OPNET中支持Flow Label的网络模型设计与实现

高 程[1] 黄小红[1,2] 孙 琼[1,2] 马 严[1,2,3]

(北京邮电大学信息网络中心 北京 100876)[1] (北京邮电大学计算机科学与技术学院 北京 100876)[2]

(北京邮电大学智能通信软件与多媒体北京重点实验室 北京 100876)[3]

摘 要 Flow Label是在IPv6报头中新增的一个20比特的域,专为实时流提供有别于尽力而为流的服务,从而提供更好的QoS管理功能。仿真是研究网络模型及应用的重要手段,基于有限的关于Flow Label应用机制的研究,构建支持Flow Label的仿真模型对Flow Label的研究与推广具有重要的意义。主要介绍了OPNET中支持Flow Label与QoS映射的客户端与网关模型的设计与实现。

关键词 流标签,OPNET,服务质量,网关

Design and Implementation of Flow Label Supported Network Module in OPNET

GAO Cheng[1] HUANG Xiao-hong[1,2] SUN Qiong[1,2] MA Yan[1,2,3]

(Information Network Center, Beijing University of Posts and Telecommunications, Beijing 100876, China) [1]

(School of Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China) [2]

(Beijing Key Laboratory of Intelligent Telecommunications Software and Multimedia, Beijing University of Posts and Telecommunications, Beijing 100876, China)[3]

Abstract Flow label is a 20-bit field in IPv6's base header. It is designed particularly to provide better service than best effort service model, which will enable better QoS management functions. Simulation is one important mechanism to evaluate the performance of network models and applications. It is of great significance to design flow label based simulation module for the research and promotion of flow label, especially with limited research on the application of flow label so far. A network module in OPNET which supports the Flow Label and QoS class mapping was proposed and implemented.

Keywords Flow label, OPNET, QoS, Gateway

1 背景介绍

QoS是解决IP网承载多业务的关键因素,其具体执行步骤如下:1.鉴别流量和它的需求:了解网络确定现行传输流量的不同类型,并且确定针对不同类型的网络流量对QoS的需求,哪些是语音流量,哪些是关键的数据流量,哪些是尽力而为的数据流量;2.将不同类型的流量根据对QoS的不同需求进行分类;3.针对流量的不同分类,定义相应的策略来保障。由此可见,流识别的功能是实现端到端QoS的基础。若没有统一的流标识,同一数据流在进入不同的自治域之后就会失去该流的原始QoS信息。在使用Flow Label之前,业界普遍采用五元组的流识别方法,在IPv6中,五元组可能会受到加密或分段的影响,可扩展性较差。此外,Flow Label的引入,给QoS策略的映射也带来了新的契机。通过使用流标签,可以实现不同自治域间的统一QoS管理以及提供不同粒度的QoS策略,从而可以实现跨自治域的QoS服务质量。

目前详细的IPv6流标签使用机制很有限,在少量的IETF草案、RFC文件和其它文献中,规定了使用流标签的若干原则,但是对于流标签的分配、管理以及路由器如何根据流标签处理数据包却没有统一的规则。因此,研究Flow Label应用中遇到的难题对解决下一代互联网中的QoS问题有着重要的意义。网络仿真是通过在计算机中构造虚拟的环境来反映现实的网络环境,模拟现实中的网络行为,从而可以有效地提高网络规划和设计的可靠性和准确性,明显降低网络投资风险,减少不必要的投资浪费。目前,OPNET中还不具备支持Flow Label的模块。因此,在当前利用仿真的办法对研究Flow的应用机制有重要意义。

针对以上现状,本文提出了在OPNET中支持Flow Label与QoS映射的客户端、边界网关模型,为基于Flow Label的域间QoS映射模型的研究提供支持。

2 模型设计

由于各大运营商都会采取保护现有投资的措施,因此,只有最大限度地减少大规模改动现有基础设施,才能使该方案有实用性。本模型在客户端和边界网关添加了相应的映射表,不更改核心网的结构,可以在减少对现有基础设施的改

到稿日期:2008-07-10 本课题受国家教育部归国实验室建设项目及国家自然科学基金委项目,国家自然科学基金项目(编号6077211)资助。

高 程 硕士研究生,研究方向为计算机网络及应用,E-mail:gaoc@buptnet.edu.cn;黄小红 讲师,研究方向为计算机网络及应用;孙 琼 博士生,研究方向为计算机网络及应用;马 严 博士生导师,研究方向为网络安全技术和IPV6技术及其应用。

动，提高其可行性。

客户端结点模型保存各种应用的 TOS 与 Flow Label 的映射表，完成 TOS->FL 映射。边界网关保存 Flow Label 映射表，入口网关完成 Local fl->DSCP 映射，出口网关完成 Local fl->Next fl 映射。图 1 为客户端与直接相连的第一个自治域的模型设计。

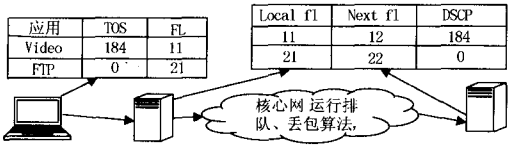

图 1　单域内模型设计

2.1　协商过程

在发送数据包之前，客户端应用 SLS 协议（SIP，NSIS 等）对服务等级进行协商。客户端向各个域内的路由器或代理服务器发送 QoS 请求，每个域根据本域内 QoS 等级状况及请求的服务类型分配该应用在本域内的 Flow Label 值以及对应的 DSCP 值。协商过程生成的 Flow Label 映射表保存在各个网关中，作为流分类的依据。Flow Label 映射表结构如表 1 所列。

表 1　Flow Label 映射表

Local Flow Label	本地 Flow Label 值
Next Flow Label	下个域的 Flow Label 值
Local DSCP	本地 DSCP 值
Time Stamp	时间戳
Forward Interface	转发接口

2.2　数据发送端

在应用发起端，根据不同的应用类型给其分配相应的 Flow Label 值。因此，在客户端需要保存如表 2 所列的项。

表 2　TOS 与 Flow Label 映射表

ToS	服务类型域
Flow Label	分配的 Flow Label 值

2.3　边界网关设计

网关处于两个自治域之间。数据发送过程中，应用发起端根据应用设置了 Flow Label 值，在其数据流进入每个自治域的入口网关时，将通过查看 Flow Label 映射表，获得在该域的 QoS 等级，这里表示为 DSCP 值，以保证数据流在本域中的 QoS 服务等级。同时，在出口网关处需要查看 Flow Label 映射表，更改 Flow Label 的值，之后再发送到下一个自治域。由此可见，应用 Flow Label 可以更好地保证端到端的 QoS 保障。该机制的关键步骤有如下两点：

在各个域的入口网关处根据收到的包的本地 Flow Label 值修改本域 DSCP 值。

在各个域的出口网关处根据收到的包的本地 Flow Label 值修改下一域的 Flow Label 值。

网关映射表结构如表 3 所列。

表 3　边界网关的 Flow Label 映射表

Local Flow Label	本地 Flow Label 值
Next Flow Label	下个域的 Flow Label 值
Local DSCP	本地 DSCP 值
Time Stamp	时间戳
Forward Interface	转发接口
GW_Type	入口/出口网关标记

3　OPNET 中模型实现

3.1　修改相关头文件

为了支持 Flow Label 操作，首先要在 IP 数据报中添加 Flow Label 域。在 OPNET 体现为头文件的“ip_dgram_sup.h”中，在 IpT_Dgram_Fields 域添加整数类型的 Flow Label 属性：

```
ip_dgram_sup.h
/* Data structure for fields in the IP datagram.    */
typedef struct
{
  ……
  int flowlabel;
} IpT_Dgram_Fields;
```

3.2　修改客户端结点

3.2.1　添加属性

“Ethernet_wkstn_adv”是 Ethernet 的用户结点模型，支持各种应用类型（Video，Voice，FTP…）。为了在客户端根据不同的应用给其分配不同的 Flow Label 值，在结点模型中添加一个“compound”类型的属性”tos_to_fl”，如图 2 和图 3 所示。包含两个整型项：TOS 和 Flow Label。

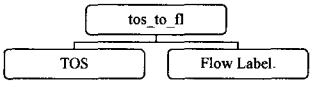

图 2　客户端新添属性结构图

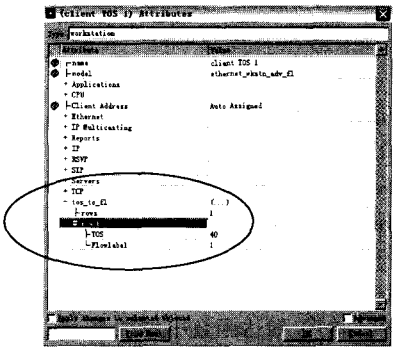

图 3　“tos to fl”属性

3.2.2　修改进程模型

更改原有的 ip_encap_v4 进程模型，在“ENCAP”状态中根据 TOS 域的值配置 Flow Label 值。具体步骤为：判断如果当前结点不是网关并且“tos_to_fl”属性存在，则读取“TOS”，将 IP 数据报中的 Flow Label 域设置为对应的“Flowlabel”值。

程序的伪代码如下：

```
IP_encap_v4_modified:
Get the "type of service" value from the ip datagram field: type_of_
service;
iFL = 0; //initialize the Flow Label value;
if (gateway == OPC_FALSE)
{
```

```
if ("tos_to_fl" exists)
{
  Get the "tos_to_fl" attribute objid;
  For every row:irow,get the "TOS" attribute;
  {
    if (iTOS == type_of_service)
    {
    Get the "Flowlabel":&iFL;
    break;
    }
  }
}
}
Set the Flow Label value into the ip datagram filed: ip_dgram_fd_
ptr->flowlabel = iFL;
```

3.3 修改网关结点

3.3.1 添加网关结点属性

在网关结点中添加"FL Table"及下属属性，如图 4 所示。

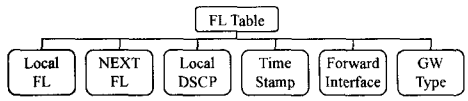

图 4 网关新添属性结构图

3.3.2 修改外部文件相关函数

在外部文件"ip_rte_support. c"中添加 Flow Label 映射表结构："FL_MAPPING_TABLE_ENTRY"，包含本地 Flow Label 值，下一条 Flow Label 值，本地 DSCP 值，时间戳，转发接口和网关类型。代码如下：

```
/ * Flow Label mapping table entry * /
typedef struct
{
    int local_fl;
    int next_fl;
    int local_DSCP;
    double time_stamp;
    int interface;
    int GW_type;
}FL_MAPPING_TABLE_ENTRY;
```

在外部文件的包到达函数中添加 Flow Label 相关操作的函数。当接收到一个从下层转发过来的包时，判断当前节点是否是网关，以及"FL Table"属性是否存在。如果存在，读取映射表并根据当前收到的包的 Flow Label 值查找映射表中对应的项。如果这是一个入口网关，则将 Flow Label 映射为本地的 DSCP 值转发给本域的核心网；如果是出口网关，则将 Flow Label 值修改为下一域的 Flow Label 转发到下一个域。

程序的伪代码如下：

```
ip_rte_packet_arrival:
{
  ……
  If this is a gateway and the packet came from a lower layer
  {
  if the "FL Table" attribute on this node exists:
    {
    Get the FL Table attribute from the node,generate_fl_mapping_
    table and set it into the list fl_mapping_lptr ;
    Get the Flow Label value from the packet field:fl_value;
    Search for the corresponded Flow Label table entry in the list fl_
    mapping_lptr,return Flow Label table entry:fl_table ;
    if(this is exit gateway)
      change the Flow Label value:fl_table->next_fl;
    if(this is entrance gateway)
      change the DSCP value: fl_table->local_DSCP;
    set the field into the packet:ip_dgram_fields_set( * pkpptr,pk_fd
    _ptr);
    }
  }
}
```

4 仿真设计和结果

在 OPNET 中搭建一个有 3 个自治域的网络拓扑模型，每个自治域由边界网关和核心网构成，如图 5 所示。

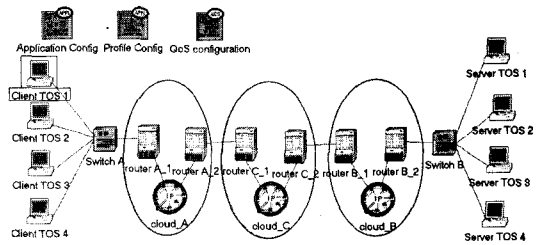

图 5 OPNET 中模型拓扑

客户端配有不同 QoS 等级的应用，DSCP 值分别为：AF11(40)，AF21(72)，AF31(104)，EF(184)，假设协商产生的对应的 Flow Label 值为 1，11，21，31。将两项对应值分别配置在"tos_to_fl"属性里。

在各个网关处，配置协商产生 Flow Label 映射表项及网关标志位。入口网关 A_1 的 Flow Label 映射表配置如图 6 所示。

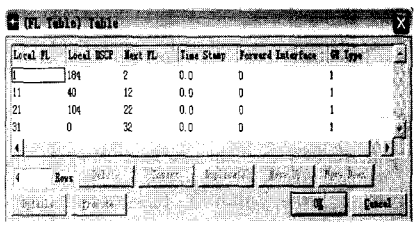

图 6 网关 A_1 的 Flow Label 映射表

运行仿真在 ODB 模式下可以看到如下结果：

在第一个自治域的出口网关 A_2 的 IP 层，Flow Label 值 21 被修改为下一域的 Flow Label 值：22，如图 7 所示。

在第二个域的入口网关 C_1 的 IP 层，Flow Label 值为 22 的包的 DSCP 值被映射为 104，如图 8 所示。

图 7 出口网关仿真输出结果

图 8 入口网关仿真输出结果

结束语 本文实现了 OPNET 中基于 Flow Label 的 QoS

映射模型，给出了详细的设计与实现方案。仿真结果表明，本文所建立的模型可以支持 Flow Label 与 DSCP 值的映射，以区分更细粒度的 QoS 等级。同时，基于 Flow Label 识别单流的特性，它可以更好地保证具有不同 QoS 策略的自治域间统一的服务等级，实现 QoS 的端到端映射。这给 Flow Label 在 QoS 保障方面的研究提供了强大的支持。

参 考 文 献

[1] Rajahalme J, Conta A, Carpenter B E. Steve Deering: IPv6 Flow Label Specification. RFC 3697, IETF, 2004

[2] Nichols K, Blake S, Baker F, et al. Black: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC2474, December 1998

[3] Robert W. McAuliffe: QoS at the Differv Network Edge. Spring, 2003

[4] Dogar F R, Zartash A. Uzmi: DiffServ Architecture: Impact of scheduling on QoS

[5] Hardy W C. QoS Measurement and Evaluation of Telecommunications quality of service. Wiley, 2001

[6] OPNET Technologies, Inc. http://www.opnet.com/

[7] 李馨，叶明. OPNET Modeler 网络建模与仿真. 2006：87-97

(上接第 283 页)

XScale、微引擎和 XScale 之间的信息交换。

5.3 电力信息网第三层防御实现

电力信息网第三层防御机制由位于电力信息子网内部的免疫计算机提供，这些免疫计算机入侵检测原理主要依据正常行为模式数据库，它通过监控自己感兴趣的应用程序，形成每台计算机特有的正常行为数据库。在计算机程序执行过程中，实时提取审计数据，将提取的审计数据转为特定的行为特征模式，供分析模块分析，检测入侵。当不匹配率超过预先设定的阈值，则产生报警。而系统自学习功能类似于生物免疫系统的再次应答，即当免疫计算机检测到新的攻击手段时，不仅产生报警，同时将该入侵的行为特征模式存入系统。当再次采用该方法入侵系统时，系统可直接向用户产生入侵信号，而不需进行入侵分析和报警，模拟生物的初次应答和再次应答，极大地提高了系统的反应速度和可靠性。

6 电力信息网关 IXP 对包的处理过程设计

首先，MSF 从外部电力信息网接收到数据包，然后将数据包交送 MSF 接口中的缓冲区 RBUF。MSF 接口中的缓冲区包括 RBUF 和 TBUF，它们可编程划分为 64，128 或 256B 的单元。一个包的数据通常要占用若干个这样的单元，存储在每个单元中的包数据，就称为一个 mpacket(MPKT)，这里采用 128B 的单元。接着，MSF 从 THREAD_FREELIST 中寻找可用线程，然后 MSF 将接收状态字写入到线程的传输寄存器中并向线程发送信号。该线程在获得信号后开始工作，读取接收信息并且将 mpacket 从 RBUF 直写到 DRAM 内存中去，然后将一个句柄放到 Scratchpad ring 上。

ME 线程检测位于 Scratchpad ring 上的可用包并取下句柄，然后对包进行检测，并取得包中的各种部分传送到 ME 的传输寄存器中。因为该入侵检测系统的各种表以及规则库存都存放在 SRAM 当中，所以它们可以被高速地查找和修改，而在 DRAM 里的数据包也将根据匹配结果被处理。接下来，被修改后的包的句柄将会被放到 SRAM 队列中，等待被调度和传送。

ME 的线程会监视 SRAM 队列中的包的句柄。如果发现已经被更新了数据的需要发送的包，那么该线程就对这些包的句柄进行出队列操作。然后该线程计算出下一个 mpacket 的位置并将它放入下一个可用的 TBUF 单元，采用直接从 DRAM 传送到 MSF。写 TBUF 单元控制字，标明 TBUF 包含有效的数据。如同接收程序，传输程序必须重复地接收 mpacket 并将其组成即将发出的包，MSF 通过 ME 支持的控制字中包含的信息检测包的结束。最后，一旦 MSF 检测到 EOP mpacket，外部设备将发出该包。接下来，IXP 网络处理器将继续处理下一个包。

结束语 本文利用 Intel 公司 IXA 架构为平台，设计了一个具有协同免疫特性的电力信息网入侵检测系统。该系统充分发挥了 IXP 网络处理器强大的分布式数据处理和快速的包转发能力，使得软件和硬件紧密结合，弥补了目前电力信息网 IDS 的不足。同时，由于使用了可编程的网络处理器，对入侵检测系统功能的升级也只需要升级软件而不需要开发硬件设备。另外，基于人工免疫的思想，提出了多层防御检测体系，使得电力信息网内每台计算机不仅仅是受保护的对象，同时参与入侵检测，大大增强了电力信息网整体检测入侵的能力。

参 考 文 献

[1] 马远东，杨文清，张官元. 电力信息网中的 RMON 网络探测器的设计与实现. 电力系统自动化，2004(12)：67-70

[2] 王焱，郑俊辉，曾家智. 一种电力信息网的新型 QoS 机制. 电力系统自动化，2007(10)：73-107

[3] 王焱，郑俊辉，易发盛，等. 电力信息网的服务元体系结构. 电力系统自动化，2007(4)：85-89

[4] Intel Corp. Intel IXP23XX Product Line Hardware Reference Manual. IXP SDK4. 2. 2004：27-195

[5] Intel Corp. Intel C Compiler for Intel Network Processors Autopartitioning Mode Reference. IXP SDK4. 2. 2005：9-25

[6] Intel Corp . Intel IXA Software Example Designs for Intel C Compiler Application Note. IXP SDK4. 2. 2005：6-55

[7] Intel Corp. Intel IXA Software Building Blocks for Intel C Compiler Developers Manual. IXP SDK4. 2. 2005：23-54

[8] Intel Corp. Intel IXP23XX Product Line Programmer's Reference Manual. IXP SDK4. 2. 2004：19-22

[9] Intel Corp. Intel C Compiler for Intel Network Processors Autopartitioning Mode User's Guide. IXP SDK4. 2. 2005：2-13

[10] 肖鸣. 分布式入侵检测系统设计[D]. 成都：电子科技大学，2002

[11] 李千目，张琨，张宏. 一种基于生物免疫学的入侵检测系统. 计算机工程与应用，2003(8)：45-48

[12] Zhang Ke, Liu Naiqi, Chen Yan. Design of Firewall Based on Intel IXP2350 and Autopartitioning Mode C // Lecture Notes in Computer Science. Vol. 3820, 2005：726-731