第 34 卷　第 1 期　　计　算　机　工　程　　2008 年 1 月
Vol.34　No.1　　Computer Engineering　　January 2008
·网络与通信·　　文章编号：1000—3428(2008)01—0131—03　　文献标识码：A　　中图分类号：TP393

# QoS 机制在 IPSec 安全设备上的分析与实现

何　军[1]，舒　莉[1]，李　奇[2]
(1. 四川大学计算机学院，成都 610065；2. 四川师范大学软件重点实验室，成都 610068)

**摘　要：**提出了在 IPSec 安全设备上实施 QoS 的体系方案。设计了适合 IPSec 安全设备特点的数据分类规则。为 IPSec 安全设备构建了一个系统排队理论模型，该模型以延迟作为系统运行目标，以带宽作为分配资源。据此设计了一个自适应带宽分配循环队列调度算法。实际运行的测试结果表明，在重载情况下，实施了 QoS 的 IPSec 安全设备可以为重要业务流提供带宽和时延保障。
**关键词：**服务质量；体系结构；分类；调度；排队

# Analysis and Realization of QoS Machanism in IPSec Security Device

HE Jun[1], SHU Li[1], LI Qi[2]
(1. College of Computer Science, Sichuan University, Chengdu 610065; 2. Key Lab. of Software, Sichuan Normal Univ., Chengdu 610068)

**【Abstract】**This paper presents a QoS scheme suit for IPSec security device, and designs a data classification regulation adapt to characteristics of IPSec security device. A principle of queuing model is constructed which takes the delay as the target parameter and the bandwidth as the allocation resource of the queuing system. By this model, an adaptive bandwidth allocation circular schedule algorithm is designed. The results of test show that the IPSec security device guarantees bandwidth and delay for key streams in the situation of heavy burden by QoS mechanism.
**【Key words】**QoS; architecture; classification; schedule; queuing

在Internet上为数据传输提供服务质量保障，是Internet和多媒体应用迅速发展的必然要求[1-3]。在网络上实施QoS要求链路中的每一个节点都实现QoS。本文所述IPSec 安全设备是基于Linux系统而设计开发的。IPSec 安全设备作为网络中的一个节点，与其他网络节点相比其最大的特点就是透明性(透明地加入网络中)。IPSec 安全设备在处理业务流时有明通、密通的处理方式。相比于其他只执行“路由”任务的网络节点(路由器、交换机)，IPSec 安全设备要执行耗时的任务如隧道封装、加密、业务流分类等。由于不可预知的网络行为，IPSec 安全设备有可能成为网络瓶颈和拥塞点，因此有必要在IPSec 安全设备上实现QoS，以保障关键业务不被阻塞。

## 1　IPSec 安全设备上的 QoS 关键技术

### 1.1　软件结构及原理

图 1 是在 IPSec 安全设备实现 QoS 的软件体系结构。

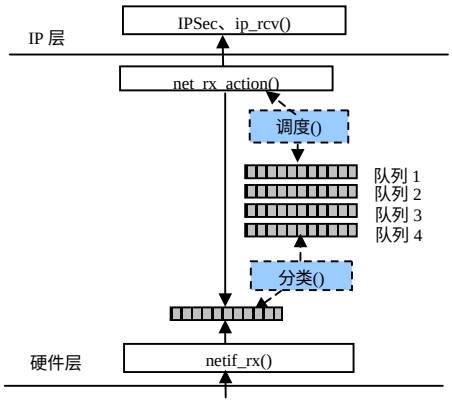


**图 1　QoS 实现的软件体系结构**

其中，由虚线连接的有阴影的模块是新增模块，系统是在 Linux 内核 2.4.8 上实现的。在原有系统中增加了 4 个排队队列和 2 个独立的功能模块：分类器和调度器，它们都是作为 Linux 的软中断而在系统中注册的。

当硬件层有数据包到达时，由 netif_rx()模块激活软中断——分类模块，将数据包放入 4 个排队队列，随后由分类模块激活软中断——调度模块，由调度模块依照制定好的调度计划调度 4 个排队队列，之后由调度模块激活软中断 net_rx_action()，最后将数据包传递给 IP 层。

### 1.2　QoS 参数的选择

由文献[4]的实验可以看出，数据发送端网络对业务流抖动的影响不显著，在这里对抖动进行控制意义不大。但在数据接收端网络，特别是在经过了骨干网后，业务流的形态会发生很大的变化，特别是在抖动、丢失等方面。因此，在接收端网络处，可能对延迟控制的效果不大，而对抖动进行控制会取得显著的效果。

图 2 是网络实时视频流的传送过程[5]。

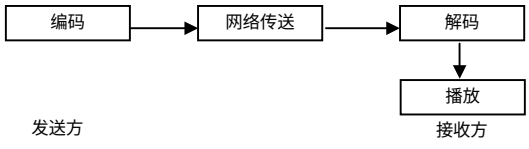


**图 2　视频流传送过程**

视频流 QoS 参数注重的是延迟与抖动。图 2 中，在发送

**基金项目：**四川师范大学软件重点实验室基金资助项目(SCSL06006)
**作者简介：**何　军(1970－)，男，副教授、博士，主研方向：网络服务质量，计算机网络及应用技术；舒　莉，讲师、硕士；李　奇，高级工程师
**收稿日期：**2007-01-15　**E-mail：**hejun_email@163.com

方处不会产生延迟与抖动，在传送过程中将产生延迟、抖动和数据丢失，在接收方处将产生延迟和抖动。但在接收方处的应用软件系统会对抖动进行处理。

IPSec 安全设备是网络链路的中间节点，因此，在 IPSec 安全设备上实施 QoS 所选取的目标参数是重要业务流的带宽与延迟，在此基础上兼顾对不同业务流进行调度的公平性。

### 1.3 数据分类策略

IPSec 安全设备的分类主要依据的 QoS 参数是：带宽，延迟，加密。本文通过 IPSec 安全设备的业务流分为 4 类(见表 1)。其中，类 1 对应加密-QoS 队列；类 2 对应非加密-QoS 队列；类 3 对应加密-非 QoS 队列；类 4 对应尽力而为队列。支持 QoS 的 IPSec 安全设备中的分类器和队列调度器依据表 1 为不同的业务流提供不同的 QoS 服务。第 1 类到第 4 类业务对 QoS 服务的要求依次降低。

**表 1 业务流分类**

| 类别 | 延迟 | 带宽 | 加密 |
|---|---|---|---|
| 1 | Yes | Yes | Yes |
| 2 | Yes | Yes | No |
| 3 | No | No | Yes |
| 4 | No | No | No |

### 1.4 队列调度算法

队列调度算法采用的是一种自适应带宽分配——循环调度算法。该算法依据网络数据流的实际变化情况，动态地为各类业务流分配带宽；对系统中的排队队列进行调度时采用批处理的方法，一个调度周期调度一批数据。当一个调度周期或多个调度周期结束时，重新制定带宽分配方案和队列调度计划，从而能够及时适应网络流量的变化。队列调度模块的目的是为重要程度高的队列提供低延迟的服务。此外，在 IPSec 安全设备中密通的数据有一个加密延迟，因此，调度算法进行队列调度时对明通、密通数据交错调度，以充分利用系统的发送端口带宽资源，获得较高的吞吐量。

#### 1.4.1 排队模型

如 1.3 节所述，IPSec 安全设备将进入的数据包分成 4 类，放入 4 个排队队列，因此，本文将其模型化为 4 个互相独立的 M/M/1 排队模型。

模型中，顾客/事件按照参数为 $\lambda$ 的泊松分布，顾客/事件到达的时间间隔与服务窗为每个顾客服务的时间均为负指数分布，服务率为 $\mu$。4 个相互独立的服务系统共享 IPSec 安全设备的处理能力。各网络流的到达率各不相同，IPSec 安全设备为 4 个 M/M/1 模型分配不同的带宽，即为各服务窗分配不同的服务能力，因此，各服务窗的服务率是不同的。同样，4 个排队队列的目标参量(如延迟、队列长度等)的值也是不同的，与各服务窗的服务能力大小密切相关。这就使得带宽分配策略及为重要，它关系到系统总体性能的优劣。

上述模型中有如下的要素：

(1)需要的带宽$b_1, b_2, b_3, b_4$分别表示类别 1~类别 4 的当前网络流量。

(2)$B_{\text{total}}$为IPSec 安全设备可以达到的最高处理能力。

(3)分配的带宽：$b_1', b_2', b_3', b_4'$分别表示系统当前分配给类别 1~类别 4 的网络带宽。显然有：

$$b_1' + b_2' + b_3' + b_4' \le B_{total}$$

(4)$d_1, d_2, d_3, d_4$分别表示类别 1~类别 4 的数据包在系统中的延迟。

(5) $\lambda_i$ 为进入流 $i$ 的到达率， $\mu_i$ 为服务窗 $i$ 的服务率。则有

$$\lambda_i = \frac{b_i}{l_{\text{avg}}}$$

$$\mu_i = \frac{b_i'}{l_{\text{avg}}} \tag{1}$$

其中，$l_{\text{avg}}$为平均包长。

#### 1.4.2 目标函数

排队系统通过为不同的业务流分配不同的带宽、制定恰当的调度计划来使数据包在 IPSec 安全设备中的停留时间尽可能短。衡量指标为数据包在 IPSec 安全设备中的平均延迟。

记系统中共有$B_{\text{total}}$的处理能力，作为资源分配给QoS-加密流、QoS-非加密流、非QoS-加密流、尽力而为流这 4 种类型的网络流。则由式(1)可知：若将$b_i'$的带宽分配给类别为$i$的网络流，即服务窗的服务率；且网络流$i$的到达率为$b_i$，网络流$i$各数据包到达的时间间隔与相应服务窗为每个数据包服务的时间均为负指数分布，则网络流$i$在系统中的平均延迟为

$$d_i = \frac{1}{\text{服务率} - \text{到达率}} = \frac{1}{\mu_i - \lambda_i}$$

$$\text{总延迟} = \sum d_i \tag{2}$$

为了在有限的处理能力下使总延迟最低，应根据系统中的实际情况合理分配网络带宽。因此，可将上述问题描述为如下的规范化数学模型：

$$\max Y = \sum_{i=2}^{4} \frac{-1}{\mu_i' - \lambda_i}$$

$$\text{s.t.} \quad \frac{1}{b_2' - b_2} - \frac{1}{b_3' - b_3} \le 0$$

$$\frac{1}{b_3' - b_3} - \frac{1}{b_4' - b_4} \le 0$$

$$\sum_{i=1}^{4} b_i' \le B_{\text{total}}$$

$$b_2' \ge 0, \quad b_3' \ge 0, \quad b_4' \ge 0 \tag{3}$$

对$B_{\text{total}}$的分配是以离散方式进行的，有一个最小的分配单位。每次分配是一个最小单位或是它的整倍数。带宽分配最小单位确定的原则是：不能太小，以免计算量过大；不能太大，以免浪费带宽。

用动态规划的方法对式(3)求解。

设 $F_i(b')$ 是系统为前 $i$ 个网络流分配的总带宽为 $b'$时系统的最低总延迟，则由最优原理可把式(3)化为

$$\begin{cases} F_1(b') = \frac{1}{\lambda_2 - \mu_2'} \\ F_i(b') = \max\limits_{0 < b_k' \le b'} \{ f_i(b_k') + F_{i-1}(b' - b_k') \} \end{cases} \tag{4}$$

逐步计算$F_1, F_2, \cdots, F_i$，可以求得最优解$F_n$。

#### 1.4.3 自适应带宽分配循环调度算法

自适应带宽分配循环调度算法动态地依据网络数据流的实际情况分配带宽。当网络流量发生变化时，及时地调整带宽分配方案；调度时采用批处理的方法，一个调度周期调度一批数据。QoS 模块为重要程度高的队列提供低延迟的服务。该模块实时检测不同类型数据流的流量，用上文的求解步骤算出为各数据流分配的带宽，并进一步求得一个调度周期内对各类数据流的调度频率，调度模块据此对各类数据流进行交错调度。基本概念如下：

(1)调度周期：是指调度计划的有效期，每个调度周期对应不同的调度计划。若调度周期的时间间隔为$\triangle t$，则在每个$\triangle t$ 的时间间隔时都会产生一次新的调度计划。

(2)平均包长：若在一段时间内到达的数据包的个数为$n$，

其中，第$i$个包的长度为$l_i$，则该段时间间隔内的平均包长　度为

$$l_{\text{avg}} = \frac{\sum_{i=1}^{n} l_i}{n}$$

(3)数据流的流量：对类型为 $i$ 的数据流，其单位时间的流量为

$$b_i = \frac{\sum l}{\Delta t}$$

其中，$l$ 为数据包的长度。

(4)数据流的调度频率：数据流 $i$ 的调度频率表示在一个调度周期中为该类数据调度的数据包个数。若根据上文计算得到为流 $i$ 分配的带宽为 $b_i'$，则调度数为

$$s_i = \frac{b_i'}{l_{\text{avg}}}$$

其中，$s_i$意味着调度算法在下一个调度周期内应该为流$i$调度的数据包个数。

## 2　测试结果及讨论

测试设备采用的是 SmartBits7.40 网络测试平台，测试项目为网络延迟。由于只能由 SmartBits Application 测试延迟，且一次只能测试一条流，因此测试方法是用 SmartBits Window 产生 3 个 10 Mb/s 的网络流，用 SmartBits Application 产生 1 个以 5 Mb/s 开始、递增幅度 5 Mb/s、直到 60 Mb/s 的网络流。测试中以 4 次测试为一个完整的测试，4 次测试分别测试 4 个分类类别的网络流。图 3 是测试结果。

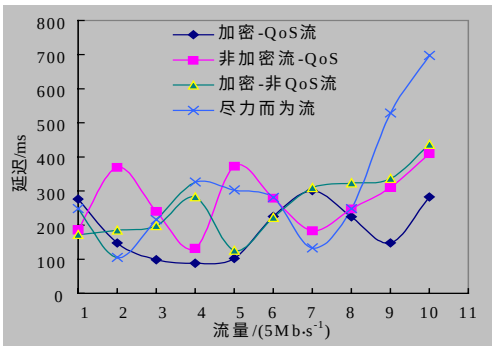


**图 3　测试结果**

可见，当网络负载重时，各排队队列的延迟都增加了，其中加密-QoS 队列的延迟最低，然后延迟依照队列的重要程度，按非加密-QoS 队列、加密-非 QoS 队列、尽力而为队列的次序依次升高，符合调度算法的调度目标；当网络负载轻时，则无明显差别。说明在 IPSec 安全设备上采用 QoS 机制后，在网络重载的情况下可以较好地达到按需为网络流提供不同服务质量的要求。

## 3　结束语

IPSec 安全设备上的 QoS 模块的目标是能保障 IPSec 安全设备不成为网络瓶颈、不阻塞关键业务。IPSec 安全设备上的 QoS 机制是与网络上的 QoS 机制相互独立的，并且 IPSec 安全设备上的 QoS 机制应对网络上的 QoS 机制有有益的作用。在 IPSec 安全设备实现了 QoS 的基础上，可以将 QoS 管理部分实现在系统的其他部分(如密钥管理中心)，将计算任务合理分配。 随着技术的发展，各种新型网络应用不断兴起，今后的工作将研究这些新业务流的特点，向 IPSec 安全设备增加新的 QoS 保障机制，为各种关键业务提供充分的服务质量保证。

### 参考文献


[1] Lee T W, Kim Y C. Implementation of a MPLS Router Supporting Diffserv for QoS and High-speed Switching, High Speed Networks and Multimedia Communications[C]//Proc. of the 5th IEEE International Conference on JEJU. [S. l.]: IEEE Press, 2002.

[2] Childs S, Ingram D. The Linux-SRT Integrated Multimedia Operating System Bringing QoS to the Desktop[C]//Proceedings of the 7th Real-time Technology and Applications Symposium. [S. l.]: IEEE Press, 2001.

[3] 汪　芸, 顾冠群. 网络服务质量(QoS)参数研究[J]. 计算机研究与发展, 1998, 35(6): 543-547.

[4] 何　军, 谭兴烈, 周明天. IPSec安全设备QoS方案的仿真及性能分析[C]//2003 中国计算机大会. 中国: [出版者不详], 2003-11.

[5] Luo Jun, Yuan Man, Hu Jianping, et al. QoS Characteristics of Video Stream Delivery and Assure[C]//Proceedings of ICCT' 03. [S. l.]: IEEE Press, 2003.


（上接第 130 页）

## 5　结束语

为了解决目前 SLA 监测系统存在的不足，本文提出了基于 Web Services 的 SLA 监测系统体系结构，描述了该体系结构中相关服务的功能和 SLA 监测流程。同时，为了实现通用的不同层次 SLA 参数的映射，提出了通用的 SLA 参数映射模型。通过原型系统在实验网络环境中的实验验证了该体系结构能够满足在下一代互联网环境下跨多个提供商的端到端业务的监测需求。下一步将要解决的问题是实现 SLA 监测系统与动态 SLA 管理中的 SLA 保障系统的更好协作，以便进行业务质量闭环控制。

### 参考文献


[1] ITU. ITU-T Rec. M.3341 Requirements for QoS/SLA Management over the TMN X-interface for IP-based Services[S]. 2004.

[2] 郭　强, 王文东, 阙喜戎. 基于 SLS 的业务服务质量监测机制[J]. 北京邮电大学学报, 2006, 29(1): 92-95.

[3] Ribeiro M B, Granville L Z, Almeida M, et al. An Architecture to Monitor QoS in a Policy-based Network[C]//Proc. of the 10th International Conference on Telecommunications. Polynesia, French: IEEE Press, 2003: 138-143.

[4] Molina-Jimenez C, Shrivastava S, Crowcroft J, et al. On the Monitoring of Contractual Service Level Agreements[C]//Proc. of the 1st IEEE International Workshop on Electronic Contracting. [S. l.]: IEEE Press, 2004: 1-8.

[5] Liu Baohua, Ray P, Jha S. Mapping Distributed Application SLA to Network QoS Parameters[C]//Proc. of the 10th International Conference on Telecommunications. [S. l.]: IEEE Press, 2003: 1230-1235.

[6] Hyo-Jin Lee, Myung-Sup Kim, James W Hong, et al. QoS Parameters to Network Performance Metrics Mapping for SLA Monitoring[C]//Proc. of APNOMS'02. Jeju, Korea: IEEE Press, 2002: 988-1000.

[7] 陈中林, 金跃辉, 牛志升, 等. 网络性能测量平台的研究与实现[J]. 电信科学, 2005, 23(11): 63-68.