中国公共安全杂志社
2005 06 07
中国公共安全 综合版

基于MPLS VPN网络的QoS技术

■

一、MPLS VPN的QoS问题

虚拟私有网络（VPN，Virtual Private Network）是一种利用公共网络来构建私有专用的技术，这种VPN网络必须提供与企业现有私网相同的安全性、可靠性和可管理性。MPLS VPN是近年来兴起的一种IP VPN技术，相对ATM/FR VPN技术而言，MPLS VPN具有高带宽、低成本、可扩展性好、支持异种介质互连、支持任意拓朴和接入等特点。因此它在以下两方面获得广泛的应用：一，企业互联，即企业总部、分支机构和出差员工通过VPN技术进行安全、可靠的通信。二、业务隔离，在一个物理基础网络上承载多种业务，为了保证每个业务的独立运营，采用VPN相互隔离。相比Internet上网业务来讲，这两类应用对网络的QoS提出了更高的要求。

为解决QoS问题，业界提出了多种模型，其中最主要的有三种：

* Best-Effort service（尽力而为服务模型）

Best-Effort是一个单一的服务模型，也是最简单的服务模型。没有提供任何QOS保证。

* Integrated service（综合服务模型，简称Intserv）

IntServ是一种理想化的QoS模型，可以为各类型的业务提供严格的QoS保证，并充分利用网络资源。但这个模型存在严重的可扩展性问题，从而使得这一模型仅具有理论上的意义，从未真正实施过。

* Differentiated service（区分服务模型，简称Diffserv）

DiffServ模型以简单性和可扩展性见长，在每一跳上，可以保证某个优先级的总流量的QoS。但在一个优先级内部不能保证每个流的QoS。

MPLS技术的产生，为解决QoS问题带来了新的希望，这是因为，相对于无连接的IP技术，MPLS具有面向连接的特点，在LSP建立起来之后，数据流将沿着固定的路径，通过标签交换到达目的地。如果针对这个LSP实施QoS，就有可能解决通过LSP的数据

流的QoS问题。按照这个思路，DiffServ/IntServ模型被运用到MPLS中。其中，MPLS同DiffServ结合，产生了MPLS DiffServ技术。MPLS同IntServ的结合，产生了流量工程(Traffic Engineer)技术。

这里我们重点阐述流量工程。流量工程关注网络整体性能的优化，其主要目标是方便地提供高效的、可靠的网络服务，优化网络资源的使用，优化网络流量。这分两个层面：一是面向流量的，即关注如何提高网络的服务质量；二是面向资源的，即关注如何优化网络资源的使用，最主要是带宽资源的有效利用。

MPLS与流量工程相结合的技术--MPLS TE应运而生。 MPLS TE在解决网络拥塞问题是有着自己的优势。运营商可以精确地控制流量流经的路径，从而可以避开拥塞的节点，解决那种一部分路径过载，另一部分路径空闲的问题，使现有的带宽资源充分利用起来。通过MPLS TE，可为用户创建具有带宽保证的隧道，但如果在隧道中同时传送EF、AF及BE业务时，业务之间会相互干扰，也就是说MPLS TE存在一个严重的问题——MPLS TE隧道不能够感知业务类型。为此，2002年业界提出了一种MPLS DiffServ-Aware TE 的解决方案。

MPLS DS-TE能够结合差分服务与流量工程的优点，能够对不同类的流进行不同带宽的带宽约束，并且根据该流的带宽约束动态调节流量，是解决骨干网QoS的有效技术。

二、VPN QoS模型

VPN用户需要的是一种端到端的QOS保证，由于VPN流量跨越了用户网络和运营商网络，与普通QoS实施方法不同，VPN的QoS保证需要分解为两个层次。第一个层次是真正的端到端，保证用户流量的QoS。第二个层次是CE到CE，从运营商的角度来看，这是它能够负责和实施QoS策略的一部分网络。从用户的角度看，运营商网络是透明的。

这种分层使得端到端QoS问题分解为两个子问题，并且它们是独立的，分别由用户和运营商解决。运营网络的责任就是解决CE-CE间QoS保证，无需将问题复杂化。下面我们将就这个问题展开讨论。

回顾MPLS VPN模型，CE-CE间又分为三段，CE-PE、PE-PE和PE-CE。其中，CE-PE间的连接是物理链路或虚连接，目前有多种方法保证链路级的QoS，是一个已经解决的问题。而PE-PE之间的带宽被多个VPN所共享，如何解决这些VPN对带宽的竞争，并具备效率和扩展性，是目前面临的一个难题。

三、现有解决方案及缺陷

1、VPN + DiffServ方式

这种方式先在PE间建立E-LSP或L-LSP，VPN流量进入PE时，或者预先设置了优先级，或者由PE设置优先级，进入MPLS域后，根据优先级在每一跳上进行PHB处理。这种方式实现简单，但存在两个问题：

第一，每一跳上为某个优先级分配的资源是被多个业务流共享的，它们之间存在着竞争。由于IP流量具有突发性的特点，如果按照高峰流量分配带宽，存在极大的资源浪费，如果按照平均流量分配带宽，则无法避免某个业务流在拥塞时发生的丢包；

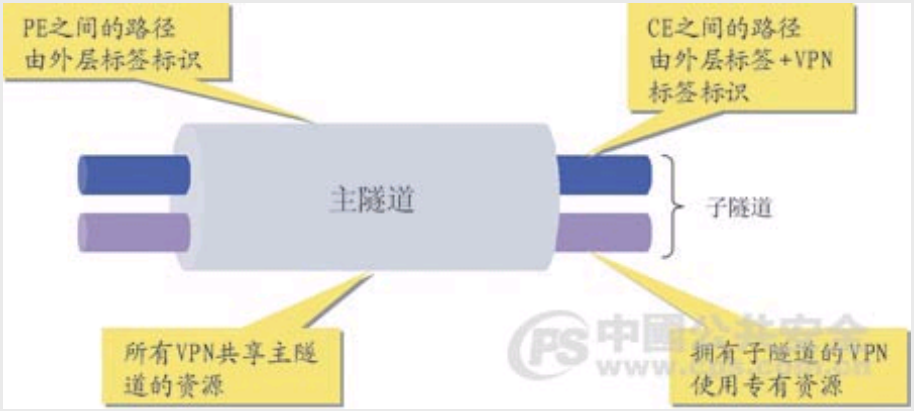
第二，业务流经过多个链路，虽然这些链路上都为优先级分配了带宽，但可能存在不匹配的情况，有些链路带宽是足够的，而有些链路可能不够，这就无法保证端到端的QoS。

2、CCC方式

CCC是Cross Connect Circuit的缩写，是通过静态配置方式实现CE-CE间虚连接的一种方式。由于CCC是专用的，包括PE-PE间的LSP及两端的PE-CE链路，因此保证了端到端的带宽。这种方式的缺点是扩展性差，由于没有采用隧道复用技术，LSP的数目与CE的平方成正比，在骨干网中需要大量的LSP。CE和PE的初始配置复杂，添加、删除和更改CE和PE时，所需的配置工作也很复杂。因此，CCC方式只适用于小数量的个别私有连接。

综上所述，目前的技术在解决VPN QoS时，仍然存在种种不足。一些显而易见的方式不具备实际的可能性，在QoS保证、效率和扩展性之间难以取得平衡，如DiffServ方案，扩展性好，但带宽利用率低，QoS保证能力差。而CCC方案QoS保证能力强，通过流量工程能提高网络资源利用率，但扩展性差，为解决问题，需要新的思路。

四、VPN-Aware TE方案



1、VPN-Aware TE方案探讨

TE可使网络的流量与网络拓朴匹配，达到提高网络资源利用率的目的。在简单的应用方式下，可根据用户需求（显示路由、带宽等）和网络的资源情况，通过RSVP-TE或CR-LDP信令建立一条跨越骨干网的从LER到LER的隧道，并完成隧道的维护、统计、属性修改（如带宽）和备份等功能。在LER与LER设备之间，可以认为通过一个隧道直连，该隧道具有严格的QoS保证，能自适应网络的拓朴，并可通过备份LSP、快速重路由等方式进行额外保护。采用TE隧道保证VPN带宽，是一种较为理想的方案。但前面已经分析，为每一对CE-CE间使用专用TE隧道的方案无法大规模部署。因此，应当通过隧道复用技术来解决这个问题。

在MPLS VPN中，多个VPN复用PE-PE间的LSP，采用TE技术建立这样的LSP，其带宽被多个VPN共享，各VPN竞争资源时必将导致QoS的下降。此时，需要引入一种机制来解决这种竞争，这种方法就是由TE隧道根据VPN对带宽的需求进行调整，这种方式又称为VPN-Aware TE。

首先，我们要解决TE隧道既共享又竞争的关系，我们可以通过CAR来解决这个问题。运营商在向VPN用户提供服务时，要和用户签订相关的QoS服务协议，运营商在接入一个VPN用户的业务时，我们可以实现确定这个VPN用户的业务类型和对应的带宽要求，那么我们将VPN用户的业务和某个TE隧道导入时，必须确保用户的流量不会超过预知的带宽，因此必须在TE隧道的入口对VPN流量作CAR来做带宽限制。实施了这样的限制后，就好像在CE-CE间建立了一个有QoS保证的子隧道，而这个子隧道是嵌套在外层的TE隧道中的，并且外层隧道的总带宽是各个子隧道带宽之和。这样就以一种高效率的方式解决了共享情况下的带宽保证的要求，CE-CE间获得了虚拟的专用带宽。

其次，我们要解决一个VPN有多种QoS需求的问题。在这里可以借鉴一下DiffServ模型中对QoS的解决办法。在我们上面对VPN中的QoS需求分析中，我们提到，现在用户的VPN业务主要可以分为以下几类： 视频和语音业务、关键的数据业务、普通的上网业务。上面的几种业务类型正好对应于DiffServ模型中的EF,AF,BE三种业务，或许用户还有其他的特殊业务类型。总之，我们可以把用户的业务类型分为有限的几种业务，那么我们可以在两个PE设备之间创建几条隧道。其中每一条隧道对应了一种VPN用户的业务类型。这样可以让两个PE之间凡是业务类型相同的两方面VPN用户的业务走一条相同的业务类型的隧道。这样可以保证几种不同类型业务之间不会有资源抢占问题。比如FTP流量不会影响到语音的时延和抖动。如果由于新增的VPN用户或是用户对带宽的需求增加了，那我们可以通过动态调整一条TE隧道的带宽，或是另外创建一条新的TE隧道来接纳VPN用户的业务。

上面提到VPN用户的不同业务被选择导入到不同的隧道，隧道有一个总的带宽保证，再对用户的每一种业务做一次带宽保证。下面我们要说明的是怎么把用户的业务根据需要分类来自动的导入到对应的TE隧道，以及TE隧道带宽根据业务流量大小自动调整过程。

在PE设备上对于收到的VPN用户的流量做自动的分类，我们可以借助MPLS VPN的路由上的属性，因为路由本身有很多可以标识网络拓朴和业务分类的属性，比如通过MPLS VPN路由我们可以区分一个路由的VPN属性，可以根据一个VPN路由的下一跳属性来确定业务是到达哪个PE的，这样就可以在两个PE之间做隧道选择，更深入的业务细分，VPN用户在两个PE之间的业务可以进一步细分，比如两点之间可能有数据业务，也有语音业务等，对于这样的业务可以进一步细分化。也可以根据VPN用户网络拓朴的分布，可以通过配置相同团体属性的方法，进行拓朴分布区分，这样在入端PE就可以根据路由的团体属性等做业务区分。

可以看出通过上面的这些路由属性做业务分类，灵活性要比根据报文的五元组做业务分类要方便很多，而且是可以动态生成的。相比较，根据路由属性来分类更容易体现用户整网的业务细分化。根据路由相关属性我们可以做到以下细分化：

a. 区分不同的VPN的业务

b. 区分一个VPN内到达不同PE的业务

c. 区分一个VPN内到达同一个PE的不同业务

d. 根据团体属性可以根据VPN用户的网络拓朴分布细分业务。

通过这些业务细分，我们可以制定每种细分业务的带宽和流类型，比如10M的EF流，10M AF流，10M BE流等。这样就可以和具体的TE隧道结合起来。

以上这些都是根据路由的细分策略，在应用上，我们可以将这些细分规则和路由的策略属性结合起来，把这些规则应用到路由策略中，比如收到一条路由后，根据路由的属性最终确定业务的类型和带宽要求。在这里就需要和PE之间的TE隧道带宽资源结合起来了，我们确定了业务的类型和带宽要求后，就需要分别向两个PE之间的TE隧道申请资源，比如申请10M的EF流资源。如果两个PE之间已经存在对应的TE隧道，且带宽有剩余，就可以直接获得资源，并把这个TE隧道的总的带宽资源减去刚分配的部分。因为当以后用户不需要这部分资源的时候，又需要把这部分的资源释放回TE隧道。如果两个PE之间没有需要的资源，那就需要动态触发调整两个PE之间的某种业务类型的隧道的带宽大小，或是另外再创建一条相同业务类型的TE隧道。

用户的业务向一条TE隧道申请了带宽以后，要确保自己的流量不能超过已经申请的带宽，因为如果超高就会影响到其他用户的业务。因此我们需要根据用户申请的带宽资源来做流量限制，如果所在的TE隧道的总的带宽资源过剩的话，可以让用户的流量有部分的突发。为了实现这一点，在实施CAR的时候，设定约定速率和突发速率，对于超过约定速率的流量，不是简单的丢弃，而是降低优先级继续转发，只有超越突发速率的流量，才全部丢弃。

2、工作过程

根据上面的VPN和TE的结合，把路由的属性融入到用户的业务分类当中，作为资源预留的条件，在这里也可以同时和根据IP报文的五元组的分类策略相结合，可以达到整网的QOS的动态部署和调整。

工作过程如下：

1.PE-PE间建立若干个TE隧道，每个隧道对应一类业务，具有初始的带宽；

2.建立VPN，这个VPN是用PE-PE间的TE隧道来承载业务；

3.在入口PE上设置针对细分的VPN流量的QoS参数，包括识别这个流量的规则、约定速率、突发速率、优先级等；

4.VPN路由从出口PE传播到入口PE，携带了Route-target、Nexthop、团体属性等路由属性；

5.入口PE根据配置好的分类规则对VPN路由进行过滤，为匹配到的路由生成特定的转发动作，如Remark、CAR等；

6.入口PE对VPN流量进行转发处理，匹配了路由规则的报文实施QoS，如Remark、CAR；

7.VPN流量的QoS参数被修改，重复5-6步动作。

通过以上理论分析，得出TE和VPN相结合，是现阶段解决VPN网络的QOS问题的最佳的手段。后来在广东移动MDCN网(全省多业务承载平台)上的实际部署，经实际运行和测试得出结论，将MPLS TE结合VPN的路由属性很好的调整了MPLS VPN网络整网的QOS，能方便、高质量、高效率的满足VPN用户的QOS要求。

采用VPN组建城市监控网络，可有效的整合城市原有的监控资源，形成统一的规划和技术协调，实现网络信息资源共享，满足了各级公安机关远程图像资源共享和诸警种跨区域图像共享的要求，形成面向公安实战的综合应用系统集成平台，充分发挥技术防范在城市社会治安管理中作用，并以城市为基础，逐步城市之间联网，全省联网乃至最后实现全国联网。

注：
本文版权归中国公共安全杂志社和中国公共安全网所有 任何媒体或个人未经书面授权严禁部分或全文转载， 违者将严厉追究法律责任。

市 场 版

综 合 版

主管　中华人民共和国公安部
2000—2005©中国公共安全杂志社　版权所有
电话：+86-755-88309125 27035172　传真：+86-755-88309166　QQ：2925872
地址：深圳市深南大道6025号英龙大厦四楼　邮编：518040

ICP证：粤B2-20070271
欢迎行业媒体及展会合作