IPv6 下网络 QoS 机制的研究*

徐　巍[1,2]，李腊元[1]

(1. 武汉理工大学 信息工程学院，湖北 武汉 430063；2. 湖北工学院 机械工程系，湖北 武汉 430068)

摘　要: IPv6 与 IPv4 在网络服务质量的机制上有着明显不同。先介绍了 IPv6 协议的特点，接着对现有 IP QoS 技术进行了分析比较，并在此基础上重点论述了 IPv6 下网络 QoS 机制。

关键词: IPv6；服务质量；Internet

中图法分类号: TP393.07　　**文献标识码**: A　　**文章编号**: 1001-3695(2005)01-0213-02

Research on Strategy of Quality of Service in IPv6 Protocol

XU Wei[1,2], LI La-yuan[1]

(1. School of Information Engineering, Wuhan University of Technology, Wuhan Hubei 430063, China; 2. Dept. of Mechanical Engineering, Hubei Polytechnic University, Wuhan Hubei 430068, China)

Abstract: IPv6 and IPv4 are different in the strategy of quality of service. This paper introduces the characteristic of IPv6 protocol, analysis some typical IP QoS techniques. Then, mainly describes the strategy of QoS in IPv6 prototcol.

Key words: IPv6; Quality of Service(QoS); Internet

1　IPv6 概述

20 世纪 90 年代，随着 Internet 的发展，出现了一些新的问题，主要表现为原来的 32 位 IP 地址不够用，难以支持实时多媒体信息及 QoS、移动上网的需求日趋高涨等。

为此，IEIF 于 1992 年提出了制定下一代 IP 的计划，1994 年 7 月选定 IPv6 作为 IPng(IP Next Generation)标准。IPv6 作为下一代的 Internet 协议，保留了 IPv4 所有正在使用的功能，主要改变和增加的功能如下:

(1) 扩展路由功能和地址功能。IPv6 的地址从 32bits 扩展到 128bits，从而拥有有更多的节点，彻底解决了 IPv4 地址不足的问题。新的地址结构支持多层次地址编码，提供了更多的地址类型，RFC2373 中描述了这些地址的相关规定。IPv6 的地址分为三大类: 单播、多播和泛播，而不再支持 IPv4 的广播地址，相对应的则是使用一个“所有节点”多播地址来替代那些必须用广播地址的情况。

IPv6 不再沿用 IPv4 的地址分配方式。IPv4 中地址是用户拥有的，要求在路由表中为每个用户的网络号维持一条表项。随着用户的增加，将无法处理路由表爆炸现象。而 IPv6 中地址变成 ISP 拥有，全局网络号由 IANA 分配给 ISP，用户的全局网络地址是 ISP 空间的子集，这样 ISP 将有效地控制路由信息，避免路由爆炸现象。

IPv6 提供了地址自动配置机制，使主机能自动生成地址，大大减轻了最终用户和网络管理者的负担。

(2) 简化了报文头。IPv6 报文头只有 40 个 Bytes，且是固定长度，这比 IPv4 的报文头要简单得多，从而减小了开销，提高了吞吐量。IPv6 的报文头格式如图 1 所示，具体解析如下: 版本: 4bits，标志 IP 协议的版本，6 代表 IPv6；优先级: 4bits，标志数据包在进行流量及拥塞控制时丢弃的顺序；流标记: 24bits，用于在源地址和目的地址之间建立特定的数据连接；负载长度: 16bits，标志在头后数据包中所承载用户数据的大小；下一个报文头: 8bits，标志报文头；Hop 限制: 8bits，标志数据包的生存时间。值得指出的是，IPv6 在保证服务质量方面，主要依靠流标记和优先级来实现。

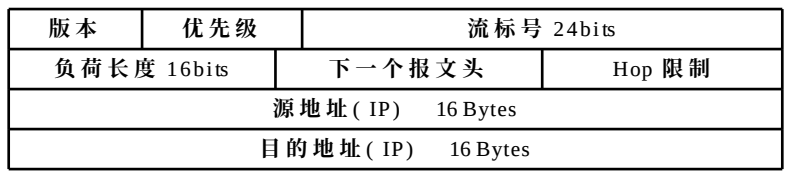

图 1　IPv6 报文结构示意图

(3) 对选项的改进。IPv6 对头选项的编码进行了改进，允许数据包更有效地转发；减少对选项长度的限制，并给未来引入新选项提供更大的灵活性。

(4) 安全性方面。在 IP 协议设计之初并没有考虑安全性，原来的 Internet 安全机制只建立于应用程序级，如 E-mail 加密、SNMPv2 网络管理安全、接入安全等，无法从 IP 层来保证 Internet 的安全。而 IPv6 实现了 IP 级的安全。IPv6 主要有三个方面的安全机制，即数据包确认、数据包的保密和数据包的完整，安全功能具体在其扩展数据报中实现。

(5) 服务质量(QoS)方面。为了更好地支持实时通信量(例如视频会议)，IPv6 对 QoS 增加了一种新功能，即流标记机制。通过该机制，可以给从一个源站发出的需要 IPv6 路由器特殊处理(如实时服务、非缺省的 QoS)的分组序列进行标志，使源端与目的端之间建立一条有特殊属性和要求的伪连接。

2　对 IP QoS 的理解

IP QoS 是分组流通过一个或多个网络时所表现出来的性

收稿日期: 2003-10-12；修返日期: 2004-03-05

基金项目: 国家自然科学基金资助项目(60172035)

能属性,主要为业务提供端到端的服务质量保证。通常用可度量的业务有效性、延迟、可变延迟、吞吐量和丢包率等参数来描述。业务有效性指用户获得的 Internet 业务连接的可靠性;延迟指两个参照点之间发送和接收数据包的时间间隔;可变延迟指在同一条路由上发送的一组数据流中数据包之间的时间差异;吞吐量指网络中发送 IP 数据包的速率,可用平均速率或峰值速率表示;丢包率指在网络中传输数据包时所允许的丢弃数据包的最高比率。数据包丢失一般是由网络拥塞引起的。

常用的 IP QoS 技术有以下几种:

(1) 集成业务模型(IntServ)。IntServ 定义了三种不同等级的服务类型:可保证业务类型、受控业务类型及尽力而为服务。可保证业务类型和受控业务类型都是要求定量的服务质量,都需要在网络节点实现信令和接入控制。这类业务可以为每一个流提供,也可以为汇聚流提供。尽管 Internet 并没有定义具体的信令协议,一般认为 RSVP 就是 IntServ 的信令协议。

IntServ 较好地适应了不同应用的服务质量要求。例如可保证业务类型较好地满足关键应用的 QoS 要求,适应型应用可以使用受控业务类型,其他弹性应用可以使用尽力而为服务;同时也保留了已经存在的尽力而为服务,也没有改变现有的 Internet 的转发机制,从而不需要修改现有的使用尽力而为服务的应用终端,这样使得该业务模型能够渐进实现。

但是,除非整条路径上的所有节点都支持 IntServ,否则端到端的服务质量是无法获得保证的;其次,由于 RSVP 要求端到端的信令支持,且必须在沿途每个路由器上为每个请求预留资源的数据流保持“软状态”,使每个路由器的负担随着网络的扩大、业务流的增多而加重,导致在骨干网络中为每一个流提供不同的服务质量存在着严重的可扩展性问题;再者,全程端到端的信令过于复杂,还有对预留资源的用户的认证、优先权的管理等都需要一个更为烦琐的上层策略机制来管理。

(2) 区分业务模型(DiffServ)。DiffServ 的含义实际上就是给业务分级。在用户和业务网的接口处分级,是基于每个数据包的不同标志。同一级别的业务在该网络域中被聚合统一传送,保证相应的延迟、传送速率、抖动等服务质量参数。每一个分组在分组头标记它所属的业务类别,网络可以很容易地为不同的业务类别提供不同的服务质量。在 DiffServ 中,灵活性和可扩性是由如下的网络资源管理的等级结构实现的:域间资源管理负责在自治域之间订立流量合同;域内资源管理负责自治域内部的资源规划和管理。DiffServ 没有明确规定业务提供商应该提供的业务类别的数目及其特征,只定义了业务使用者和业务提供者之间的本地业务合同。端到端的服务质量由源到目的地路径上业务相邻提供商之间的业务合同组成,DiffServ 并不提供从发送者到接收者的端到端服务质量保证,而是在域的范围内保证与业务分类相对应的服务质量,每个域之间对于不同类别业务的服务质量都应有一定的约定和包标志翻译机制。

由于对进入网络的 IP 分组进行分类、标记以及可能的调整等复杂工作都是由网络的边缘设备完成的,使得高性能的核心交换机和路由器能以极高的速度转发分组穿过网络,网络中也不需要维护每个业务流的信令或状态,从而核心路由器和交换部件只需要很少的改动或者根本不需要改动就将具有良好的扩展性和可升级性;此外,DiffServ 还可以为无法表示其服务质量要求的应用提供定性或者相对的服务质量。

DiffServ 存在的主要问题是:网络所提供的服务在带宽和时延方面可能得不到保证;边缘组件仍然需要高性能的分组分类器;如何在潜在数量很大的边缘组件上进行分类器状态的管理值得进一步探讨。

(3) 多协议标签交换(MPLS)。MPLS 的主要思想是将大部分业务从第三层的转发切换至第二层交换,通过定义一种基本的标记交换技术,从而用不同的标记分配协议在不同的环境下实现流量的交换。在 MPLS 中,网络节点将虚通道与 QoS 的优先级别和排队策略结合起来,使 QoS 流通过高优先级的队列输出。为了支持 QoS,MPLS 提供了 CoS 以在一个标记里提供不同的业务类型。对于颗粒度更小的 QoS 要求,可以忽略 CoS 而另用一个标记来表示不同的 QoS 要求,在这种情况下标记同时代表转发和业务类型。MPLS 可以用流检测和 RSVP 分配标记来实现 QoS,更为一般的 QoS 可以通过为每一个用户分配标记和流量工程来实现。

MPLS 通过有效的分组交换来实现高速分组转发,提供了一种把传统电信中链路层交换与传统的数据报路由集成在一起的方法;由于 MPLS 的路由和交换功能已经有硬件实现,所以可以提高数据转发的吞吐量;通过受限路由实现对流量工程的支持,从而在提供满足某一个流 QoS 要求的路由之外还能够支持其他网络策略。但是 MPLS 试图在无连接的技术中引入面向连接的概念,降低了 IP 的灵活性和增加了实现复杂度;要求所有的网络元素都支持 MPLS,并且使用同一种标记分配协议,且不同的标记分配都有可能造成非常大的开销。

(4) 业务量工程(TE)。业务量工程的功能模块由性能监视系统和网络管理配置系统两部分组成。性能监视系统实现在每个网络分支点对网络上实时传递的业务流和网络资源的使用状况的统计;网络配置管理系统在实时获取网络状态信息的基础上,根据一些预先设置的调整策略,实现对网络的相应调整。可调整的内容包括:业务量管理参数、与路由选择相关的参数以及与网络资源相关的属性和限制。通过对网络参数的调整,可以将业务流置新导向、分流,从而减轻网络的局部压力,同时也可以使业务流的传输性能得到改善。

3 IPv6 下的 QoS

由于 IPv6 和 IPv4 的相似性,在 IPv4 下存在的大部分 QoS 控制策略仍然可以应用到 IPv6 网络中来,如集成服务、区分服务模型等,拥塞控制也将继续在 IPv6 下起作用。但是,IPv6 作为下一代 Internet 协议,在网络服务质量的机制上与 IPv4 又有着明显的不同。譬如,IPv6 简化了头部格式,对各种选项利用扩展头部来实现,使得 IPv6 具有固定的头部,从而加快了信息包在网络上的分发速度;IPv6 具有比 IPv4 更长的地址和更合理的地址划分,使路由选择和处理速度加快;IPv6 还支持巨型包的传递,能为某些应用提供更好的服务;IPv6 协议中明显加强了对提高安全性的支持,与此相关的扩展头部有:身份验证、加密的安全性有效载荷等,可以实现路由器级的安全保证,进而保证整个路径上数据报的安全传输。此外,为更好地支持网络 QoS,IPv6 中定义了流标记和优先级两个字段,用来提供通信服务质量保证,使吞吐量、延时和抖动保持在一定限度内。

(1) 流标记。流标记字段由源节点用来给 (下转第 238 页)