

IP网络 QoS ATM Internet 路由器

IP 网络中的 QoS 策略控制技术

The QoS Policy Control in IP Networks

76-80

洪佩琳 刘晓湘 杨凯峰 李津生 TP393

(中国科技大学电子工程与信息科学系 合肥 230027)

Abstract It is necessary to provide Quality of Service(QoS)with the continuous growing of the multi-media traffic in the Internet. In this paper,we analyze several QoS models,describe that why the QoS should be policy control in the Internet,present the detail realization scheme of QoS policy control.

Keywords QoS,Policy control,Differentiated service

一.引言

随着 Internet 规模的不断扩大,IP 网上的实时业务量也在不断增长,由于实时业务对网络传输的延时、延时抖动等特性较为敏感,当突发性高的 FTP 或含有图像文件的 HTTP 等业务量在网络上传输时,实时业务会受到影响,因此应在 IP 网络上导入 QoS 技术,以确保实时业务的通信质量。

最初,QoS 是与 ATM 技术紧密相连的,随着 IP 网络上实时业务的增多,人们开始研究 IP 网络上的 QoS 技术。早期的许多工作都源于资源预留协议(RSVP, Resource Reservation Protocol),但是由于 RSVP 的实现比较复杂,用户在通信前必须通过信令在收发两端沿途各转发节点上进行资源预留,也就是说,沿途各节点上的路由器都要支持 RSVP 协议。这种实现方法既加重了路由器的处理负担,又会增加网络的数据量,因此没能得到普及。

近两年来,随着 IP 电话、可视电话、远程教学等多

媒体实时业务的开发和普及,对 IP 网上的服务质量的要求更加迫切,并相继提出了各种与 QoS 有关的技术,IETF 还成立了区分服务(Diff-serv)工作组,专门从事区分服务的标准化工作。一些大的通信厂商也联合成立了 QoS 论坛,协商各种 QoS 技术标准的实施方案。

二、多种多样的 QoS 技术

1. 按层次对 QoS 技术分类

广义地讲 QoS 技术的种类有很多,由于处理的层次及采用的技术不同,其效果也不一样。如图1所示,从物理层到应用层,QoS 利用了各式各样的技术,每一层都试图通过对业务流的适当控制来改善或保证通信质量。

物理层中按业务量分配固定带宽的 TDM(时分复用),虽然能够严格保证 QoS,但往往不称其为 QoS 技术;在 ATM 网络中,各种业务流可分成四种不同的业务类型,终端在通信前首先要建立连接,网络根据用户

2 Diks K, Pele A. Broadcasting with Universal Lists. Networks, 1996, 27(3): 183~196

3 Koren I. A reconfigurable and fault-tolerant VLSI multi-processor array. In: Proc. 8th Int. Symp. Comput. Architecture. Minneapolis, MN, May 1981. 425~442

4 Chung F R K, et al. DIOGENES: A methodology for designing fault-tolerant VLSI processor arrays. In: Proc. 13th Fault-Tolerant Comput. Symp. June 1983. 25~32

5 Samu M, Stefanelth R. Reconfigurable architectures for VLSI implementation. In: Proc. Nar. Comput. Conf. May 1983. 565~577

6 Hedlund K S, Snyder L. Water-scale integration of configurable highly parallel processor. In: Proc. Int. Parallel Processing Conf. Aug. 1982. 262~264

7 Snyder L. Introduction to the configurable, highly parallel computer. Computer, 1982, 15(1): 47~56

8 Pease M C. The indirect binary n-cube microprocessor array. IEEE Trans. on Comput, 1977, C-26(5): 458~473

9 Atallah M J, Kosaraju S R. A generalized dictionary machine for VLSI. IEEE Trans. on Comput, 1985, C-34(2): 151~155

10 Stone H S. Parallel processing with the perfect shuffle. IEEE Trans. on Comput, 1971, C-20(2): 153~161

11 Preparata E P, Vuillemin J. The cube-connected cycles: A versatile network for parallel computation. Commun. ACM, 1981, 24(5): 300~309

12 Nian-Feng Tzeng. A cube-connected cycles architecture with High reliability and Improved Performance. IEEE Trans. on Comput. , 1993, 42(2): 246~253

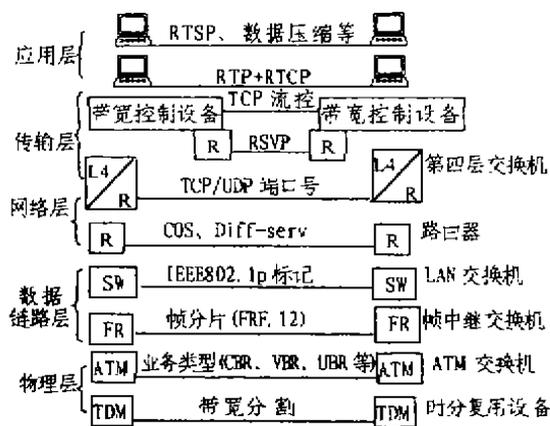


图1 QoS控制技术在不同层上采用不同的方式

所申请的带宽等参数对业务量进行QoS控制,以确保通信质量;链路层及网络层实现QoS是通过通过对帧或分组进行优先级的处理来保证服务质量的,也就是说,按优先级将各个帧或分组分成多个队列,减少特定业务量的时延并吸收延时抖动;有时还象帧中继中的报片化(fragment)那样,将长数据作截短处理来降低转发处理所带来的延时;传输层以上的QoS控制与网络层以下的技术不同,它与网络设备无关,传输层的TCP流控只在用户终端对发送速率进行适当的控制,以防止网络的拥塞和数据的丢失;在应用层通过各种数据压缩技术减少待传输的数据量,同时采用RTP/RTCP技术可对实时业务进行适当的控制,以保证实时多媒体业务的质量。

2. 按分组处理方式对QoS技术分类

除此之外,IETF还建议了数种保证QoS的方案,主要有:综合服务(Int-serv)/RSVP;区分服务;多协议标记交换MPLS;业务流量工程和基于约束的寻路。综合服务模型的主要特征就是资源预留,它使用RSVP作为信令协议来建立通道和进行资源预留。区分服务通过给分组打上不同的标记,把分组分成不同的类别,对不同类别的分组给予不同的服务。MPLS是一种转发方案。分组在进入MPLS域时被赋予一个标签,以后就根据这个标签对分组流进行分类、转发、服务。业务流量工程的目的是让网络上的业务流量更加均衡。基于约束的寻路要解决的是根据某些约束条件,如:带宽和延时要求,寻找一条合适的路径。

(1)保证型QoS技术 QoS技术分“保证型”和“尽力型”,保证型的QoS在终端双方通信之前先要建立连接,确保通信过程中的网络带宽。如ATM业务类型、IP网络中的RSVP。IETF称之为综合服务(Int-serv)。一旦连接建立,通信中所需的带宽就能保证,与连接相关的应答时间、时延要求也能保证。如果网络不能提供所需的带宽,它就会拒绝建立连接。因此,这种技术的线路利用率相对要低一些。

(2)尽力型QoS技术 另外,在非连接型通信中,常常使用的是一种不能确保带宽的尽力型QoS技术。例如,在IEEE 802.1p/Q的标记帧或IP分组头中的TOS域有3bit的优先级,供LAN交换机或路由器进行优先级控制,由于采用这种方法不能在通信中确保带宽,只是按优先级顺序进行交换或转发,因此也称为“COS(class of service)”,以区别能保证带宽的狭义QoS技术。这种方法的线路利用率高,但具体的效果难于预测。

IP优先级只支持8个不同的等级或类别,这对某些网络来说是不够的。网络上的业务量有的是实时多媒体业务,对延时有很高的要求,但却能容忍少量的分组丢失;有的对延时的要求不高,但却不能容忍分组的丢失,一旦丢失,必须重传,这又加重了网络的负担。因此不是简单地定义成高、中、低等级就能解决网络的QoS问题的。

三、区分服务

在区分服务中IETF重新定义了IPv4的TOS域,改称它为DS(区分服务)域。TOS域的3个优先级比特可定义8个优先级状态。IETF区分服务工作组提出将比特数扩展到6个,有64个可用的状态。这6个比特称为区分服务码点(DSCP),如图2所示。DSCP的比特位图

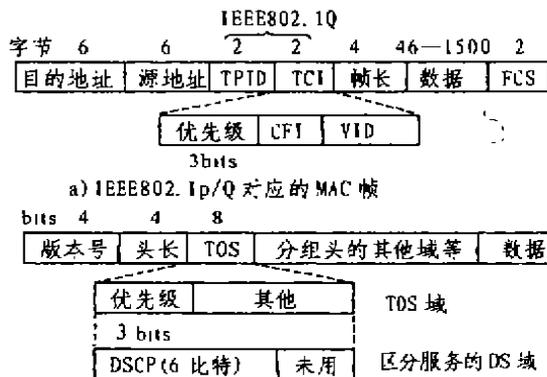


图2 带IEEE 802.1p/Q标记的MAC帧和IP分组头中的COS域与DS域

用来对应路由器的每一个转发处理(即每一个中继点行为 PHB, Per-Hop Behavior)。在网络的核心节点处, 路由器根据分组上的 DS 码点用相应的 PHB 对其进行转发。

区分服务是由综合服务发展而来的, 它采用了 IETF 的基于 RSVP 的服务分类标准, 抛弃了分组流沿路节点上的资源预留。区分服务将会有效地取代跨越大范围的 RSVP 的使用。区分服务区域的主要成员有: 核心路由器、边缘路由器、资源控制器(BB, Bandwidth Broker)。在区分服务中, 网络的边缘设备对每个分组进行分类、标记 DS 域, 用 DS 域来携带 IP 分组对服务的需求信息。在网络的核心节点上, 路由器根据分组头上的 DS 码点(Dcode Point)选择码点所对应的转发处理。资源控制器 BB 配置了管理规则, 为客户分配资源, 它可以通过服务级别协定 SLA 与客户进行相互协调以分享规定的带宽。

区分服务将 6 比特的码点空间分成 3 个部分: “xxxxx0”用于标准行为; “xxxxx11”用于本地实验; “xxxxx01”也可用作本地实验, 但当将来第一部分的码点耗尽时, 也可用于标准行为(这里的 x 为“1”或“0”)。为了与当前流行的 COS 服务兼容, 区分服务定义了码点“xxxx000”为等级选择器码点, 用这种码点标记的分组可接受由前 3 个比特决定的优先级服务。因此, 也可以说 COS 是区分服务定义的服务行为集中的一个子集。

总之, DS 域将决定路由器对分组的处理, 通过在

网络的边界对分组设置 DS 域以及接纳控制功能可以实现一系列的服务: 有保证的服务、高价服务(premium service)和尽力服务。有保证的服务是为那些即使在网络拥塞时也能够享受可靠服务的客户提供的; 高价服务的延时和延时抖动都很小, 主要是为那些峰值速率恒定的实时数据流提供的, 它适合于 IP 电话、视频会议或虚拟专用网中的虚拟租用线。区分服务是可以逐步推广、渐进采用的。不支持区分服务的路由器可简单地忽略分组的 DS 字段, 并以尽力服务或只考虑优先级的方式处理分组。

四、IP 网上 QoS 策略控制方法

不同的 QoS 技术将产生不同的服务质量。在一个 IP 网络上, 如果各转发节点采用的 QoS 技术不相同, 数据流的分类规则、优先级设置规则也各不相同, 那么对某一个应用来说, 它在每个节点上获得的服务质量也不相同, 这样, 既浪费网络资源, 又不能使用户获得好的服务质量。为了在 IP 网络上实现高效、统一的 QoS 技术, 解决 QoS 技术中存在的一系列问题, 3com、Cisco、Nortel 等通信设备制造商提出了策略服务的概念, 对网络上由企业、网络提供商提供的多数设备用一个统一的规则进行策略设置、运营、管理一体化, 实现统一的 QoS(图 3)。

“策略”这个词在网络上是一个广义的概念, 是指网络上设备选择的一系列服务规则, 并不具体地关注某一设备或接口, 而是关注用户将在网络上接受何种

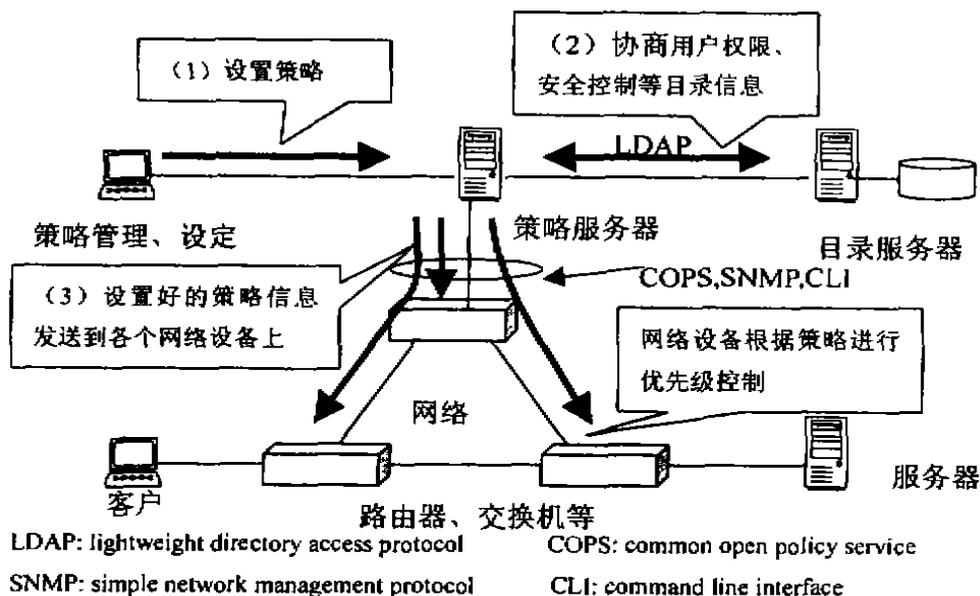


图3 策略网络的构成

服务。

在策略性网络中按四个策略规则决定网络的操作,它们是服务质量、安全、监控和配置。服务质量是根据业务的类型(如话音、图像等数据)决定业务的优先级,然后路由器或交换机再根据优先级进行处理,高优先级的业务先得到服务;安全是为了防止用户的权益受到非法侵犯,通常采用密码、身份认证、防火墙和加密来实现;监控是检测网络的设备和链路是否处于正常工作状态,一般与网络的管理有关;配置则是为网络设置工作方式。

构成策略服务的四个关键组成部分是:目录服务器、策略服务器、策略管理者和策略实施者。

目录服务器是用来存放网络状况和策略信息的数据库,用 LDAP(轻权目录访问协议)可以访问它;策略服务器的功能是根据收到的策略请求和事前收集的有关信息作出决策,并将决策回送给请求的发送者;策略管理者一般就是网络管理员,他可以配置策略,并将它们写入 LDAP 目录库中;策略的实施者就是网络的节点(路由器或交换机),它们可以在分组过滤、带宽预留、业务量分类、多转发队列等等中去实施策略。

对支持不同 QoS 的路由器或交换设备进行策略管理的核心技术就是目录服务器和策略服务器。可以说,目录服务器是 QoS 统一的基础,因为它集中了所有与 QoS 有关的状态及策略信息。在这里,网络管理员可以设定统一的标准,也可以灵活地修改这些信息。例如设定某一具体应用在某一时段的特定优先级等。

策略服务器相当于一个决策者以及决策的传递者,它与目录服务器之间是一种客户/服务器的模式,通过 LDAP 协议进行通信。策略服务器作为目录服务器的客户,访问目录服务器,并作出决策。同时,策略服务器又通过 COPS(公共开放策略服务)协议与支持不同 QoS 服务的路由器或交换设备(即策略服务器的客户)建立联系,它通过这种点到点的联系通知客户它所作出的决策。于是,在全网内实现了统一的服务质量控制策略。

目录服务器和策略服务器都是用软件实现,由网络管理员配置管理的。这样提供的 QoS 服务能更好地适应网络整体状况,更有效地利用网络资源。

五、QoS 策略服务的实现方案

在策略服务中,目录服务器和策略服务器是策略性网络的核心,在实际应用中,必须根据所管理的网络的情况来决定这两个服务器的具体实现方案。

1. 目录服务器(directory server)

目录服务器的主要目的就是网络的各种信息进行收集、综合以及更新。一个目录服务器可以是专门配

置的某个策略服务器,也可以是一个通用的目录服务器。一个目录服务器应该具有以下功能:

(1)网络目录数据库,在目录服务器中,设置一个数据库专门存放收集来的网络信息,此信息库的内容视策略服务器的需要而定,如果策略服务器根据业务等级制定策略,那么存放的信息内容就要包括业务编号、此类业务所需的资源、业务优先级等。对一个为策略服务器服务的目录服务器来说,除了上述的一般描述型的信息外,还要存放策略信息、网络现行资源使用信息等。

(2)信息的收集及对数据库的维护与刷新。如果只由管理员完成所有信息的收集和设置的话,工作量可能会很大,因为我们不但要了解网络设置的状况,还要监视网络资源的使用状况、业务状况,为了得到这些信息,可以通过 SNMP 或其他方式获取整个网络的设备分布、资源状况等信息(如路由器支持的优先级个数、业务类别数),形成自己的目录库。当数据库建立后,还要维护、定时刷新数据库。

(3)查询功能。可以根据收到的具体要求,利用关键字,对目录库进行检索,查找用户信息或策略信息。

(4)通信功能,通过 LDAP 协议与其它客户之间进行通信,因此目录服务器应该支持 LDAP。

2. 策略服务器(policy server)

在策略性网络中,为减轻网络管理员的负担,应通过策略服务器完成策略管理,配置一些路由器或交换设备的业务分类规则、业务等级或安全策略,并通过 COPS 协议下载给有关网络上的设备,策略服务器应该具有以下功能:

(1)信息检索。当收到策略请求后,策略服务器应该找到制定策略所需的信息,包括通过 LDAP 从目录服务器那里得到的信息和在本地高速缓存或数据库中存储的以前的一些决策信息。

(2)决策机制。根据得到的信息,策略服务器制定策略。策略信息可以存储在目录服务器中,也可以在本地有个策略数据库。一般来说,大多数策略还是应该存在目录服务器里,因为这便于管理与修改。不过本地也可以存储一些常用策略,这样就不必每次都向目录服务器查询了。

(3)决策传送。通过 COPS 协议规定的消息,将决策送回请求的客户。

(4)配置功能。策略服务器应该可以对刚建立联系的客户进行一些自动配置。

3. COPS 协议

COPS 是 IETF 为了统一 QoS 管理专门提出的一个新协议,迄今为止,它还只是草案,并没有形成一个标准。尽管如此,很多公司的产品中已经开始支持

COPS,并且采用了它所建议的客户/服务器模型。

策略服务器(也称为策略决策点,PDP)和它的客户(策略实施点,PEP)(即路由器、交换机等策略执行者)通过 COPS 来交换策略信息,该协议基于一种请求、应答的工作机制,能够适用于不同的客户类型,并支持不同 QoS 标准的客户。

在 COPS 的客户/服务器模式中,PEP 发送请求、更新和删除信息给 PDP,PDP 则返回决策信息。协议使用 TCP 作为传输层协议,因为在 PEP 与 PDP 间需要建立一种可靠连接,COPS 是可扩展的,支持多种客户信息并且无需对协议进行相应的修改,请求/应答状态对为 PEP 和 PDP 共享,即对于 PEP 发出的请求,在 PEP 自己删除之前,PDP 都应保存对这个请求的记忆。不同状态之间是有联系的,即 PDP 对本次新请求的决策应答和以前存储的状态有关,协议的一些状态可以为 PDP 所控制,以便于 PDP 向 PEP 发出一些配置信息,当不需要时,可以由 PDP 决定 PEP 的状态转移。

COPS 工作过程如下:(1)PDP 和 PEP 建立连接,PEP 提供自己的信息,完成 PEP 的初始化。(2)当 PEP 需要进行 QoS 服务时,向 PDP 请求策略,PDP 根据已有信息及这次请求中的包含信息,选择相应的决策传给 PEP,同时 PDP 保留这个策略的状态。(3)当不需要这次的策略时,由 PEP 自动向 PDP 提交删除策略状

态请求。如果在服务中间,PEP 想更改策略,就必需重新向 PDP 提交请求 PDP 完成重新决策和删除旧策略状态的操作。(4)在不需策略服务的时候,PEP 提交 close 请求,关闭连接。

4. LDAP 协议

LDAP 协议是对 OSI 的目录标准 X.500 中定义的目录访问协议 DAP 协议的简化,在 LDAP 协议里,主要定义了:(1)基于客户/服务器方式的协议运行模式;(2)数据模式,例如条目的属性值等;(3)与 X.500 的关系;(4)客户与服务器进行的操作和传送的消息格式以及描述方法,这些操作主要有建立连接(包括捆绑请求、应答)、查询、修改、添加、删除和关闭连接等等;(5)对编码技术和传送协议的要求;(6)对客户端和服务端的要求。

在实现过程中,首先要建立一个有关 QoS 技术和决策信息的数据库,再通过 LDAP 协议对它进行访问,实现策略服务器与目录服务器之间的通信。

结束语 为了解决 IP 网络中服务质量所存在的问题,3com、Cisco、Nortel 等大公司提出并研制了策略服务系统(见表1)。目前这些系统大都只支持管理各自企业的网络产品,但是只要策略服务标准化,不同厂商的策略服务系统就能管理其他厂商生产的网络产品。因此,网络的管理者或网络提供商(ISP)可以对网络用一定的规则进行策略设置,实现统一的 QoS。

表1 国外策略服务的主要产品

厂商名	3com	Cabletron systems	Cisco systems	Nortel networks
产品(推出时间)	Transcend Policy Server (99年第3季度)	SPECTRUM Policy Manage (99年第3季度)	Cisco QoS Policy Manage (99年4月)、Cisco Security (99年第3季度)	Optivity Policy Server (99年第3季度)
管理对象	NETBuilder 系列、NIC、SuperStack II Switch 系列、CoreBuilder 9000 系列	Smart Switch Router 系列、SmartSwitch 系列	Cisco 2500-7500 系列、Catalyst 8500 系列	Accelar 1000 系列、Passport 系列

3com 公司还为下一代 Internet(I2)设计了策略性网络配置,在 I2 的边缘路由器上配置策略服务器和目录服务器,以统一网上的 QoS 及其它安全等方面的策略。预计在新的宽带 IP 网络上策略服务器将成为网络的一个重要组成部分,配置了策略服务器的网络可以在网络上实现统一的 QoS、安全等方面的策略,便于实时多媒体业务的传送,减少网络管理员的负担,形成统一的管理平台。

由于策略服务可以用于网络的服务质量、安全、监控和配置,关系到网络的安全和可靠性,因此我国必须

研究开发适合我国国情的策略服务系统。

参考文献

- Nichols K, Blake S. Definition of the Differentiated Services Field(DS Byte)in the IPv4 and IPv6 Headers. Internet Draft, May 1998
- Blake S, Black D. An Architecture for Differentiated Services. RFC 2475. 1998, 11
- Boyle J, Cohen R. The COPS(Common Open Policy Service)Protocol. Internet Draft, Aug. 1999