QoS VPN IP协议 服务质量 ⑧

计算机科学2000Vol. 27№. 11

Internet网

基于 IP VPN 的 QoS 实现技术

Implementation Technology on QoS Based on IP-VPN

张 虹 李 冬 TP393.4 TP393.01

32-35 (中国矿业大学计算机科学与技术系 徐州221008)

Abstract This article analyzes QoS's guarateed mechanisms of main VPN's networks flat and some QoS'typical solutions,to table a proposal on QoS implementation technology based on IP VPN.

Keywords VPN,IP,QoS,Tunneling technology

1 引言

虚拟网络(Virtual Private Net,VPN),是一种基于交换技术的网络。以公用开放的网络(如 IP 网、FR 网、ATM 网等)作为基本传输媒介,利用隧道技术将物理位置独立、分散的 LAN 逻辑地连接在一起,其本质是把同构或异构网络的物理拓扑结构抽象成逻辑视图,通过上层协议附加的多种技术,向最终用户提供类似于专用网络性能的网络服务技术。比较典型的构建 VPN 的网络平台是基于 IP(v4)的 Internet。

随着 Internet 上业务量的不断增长,越来越多的服务网络系统涌现出来,这些发展使得 IP(v4)本身的缺点也日益变得明显起来,其中最为突出的是 IP(v4)对于时间要求颇高的数据包(如视频、音频数据包)和一般性的类属数据包(如文件传送、电子邮件等数据包)的处理并不加以区分。这种等同对待的处理方式使得网络管理和带宽分配问题成为网络管理员最关切的难题,其所导致的后果不仅仅是阻塞通道,还要丢失数据。特别是对于连贯性和时间性要求很高的视频和音频数据来说,数据丢失将是一个致命的问题。通常的解决办法是在 TCP/IP 中要求对数据包进行重新发送。特别是当系统处于由数据分类和路由器引起的延迟状态时,服务中止极易引起整个系统的瘫痪。

QoS(Quality of Service)能够解决这个难题。QoS 可以对数据包进行合理的排队,对含有内容标识的数据包进行优化,并对其中特定的数据包赋以较高的优先级,从而加速传输的进程,并实现实时交互。QoS 能够保证传输质量,使数据包不仅要到达欲传输的目的地址,而且要保证数据包的顺序性、完整性和实时性。通过 QoS,网络可以按照业务量的类型或级别加以区分,并能够依次对各级别进行处理。

企业内部网与 Internet 和 IP 技术的成功使得对 IP VPN 的需求逐渐增长,同时 IP VPN 也是数据寄存、网络商务和电话业务这些增值业务的基础。IP VPN 目前已被人们广泛关注,引发了诸多讨论与疑问,特别是关于 IP VPN 的 QoS 机制问题。QoS 问题主要包括信息传输的实时性和信息丢失的管理与控制等问题。在 IP VPN 网络中,由于不同用户可能有不同的传输要求,因此,要保证信息传输的实时性和丢失的综合要求是网络传输控制的一个重要问题。本文针对 IP VPN 的 QoS 机制,讨论了基于 IP-VPN 的 QoS 解决方案,提出了基于 IP-VPN 的 QoS 实现技术。

2 IP VPN 网络平台的 QoS 实施机制

2.1 QoS 概念

服务质量 QoS 是以不同的网络技术为基础,应用端到端的策略,为具有不同 QoS 的应用业务对网络的带宽、延迟、抖动、传输费用、包丢失的优先级、业务优先级等复杂的需求提供服务的能力。因此,QoS 是一种合理分配交换机和路由器资源,使数据快速、连续且可靠地到达目的地的方法。QoS 的最终目标不仅要保障数据包准确到达目的地址,而且要保障它的顺序性、完整性和实时性。QoS 有三种不同层次的端到端类型(按照 DifferServ 标准):尽力(Best Effort)型、区别型和保障型。尽力型服务是一种没有任何 QoS 保证的基本连接,它可以最大限度地利用带宽,Internet 是尽力服务的典型实例;区别型服务是根据服务级别协定(SLA)在网络输入端检测业务特性并赋于一定服务级别。路由将根据 SLA 采取相应的 QoS 保障机制;保障服务型是专门为某个应用保留一定的带宽,使用相应排队规则保留缓冲区空间,可保证特定流量获得特定 QoS 水平。保障型业务由 IETF 的 INTSERV 工作组定义,

张 虹 副教授,主要从事多媒体网络技术、图像压缩技术和软件工程等教学与科研工作。

为用户提供明确的、严格的、端到端的质量保证。目前IETF定义了两种保障型业务：控制负载业务和保证质量业务。

2.2 IP VPN网络平台的QoS实施机制

2.2.1 ATM ATM的核心技术之一是针对不同业务提供不同的QoS，它具有严格完善的QoS支持保障体系，通过在其业务属性中定义CBR（恒定比特率的比特流）、rt-VBR（实时可变比特率的比特流）、nrt-VBR（非实时可变比特率的比特流）、UBR（非限定比特率的比特流）、ABR（可用比特率的比特流）五种业务量类型（在VC或VP内）来实现QoS。

2.2.2 IP 基于IP(v4)的路由网络由于缺乏对QoS的支持，所以在IP网络中完全实现QoS基本上是不可能的，一般应用图1模型构造在IP层实现QoS方案。

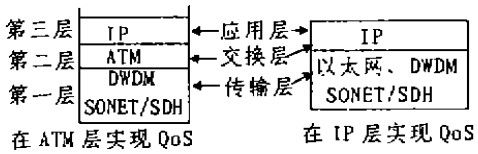

图1 IP承载QoS层次图

2.2.3 FR FR通过三个带宽控制参数：Bc（网络允许用户在Tc时间传送的数据量）、Be（网络允许用户在Tc时间传送的超过Bc的数据量）和CIR（网络与用户约定的用户信息传送速率）为部分端到端的连接提供QoS。

3 IP VPN的QoS解决方案

3.1 基于IP交换和标记交换MPLS

MPLS（Multi-Procotol Label Switching）融合了ATM与IP两种技术，满足宽带分配和QoS的一种WAN解决方案。MPLS工作组已经把在FR、ATM、PPP链路、IEEE802.3 LAN上使用的标记标准化，其技术实质是把第三层的业务映射、加载到面向连接的第二层上完成，其交换操作原理如图2所示。在MPLS网络的边缘，把每一个IP业务组封装在新的32位路由头标记中，并加上包含下一跳（hop）路径的标记。此时，IP业务组的MPLS标记和表示QoS级别的MPLS三位实验位都将在进入MPLS网络时决定。MPLS的LSR（Label Switching Router）将通过LDP（Label Distribution Procotol）通知其他路由器。MPLS自始至终查看这些标记信息，而不使用包的IP头，将这些有标记的包交换至其目的地。由于标记处理减少了对IP数据的依赖性，路由处理和网络的等待时间减少，而使网络的伸缩性随之增加。

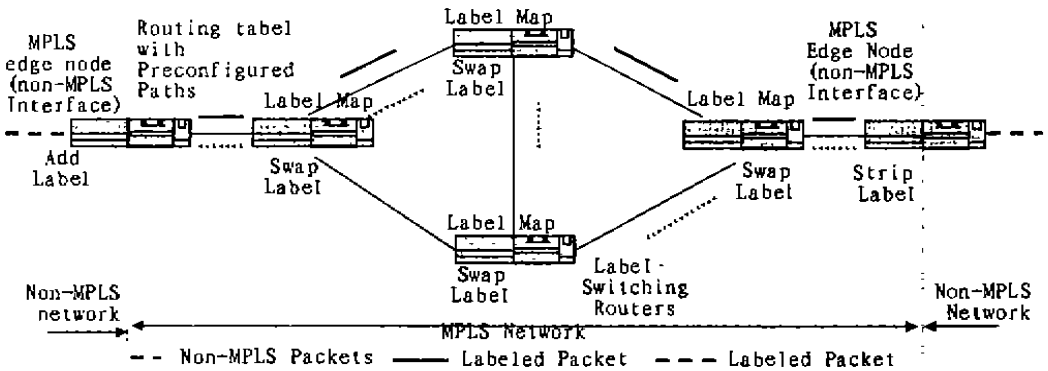

图2 MPLS工作原理

使用MPLS可将现有的路由协议建立到终点网路的连接，LDP完成标签到终身网路的映射，输入端标签边缘路由器接收到分组，完成第三层功能，并给分组贴上标签，支持标记交换机的交换机对带有标签的业务分组进行交换。在输出端的MPLS边缘路由器中去掉标签，并将分组传送给终端用户。

MPLS集成了交换和路由，简化了核心路由功能，提高了IP路由的效率，促进了网络链路间的负荷平衡，满足了带宽分配和QoS需求。典型的应用是Cisco针对QoS需求不同的Intranet VPN、Extranet VPN，应用MPLS构建的VPN解决方案。其特点是基于工业标准、具有IP QoS保证、WAN带宽优化时省却了PVC配置等。

3.2 DiffServ

DiffServ（Differentiated Services）是IEFT针对WAN提供QoS开发的标准，它使用IP(v4)分组头标记中的ToS（Type of Service）8-bit字段（又称DS字节）来携带IP业务需求信息，类似于ATM中的交通

类别和合同信息等内容。其结构如图3所示。

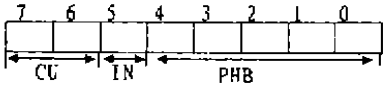

图3 DS 字节结构图

PHB(Per-Hop Behavior)为逐跳特性字段，是路由器选择特定的分组路径处理机制，为 DiffSer 网络提供常规 IP 网络业务和 QoS 保证业务。例如：当 PHB=00000(默认模式)时，业务处理按 FIFO 队列顺序(队列实际上只是路由器或交换机中的一块内存区，被设置用来保存不同优先级的 IP 包)，与常规 IP 的"Best Effort"策略一致。当 PHB=11100时，业务处理将获得较快的速度，QoS 保障在一定范围内，与区别型 QoS 保证策略一致。

IN 为表征共享路由器资源(如队列)等如何和特定的 PHB 字段相关联的档案位，其本质是标记 DiffServ 网络边缘的业务申请是否和合同业务相同。当 IN=1时，此类业务分组与队列中合同业务类型相同，相反则 IN=0时，类型不同，则此类业务分组将在发生拥塞时被丢弃。

CU 为保留未用，现置00，路由器将不做任何处理。

由于 DiffServ 工作在第三层上，无须过多考虑支撑网络的协议。其应用主要在业务接入点，依靠位于边缘的应用业务分析路由器，确定业务 QoS 需求和对链路的申请，而不必对第二层作任何调整。

IEFT DiffServ 借用 ATM 的 QoS 概念，在第三层实现了跨越主干的 QoS，增加了新的拥塞管理机制和对动态 QoS 的支持，使网络在同一基础设施支持不同的 QoS 得以实现。另外基于 DiffServ 的方案在升级时，只要在网络接入点增加软硬件就可轻易实现，是一种简便有效的 Internet QoS 解决方案。而且标签技术和 QoS 参数格式适用于整个 WAN。

3.3 端到端的 QoS

针对不同的网络端到端的 QoS 主要有三种不同的技术实现：面向 LAN 的 IEEE 802.1d、面向 IP-Internet 的 IEFT DiffServ 和面向 ATM 的交通合同(Traffic Contracts)协议。实现基于 IP-Internet 的 VPN 完全的端到端 QoS，WAN 的 QoS 机制则要与基于 LAN 的 QoS 机制相结合。实现时使边缘路由器接收不同应用的 QoS 请求，完成 QoS 的分类、归档、集成，并把使用资源预留协议(RSVP)和802.1p 链路层协议描述的、基于 IP LAN 的 QoS 应用映射为跨越 WAN 的(DiffServ)PHB。

4 IP VPN 的 QoS 实现技术

4.1 IP 包分类

把对具有不同 QoS 需求的 IP 包利用802.1p 设置成具有不同优先级(QoS)组，形成规模相异的单流或子流，通过路由器或交换机快速传送时，不同的 QoS 流将采取不同的策略(优先传送、等待、丢弃)。分类一般依据 IP 包报头的某些内容，包括 L2、L3、或 L4报头中的信息、IP 地址、TCP/UDP 端口号、IP 包的优先顺序、URL 和子 URL、信息包中的净负荷中的信息、应用以及时间等。

QoS 的标记体系在特征上可分为隐式和显式两种。隐式是网络设备(如路由器、交换机等)自动根据既定规则，如应用类型、协议等分配服务等级。几乎所有的路由器和部分交换机支持隐式 QoS，但目前隐式 QoS 只能提供有限的优先级功能。例如，交换机可以根据 VLAN 的类型、时间、源地址、目的地址进行优先级排队，但不能对更高层次的信息，如应用或协议类型提供优先级。只有基于策略的网络系统才会使交换和路由设备具有更强大的优先级功能。显式 QoS 使 IP 包得到特定优先级的服务，网络设备将尽力满足该服务请求。IP 优先级(IP Precedence)，即所谓的 IP 服务类型(IP Type Of Service，TOS)将成为最广泛应用的显式 QoS 技术。

4.2 带宽管理

在包被赋予一定的 CoS 后，队列以及队列算法将被用来提供合适的或需要的 QoS。队列算法决定保存在队列中的包的发送顺序。其原则是在向高优先级的流提供更好的服务的同时，确保较低优先级的包也能获得一定的服务。如果网络发生拥塞，队列系统不能保证关键数据及时到达目的地，它只能保证高优先级包先于低优先级包到达目的地。更复杂的 QoS 系统将利用带宽预留协议解决这一问题。该系统将预先约定的带宽数分配给不同的队列或队列组，保证高优先级队列总有可用的带宽。除了队列所需带宽超出了预留带宽的情况，QoS 都将得到保证。如果超出预留带宽情况发生，队列算法将从低优先级队列中划取带宽分配给高优先级队列。

队列控制有基于流的 WFQ(Weighted Fair Queuing)和基于类的 WFQ。基于流的 WFQ 是将包按照流分类，每个流对应单独的输出队列。当一个包被分配到某个流，它就在这个流的队列里排队，当拥塞发生时，WFQ 将可用的带宽分配给每个激活的队列。

基于类的 WFQ 的目的是用 WFQ 机制使用户通过 ACLS 等机制创建的类，然后为每个类分配部分输出带宽。两者的根本区别在于，基于流的带宽分配机制

与其他流相关，而基于类的带宽分配是绝对的，允许某类流量占有固定的带宽。

4.3 IP 包整形

IP 包整形是一种处理和修改数据、以保证 QoS 的技术，如 IP 包分段。ATM 网络提供高 QoS 的原因之一是它采用了短包或信元。任何信元可以被延时的最大限量是传输一个信元所需的时间。Cisco 公司的 12000系列路由器内部将骨干网传输的包分割成64字节长度的包，这样有助于在路由器内保证持续的 QoS。一些 FR 厂商在 WAN 链路上将传输的包进行分割，以此作为保证可预测提交和最小时延的手段。

传输流测量是传输流整形的另一种形式。传输流测量功能是暂时将包存储在缓冲区中，在传输前为包串留出空间，确保网络不出现过载。另外，传输流测量还用于网络边缘以减少突发事件。

4.4 避免拥塞

4.4.1 *拥塞管理* 在网络中的复用点上处理拥塞，包括如何对流量进行排序，让拥塞接口为一个流或一组聚集流提供适当 QoS。通常，拥塞管理可使用几种排队机制。流量整形也可被看作一种拥塞管理机制，这将由网络中的特定应用而定。

4.4.2 *拥塞避免* 拥塞避免(即丢弃/流量控制)是网络为避免拥塞发生采取的行动。拥塞是指在网络中的某些点上、由于流量过载、单个流或聚集流不能享受相应服务的情况。拥塞避免行动可通过多种方法实现，如建设性的丢弃政策应用，为主机系统提供隐含反馈信息或当拥塞发生时可减少网络流量等。

拥塞控制与避免机制是 QoS 另一个重要方面。拥塞控制使终点站在网络发生掉包时降低传输流速度。几年前，TCP/IP 和 SNA 就开始支持拥塞控制。

随机早期检测(RED，Random Early Detection)技术是作为标准的拥塞避免方法问世的。基本作法是每当队列满时，RED 就随机地丢弃一些包或设置拥塞标识，并提前通知各 TCP 连接降低数据包发送率。其实现技术是由路由器把平均队列长度和两个高、低门限比较。当平均队列长度小于低门限时，路由器不丢弃任何数据包或在数据包报头设置拥塞标识。当平均队列长度大于高门限时，路由器在每个数据包报头设置拥塞标号。若平均队列长度在高、低门限之间，路由器以概率 Pa 在每个新到达 IP 包报头设置拥塞标识。这样，RED 路由器可维持一个相对短的平均排队长度，以减少数据包排队时延，同时按各连接数据包到达速率成比例地丢弃数据包，可保证一定的公平性和防止所有连接同步地降低吞吐量。

例如 Cisco 的 IOS 实现了基于 RED 的 WRED(加权 RED)机制，它通过给每个队列加上表示发生丢包现象的阈值，对多达6个不同流量提供不同的处理方式，当发生拥塞时，WRED 的处理方式是先丢弃优先级低的流量中的包，然后再丢弃优先级高的流量中的包。

4.5 隧道支持

隧道(Tunneling)技术是 VPN 的核心技术，目前支持隧道技术的有关协议有 PPTP、L2TP、L2F 和 Ipsec。隧道协议采取的方法是将用户的整个数据包，包括附加的协议信息，作为网络的净荷(PayLoad)部分封装后再进行传输。隧道是利用 GRE 建立的。不论何种支持 QoS 隧道，其 QoS 的信息应该从 IP 包头反映到隧道封装后的包头中。这样，不同的 QoS 业务分组在通过支持隧道的网络设备时，QoS 才能得到保障。

小结 随着 Internet 的广泛应用，IP(v4)本身的缺陷也日益明显，在 IP(v6)没有广泛应用之前，利用 MPLS、DiffServ 等标准借鉴或移植 ATM 完善的 QoS 体系，将 QoS 引入 IP，加上业已成熟的基于 LAN 的 QoS 保证，给基于 IP-Internet VPN 的用户提供端到端的服务体系架构。QoS 的实现不仅需要一定的国际标准，更需要网络设备，例如交换机、路由器等对 QoS 特性的支持，新特性包括多个方面，每个方面都要通过新的技术实现，这样就确保了不同业务质量需求的全面实现。QoS 目前也面临着挑战，即网络中不同的 QoS 在一个公共的 QoS 体系下加以规制和运作，因此，还需要制定一个标准的 QoS 标准。

参 考 文 献

1 Dixit S. Service and Network Interworking in a WAN Environment. IEEE Communications Magazine, 1996(June)
2 Maufer T A. What Everyone Needs to Know About Addressing &Routing, Prentice Hall PTR. 北京：机械工业出版社，2000. 159～177，275～280
3 Metz C Y. IP Switching Protocols and Architectures. The McGraw Hill Companies Inc. 北京：机械工业出版社，1999. 28～41，52～59，214～221
4 Draft Standard P802.1Q IEEE Standards for Local and Metropolitan Area Networks Virtual Bridged Local Area Networks. December 1997
5 Blake S，et al. A Framework for Differentiated Service ftp：// ftp. ietf. org/internet-drafts/draftietf-diffserv-framework-01. txt
6 IEFT Working Group on Differentiated Service. Available at，http. // www. ieft. org/html. charters/diffe charter. html
7 Blake S，et al. An Architecture for Differentiated Service [OL]. ftp：// ftp. ietf. org/internet-drafts/draft-ietf-diffsev-arch-02. txt，1998-10
8 Hamzeh K，Pall G S. Point-to-Point Tunneling Protocol Draft-ietf-pppext-pptp-04 txt，1998
9 Valencia A，Hamzech K，Rubens A. Layer Two Tunneling Protocol-L2TP，Draft-ietf pppext-12tp-11. txt，1998
10 赵慧玲，张国宏，等. ATM、帧中继、IP 技术与应用. 北京：电子工业出版社，1998. 8
11 Cisco 公司. 支持 QoS 的产品技术资料
12 金宇航 Internet 的 QoS 选择. 中国计算机报，第62期，B10版
13 赵信. 将 QoS 引入 IP-在 WAN 上提供质量服务. 计算机世界，1999-11-22，D18版
14 李冬. 虚拟网络的构建研究.[硕士学位论文]. 中国矿业大学，徐州，2000