朱诚　　导师：徐丹

2005.5.27

致谢

在本课题的研究及论文的写作过程中，我的导师徐林给予了我悉心的指导和不倦教诲。徐老师严谨的治学态度、活跃的学术思想、忘我的工作精神、实事求是的科学态度将使我终生受益。在我的学习和研究工作中，徐老师自始至终都给予我严格的要求和亲切的关怀，在生活中给予我很大的关心与帮助。在此谨向徐老师表示深深的谢意和崇高的敬意。

在这里我还要特别感谢中国电信成都分公司经营支撑中心的领导和同事，在我实习期间给予我热情和无私的帮助使我能顺利的完成我的毕业论文，另外我还要感谢在我读研究生阶段的我同学，他们无论在学习上还是在生活上都给了我无私的关怀和帮助，在此向他们表示衷心的感谢。

再次向所有关心和帮助过我的老师和同学们表示感谢。