

MPLS技术白皮书

摘要

本文详细介绍了Quidway系列路由器所应用的MPLS技术，包括MPLS的一些基本概念、MPLS VPN、MPLS 流量工程等

关键词

BGP:Border Gateway Protocol, 边界网关协议

CE: Customer Edge, 用户边界路由器

COS: Class of Service, 服务等级

CR-LDP:Constraint-Based Route LDP, 基于受限路由的标签分发协议

DF: Default Forwarding, 缺省转发

DoD: Downstream On Demand, 下游按请求分配标签

DS : Differentiated Services, 差分业务

Du: Downstream Unsolicited, 下游未被请求标签

EBGP: External BGP

EF: Expedited Forwarding, 快速转发

FEC: Forwarding Equivalence Class, 前向等价类

IGP: Interior Gateway Protocol, 内部网关协议

LDP:Label Distribution Protocol, 标签分发协议

LER: Label Edge Router, 边缘标记交换机

LSP: Label-Switch Path, 标记交换路径

MP-BGP: 多协议扩展BGP

MPLS : 多协议标记交换技术

PE: Provider Edge, 运营商边界路由器

P router: Provider Router, 骨干网核心路由器

PIM: Protocol-Independ Multicast, 协议无关组播协议

QOS: Quality of Service, 服务质量

RD: Route Distinguisher

RR: Router Reflector, 路由反射器



RSVP:Resource Reservation Protocol, 资源预留协议

SLA: Service Level Agreement, 业务等级协定

TE : Traffic Engineering, 流量工程

VPN: Virtual Private Networks, 虚拟私有网

VPN Site: 是VPN中的一个孤立的IP网络, 可以属于一个或几个VPN。每个Site通过RD标识。

VRF: Virtual Routing Forwarding Table, 虚拟路由转发表

1 概述

Internet在近些年中的爆炸性增长, 为Internet服务提供商(ISP)提供了巨大的商业机会, 同时也对其骨干网络提出了更高的要求, 人们希望IP网络不仅能够提供E-Mail、上网等服务, 还能够提供宽带、实时性业务。ATM曾经是被普遍看好的能够提供多种业务的交换技术, 但是由于实际的网络中人们已经普遍采用IP技术, 纯ATM网络已经不可能, 现有ATM的使用也一般都是用来用来承载IP。如此人们就希望IP也能提供一些ATM一样多种类型的服务。

MPLS (Multiprotocol Label Switch, 多协议标签交换)就是在这种背景下产生的一种技术, 它吸收了ATM的VPI/VCI交换一些思想, 无缝地集成了IP路由技术的灵活性和2层交换的简捷性, 在面向无连接的IP网络中增加了MPLS这种面向连接的属性。通过采用MPLS建立“虚连接”的方法, 为IP网增加了一些管理和运营的手段。

MPLS的最早原型是90年代中期由Ipsilon公司率先推出的IPSwitching协议, 其目的主要是解决ATM交换机如何更好地支持IP, 该协议使ATM交换机成为一台路由器, 因而具有ATM交换机的高性能, 突破了传统路由器的性能限制。一时间Ipsilon名声大震。继之Cisco推出Tag Switching, IBM推出Aggregate Route-based IP Switch (ARIS)等。当时路由器厂家实现标记交换的目的是为了解决IP路由查找不能达到线速的问题(因为IP路由查找采用的是最长地址匹配的方式, 在路由器端口速度达到155M或622M时软件查找会由困难)。这些早期不同厂家的标签交换的实现存在互通问题, 所以在1997年IETF成立一个负责标记交换标准化的工作组---MPLS工作组。它独立于各个设备实现厂家。现有的MPLS相关协议和草案基



本商来自于这个工作组和它后来派生出来的流量工程工作组和MPLS VPN工作组。

随着网络处理器技术的迅速发展，2.5G甚至10G的端口的路由线速查找都已经不成问题，MPLS应用也逐步转向MPLS流量工程和MPLS VPN等。在IP网中，MPLS流量工程技术成为一种主要的管理网络流量、减少拥塞、一定程度上保证IP网络的QoS的重要工具。在解决企业互连，提供各种新业务方面，MPLS VPN也越来越被运营商看好，成为在IP网络运营商提供增值业务的重要手段！采用MPLS VPN技术可以把现有的IP网络分解成逻辑上隔离的网络，这种逻辑上隔离的网络的应用可以是千变万化的：可以用在解决企业单独互连、政府相同/不同办事部门的单独互连、也可以时用来提供新的业务---如为IP电话业务专门开辟一个VPN、以此解决IP网络地址不足、QoS保证、以及开展新业务等问题。

在MPLS越来越被看好的同时，反对使用MPLS的声音同样越来越尖锐。主要的反对声音来自于AT&T的两位Internet研究者---安全权威Steve Bellovin和网络运行专家Randy Bush。MPLS的反对者认为MPLS，尤其是MPLS VPN对IP网络来说是一个灾难！认为MPLS彻底破坏了IP网络的现有结构，在IP网上增加了复杂的、难于管理和控制的VPN结构，在VPN数量很多的时候会严重影响骨干网的稳定性和可扩展性。另外象三层MPLS VPN的安全也是一个问题，在VPN配置错误时，错被配进VPN的客户在VPN中没有任何阻碍。MPLS的反对者认为MPLS是没有必要的，解决VPN采用IPSec是一种更好、更安全、对现有网络改动也最小的解决方案。MPLS的反对者认为给有拥塞的链路扩容也会是解决网络拥塞的更简单的办法。

以上观点虽然有些极端，但是MPLS技术确实给运营商提出了新的挑战，在实施MPLS时整个网络管理的复杂度明显增加！如使用流量工程时需要对网络流量进行全面周期性测量、使用MPLS VPN需要针对每一个VPN管理一个VPN路由表！在有成千上万个VPN的时候，管理成千上万个VPN路由表会是一个非常头痛的事。所以并不是所有的VPN（如Site很少、端口速度又小的VPN）都要用MPLS/BGP VPN，能用IPSec或专线的不必一定要用MPLS/BGP VPN。MPLS/BGP VPN比较适用于Site较多、端口速度大的VPN。MPLS的另一个问题是标准还有待完善，很多都是草案，这些草案常常也只要一两个设备商支持，有些问题---如

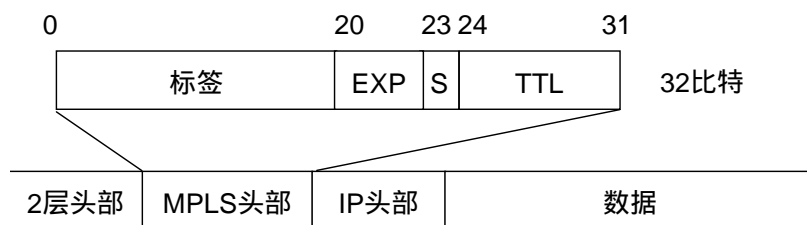


MPLS QoS、二层VPN互通、三层VPN跨域都还在发展之中，安全性也确实要差一些。

华为公司提供全面的MPLS解决方案，支持MPLS VPN，支持MPLS流量工程，认为MPLS是IP网中解决网络QoS问题、VPN问题的一个重要手段。随着MPLS标准的不断完善，华为公司将能够及时的、全面的、满足标准的MPLS解决方案。

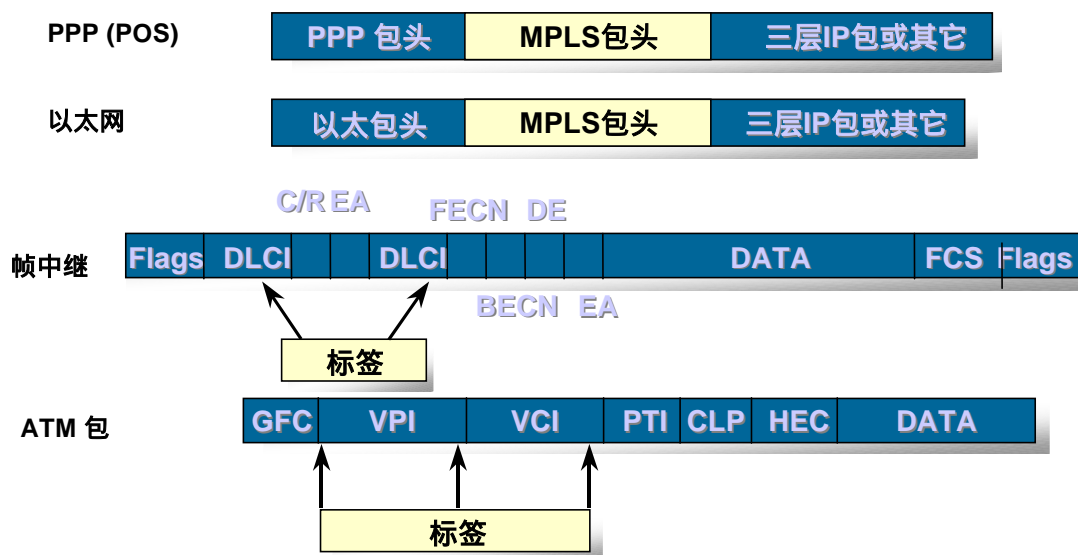
1.1 MPLS包头结构，在协议栈中的位置

通常，MPLS包头的结构如下图所示，包含20比特的标签，3个比特的EXP，现在通常用做CoS，1个比特的S，用于标识这个MPLS标签是否是最低层的标签，



和8个比特的TTL-Time To Live。

MPLS包头的位置介于二层和三层之间，俗称2.5层。MPLS可以承载的报文通常是IP包（当然也可以改进直接承载以太包、ATM的AAL5包、甚至ATM信元等，这在MPLS VPN中有详述）。可以承载MPLS的二层协议可以是PPP、以太网、ATM和帧中继等。对于PPP或以太网二层封装，MPLS包头结构如上图所示，但是对于ATM或帧中继，MPLS则直接采用分别采用VPI/VCI或DLCI做为转发的标签。具体结构如下图所示：



MPLS可以看做是一种面向连接的技术。通过MPLS信令或手工配置的方法建立好MPLS标记交换连接(Label Switched Path, 简称LSP)以后, 在标记交换路径的入口把需要通过这个标记交换路径的报文打上MPLS标签, 中间路由器在收到MPLS报文以后直接根据MPLS报头的标签进行转发, 而不用再通过IP报文头的IP地址查找。在MPLS标记交换路径的出口(或倒数第二跳), 弹出MPLS包头, 还回原来的IP包(在VPN的时候可能是以太网报文或ATM报文等)。

1.2 MPLS信令

通常使用的建立MPLS标记交换路径的信令有LDP/CR-LDP, RSVP-TE, BGP扩展等, 其中LDP/CR-LDP和RSVP-TE是用来建立标签连接通路, LDP的标签分配模式有DoD (Downstream On Demand: 下游按请求分配标签模式) 和Du (Downstream Unsolicited: 下游未被请求标签分配模式) 两种方式, LDP能够建立到某个目的路由或目的子网的LSP, 它的路由的每一跳是根据路由表确定的, 也就是说LDP建立的LSP只有把需要转发的IP报文打包成MPLS, 实际走的路由还是和原来的IP包走的路由是一样的。LDP建立的LSP没有平衡流量的功能, 只能起到建立虚连接的作用。

CR-LDP和RSVP-TE则能够携带带宽、部分明确路由、着色等约束参数, 其中着色约束条件可以用来标识一个链路的性能---如是否支持Voip等、还是只支持



Best-Effort业务，也可以用来做为地域的标识。CR-LDP或RSVP-TE要建立满足这些约束条件的LSP，必须通过流量工程的约束路由计算。从完成的功能来说，两者是一样的，两种协议都可以做各种扩展满足QoS的要求。从内部实现机制来看CR-LDP信令协议是基于TCP的，RSVP-TE是对原有的RSVP做扩展，是基于Raw IP的。由于UDP的传输是不可靠的，RSVP-TE需要对LSP的状态定期刷新，存在一定的可扩展性问题。这两种协议在国际/国内标准认可方面大家都是比较偏向LDP/CR-LDP，它是ITU-T认可的MPLS信令标准，也是中国国标中认定的MPLS信令标准。CR-LDP和RSVP-TE的争论还在继续，现在大多数设备厂家都同时支持CR-LDP和RSVP-TE扩展。

BGP协议的各种扩展则可以为MPLS VPN建立跨AS域的外层承载隧道、或者是VPN应用分配VPN的内层标签。

2 MPLS VPN

MPLS的一个重要应用是VPN。根据扩展方式的不同MPLS VPN可以分为BGP扩展实现的MPLS VPN，和LDP扩展实现的VPN。根据PE（Provider Edge）设备是否参与VPN路由又细分为二层VPN和三层VPN。三层MPLS BGP VPN相对来说比较成熟，但是整体来说MPLS VPN还是在发展和成型阶段。

2.1 BGP扩展实现的MPLS VPN

2.1.1 三层MPLS BGP VPN

1. 单个自治域的MPLS BGP VPN

BGP扩展实现的MPLS三层VPN包含下列组件：

PE： Provider Edge Router， 骨干网边缘路由器， 存储VRF（Virtual Routing Forwarding Instance）， 处理VPN-IPv4路由， 是MPLS三层VPN的主要实现者。

CE： Custom Edge Router， 用户网边缘路由器， 分布用户网络路由。

P router： Provider Router， 骨干网核心路由器， 负责MPLS转发。

RR： Route Reflector， BGP路由反射器。

ASBR： 自治系统边界路由器， 当实现跨自治系统的VPN时， 同其它自治系统交换VPN路由

MP-BGP： 多协议扩展BGP， 承载携带标签的IPv4/VPN路由， 有MP-IBGP和MP-EBGP之分。



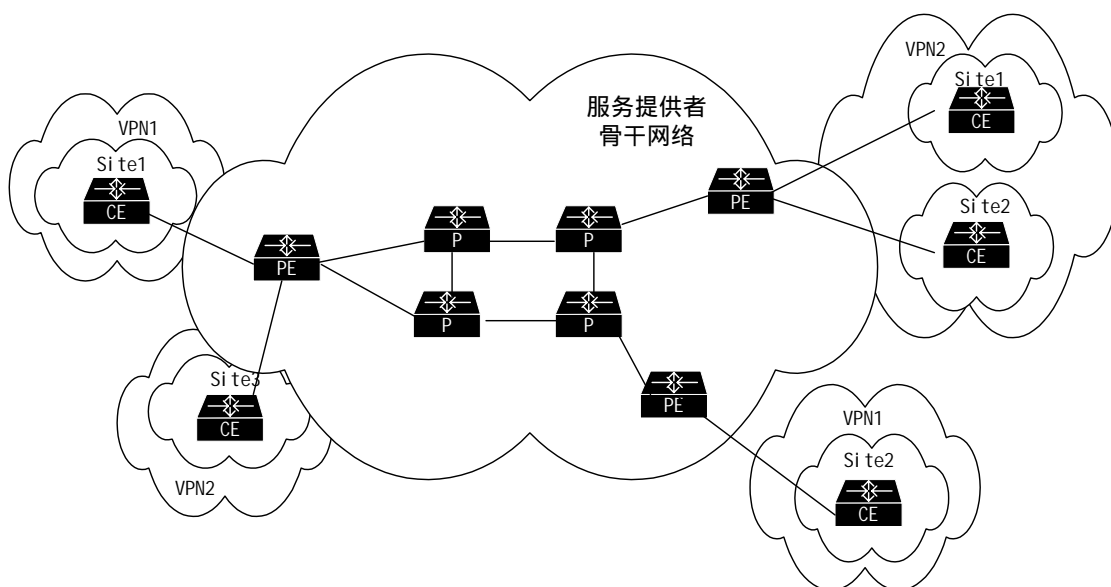
PE-CE路由协议：在PE和CE之间传递用户网络路由，可以是静态路由、也可以是RIP、OSPF、ISIS或BGP。

LDP：在PE之间建立Best-effort的LSP，经过P路由器，所有PE和P路由器均需要支持。

RSVP-TE：在PE之间建立具有QoS能力的ER-LSP，当VPN需要QoS时使用。

VRF：Virtual Routing Forwarding Table，虚拟路由转发表。它包含了同一个site相关的路由表、转发表、接口（子接口）、路由实例以及路由策略等。在PE设备上，属于同一个VPN的物理端口或逻辑端口对应一个VRF。VRF通过命令行或网管工具来配置，主要的参数包括RD（Route Distinguish）、import route-targets、export route-targets、接口（子接口）表等。

VPN用户站点（site）：是VPN中的一个孤立的IP网络，一般来说，不通过骨干网不具有连通性，公司总部、分支机构都是site的具体例子。CE路由器通常是VPN Site中的一个路由器或交换设备，Site是通过一个单独的物理端口或逻辑端口（通常是VLAN端口）连接到PE设备上。



用户接入MPLS VPN的方式是每个site提供一个或多个CE，同骨干网的PE连接。在PE上为这个site配置VRF，将连结PE-CE的物理接口、逻辑接口、甚至L2TP/IPSec隧道绑定的VRF上，但不可以是多跳的3层连接。



BGP扩展实现的MPLS VPN扩展了BGP NLRI中的IPv4地址，在其前增加了一个8字节的RD（Route Distinguisher）。RD是用来标识VPN的成员---即Site的。每个VRF配置了一些策略，规定一个VPN可以接收哪些Site来的路由信息，可以向外发布哪些Site的路由信息。每个PE根据BGP扩展发布的信息进行路由计算，生成每个相关VPN的路由表。

PE-CE之间要交换路由信息一般是通过静态路由，也可以通过RIP、OSPF、BGP等。PE-CE之间采用静态路由的好处是可以减少CE设备可能会因为管理不善等原因造成对骨干网BGP路由产生震荡，影响骨干网的稳定性。

MPLS BGP 三层VPN适用于固定的Intranet/Extranet用户，每个site代表了Intranet/Extranet中的总部、分支机构等。

MPLS三层VPN的CE设备与PE设备之间只需要一条物理或逻辑的链路，但PE设备需要保存多个路由表。在CE与PE之间如果运行动态路由协议时，PE还要支持多实例，对PE性能要求较高。PE与PE之间需要运行BGP协议，存在可扩展性问题。现在一般通过一个一个或多个路由反射器方式解决。对于同一个AS域VPN，需要建立运营商间路由器IBGP连接的PE，与路由反射器建立IBGP连接即可。

MPLS BGP三层VPN通过和Internet路由之间配置一些静态路由的方式，可以实现VPN的Internet上网服务。MPLS BGP VPN还可以为跨不同地域的、属于同一个AS的、但是没有自己的骨干网的运营上提供VPN互连，即提供“运营商的运营商”模式的VPN网络互连。

2.1.2 跨域的MPLS VPN

由于现有城域网或地区网有时会自成一个自治域（AS），通过BGP扩展实现的三层VPN需要解决跨域的问题。现有的跨域解决方案有VRF-to-VRF，MP-EBGP，Multi-Hop MP-EBGP三种方式。

VRF to VRF方式：要求两个域的ASBR能够做PE。两个AS域各自运行自己的VPN。对于每一个需要跨域的VPN，需要在本端跨域的PE设备上配置对应于这个VPN的VRF，把对端的PE设备做为 本域VPN的CE，PE-CE之间运行EBGP协议，携带对端的VPN路由信息。这个方法的优点是在ASBR之间不需要运行MPLS，但缺点是每个跨域的VPN需要与一个子接口绑定，子接口的数量至少要和跨域的VPN的数量相当。跨域的PE路由器需要维护跨域VPN的路由，因而存在可扩展性问题。



MP-EBGP方式：通过直连的ASBR传播VPN路由，并且为给相应的VPN路由分配一个标签。这种方法的优点是不需要在ASBR处为每个VPN的用户站点分配一个子接口。但缺点是在ASBR处维护VPN路由，从PE ingress到PE egress需要一条完整的LSP，ASBR之间需要互相信任。

Multi-hop MP-EBGP方式：这种方式是首先路由扩散在ingress与egress之间通过LDP或MP-BGP+LDP的方式建立LSP，然后不同AS域之间的PE通过EBGP方式传播VPN路由信息。这种方式有较好的可扩展性，不需要在ASBR上维护具体用户的VPN路由信息。

2.1.3 二层MPLS BGP VPN

对于MPLS二层VPN，网络运营商负责提供给二层VPN用户提供二层的连通性，不需要参与VPN用户的路由计算。在提供全连接的二层VPN时，和传统的二层VPN一样（如ATM PVC提供的VPN），存在N方问题，每个VPN的CE到其它的CE都需要在CE与PE之间分配一条连接。对于PE设备来说，在一个VPN有N个Site的时候，CE-PE必需有N-1个物理或逻辑端口连接。由于与用户的路由无关，二层MPLS VPN的可扩展性也只与连接的VPN用户数目相关。

2.2 LDP扩展实现的MPLS VPN

LDP扩展实现的二层VPN也同样可以承载ATM、帧中继、以太网/VLAN、PPP等，但它的主要应用是以太网/VLAN的情况。实现上非常简单，只需增加一个新的能够标识ATM、帧中继、以太网/VLAN、PPP的FEC类型即可。相对于BGP扩展的它的缺点是只能建立点到点的VPN二层连接，没有VPN的自动发现机制。优点是可以在城域网的范围内建立透明LAN服务（TLS，Transparent LAN Service），通过LDP建立的LSP进行MAC地址学习。

尽管现在的LDP扩展实现的二层VPN还主要是通过点到点的手工配置建立LSP的方法实现VPN，但是通过这些实现展示了LSP和各种二层、三层协议结合而产生新的应用的无穷的可能性。有理由相信MPLS技术将会使IP网提供更多业务的重要手段。

3 MPLS隧道透传--电路交叉连接（CCC-Circuit Cross Connect）

在MPLS标记交换连接建立好了以后，理论上通过它可以承载任何的二层、三层数据报文。其中二层数据报文可以是：ATM、帧中继、以太网/VLAN、PPP等，三层可以是IPv4、IPv6、IPX等。电路交叉连接就是在IP网上实现的一种



ATM、帧中继、以太网/VLAN、或PPP在IP网络中点到点地透传的技术。原理上CCC就是把ATM、VLAN等直接粘和到电路交叉连接也可以用来粘和不同的LSP。

4 MPLS流量工程

由于现有的IP网络采用IGP/BGP路由协议，其中IGP协议通常采用的是OSPF，超大型核心骨干网也有采用ISIS的。IP路由协议具有协议简单、面向无连接、在出现链路故障时路由重新收敛速度快的优点。IP网络原本考虑的只是网络的互连，对网络的QoS基本没有考虑。现在的IP网络需要解决QoS的问题，采用的技术一般都是MPLS流量工程或简单的区分业务的方法。

MPLS流量工程就是通过在网络中建立一条、数条、甚至全连接的LSP、对网络流量进行调度的方法实现网络流量的均衡。通常在网络中有一些链接可能负荷饱满甚至超负荷，另外有一些链接却流量较少，在建立进行流量旁路的LSP的时候，就需要绕开负荷较大的链路，而选择负荷较小的链路。如此就可以有目的的把流量从负荷大的链路转移到负荷较小的链路，从而达到平衡网络流量的目的。

流量工程通常限制在一个自治域的区域，这个区域一般都取为网络的核心骨干网，对OSPF的一般取为Area 0，对ISIS通常取为Level 2。对于较小的网络采用MPLS流量工程也是可以的，但由于对运营者要求较高，显得复杂，通常暂时不建议采用。小一些的网络可以通过采用改变链路权值等方法实现流量的均衡。

MPLS流量工程支持带宽约束：对于有带宽要求的LSP，支持MPLS的流量工程可以计算出一条满足带宽要求的LSP。

MPLS流量工程可以支持LSP的抢占：对于带宽较大的LSP，或比较重要的用户，我们可能希望它有较高的抢占优先级，可以去抢占其它的LSP的资源。对于一些不是非常重要的LSP则可以被抢占。同样，一些LSP在建立好了以后可能就不希望它被抢占。现在的MPLS流量工程支持8个抢占优先级和8个保持优先级。

MPLS流量工程支持着色：每个链路可以含有一个或多个颜色，它可以被用来标识这个链路是否支持Voip业务，或者只支持尽力传输业务。也可以用来标识链路的地理位置，在建立LSP的时候保证在一个区域里的LSP不会绕出本区域。

4.1 MPLS流量工程



MPLS流量工程包含四个组成部分：ISIS或OSPF流量工程扩展、MPLS信令、约束路由计算（Constraint Shortest Path First，或简称CSPF）、BGP/IGP横切。

4.1.1 ISIS/OSPF的流量工程扩展

ISIS/OSPF流量工程扩展对现有的ISIS或OSPF协议进行扩展，在链路状态中增加流量工程需要的链路的带宽等流量工程相关的属性。具体来说这些属性包括：

- ✓ 链路的本端IP地址
- ✓ 对端IP地址
- ✓ 链路的带宽
- ✓ 链路的最大可预留
- ✓ 链路的着色
- ✓ 链路的8个优先级的未被预留带宽

其中最重要的是链路的最大可预留带宽和每个优先级的链路未被预留带宽，它们携带了链路的主要带宽信息。每一个路由器都收集本区域的所有路由器的链路的流量工程相关信息---每个链路的，产生流量工程数据库（TED）。

4.1.2 约束路由计算

约束路由计算的输入有两个：一个是需要建立的LSP的带宽、着色、抢占/保持优先级、部分明确路由等约束条件，这些都是在LSP的入口处进行配置（手工配置或网管配置）实现的。另外一个就是通过ISIS或OSPF流量工程扩展产生的TED。

有了以上两个输入，约束路由计算从逻辑上来说就是针对LSP的要求，对比流量工程数据库中的每一个链路进行剪切，把不满足带宽要求的链路剪掉，把不满足颜色要求的链路也剪掉，在剪切以后的拓扑中采用OSPF或ISIS的最短路径算法（SPF算法），得到一条满足LSP的约束条件的最短路径。这里需要注意的是：ISIS或OSPF的SPF计算出来的下一跳就是直接的下一跳，每一个路由器都需要运行SPF算法。CSPF计算的结果是一条满足约束条件的完全明确的路径，它通常只在需要建立的LSP的入口点进行计算，这条路径要起作用必须通过MPLS信令建立起LSP，MPLS信令把CSPF计算出来的完全明确路径通过信令中的明确路径传



到下游接点。LSP建立成功以后，把需要进入这个LSP的IP包在LSP的入口被打上相应的MPLS标签，剩下的过程就是MPLS包就沿着这个LSP进行MPLS转发，直到到达LSP的出口。

4.1.3 MPLS信令

流量工程采用的MPLS信令可以是CR-LDP或RSVP-TE，两者只要有一个就足够了。但是要求一个支持流量工程的Area或Level里的所有路由器支持相同的信令协议。CR-LDP或RSVP-TE把带宽、着色、抢占/保持优先级、和CSPF计算的完全明确路由打包到信令中，信令根据完全明确路由确定LSP的下一跳，并且逐跳检测带宽、着色等资源是否符合或够用。

4.1.4 BGP/IGP流量横切

带约束条件的LSP在建立成功以后，需要能够把一些流量映射到这条LSP上去。流量工程通常采用的方法是BGP/IGP横切的方法，他们都是把建好的LSP当做一个虚端口来使用，但是不向网络发布这个虚端口的存在。BGP横切时要求建立好的LSP是从ASBR到ASBR的，在LSP入口的ASBR进行BGP路由迭代的时候，如果有LSP建到对端的ASBR，就首选这个LSP为下一跳，而不用在查IGP路由表确定下一跳了。在IGP横切的时候，只要求LSP两端的端口属于同一个OSPF的AREA或ISIS的LEVEL。IGP横切的时候需要对现有的SPF算法做一些改进，在OSPF或ISIS进行SPF计算时，如果有LSP存在也首选这个LSP做为IGP的下一跳。

4.2 MPLS流量工程与QoS

4.2.1 IP骨干网上的可能采用的QoS技术

人们希望IP网络能够提供高带宽、低延时的服务，这就要求在IP网上实现一定的QoS功能。IP网中的QoS不可能实现成和ATM一样，因为IP网是一种面向无连接的网络，IP QoS的一个基本要求就是对现有网络结构改变要求尽量的小。适合这个要求的IP QoS机制现在有流量工程和Diffserv/CoS。

流量工程就是一种QoS机制！在IP网这会是非常重要的一种机制。这是因为在影响网络QoS的最主要原因就是因为网络存在拥塞，IP包的网络延时主要来自于路由器调度时队列调度时的排队延时。在一个没有拥塞的网络中，QoS是可以



得到很好的保证的。而流量工程的作用就是调配网络流量，使得LSP的流量能够避开网络拥塞点，从而达到均衡网络流量，减少网络的拥塞的目的。

另外采用MPLS流量工程可以支持快速重新路由。快速重新路由是一种对需要备份的LSP的每隔一跳建立局部备份路由进行备份的一种机制。由于快速重新路由在发现链路或路由器故障以后，是通过硬件直接进行切换的，可以做到从链路故障到快速重新路由切换成功的延时小于50ms！在没有SDH环路备份的链路上，快速重新路由是一种更加灵活的备份机制！

IP网要实现QoS可以只支持Diffserv或CoS，也可以是MPLS流量工程，或者两个同时采用。采用Diffserv/CoS的方法需要对所有的IP包在网络边缘或用户侧进行流分类，打上Diffserv或CoS标识，MPLS包则继承IP包的Diffserv/CoS的IP优先级，在转发的时候直接根据优先级进行转发，不同优先级分别如不同的优先级队列。现有的硬件调度算法有PQ，WFQ等。如果是支持的数据业务只有实时的业务和Best-Effort时，采用PQ调度算法就足够了。这样实时业务的包相对于Best-Effort有严格的优先级。采用MPLS流量工程的方法则可以在网络中存在拥塞的情况下，对流量进行调配，减少网络拥塞发生的可能。这种方法可以避开对进入运营商管理的网络的所有流量都要打上Diffserv/CoS的复杂工作，但是条件是运营商的所有设备都支持流量工程。另外一种可选方案是同时支持流量工程和Diffserv/CoS。

无论采用哪种QoS方案，都需要对全网进行全面的升级，网络管理复杂度也明显增加。最简单的方法还是对网络容量进行升级：每当发现一个链路的容量超过一定程度，就对它进行升级。也就是对拥塞采取增加带宽的方法。当然这种方法的缺点就是从运营的角度来看没有办法实现严格的QoS，然而MPLS的严格QoS保证在标准上还不够成熟，各厂家之间存在互通问题。