

IPv6 单播 QoS 路由实现的障碍和潜能

张 静¹, 程 楠², 莫有权¹, 胡捍英¹

(1. 解放军信息工程大学信息工程学院通信工程系, 郑州 450002; 2. 郑州大学信息工程学院, 郑州 450052)

摘要: 基于 IPv6 及其主流的 OSPFv3 路由协议, 分析 IPv6 实现单播 QoS 路由可能遇到的障碍, 如现有 IPv4 QoS 路由机制的实用性缺陷、多 QoS 度量表达困难和洪泛更新开销大。利用 IPv6 的简化报头、流概念、流量类型和流标签域支持 QoS 路由的潜能。

关键词: QoS 路由; 度量; 洪泛

Obstacles and Potential of IPv6 Unicast QoS Route Implementation

ZHANG Jing¹, CHENG Nan², MO You-quan¹, HU Han-ying¹

(1. Dept. of Communication Engineering, School of Information Engineering, PLA Information Engineering University, Zhengzhou 450002;

2. School of Information Engineering, Zhengzhou University, Zhengzhou 450052)

【Abstract】 Based on IPv6 and its main OSPFv3 route protocol, this paper analyses the obstacles met possibly by IPv6 unicast QoS route, such as the current IPv4 QoS routing schemes are not applicable, the multiple QoS metrics are difficult to be expressed and their updates cost much to be flooded and so on. It develops the potential for IPv6 of how to use its simplified packet header, flow concept, traffic class and flow label fields to support QoS route.

【Key words】 QoS route; metric; flooding

1 IPv6 QoS 路由的需求及其研究现状

网络规模的扩展、业务的开放及服务需求的多样性要求下一代 IPv6 互联网提供更完善且实用的措施以解决 QoS 问题。未来有 QoS 能力的 IPv6 网络运营商将拥有更多增值业务、更高的利润空间和更强的竞争力。虽然 IPv4 下的大部分 QoS 控制策略仍然可应用于 IPv6 网络, 但如何利用 IPv6 特有的 QoS 元素(如流量类型(Traffic Class, TC)、流标签(Flow Label, FL)、逐跳扩展头等)开发有效的 QoS 方案具有更大现实意义。

QoS路由^[1]的目标是为接入业务选择满足其多度量QoS要求的可行传输路径, 优化全局资源利用率并平衡网络负载, 是解决IP QoS问题的关键技术。未来IPv6 路由器具有大容量内存、高速CPU和接口, 有能力支持QoS路由算法的实现和相关信息的存储与处理, 通过在一定区域内合理配置基于链路状态的QoS路由协议, 算法及相关处理引入的开销可以被接受^[1]。IPv6 是唯一能在IP的基本体系架构上实现QoS路由的网络。目前, 适应于IPv6 网络的QoS路由技术的研究成果不多。文献[2]利用IPv6 的FL字段, 扩展首部的逐跳头和路由头, 提出一种基于扩散的多约束QoS路由算法; 文献[3-4]为IPv6 分别设计了由多QoS度量线性组合成的单混合度量, 以及与多QoS度量相关的单度量以控制多度量更新和多约束路由计算的开销, 提高QoS路由的可行性。本文基于IPv6 广泛应用的单播通信模式及主流的OSPFv3^[5]协议, 分析IPv6 支持单播QoS路由可能遇到的障碍及其潜能。

2 IPv6 单播 QoS 路由的实现障碍

2.1 IPv4 QoS 路由技术的实用性缺陷

上述QoS路由方案没有在实际运营的IP网中得到实现和应用, 未能给从IPv4 起步的大规模多业务的IPv6 QoS路由研

究提供可借鉴的实践经验。本文认为主要是技术和运营 2 个层面的因素制约着QoS路由技术的实施。

(1)QoS 路由技术不够成熟

文献[1]指出目前的 QoS 路由研究在一定程度上改善了网络的服务质量, 但是还需要突破以下技术障碍: 1)多约束求解可行路径的 NPC 问题; 2)多径路由的同步与重路由由开销问题; 3)路由理论模型欠缺; 4)优化目标多且评估标准不一致; 5)接入业务的变化对网络状态影响大; 6)状态信息陈旧和不准确; 7)节点控制与路由过程脱离等。

QoS路由由算法也存在以下不足: 1)算法复杂度过高而不能在网络中实用; 2)算法性能过低而找不到实际存在的可行路径; 3)大部分算法只是针对QoS路由问题中某些特殊情况设计; 4)算法的路由计算及网络状态信息处理(表述、存储、收集、分发)开销大, 影响算法的可扩展性; 5)算法如何与标准路由协议有机结合方面的考虑很少。此外, QoS路由研究的发展趋势是综合多种QoS体系(IntServ, DiffServ, MPLS等)全面改善IP网的服务质量。目前将这些QoS技术结合在一起的方案尚未标准化。

(2)QoS 路由运营不太理想

运营商未部署QoS路由的主要原因如下: 1)需求不紧迫。目前成熟的DWDM技术及线速路由交换设备, 通过科学的网络流量配置基本能保证有限IPv4 业务的QoS, 因此, 在没有理想QoS路由技术的情况下, 运营商(如美国运营商Sprint)宁

基金项目: 国家“863”计划基金资助重大项目(2005AA121210)

作者简介: 张 静(1970 -), 女, 副教授、博士研究生, 主研方向: 通信与信息系统; 程 楠, 讲师; 莫有权, 副教授; 胡捍英, 教授、博士生导师

收稿日期: 2007-09-29 **E-mail:** zhangjingok@sina.com

愿铺设足够带宽的网络,用相对廉价的带宽换取QoS,而不愿冒险尝试QoS路由。2)部署不简单。如果所引入的QoS路由方案(如探测类、路径子空间搜索类等)需要全新的网络运营环境,对现有路由节点的协议功能改动较大,并且不兼容既有的尽力而为服务,都可能影响不同组织制定的网络架构的互通和增加现有网络的升级成本,使部署QoS路由得不偿失。3)管理水平不足。QoS路由的运营涉及QoS管理(网络拓扑、节点及链路状态信息的收集和网路资源管理)、QoS测量(获取网络性能,服务质量指标及用于路由目的的QoS度量参数)和QoS计费(根据用户使用网络资源的情况及网络满足业务QoS请求的程度核收费用),但关于这些领域的研究成果较少且未标准化。

2.2 IPv6 OSPFv3 路由协议的缺陷

传统的尽力而为路由协议一般采用单度量(如跳数、成本)计算最短路径,而QoS路由面对应用业务对网络传输服务所提出的一组QoS请求,必须考虑多种不同度量参数(如带宽、时延、可靠性等)来选择路由。因此,基于OSPFv3扩展的QoS选路有2个基本任务:(1)改进链路状态通告(LSA)和链路状态数据库(LSDB)以收集和存储多QoS度量的状态更新信息;(2)改进路由算法,根据获得的网络状态信息计算满足多QoS约束的可行路径。相应地,QoS路由性能也取决于两类开销:网络状态信息更新开销和路径计算开销。当前大多数的QoS路由由成果都重视后者,而忽视前者,其实对网络状态信息的处理较复杂,与其他问题密切相关,而且QoS路由所需的的信息量更大,因此,更新和洪泛寻径信息所引入的通信开销对QoS路由性能的影响很大,值得重点考虑。

下文从链路状态通告及多QoS度量洪泛两方面分析OSPFv3支持QoS路由的不足之处。

(1)链路状态通告表达多QoS度量困难。尽管在IPv4的OSPFv2中,度量类型(TOS)、TOS编号(#TOS)和对度量值(TOS metric)的定义(图1(a))可以支持多度量(#TOS≠0)的QoS路由,但实际的IPv4网络并没有应用QoS路由,为保证兼容标准OSPF协议,目前路由器的OSPFv2 LSAs中虽保留TOS,但通常只选取TOS=0的默认服务,路由器并不对其作任何处理。IPv6的OSPFv3协议保留了OSPFv2的基本机制(如洪泛、DR选举、区支持、SPF算法等),却简化其LSAs定义,从中删去了OSPFv2中未用的TOS和对应的TOS metric(图1(b)),这样就给IPv6网络通过LSAs表达多QoS度量及其更新信息带来困难。

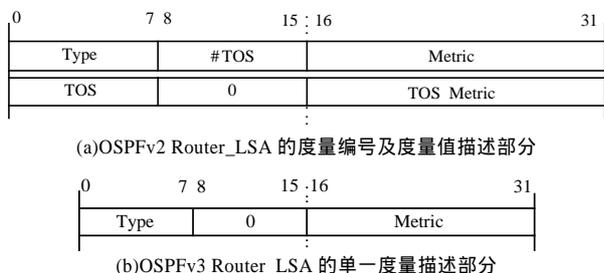


图1 OSPFv2和OSPFv3的Router_LSA度量描述部分

(2)洪泛多QoS路由度量的通信开销大。OSPFv3协议通过可靠洪泛(Flooding)链路状态通告(LSA)的方式来建立、更新和同步链路状态数据库。假设洪泛 k -QoS($k \geq 1$)度量的更新,OSPFv2可以只用一个LSA来通告 k 个QoS度量(TOS描述 k 个度量类型,TOS metric取相应度量值),而OSPFv3

由于上述表达多度量的困难,必须通过 k 个LSAs才能通告 k 个QoS度量。假设每个链路状态更新(LSU)分组只携带1条LSA,那么区域内的OSPFv3节点每次向一个邻点洪泛 k -QoS度量更新时,就必须发送 k 个LSU分组。文献[6]理论分析和仿真验证了OSPFv3洪泛多QoS路由度量的平均洪泛效率和平均洪泛分组数性能,发现网络规模,节点邻接关系和QoS度量数的增多会给网络带来严重的消息冗余、慢速收敛等问题,引起急剧增加的通信开销。此外,判断LSA的新旧,LSA的确认或重传,特别是OSPFv3新增的洪泛范围的处理(根据LSA中的LS类型和U比特设置选择正确洪泛接口),都势必因洪泛多QoS度量而大大加重网络负担。

3 IPv6 单播 QoS 路由的实现潜能

IPv6对IPv4的最大革新之处在于对QoS的支持,体现在报头简化,流(flow)概念的提出及IPv6首部(图2)中的TC和FL两个域。



图2 IPv6首部结构

IPv6的QoS新特征具有支持QoS路由的潜能,具体如下:

(1)报头简化提升路由器处理速度。大多数IPv6扩展首部不受中间节点检查,而是留给目的主机处理。幸运的是,IPv6的40B基本首部中已包含业务流的类型、优先级和QoS需求的描述,提供给路由器做QoS选路的充足信息。此时,规整简化的IPv6报头便于用硬件高速处理,加快了信息包的路由选择和处理速度。

(2)以流为单位选路提高流转发效率。传统IPv4网络一般用<源地址,目的地址,源端口号,目的端口号,协议类型>五元组来识别流,但获取端口号这样的越层处理加重了中间节点的负担,加密分组的高层信息更是难以获得。IPv6首次提出流概念并以二元组<IP源地址,FL>唯一标识流,可方便用户以业务流为单位提出QoS请求,路由器也基于每流建立QoS路由表(降低了路由表的存储开销),处理和路由QoS流(基于FL的流分类要比传统方式的流分类效率高3倍~6倍):比如只需为新流的第1个分组,以二元组为索引查找QoS路由表和选路,属于该流的其余分组则按同一路径转发,而不必为每个数据包重新选路,从而提高了数据包的转发效率和降低了端到端的延时。

(3)以TC字段为流分类分级并指示敏感QoS度量。IPv4试图通过首部中的TOS字段,根据业务流量属性分类来进行传输服务质量的控制,但在因特网内并未成功。IPv6在全部引入IPv4网络业务的基础上,将增加大量的IPv6特色业务,为IPQoS问题的解决提供了契机。IPv6重新设计了8bit的TC字段来兼容IPv4的TOS字段,节点可以使用该字段来根据多媒体信息的紧急程度标记和识别IPv6数据包的类别和优先级,并指出该流要求QoS保证的敏感度量参数(TC的编码及如何使用尚未明确,如图3所示,可以借用RFC1349^[7]第0位~第2位的TOS定义把流分为2类,每类8个优先级;用剩余5bit扩展编码流敏感的QoS度量),这是实施QoS路由的基础,因为只有区分各业务流及其敏感度量,才能由FL或逐跳扩展头为某类某优先级的通信流提出适当的QoS请求(如音视频流的延时和抖动请求,FTP的可靠性请求等),为后续的QoS

选路做好充分准备。

0	1	2	3	4	5	6	7
优先级			流敏感的QoS度量编码				
			0	0	0	0	0
			0	0	0	1	0
			0	0	1	0	0
			0	0	1	1	0
			0	1	0	0	0
			0	1	0	1	0
			0	1	1	0	0
			0	1	1	1	0
			1	0	0	0	0

默认 Best-effort 服务
开销
可靠性
带宽
延时

图3 IPv6 中支持 QoS 路由的 TC 字段扩展编码

(4)以FL字段为流提出QoS路由请求。目前IPv6 新增的 20 bit FL字段的定义尚未明确，离实用有一定距离。FL字段可配合TC字段指示的流分类和敏感度量，为该流提出其QoS约束值。Banerjee草案^[8]虽阐述了一种在FL中存放各种QoS请求参数的思想，简单且额外开销小，但在FL的空间限制下，以16 bit表达多度量类型及高约束值的能力有限，因此，可考虑采用指数编码扩展度量约束的取值范围，如图4所示。

0	1	2	3	4	5	6	7	8	9
1	0	1		E			M		
带宽			延时				可靠性		

第0位~第2位为101: 用FL描述QoS度量的约束值。
E(exponent): 编码的指数部分; M(mantissa): 编码的尾数部分。
例: 带宽的表达范围(基数为10): $0 \text{ bit/s} \sim 127 \times 10^{19} \text{ bit/s}$;
延时的表达范围(基数为6): $0 \text{ s} \sim 648 \text{ s}$;
可靠性的表达范围(基数为4): $0\% \sim 64\%$ 。

图4 IPv6 中支持 QoS 路由的 FL 字段扩展编码

4 结束语

实现 IPv6 QoS 路由面临着巨大困难，需要在理论指导下开发实用性强的 QoS 路由方案来实现未来 IPv6 QoS 的关键技术：(1)IPv6 Multicast, Anycast QoS 路由；(2)移动 IPv6 QoS

路由；(3)保证端到端 QoS 路由的可扩展性；(4)QoS 路由运营管理；(5)与其他 QoS 技术的融合。

参考文献

- [1] 崔 勇, 吴建平, 徐 恪, 等. 互联网络服务质量路由算法研究综述[J]. 软件学报, 2002, 13(4):1-11.
- [2] 李 茹, 黄晓璐, 叶新铭. IPv6 网络环境中的多约束 QoS 路由算法[J]. 计算机工程, 2005, 31(4): 53-55.
- [3] Zhang Jing, Tang Hongbo. Pre-computation for Multi-constrained QoS in IPv6 by Applying Single-mixed-metric and Admission Control[C]//Proceedings of International Conference on Sensing, Computing and Automation. Chongqing, China: [s. n.], 2006.
- [4] Zhang Jing, Hu Hanying. QoS Routing in IPv6 with Link-utilization-ratio Single Metric[C]//Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing. Wuhan, China: [s. n.], 2006.
- [5] Coltun R, Ferguson D, Moy J. OSPF for IPv6[S]. IETF, RFC 2740, 1999.
- [6] 张 静, 程 楠, 童 珉, 等. IPv6 网络中 OSPFv3 洪泛多 QoS 路由度量的性能研究[J]. 北京邮电大学学报, 2007, 30(6): 46-50.
- [7] Almquist P. Type of Service in the Internet Protocol Suite[S]. RFC 1349, 1992.
- [8] Banerjee R, Mahaveer M. A Modified Specification for Use of the IPv6 Flow Label for Providing an Efficient Quality of Service Using a Hybrid Approach[Z]. Internet Draft, 2002.

(上接第 122 页)

4 安全性和性能分析

4.1 安全分析

单点登录服务是在不安全的网络中对整个应用系统形成的一个门槛效应^[5]，即各应用系统对单点登录服务提供的认证服务给予充分认可，其中一个应用受到威胁时，整个集成在SSO服务中的应用系统安全都没有保障，与不实施单点登录相比，安全性成为SSO服务一个更突出的问题。

在单点登录协议中，用基于 Kerberos 票据的原理进行安全性控制。协议给应用颁发 2 种票据凭证，TGT 是 ST 的基础，安全性更为重要，在单点登录协议中用安全的 https 协议在网络中加密传输，保证对传输过程中安全不受重放、篡改、窃听和其他中间人的攻击。而对于 ST，是相对特定应用的访问票据，又称为服务票据，在协议中只限定一次认证有效，因此可以在暴露在网络中传输，即使有攻击 ST 的存在，也会因为对 ST 的失效不会对应用造成威胁。单点登录协议通过对票据的处理策略完成对应用的安全保护。票据凭证都存放在内存域中，在关闭 UI 的情况下对票据进行自动处理并使一定时间内的凭证票据失效，保证消除因操作上的失误带来的安全威胁。

4.2 性能分析

单点登录服务把多个应用系统的认证工作集于一身，是各应用系统的中枢神经，单点登录本身的性能直接影响认证服务的进行。在单点登录协议中，票据凭证是直接存放在内

存地址中以加快切换应用系统的响应，另外，当成百上千终端用户同时进行处理时，内存地址的有限性^[5]也影响SSO的性能。协议中对票据凭证实现控制策略，定时对凭证做自动处理以保证响应速度。

5 结束语

本文为单点登录协议提出一种可插入式单点登录技术解决方案，在单点登录协议基础上增加异步协同机制和代理服务机制实现单点登录应用的可扩展和可配置。插件方式具有不影响 SSO 服务正常运行的优势。要完成与 SSO 的协同，必须能对应用系统做相应改进，如何实现客户端应用的最少改动是下一步研究的重点。

参考文献

- [1] John T K, Lifford B C N. The Kerberos Network Authentication Service[D]. Massachusetts, USA: Massachusetts Institute of Technology, 1992.
- [2] 邱 航, 权 勇. 基于 Kerberos 的单点登录系统研究与设计[J]. 计算机应用, 2003, 23(7): 142-144.
- [3] 周风丽, 邵平凡, 万程鹏. 设计模式在 B/S 开发中的应用[J]. 科技创业月刊, 2005, 18(12): 167-168.
- [4] 陈云海. .NET Passport SSI 技术研究及漫游扩展[J]. 广东通信技术, 2002, 22(11): 8-15.
- [5] Li Gong. Increasing Availability and Security of an Authentication Service[J]. IEEE Journal on Selected Areas in Communications, 1993, 11(5): 657-662.