

# IGMP Snooping 在 EPON 中的实现方案

马东超, 陈 雪, 王立芊

(北京邮电大学光通信与光波技术教育部重点实验室, 北京 100876)

**摘 要:** 阐述一种利用 VLAN 划分组播域, 依靠侦听 IGMP 消息来维护组播 VLAN 表的 IGMP Snooping 实现思想。提出该思想在 EPON 上的基于 MAC 层和 RS 层 2 大类共 6 种实现方式。指出当前研究成果中存在的协议鲁棒性问题并给出针对数据存储和运行流程上的修改建议。得出一种无明显缺陷并克服鲁棒性问题的最优方案。

**关键词:** Internet 组管理协议嗅探技术; 以太网无源光网络; 组播

## Implementation Scheme of IGMP Snooping on EPON

MA Dong-chao, CHEN Xue, WANG Li-qian

(Key Laboratory of Optical Communication and Lightwave Technologies, Ministry of Education,  
Beijing University of Posts and Telecommunications, Beijing 100876)

**【Abstract】** This paper expatiates an Internet Group Management Protocol(IGMP) Snooping implementation thought based on dividing multicast area by VLAN and maintaining VLAN table by snooping the IGMP message. The paper subsequently brings forward and compares six implementation methods based on tow type thoughts which are on MAC layer and RS layer of Ethernet Passive Optical Network(EPON). The protocol robust problem in current research is brought forward and some modification proposals in data storage and running process aspect are given, and the most superior one is got.

**【Key words】** Internet Group Management Protocol(IGMP) Snooping technology; Ethernet Passive Optical Network(EPON); multicast

### 1 概述

组播作为一种新兴业务越来越受到人们的关注。Internet 组管理协议嗅探(IGMP Snooping)技术作为二层组播协议就是在边缘网上为了避免交换机冗余转发组播数据导致带宽损失而产生的。EPON 作为一种宽带接入方式具有很多优势。由于 EPON 系统与以太网交换机相比具有自身的特殊性, 因此就出现了 IGMP Snooping 协议在 EPON 中如何实现的问题。当前的研究成果中已经有一些实现方案<sup>[1-3]</sup>, 但实现方式存在诸如数据转发、运行效率、协议完备性方面的众多问题。本文在简述 IGMP Snooping 协议的基础上, 提出了 6 种可能的实现方案, 并作了详细比较。得出了最优方案, 有效地解决了上述的诸多问题。

### 2 IGMP Snooping 的实现简述

#### 2.1 基本思想

IGMP Snooping 基本思想是利用 VLAN 划分组播域, 侦听 IGMP 消息用来维护组播 VLAN 表。主要工作方式是: 交换机提取 IGMP 信息包, 利用侦听到的 IGMP 信息获知收听者所连接口, 为每一个组创建一个 VLAN 及组播地址和 VLAN 的映射; 交换机向所有的端口(除接收)转发侦听到的 IGMP 查询信息, 向属于同一组中的端口转发 IGMP 报告消息, 保证路由器和主机之间的 IGMP 协议状态与原来一致; 交换机根据 VLAN 表转发组播数据。采用 IGMP Snooping 的优点在于主机和路由器的软硬件设备不需要进行任何修改, 只需在两者之间加一个支持 IGMP Snooping 的交换机, 即可提供 3 层组播在二层的实现, 将组播的范围扩展到边缘子网。

交换机针对 IGMP Snooping 而定义的数据结构如下:

```
typedef struct igmp_snooping_vlan
```

```
{Int iVlanId; /*vlan id, 用以唯一标识一个 VLAN*/  
IGMP_SN_IF *pstIfHead; /*接口链表头指针*/  
VOS_IP_ADDR iGroupAddr; /*组播组地址, 32 位*/  
BOOL blReport; /*标识本次查询是否已经转发过了报告*/  
}IGMP_SNOOPING_VLAN  
typedef struct  
{ Int iIfIndex; /*接口索引, 用以唯一标识一个接口*/  
VOS_TIMERID stKeepAlTimerId; /*该接口超时定时器*/  
}IGMP_SN_IF;
```

IGMP\_SNOOPING\_VLAN 在系统中是以链表形式存放的, 每个组播组对应一个此结构变量, 即每个组播组对应一个 VLAN。而此结构中的接口链表头指针指向该 VLAN 所包括的接口集合, 其中对应每个接口存在保活定时器, 如果超时没有更新会删除该接口。接口全部删除后该 VLAN 也就不复存在, 所以每个 VLAN 是依赖于接口存活的。

#### 2.2 协议运行机制和过程(控制流)

##### (1) 初始化过程

初始时, 假设先运行了组播路由器发现协议(RFC 4286<sup>[4]</sup>), 交换机已经获知了哪些接口上连接着路由器。IGMP Snooping 创建路由器组(224.0.0.2, 与路由器相连端口)。

##### (2) 查询和报告过程

收到普通询问后, 如果当前存在对应某组播组的 VLAN,

**基金项目:** 国家“863”计划基金资助项目(2007AA01Z243, 2008AA01A328); 长江学者和创新团队发展计划基金资助项目(IRT0609); 高等学校学科创新引智计划基金资助项目(B07005)

**作者简介:** 马东超(1980-), 男, 博士研究生, 主研方向: 组播, 接入网; 陈 雪, 教授、博士生导师; 王立芊, 博士研究生

**收稿日期:** 2009-11-25 **E-mail:** madongchao@sohu.com

则遍历该结构下的所有接口，将其中的保活定时器设置为询问报文中的最大回应间隔和当前剩余值的小者。这样做的目的是为了防止路由器突然改变了最大回应间隔而能够尽量与其保持状态和参量一致。然后需要把 blReport 变量置为 TRUE。因为此时收到报告后会转发给路由器。最后把该询问报文的源 IP 改为全 0 后由从所有接口转发出去。

收到报告后首先根据报告中的组播地址查到对应的 VLAN 结构，然后在 VLAN 的接口链表中查找该接口，如果没找到就新增一个，然后启动接口保活定时器。如果找到了就仅重启保活定时器。然后查看 VLAN 结构中的 blReport 变量，如果为 FALSE，就不转发了，只有 TRUE 的时候才把该报告报文向所有路由器接口的转发。这样交换机就代理实现了报告报文的抑制功能。

### (3)离开过程

交换机不关心 IGMP 的完成报文，收到此报文后，直接向路由器所连的口转发。随后应该会收到路由器的指定地址查询报文，此时要把报文中指定的组播地址对应的 VLAN 结构找到，然后按照收到普通询问那样处理，此时需要注意的是接口保活定时器的值会按照指定地址询问报文中的回应间隔设置，也就是说会设得很小，这完全符合 IGMPv2 协议的快速离开的思想，与路由器保持了同步。

### (4)超时过程

每个 VLAN 结构中的接口的定时器超时后都要从 VLAN 结构中删除该接口，此时应该继续检查该 VLAN 中是否还存在其他接口，如果没有了就将整个 VLAN 结构删除。

## 2.3 数据转发机制(数据流)

当交换机从任一接口收到组播数据时，首先以组播 IP 地址为索引找到对应 VLAN，然后在该 VLAN 所有接口以及由路由器发现协议发现的接口上转发数据包。由于路由器所连的接口有可能也连有 PC 机，而 IGMP 报告向这个端口发送后会抑制了该 PC 机发送报告，导致交换机无法获知该接口上连有 PC 机，因此只有把组播数据报文也向路由器所连接口转发，才能避免此问题。这样做符合 RFC4541<sup>[5]</sup>。此问题的具体分析如图 1 所示。

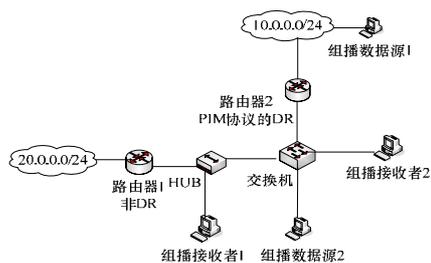


图 1 网络拓扑

路由器 1 和组播接收者 1 连在一个 HUB 上以后连在交换机上的一个口。其中组播接收者 1 和接收者 2 均想加入组 G1，交换机根据路由器发现协议发现了 2 个路由器所连接口，组播接收者 2 发送的 IGMP 报告会被交换机发送到路由器 1 和路由器 2 的 2 个接口上去，而此报告会抑制了接收者 1 的报告报文。假设组播数据源有 2 个，分别处于路由器 2 远处的 10.0.0.0/24 网段处和交换机的本地网络中，由于路由器 2 就是 DR，数据会顺路由器 2 下发下来，此时交换机跟路由器 2 所连的接口处于所有路由器的 VLAN 中，除了查找组播组对应的 VLAN 转发数据外，还要在所有路由器所在的 VLAN 中转发数据，组播接收者 1 和接收者 2 都能够正常接

收数据；但另外一个组播数据源 2 发出的数据就会出问题。数据源 2 所连的交换机的接口不在所有路由器所在的 VLAN 中，该数据只会自己在自己所在的组的 VLAN 中转发，此时组播接收者 1 由于报告报文被抑制而没能加入到这个 VLAN 中，会导致其收不到数据源 2 发来的数据。因此，要么把路由器所连的接口集合加入所有 IGMP SNOOPING 的 VLAN 中，要么在转发所有组播报文时交换机也要兼顾路由器所连接口。

## 3 IGMP Snooping 在 EPON 上的各种实现方式

EPON 系统在实现 Snooping 协议的层面上可以认为是一种分布式的以太网交换机。OLT 与路由器所连的接口可看作交换机与接入路由器所连的口，ONU 与 PC 所连口可看作是交换机连接 PC 机的接口。协议实现在 EPON 这种特殊的交换机上就会有其自身的特点，也有一定变化，具体叙述如下：

### (1)基于 MAC 层以上的实现

#### 1)仅在 ONU 侧实现

此种方式的 OLT 侧与普通 EPON 没什么区别，只在 ONU 侧加入支持 IGMP SNOOPING 的代码即可，适用于 ONU 侧有操作系统和软件模块的设备。

控制流：每个 ONU 使用的数据结构与 2.1 节中类似。协议运行机制基本一致，也要保存接口和组的对应关系以便转发组播报文时使用。

数据流：OLT 收到路由器下发的组播数据后，直接将 LLID 填为 SCB 后向 ONU 侧发。每个 ONU 的 RS 层都会收到此报文，随后会上交给 MAC 层。MAC 层此时应该根据该报文的 MAC 地址查找自己存储的组 MAC 和接口的对应关系表后转发。

#### 2)仅在 OLT 侧实现

此种方式的 ONU 侧与普通 EPON 基本一致，只在 OLT 侧加入支持 IGMP SNOOPING 的代码即可，适用于 OLT 侧有操作系统和软件模块的设备。

控制流：此方式只有 OLT 在监听 IGMP 报文，而 ONU 不听。当 OLT 发现从某个 ONU 来的报告报文后，要记录下该 ONU 和报告报文中的组播组的一个对应关系，并且向路由器侧转发此报告报文。但关于报告报文是否向路由器转发也应该遵循 2.2 节提到的抑止机制，即只报告询问后的第一个报告报文，后面只要没再收到新的询问，就不再把报告报文转发给路由器。

数据流：OLT 收到路由器下发的组播数据后，查找到对应的 N 个 ONU 后，填写 N 份数据，LLID 分别是转发表中的那些 ONU。

此种方式的缺陷是数据复制了 N 份，转发效率会因此受到影响。另外，ONU 收到后就只能转发给自己的所有接口，没能实现只向参与了该组播组的终端转发。但适用于 ONU 没有操作系统和软件模块，即 ONU 比较简陋的情况，可以做到只升级 OLT 就可达到目的。并且，在人为管理上将大量参与组播业务的终端集中连接在 1~2 个 ONU 上优化后数据的冗余转发也不会导致太大的影响。

#### 3)在 OLT 侧和 ONU 侧均实现方法 1(ONU 为主)

控制流：此种方式与只在 ONU 侧实现的唯一不同就是 ONU 要把得到的组信息用一种特殊的 OAM 报文告知 OLT，从而能够使 OLT 也能得知当前所连的接入网众多终端参与了哪些组播组。

数据流：OLT 收到路由器下发的组播数据后，先根据自身所存的信息查找对应的组播组，如果查找不到就直接丢弃

该报文,如果找到了仅填上广播的 SCB 形式的 LLID 后下发,即与只在 ONU 侧实现的方式相同。ONU 收到后所做的处理也相同。

文献[3]所提出的实现方法并不完善,具体分析如下:

4)在 OLT 和 ONU 侧均实现方法 2(OLT 为主)

**控制流:**此种方式由 OLT 监测 IGMP 报文,监测的具体机制与 2.2 节中提到的一致。需要特别注意的是,当 OLT 通过 IGMP 报告报文获知一个新的主机加入某一个组播组时,取出该报文的 LLID 和源 MAC 地址(即发出该报告的 PC 机上网卡的 MAC 地址),然后给该 LLID 所标识的 ONU 发送一个 OAM 报文,此 OAM 报文可以用新定义的一种类型实现。此 OAM 报文中要携带的信息有该 PC 机的 MAC 地址和该组播组的组播 MAC 地址。只有该 LLID 指定的 ONU 会收到此报文,它收到后首先要在自己的 MAC 地址转发表中找到该 MAC 地址对应的 PC 机所连的接口,然后新增一个转发表项,以该组播 MAC 地址为该转发表项的 MAC 地址,刚获取的 PC 机所连接接口为出接口。此出接口应该可以为多个,如果过了一段时间又收到 OLT 发来的带有同一组播 MAC 地址的另一个 PC 机的 MAC 地址的新的 OAM 报文后,要把另一个 PC 机所连的接口也加入那条转发表项的接口集合中。离开的过程在 OLT 侧与 2.2 节中提到的一致,并且 OLT 也需要给 ONU 发送 OAM 报文,通知 ONU 在对应的转发表项的接口集合中删除某一个接口即可。

**数据流:**OLT 收到路由器下发的组播数据后,只要发现 MAC 地址是组播地址,就仅是填上广播的 SCB 形式的 LLID 后下发。ONU 收到后跟单播报文的处理方式类似,就是简单地以目的 MAC 查找转发表后从出接口转发而已。但此处需要特别注意的是,此种转发表的出接口可能不止一个,要在出接口列表中的所有出接口都转发该组播报文。

此种方式虽然看似实现方式较为繁琐且舍近求远,但却有其特定的应用场合。在 EPON 系统中,OLT 和 ONU 是一对多的关系,整个系统的成本与 ONU 的成本关系很大。如果按照上文提到的在 ONU 侧实现的方案,则 ONU 的复杂度要增加很多,对 CPU,操作系统和软件模块的支持要求较高。EPON 系统的成本会由于 ONU 的数量而成倍地增加,其负面效应是可观的。如果按照“在 OLT 侧和 ONU 侧均实现方法 2”的方案实现,ONU 侧只不过把组播 MAC 也放入单播转发表中,改动非常微小,对成本的影响也比其他方法小。因此,可以在基于降低成本的考虑上采用这种方案。

(2)基于 RS 层的实现

EPON 中的 RS 层的主要作用是针对前导码中 LLID 的操作,该层处于 MAC 层的下面。设想利用 LLID 的扩展,生出一种组播 LLID,使得 IGMP snooping 得以在 RS 层实现。基本思想是定义 LLID 的最高 2 个 bit 作为模式标识,标识是组播还是单播,剩下 14 个 bit 用作容纳组播 MAC 地址的映射,即把组播 MAC 地址的最后 14 个 bit 原封不动地拷贝到 LLID 的后 14 个 bit。但是,组播 LLID 与组播 MAC 地址之间的映射以及组播 MAC 地址和 D 类 IP 之间的映射,存在同样的缺陷,都不是一一映射。但这种缺陷对 EPON 性能的影响并不大。首先低 14 bit 完全相同的可能性不大,另外即使低 14 bit 位相同了,用户端也可以在高层过滤,但容纳这种缺陷的好处是使组播得以在 RS 层实现,总体来讲还是利远大于弊。

此方式须在 OLT 和 ONU 两端实现,需两端均有操作系统支持,均能添加软件模块以实现本功能。

1)方法 1(ONU 为主)

**控制流:**与基于 MAC 层的在 ONU 侧实现的方式基本一致,唯一区别就是要在 RS 层新增一个转发表,即由组播 LLID 对应出接口集合的一种一对多的转发表。而对于 OLT,控制机制无任何变动,只有转发组播报文时有一点变化。

**数据流:**OLT 收到路由器下发的组播数据后,直接把映射后的 LLID 作为该报文的 LLID 后向 ONU 侧转发。ONU 收到后查找自己所存的 LLID 和接口的对应表后从对应接口转发。ONU 的整个处理过程不涉及对报文 MAC 地址的各种查询和操作,仅在 RS 层完成全部工作。此方式对 ONU 的改动主要是 RS 层的修改,增加了组播 LLID 的概念。即 ONU 在收到帧后 RS 层需要做 2 件事情:LLID 是自己的或广播的,此时要上交给 MAC 层作进一步处理,此种情况为单播和广播的情况。LLID 为组播的,此时要查找上文控制流中提到的为组播 LLID 新增的转发表,然后向该表项的所有出接口转发。

2)方法 2(OLT 为主)

**控制流:**此方法与基于 MAC 层实现的方案 4)较类似,也由 OLT 监测报告报文,如发现有新的组加入,则给 ONU 发送特殊的 OAM 报文。此报文要携带的信息有该 PC 机的 MAC 地址和由该组播组的组播 MAC 地址映射以后的组播 LLID。后面的处理与该方案基本一致,唯一的区别是 ONU 根据该 OAM 报文建立的组播转发表不是 MAC 层的了,而是 RS 层的,索引也由组播 MAC 地址更改为组播 LLID。

**数据流:**此方法与方法 1 一致,不再赘述。

4 各种实现方式的综合比较

上述实现方式均能满足协议,但具体在带宽利用率、对 EPON 本身的修改程度、实现复杂度以及适用环境方面有很大的差别。根据表 1 可见,第 3 种方法最优,第 6 种其次,其他方法均要差一些。

表 1 各种实现方式比较

方案名称	带宽利用率	对 EPON 本身的改动程度	实现复杂度	适用环境	综合评价
MAC 层 ONU 侧	高 (SCB)	小 (基本无修改)	小	OLT 处理能力不强,以及不希望改动 OLT 而仅改动 ONU 的情况	实现简单,功能完善,但对成本的不利影响较大
MAC 层 OLT 侧	低 (复制 N 份)	小 (基本无修改)	小	ONU 侧不希望改动,完全靠修改 OLT 就在整个系统实现该功能的情况,且对带宽利用率不敏感	存在数据冗余转发的重大缺陷,不推荐此方案
MAC 层 双侧方法 1 (ONU 为主)	高 (SCB)	中 (修改了 OAM 部分)	中	希望组播流量的过滤在 OLT 就实现的情况	与第一种基本相同,OLT 所增内容意义不大
MAC 层 双侧方法 2 (OLT 为主)	高 (SCB)	中 (修改了 OAM 部分)	中	ONU 修改少,处理能力弱,对成本影响最小的情况	实现比较简单,功能完善,同时实现成本的最小化,是最优的方法
RS 层 ONU 为主	高 (SCB)但存在非一一对应问题	大 (修改了 OAM 部分和 RS 层的 LLID 格式)	中	不希望 MAC 层以上过多参与组播的情况	实现比较简单,功能也算完善,但对 IEEE802 协议的修改会影响设备的互通性
RS 层 OLT 为主	高(SCB)但存在非一一对应问题	大 (修改了 OAM 部分和 RS 层的 LLID 格式)	中	同上,并要求 ONU 修改少,处理能力弱,对成本影响最小的情况	实现比较简单,功能也算完善,同时实现成本的最小化,但对 IEEE802 协议的修改会影响设备的互通性

## 5 现存的问题及解决方案

### (1)关于路由器所连接口的数据转发问题

组播数据报文除了向该组播组对应 VLAN 的所有接口转发外,也不能忽略路由器所连接口,具体原因及拓扑图见 2.2 节的数据流部分。此时如果一味地追求避免冗余转发,很有可能导致某些接收者接收不到数据的情况。根据文献[6]中的加入 VLAN 的机制会有此问题存在。只有把路由器所连接口加入到每一个组播组对应的 VLAN 中,才能保证所有收听者均能正常收到组播报文。

### (2)关于 EPON 系统运行 IGMP Snooping 的效率问题 1

MAC 层双侧方法 1(ONU 为主)和文献[1,3]中提到的 OLT 通过 ONU 上发的特殊 OAM 报文学习组播组信息的方法对系统效率有影响。OLT 保存这些信息的唯一目的就是过滤组播数据报文,即每次 OLT 从路由器处收到下发的组播报文后,都要查看组播组信息是否存在,如果不存在就丢弃,如果存在,也并无特殊处理,仅将 LLID 填为 SCB 后下发。这样做不妥的原因有以下几点:

1)路由器不会无端下发组播报文。路由器只有收到了报告报文才会在组播路由协议如 PIM 中的(\*,G)表项中加入此出接口,从而导致路由器将该组的数据报文转发到 OLT。

2)OLT 做的检查是 MAC 层的检查,检查如发现存在该组,则报文将发到 ONU 处,ONU 还要检查该组播 MAC 地址对应自己的那个接口,然后将该组播报文转发给接收者。在此情形下,绝大多数正确的报文要检查 2 次,OLT 和 ONU 各一次,有失效率。如果 OLT 不作此检查,一方面在控制流上省去了对 IGMP 协议的支持,一方面在数据流上省去了一次对每个组播报文的检查(对整个 EPON 系统而言),还是有效率的。

### (3)关于 EPON 系统允许 IGMP Snooping 的效率问题 2

EPON 系统对组播组成员状态的保存有 2 种选择:1)按文献[3]中保存每个成员到一个成员列表中。2)按上文提到的仅保存某一组有成员还是没成员。根据 IGMP 的基本思想,只关心有没有人听,而不关心收听者都有谁,也不关心收听者的数量和其他信息,进而达到协议的最优化。存储全部成员网卡的 MAC 地址并无实际意义,并且对整个系统的存储空间和运行效率提出更高要求。

### (4)关于 ONU 退出组播组的协议完备性问题

一味追求退出时组播分支快收敛会导致协议不完备。按

照文献[1,3]的方法,当 OLT 收到来自 ONU 的特殊 OAM 帧时删除该组播组虽可能快速剪枝,但该 ONU 只知道自身上无其他成员存在,对其他 ONU 上是否有组成员存在并不了解。此时如果通过 OAM 报文的方式在整个 EPON 系统中删除该组的话,其他 ONU 上如确实存在组成员,就会引起组播转发表动荡,使正常的终端短时间内无法收到数据。按照上文提到的方式可避免此问题。

### (5)关于组播 MAC 的非一一对应问题

文献[1]将组播 MAC 地址的低 14 位映射进组播 LLID 的低 14 位和文献[3]中组播转发表用 MAC 地址作为索引都会带来非一一对应问题。但若若干低位完全相同的可能性不大,另外即使若干低位相同了,用户端也可以在高层过滤,对整个系统影响不大。解决此问题的办法是:要么认为此问题是小概率事件,影响不大而不加处理;要么按照 2.2 节描述的机制,即在转发表中用组播 IP 地址标识<sup>[5]</sup>(符合 RFC 4541),再处理组播报文时,要取得 IP 头中的 IP 地址,这虽然使得 EPON 系统读取了本不该自己关心的层次,但具体实现中也仅是指针后移几位的问题,不会对效率和系统其他方面有很大影响。

## 6 结束语

本文提出了 6 种 IGMP Snooping 协议实现方法,从多个角度全面地比较了这些方法的优劣。第 1 种方法从综合起来考虑是最优的,即在 MAC 层、ONU 端实现,无论是从改动工作量、复杂度还是带宽占用率等方面看,都占有明显优势。后续的研究就是在不提高 ONU 成本的前提下,部署和贯彻这种方法。

### 参考文献

- [1] 张伟,肖定中,孟玉. EPON 系统 LLID 组播实现初探[J]. 光通信研究, 2005, (3): 28-30.
- [2] 杜旭,张连靖,余江,等. IGMP Snooping 协议实现方案[J]. 计算机应用, 2004, 24(z1): 14-15.
- [3] 王光伟,邹郁妮,叶家骏. 组播技术在 EPON 中的实现[J]. 光通信技术, 2005, 29(6): 7-9.
- [4] Haberman B. Multicast Router Discovery[S]. RFC 4286, 2005.
- [5] Christensen M. Considerations for IGMP and MLD Snooping Switches[S]. RFC 4541, 2006.
- [6] 王军,吴志美. 交换式以太网上的多播协议[J]. 软件学报, 2003, 14(3): 496-502.

编辑 顾逸斐

(上接第 106 页)

在以后的应用中如果需要改变当前网络的状况,可以根据网络业务类型调整关键指标,使其参数值保持在用户可接受的范围内。如在用 TCP 协议传输数据时,为保证数据的正常传输,实际可用带宽至少为数据传输可用带宽临界值的 2.5 倍。

## 7 结束语

本文介绍基于 LMS 模型的卫星通信网络实验平台、测试系统和评估方法,分析一般的卫星通信网络测试方法,通过实验数据得出性能指标集对网络当前性能状况的影响。卫星通信网络评估技术是前沿课题,今后将进一步完善卫星通信网络的测试工具和评估技术,从而为卫星通信网络的应用和

管理提供理论依据,提高通信质量。

### 参考文献

- [1] 王丽娜,王兵,周贤伟,等. 卫星通信系统[M]. 北京:国防工业出版社, 2006.
- [2] 马 上. 实时 LMS 信道模拟器设计与实现[D]. 成都:电子科技大学, 2006.
- [3] Balakrishnan H, Padmanabhan V N, Fairhurst G, et al. TCP Performance Implications of Network Path Asymmetry[S]. RFC 3449, 2002.

编辑 陈 晖