分类号_____ 密级_____

U D C_____ 编号_____

華東交通大學

硕 士 学 位 论 文

10G EPON 安全承载多业务下的组播 IPTV 调度设计

学 位 申 请 人： 丁以胜

学 科 专 业： 信息与通信工程

指 导 教 师： 殷爱菡 教授

答辩日期：

华东交通大学 2016 届硕士学位论文

10G EPON 安全承载多业务下的组播 IPTV 调度设计

信息工程学院

丁以胜

独创性声明

本人郑重声明：所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表和撰写的研究成果，也不包含为获得华东交通大学或其他教育机构的学位或证书所使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

本人签名_____日期_____

关于论文使用授权的说明

本人完全了解华东交通大学有关保留、使用学位论文的规定，即：学校有权保留送交论文的复印件，允许论文被查阅和借阅。学校可以公布论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存论文。

保密的论文在解密后遵守此规定，本论文无保密内容。

本人签名_____导师签名_____日期_____

10G EPON 安全承载多业务下的组播 IPTV 调度设计

摘要

近年来，随着“三网融合”的不断深入，HDTV、VoIP、视频广播、多画面分割、时移窄播等先进的多业务相继涌现，10G EPON 网络作为一种先进的接入技术，无疑成为承载多业务的首选。然而由于 10G EPON 点到多点的拓扑结构，导致系统具有一定的安全威胁。同时，用户对业务需求呈现多样化，而不同的业务对于服务质量(QoS)的要求也并不相同，所以研究安全环境下的 10G EPON 承载多业务变得十分重要。

本文首先简单的介绍了 10G EPON 的基本结构和上下行数据传输原理，重点分析了其点到多点的网络拓扑结构带来的安全威胁，提出了 OLT 和 ONU 双向认证的必要。接着提出了基于 NTRUsign 的身份认证方案，利用 MPCP 协议帧，嵌入到 10G EPON 的注册过程中，解决了 OLT 和 ONU 的双向身份安全问题，为 10G EPON 承载多业务提供了安全保障。然后根据不同业务对 QoS 需求不同，尤其是 IPTV 业务占据大量带宽，对其它业务造成冲击，论文提出了基于 VLAN 单/组播技术的多业务情形下 IPTV 队列分类调度方案，首先根据区分服务模型进行分类，一般类业务和 IPTV 类业务分别进入单播和组播缓存队列中，然后再利用 WRR 调度算法给组播 IPTV 业务的不同等级队列分配合理带宽，最后传送给用户，满足不同用户需求。

论文最后给出了 10G EPON 网络系统安全承载多业务下组播 IPTV 业务队列调度方案的 FPGA 硬件设计，包括 OLT 端的 MPCP 控制、Frame 过滤、RS 发送、Proxy_Up 侦听和 OLT 分类调度五个模块，以及 ONU 端的 RS 接收、MPCP 控制、Snooping_Up 侦听和下行数据传输四个模块，初步实现了硬件设计。

关键词：10G EPON，NTRUsign 认证算法，双向认证，组播 IPTV，分级调度

A DESIGN OF MULTICAST IPTV SCHEDULING ALGORITHM UNDER MULTI-SERVICE-BASED 10G EPON

ABSTRACT

In recent years, HDTV, VoIP, video broadcasting, multi-split screen, time-shifted narrowcasting and other advanced multi-service have emerged with the deepening of the "triple play". As an advanced access technology, 10G EPON is regarded as the best choice of multi-service bearer undoubtedly. However, due to the point-to-multipoint topology of 10G EPON, it faces some security threats. Simultaneously, business users requirements remian diversified, and the quality of different business service are also not the same, thus it is essential to study how 10G EPON carries multi-service under secure network.

This paper simply introduces the basic structure and uplink/downlink data transmission principle of 10G EPON, analyzes the network topology of its multipoint security threats, and proposes the necessarity of mutual authentication between OLT and ONU. Then we have proposed a scheme that emdeds NTRUsign into the registration phase of 10G EPON to solve the two-way identity of OLT and ONU, which provides a secure condition for 10G EPON to carry mulitiple services. As for different business remain different QoS needs, especially IPTV service occupies much of the channel bandwidth and causes negative influence on other business. Thus, the paper proposes a multi-service scenario based on a single VLAN / Multicast IPTV queue scheduling classification scheme, first all business can be classified into general class services and IPTV multicast services according to Differentiated Services Classification model, then they respectively step into unicast and multicast cache queue, and WRR scheduling algorithm is used for allocating reasonable bandwidth to satisfy the needs of different users.

Finally, FPGA hardware design of queue scheduling program of IPTV services under multiple service based on 10G EPON is given, including OLT MPCP control terminal, Frame filter, RS transmission, Proxy_Up listening and OLT classified scheduling five modules, and ONU receiving end of the RS, MPCP control, Snooping_Up listening and downstream data transfers four modules, realizing the basic hardware design of EPON network.

Keywords: 10G EPON, NTRUsign authentication algorithms, mutual authentication, multicast IPTV, hierarchical scheduling

目录

主要符号说明

PSK	预共享密钥
KD-HMAC-SHA256	密钥导出算法；
K	临时加密密钥；
d_f	密钥 f 的参数；
d_g	密钥 g 的参数；
NormBound	验证签名值有效的边界值；
$E(x, y)$	用密钥 x 加密 y；
$D(x, y)$	用密钥 x 解密 y；
r_1	ONU 端随机生成参数；
$a\|\|b$	a 和 b 串联起来；
PK_X	X 的签名公钥；
SK_X	X 的签名私钥；
K_{XY}	X 和 Y 的会话密钥；
R_X	X 产生的随机值；
s_X	NTRUSign 算法中 X 的签名；
$h(X)$	X 的哈希函数；
C_X	X 的证书；
W_i	WRR 算法权值；
n_{ij}	第 j 个队列当中第 i 个数据流的分组数；
k_i	第 i 个队列中数据流的个数；
q_i	服务优先级；

第一章 绪论

1.1 引言

近年来，随着 IPTV 视频、互动游戏、社交网络等各种业务的发展，数据流量激增，对运营商和制造商在网络带宽、系统成本、功耗方面提出了更高的挑战。因此，当前的 EPON 接入技术无疑成为了最具吸引力的解决方案[1]。

据悉，截止到 2016 年，亚太地区超过 50%的宽带用户将会使用 FTTx 技术[2]，在中国，“宽带中国战略”推动 FTTX 宽带提速快马加鞭，在三大运营商的推动下，中国成为 FTTX 发展最快的市场[3]。尤其是中国三网融合的诉求，更需要具有演进能力与领先带宽的接入网络，EPON 技术也成为目前广电双向改造的最佳选择，尤其是 10G EPON，能快速提升网络带宽，满足多层次的业务需求，快速提升网络综合竞争力。

众所周知，利用 10G EPON 接入网技术承载 IPTV 业务、VoIP 业务和高速上网，即所谓的“三网融合”，其中，IPTV 业务近年来尤为受到大众的欢迎[4]。但是，随着 10G EPON 网络承载多种业务应用的同时，有两个方面的问题急需解决，一个是 xPON 网络固有的身份安全问题[5]，另一个是多业务传输的情况下如何保证当前用户喜爱的 IPTV 业务与其它业务的带宽合理分配问题[6]。

1.2 EPON 发展现状

据 2013 年的中国互联网发展报告显示，中国互联网用户近期高达 5.64 亿。随着网络游戏、高清视频、专网互联等各种应用的广泛使用，用户对接入网的带宽要求也不断提高，传统的 ADSL、LAN 和 WLAN 等接入技术因距离、带宽和接入介质等因素限制已无法满足用户的业务需求[7]。从而，无源光网络 (Passive Optical Network，PON)作为一种良好的接入技术尤其受到人们的关注。

在 IEEE 标准下，基于 IEEE 802.3 以太网帧结构的 EPON 标准在 2004 年完成，能够为终端用户提供各种高速可靠的的数据、语音和视频等业务。然而，近年来 EPON 提供的上下行对称 1Gbit/s 速率已不能满足用户日益增长的业务需求，人们又在 2006 年提出 10G EPON 系统标准 IEEE802.3av，并在 2009 年 9 月正式获得批准。此标准能够和 1Gbit/s EPON 设备进行无缝兼容，完成 1Gbit/s 到 10 Gbit/s 速率的平滑过渡。现阶段投入使用的 EPON 网络是 1G 和 10G 两种速率共存。由于 EPON 帧结构和以太网 IEEE802.3 帧结构基本相似，可以实现无缝兼容，并且受地域用户居住楼层分布原因影响，当前 EPON 网络在韩国、中国、日本等亚洲国家使用尤为普遍，占据主导地位[8]。截至 2013 年底 EPON 用户总数已达到 8000 万，仅在 2015 年 1-3 月，我国三家基础电信企业互联网宽带接入用户就净增 137.2 万户，总数达到 2.04 亿户。目前，10G EPON 网络系统技术成熟，进入门槛很低，拥有广泛的市场使用前景[9]。但是，随着 10G EPON 网络部署

规模的逐渐增大，其固有的 PON 树形拓扑结构带来的安全问题也突显出来，因为其下行数据传输采用广播发送的方式，非法用户能够窃听下行传输的信息，然后根据这些信息伪装成合法的 ONU 甚至是 OLT 来攻击 EPON 网络系统，造成网络瘫痪。因此，为避免这些安全问题，对 EPON 网络的 OLT 或者 ONU 进行身份验证很有必要。

1.3 IPTV 发展现状

自从 1999 年英国的 Video Networks 公司率先推出 IPTV 业务以来，IPTV 这项新兴技术就一直广泛受到市场的关注，全球多家电信运营商也纷纷进驻 IPTV 市场。从全球 IPTV 的用户和分布区域来看，欧洲、北美和亚太部分国家业务发展的更为迅猛，而且随着带宽需求的剧增和“光进铜退”方针在全球的推广和实施，传统的 DSL 接入技术已逐渐淡出历史舞台，大部分运营商都采用 FTTB 传输技术，甚至部分国家直接全部采用光纤接入，如奥地利电信就使用 FTTH 的接入方式[10]。

近年来，随着亚太地区、中东、非洲和拉丁美洲持续增长的宽带注入，IPTV 业务必将极大发展，同时用于传输 IPTV 业务的基础设施建设也将全面展开。全球情报及市场调研精确供给公司 Transparency Market Research 在《IPTV Market：Global Industry Analysis, Size, Share, Growth, Trends and Forecast,2014-2020》报告中指出[11]：全世界的 IPTV 市场在 2013 年评估为 249.4 亿美元，预计到 2020 年达到 793.8 亿美元，从而 2014 年到 2020 的 CAGR（Compound Annual Growth Rate,符合年增长率）为 18.1%。促进 IPTV 市场增长的关键因素有四点，即高清和点播业务的需求、伴随 IPTV 业务的各种混合业务的添加、各国家政府政策引导的宽带业务扩展以及 IPTV 业务费用的降低，而在 IPTV 生态系统当中由于大量的市场参与者使得 IPTV 市场主要分为五大部分，为 IPTV 运营商、软件解决方案供应商、中间设备供应商、业务传输网络供应商和机顶盒供应商。同时，报告还指出 IPTV 的终端用户使用群主要分为小型企业、中型企业和大型企业，在 2013 年的 IPTV 市场评估中，中型企业占据主导地位。其中，IPTV 业务供应商领先者为了提高市场收益将重点关注中型和小型企业，预期小型企业在不久的将来也使用 IPTV 业务，促进用户收益在 2020 年达到预估目标。另外，IPTV 业务供应商提供的交互业务、多屏幕多视角业务以及多种定制级的 IPTV 业务是小型、中型和大型企业使用 IPTV 业务最大的源动力。

在西欧 IPTV 市场中，法国、德国、荷兰、英国、比利时一路领先，拥有最大数量的 IPTV 订购用户，而持续的宽带注入和基础设施的支持是 IPTV 使用市场增长的主要原因。IPTV 业务的注入（包括追看和记录电视服务）在法国尤为受到欢迎，超过 70%的电视机都拥有 IPTV 连接。在英国，IPTV 市场用户受到有线电视和卫星电视严重冲击，IPTV 业务的注入明显少于其它国家。

在北美国家的 IPTV 市场中，加拿大走在美国的前面，但是美国的 IPTV 发展的更为平稳。加拿大的电信公司 MTS 和 SaskTel 利用 xDSL 技术最早开通了 IPTV 业务，到

2007 年，加拿大的 IPTV 用户为 10 万，截至 2014 年，加拿大电信商的 IPTV 网络电视用户保有量为 880 万左右，市值达到 65 万亿美元。美国的 IPTV 业务是从 2001 才刚刚踏入商用阶段，并由德克萨斯州慢慢扩展到其他城市，当时能提供的 IPTV 业务只有 180 个数字及音乐频道。到 2013 年，美国 IPTV 的市场用户总数突破 1550 万。2015 年 5 月，美国广播电视协会（NAB）的副总裁克里斯.布朗在北京港澳中心的发布会上表示美国卫星电视用户有所下降，而通过互联网收看电视的用户则以每年 10%的速度增长，其中 IPTV 业务发展最为迅速[12]。同时，美国网络解决方案供应商，思科（Cisco）公司发布了 2009-2014 全球网络协议流量增长数据分析统计示意图，预期从 2009 年到 2014 年将实现以四倍的速度增长，达到 63.9 艾字节/每月，766.8 艾字节/每年，其中 IPTV VOD 业务占据重要地位[13]，如图 1-1 所示。

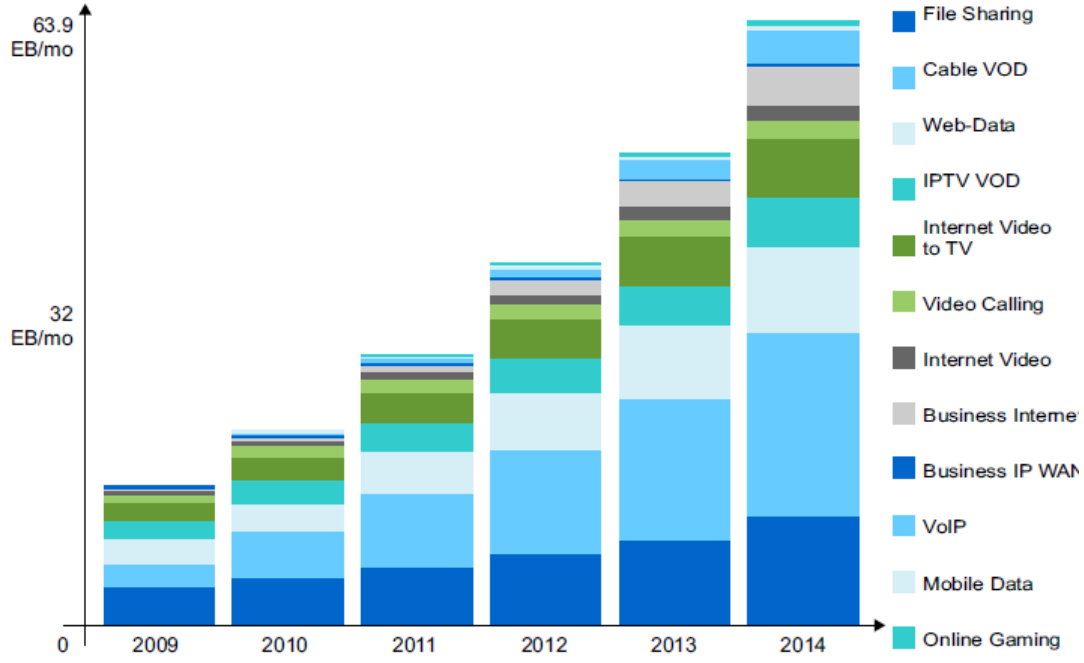

图 1-1 来自思科的全球因特网协议流量统计 2009-2014

Fig.1-1 Statistics of the Global Internet Protocol Traffic from Cisco 2009-2014

2005 年，中国通信标准化协议成立了 IPTV 特别工作小组，开始着手研究和制定我国 IPTV 标准的工作。中国香港电讯盈科在开展 IPTV 业务方面是全球最好的运营商之一，到 2005 年 6 月其带宽电视用户已经到达 44 万。同年，上海文广新闻文化公司和中国电信进行合作，在上海推出 IPTV 业务，并获得中国大陆第一张 IPTV 牌照，以百事通公司（BesTV）为品牌，而且由百事通公司提供内容的 IPTV 用户近年来发展势头良好。在 2010 年初,国务院做出了推动电信网、互联网以及广电网三网融合的决定，促进了我国 IPTV 市场快速发展。IPTV 的用户总数从 2004 年的 4.6 万增长到 2007 年的 120.8 万，而到 2008 年底，全国 IPTV 用户数突破 300 万，到 2011 年，IPTV 用户规模首次突破千万。而且在 2012 年初，上海广播电视台和中央电视台原建设的 IPTV 集成播控平台

进行合并，成为中国唯一的 IPTV 中央集成播控总平台，双方将把各自拥有的频道和节目资源投入到总平台[14]，对中国 IPTV 产业市场有着重要意义，IPTV 真正驶入快车道，用户数目达到 2300 万，2013 年 IPTV 国内用户数目达到 3300 万，截至 2015 年，工信部统计国内 IPTV 用户数达到 3600 万[15]。

IPTV 用户在全国激增，占据巨大带宽，无疑给其它新业务带来冲击，如网络高清直播视频、视频广播、多画面分割、时移窄播等。10G EPON 网络在承载这些多业务的情形下，如何根据用户订购需求进行区分对待，合理分配带宽，将是本文需要解决的问题。

1.4 EPON 承载 IPTV 研究现状

在 EPON 网络系统上承载 IPTV 业务，当前亟待解决的为两个方面的内容，一个是 PON 网络当中固有的身份安全问题在 EPON 网络系统中仍然存在。为此，人们提出了很多的身份认证方案。最早的认证方案是直接边缘认证模型，即在 OLT 和 ONU 之间需要添加可信任的第三方认证服务器，每当 ONU 需要验证身份时，先发送请求给 OLT，当 OLT 收到该信息时，不是立刻进行身份核查，而是转发给第三方认证服务器进行身份核对，然后告知 OLT 结果。文献 16 和 17 通过有效的密钥管理，分别实现用户认证和 ONU 认证。文献 18 和 19 在有效密钥管理的基础上，分别使用 MD5 和 ECC 算法实现 OLT 对 ONU 的身份认证。另外，文献 20 提出了基于 GMAC 的高级身份认证方案，能同时完成认证和加密功能。然而，这些身份安全解决方案虽然能提供高等级的认证，但是要么总体结构过于复杂（需要第三方认证服务器），要么与已有的 MPCP 帧不兼容，从而带来许多的缺点，诸如降低注册效率、更长的传输延迟响应、与已有的 EPON 网络基础设施不匹配。

EPON 网络承载 IPTV 业务急需解决的另一个问题为服务质量（QoS）问题。因为随着 IPTV 业务的需求（如高清视频及图像）成指数倍剧增，产生大量的数据，占据较大的接入带宽，对其它业务造成冲击，而实现多业务环境下的 IPTV 业务队列合理调度是目前迫切需要解决的问题。现有的文献研究中主要方案有（1）采用一种新型的双 PON 通道 EPON 扩展网络结构，即在原有 PON 结构上新添加一条无源光网络通道单独传送 IP 组播数据流[21]。（2）组播 LLID 方案[22]。通过新定义 LLID 字段，增加组播逻辑链路标识 LLID，把高两位作为模式位：“00”为单播数据，“11”为广播数据，“01”为组播数据。而且组播 LLID 的其它 14 位由组播 MAC 地址的低 23 位经过函数映射得到，实现在 RS 子层过滤组播数据。再结合运用 IGMP Snooping 机制以及操作管理维护（OAM）帧对用户进行管理。（3）基于 VLAN 的组播方案[23]。该方案是采用端口划分 VLAN 方式，将组播成员按端口划分到同一个组播 VLAN 中，并在 EPON 帧的源地址字段和类型字段之间插入一个 4 字节的 VLAN 标识。上述各种方案在解决 EPON 系统承载 IPTV 业务方面取得了一定的成效，但是仍然存在许多不足之处如 EPON 网络结构变的复杂、OAM 帧的传播延迟影响组播通信性能、ONU 到各用户之间局域网仍以广播方式发送组播数

据、OLT 端把 IGMP 响应报文透传到上端服务器而造成核心网带宽损失等。因此，如何设计一种在安全的 EPON 网络环境中实现 IPTV 业务合理分配，满足用户体验，是本论文重点研究的内容。

1.5 课题来源及论文结构安排

本课题来源于导师国家自然科学基金项目“PON 网络架构加密机制及时间相关函数算法研究”(61262079)。

本文研究的主要内容为在身份安全保障的 10G EPON 网络系统中如何实现多业务情形下合理分配 IPTV 业务和其它业务。针对 EPON 网络系统固有的身份安全问题，本文首先设计了一种基于 NTRUSign 的签名算法实现对 OLT 和 ONU 的双向身份认证。在保证 EPON 系统身份安全的基础上，进一步研究当前 EPON 承载多业务下用户关注的 IPTV 业务的 QoS 问题，提出了一种基于 VLAN 的单/组播多业务划分方案，并给出了详细的设计方案和模块设计。论文的主要结构安排如下：

（1）第一章首先介绍了当前 10G EPON 和 IPTV 发展现状，然后重点分析了 10G EPON 亟待解决的身份安全问题和 10G EPON 承载 IPTV 需要解决的 QoS 问题，最后介绍了本论文课题来源以及结构安排。

（2）第二章首先简要概述 EPON 体系结构和工作原理，重点介绍了多点控制协议帧结构及其功能，分析了 EPON 系统的安全威胁，指出双向身份认证的必要性。然后介绍了认证技术的基本概念和常用的数字签名认证技术，选用目前较新的认证算法 NTRUsign 作为本文的认证算法。最后介绍了 IPTV 业务，分析了 EPON 承载 IPTV 业务的可行性，指出组播技术和区分服务模型的必要性。

（3）第三章重点介绍本文设计的一种基于 NTRUSign 签名算法的双向认证方案。首先概述了本方案的实现流程，然后详细描述了本方案的具体内容和本文自定义的三个帧的结构及其作用。最后对本方案进行抵抗攻击能力和注册效率影响分析。

（4）第四章在解决掉 EPON 系统固有的 OLT 和 ONU 身份安全问题的基础上，重要分析 EPON 承载多业务情况下如何设计 IPTV 业务的 QoS 问题。本章首先分析了 EPON 承载 IPTV 业务需要解决的几个关键问题，然后给出了具体的设计方案和详细的模块设计，最后介绍 IPTV 业务授权、加入、切换等实现流程。

（5）第五章根据第四章的设计方案对 EPON 系统中的 OLT 和 ONU 控制模块进行了详细的 FPGA 模块设计。

（6）第六章对论文进行总结和下一步工作的展望。

第二章 EPON 技术、IPTV 业务和 NTRUsign 认证算法

2.1 EPON 网络系统

2.1.1 EPON 基本结构和工作原理

EPON（Ethernet Passive Optical Network,以太无源光网络）是 PON 网络中发展比较成熟，利用 WDM（Wavelength Division Multiplexing,波分复用器）技术在单纤上实现双向数据传据的光接入网络，其网络拓扑结构为典型的树型结构，采用点到多点的广播方式向下行方向发送数据。

EPON 网络系统以标准以太网协议作为基础,继承了以太网使用过程中积累的宝贵技术经验，力争将标准化工作框定在 802.3 体系当中，重点对 EPON 的 MAC 层接口、MPCP(Multiple Point Control Protocol,多点控制协议)、OAM (Operation、Administration、Maintenance,运行管理维护)等关键新技术重新进行了明确的定义。

EPON 网络系统的基本结构如图 2-1 所示，主要包括 OLT（Optical Line Terminal，光线路终端）、ODN（Optical Distribution Network，光分配网络）、ONU（Optical Network Unit，光网络单元）三个部分，其中 SNI 为业务节点接口，NMI 为网络管理接口，IFPON 是 PON 网络的专用接口，UNI 为用户网络接口。

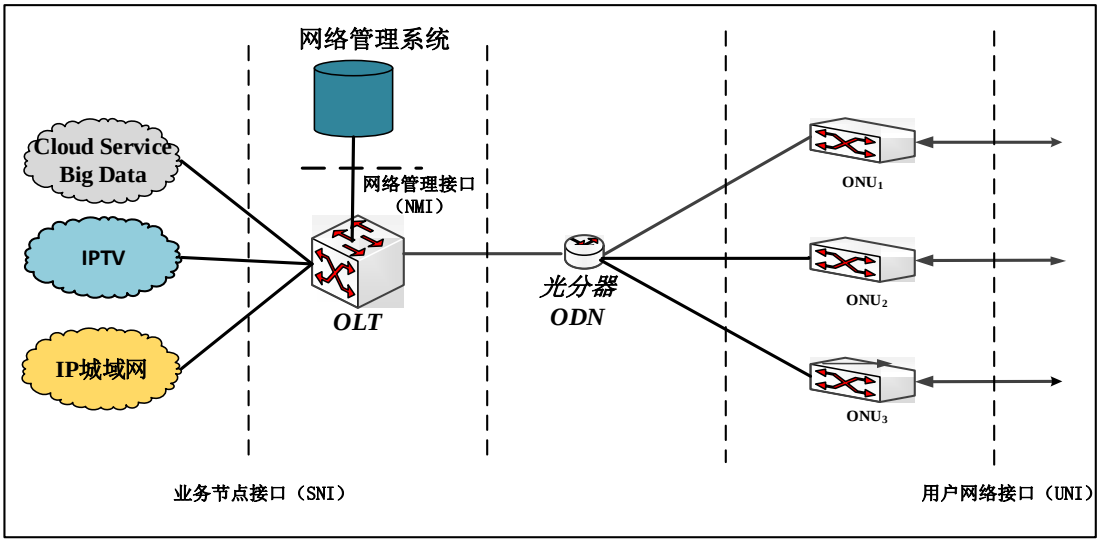

图 2-1 EPON 网络系统基本结构图

Fig.2-1 The Basic Structure of EPON System

（1）OLT：是 EPON 网络系统中的关键设备，工作在 ODN 与城域核心网之间，能够实现城域核心网与用户间不同业务的区分和转发，并管理局端 ONU 相关的监控信息和控制信令。OLT 主要携带两类接口，即 SNI 接口和 IFPON 接口。SNI 接口主要用于为核心网和城域网提供接入服务，IFPON 接口主要作用是连接 ODN 网络，为 ONU 向用户端发送信息提供点到多点的业务服务。

（2）ODN：位于 OLT 和 ONU 之间，为 OLT 和 ONU 的物理连接和数据传输提供技术支持，主要包括 POS（Passive Optical Divider，无源光分路器）、光衰减器和光纤等无源器件。ODN 主要有两个作用：一是将来自 OLT 端的下行业务流按照分配机制发送给各个 ONU 局端；另一个是将来自 ONU 端的上行请求信号有序的耦合到同一根光纤中，传送给 OLT。

（3）ONU：拓扑中位于 EPON 网络系统的用户端和 ODN 之间，主要包括两类接口，即 IFPON 接口和 UNI 接口。IFPON 接口同 OLT 端的 IFPON 接口是一一对应的，接收来自 OLT 端发送的下行信息；UNI 接口同终端用户直接相连，将来自 OLT 的数据信息经过 ONU 处理分类后，分发给相应的终端请求用户。

EPON 网络系统通过在一根光纤上使用不同的波长来传输上、下行方向的业务信息，其中下行数据通道一般使用 1480-1510mn 的波长，上行数据通道通常使用 1260-1360mn 的波长。为了适应这种单纤上传递多个用户的数据包并分离信号的传输模式，上下行传输方向需要用到两种不同的复用技术，即 TDM 方式（Time Division Multiplexing,时分多路复用）和 TDMA （Time Division Multiple Address，时分多址）方式。下面对 EPON 上下行方向的数据传输做详细介绍：

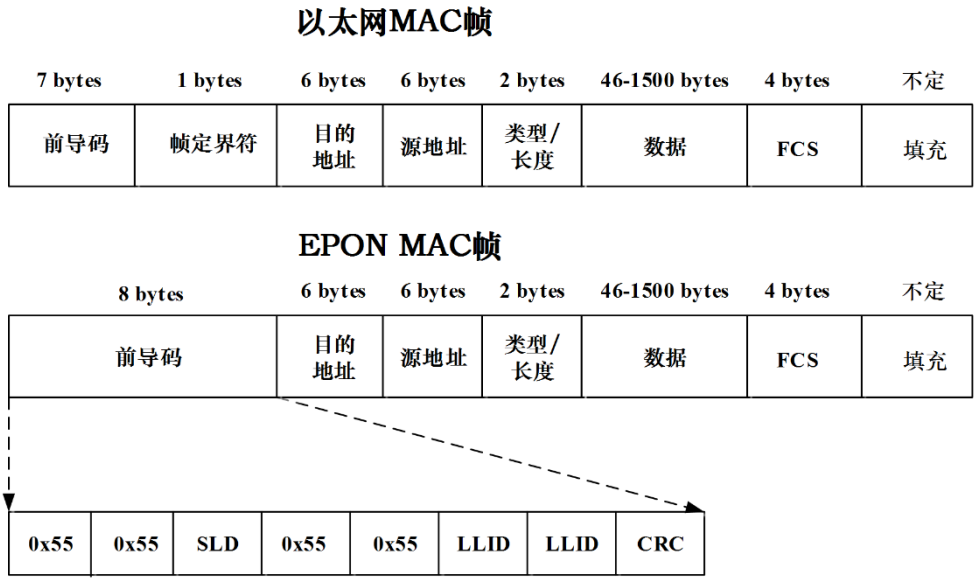

图 2-2 EPON 的帧结构

Fig.2-2 The Frame Structure of EPON System

EPON 下行数据传输工作原理

EPON 网络的数据帧格式是基于 IEEE802.3 的，为 IEEE 802.3ah，在不增加帧长度的基础上，只是对标准以太网帧头部分的前导码和 SFD (Start Frame Delimiter，帧首定界符)字段做了一些简单更改，前导码外的后续相关帧字节的定义同标准以太网帧结构是完全相同的，如图 2-2 所示。其中一个字节长度的 SLD（Start of LLID Delimiter，定界符）携带同步信息，每隔 2ms 便会自动发送一次同步标记，使 ONU 和 OLT 始终保持

同步。第 2、4、5 这三个字节为 EPON 网络前导码的保留字节，作为未来扩充功能使用。第 6、7 这两个字节用来存放 EPON 网络帧格式中新增加的 LLID（Logical Link ID，逻辑链路标识符）信息,它是 ONU 接收数据的唯一标识，用于说明哪个 ONU 应该接收此数据帧。其中 LLID 只能在 EPON 系统内部才有效，当 ONU 接收到来自 OLT 发送的 EPON 帧后，将去除 LLID 等相关信息，转换成标准以太网帧转发给请求业务的终端用户。标准以太网的 SFD 字段作为 EPON 网络前导码的 CRC 校验码,用于增加前导码的可靠性。

图 2-3 为 EPON 网络系统下行方向传输数据的流程图。首先 OLT 会将终端用户请求的数据以 TDM 的方式统一复用到一根光纤上，这些数据信息通过协议过滤机制各自携带一个唯一身份标识 LLID，然后，经过光分配网络 ODN 把这些数据采用广播的方式发送给所有的 ONU。每个 ONU 都可以接收到 OLT 广播的所有信息，然后根据 LLID 的唯一性来检测该信息，只接收属于自己的数据，将不属于自己的信息直接丢弃，图 2-3 中终端用户 1 只接收信息 1，终端用户 2 只接收信息 2，终端用户 3 只接收信息 3。

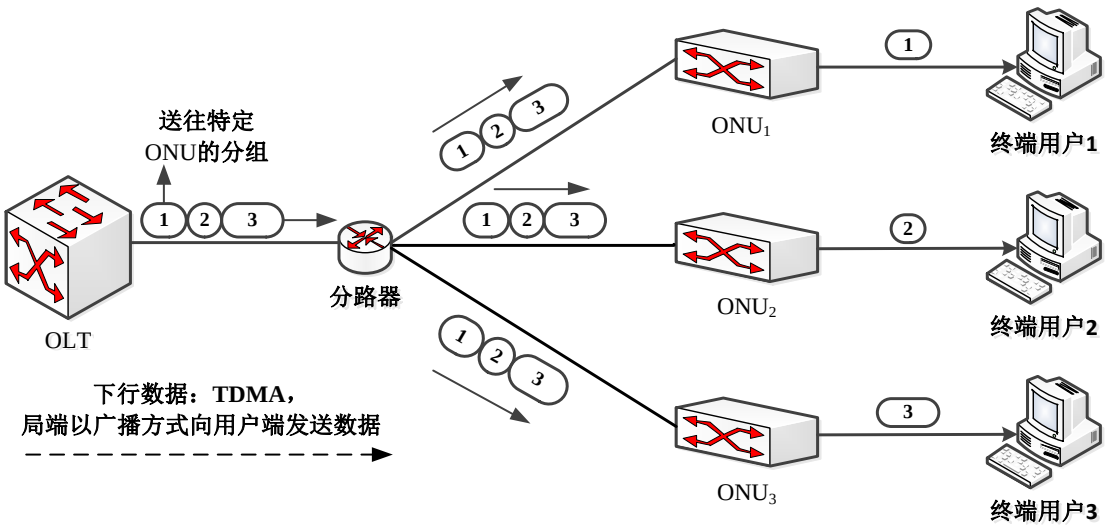

图 2-3 EPON 网络系统下行方向数据传输原理

Fig.2-3 The Downstream Data Transmission Principle of EPON System

图 2-4 为 EPON 网络系统上行传输数据的工作流程图。对于终端用户请求的上行数据，将根据 OLT 分配给 ONU 的固定时隙，利用光分路器将各个 ONU 发送的数据流进行耦合，然后将彼此独立的数据流以 TDMA 方式复合成连续的数据流后汇聚到单一光纤线路中来，从而避免数据在上行传输过程中发生争抢和冲突。OLT 向 ONU 分配带宽根主要有两种情况：当 ONU 完成初始的注册时，OLT 给 ONU 分配带宽的依据是系统中原始的配置；在动态测距的过程中，ONU 会根据用户上传的数据请求将需求的带宽报告给 OLT，然后 OLT 就会动态的给 ONU 分配带宽。

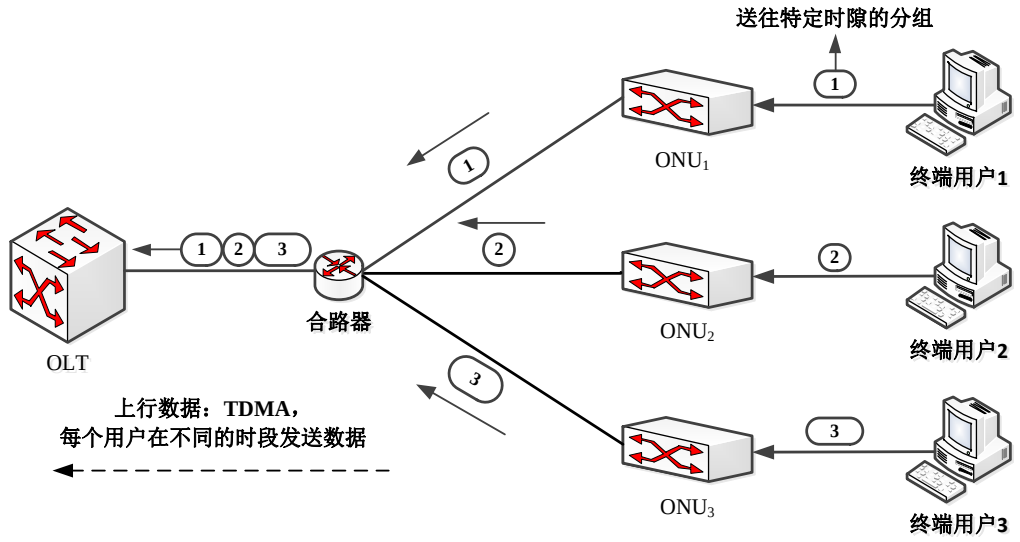

图 2-4 EPON 网络系统上行方向数据传输原理

Fig.2-4 The Upstream Data Transmission Principle of EPON System

2.1.2 多点控制协议（MPCP）

EPON 网络系统的工作原理在具体实现过程中，起决定性作用的主要为以下几个关键技术[24]:（a) 动态测距技术;（b) DBA (Dynamic Bandwidth Allocation，动态带宽分配)技术;(c) 突发光接收技术;(d) MPCP 协议技术。本论文主要使用到 MPCP 协议技术[25]。

多点控制协议是 MAC（Media Access Control，介质访问控制）子层的一项基本功能，它对光网络中一点控制多点的 MAC 机制做出了明确的定义。为了实现 EPON 网络中 OLT 与 ONU 之间数据的有效发送与接收， IEEE802.3ah 在 MAC 控制子层上定义了 MPCP 协议。通过 MPCP 核心控制协议操作，可以使 OLT 实现下行多点控制，ONU 实现上行多址接入、注册、动态测距等功能[25]。

EPON 网络中根据 OLT 和 ONU 之间的相互数据传输 MPCP 协议定义了 5 种具体的 MAC 控制帧，具体格式及功能介绍如下：

（1）MPCP 协议帧格式

MPCP 协议在原有标准 Ethernet 控制帧的基础上重新定义了 5 种控制帧，即 REGISTER 帧、REGISTER_REQUEST 帧、REGISTER_ACK 帧、GATE 帧和 REPORT 帧，其中 GATE 帧根据工作时间段不同又分为 Normal_GATE 和 Discover_GATE。同时，MPCP 协议根据这 5 种帧给出了 2 类相应的工作模式：当系统处于初始化工作模式时，OLT 通过 REGISTER、REGISTER_REQUEST 和 REGISTER_ACK 三个控制帧来发现未注册的 ONU，并分配注册地址，完成时钟同步和动态测距等功能；在正常工作模式下，可以通过 GATE 和 REPORT 两个以太控制帧来进行带宽的分配，ONU 向 OLT 发送 REPORT 帧报告队列情况，请求分配带宽，OLT 通过 GATE 帧给 ONU 发送授权带宽。这 5 种 MPCP 消息均采用标准的以太网帧格式，长度为最小以太网帧的长度（64 个字节），具体帧格式如图 2-5 所示。

图 2-5 MPCP 控制帧格式

Fig.2-5 The Format of MPCP Control Frame

与普通以太网帧的不同之处在于，EPON 网络系统中 MPCP 控制帧的类型字段为 88-08，操作码字段一般用来区分不同的 MPCP 消息，例如 00-02 和 00-03 分别代表 GATE 帧 REPORT 帧，各类信息的操作码字段如表 2-1 所示。其中，GATE 帧和 REPORT 帧通常用于 OLT 带宽分配和系统测距，而 REGISTER_REQUEST 帧、REGISTER 帧和 REGISTER_ACK 帧用于 ONU 的自动发现和注册过程。

表 2-1 MPCP 消息操作码表

操作码	MPCP消息
00-02	GATE
00-03	REPORT
00-04	REGISTER_REQUST
00-05	REGISTER
00-06	REGISTER_ACK

（2）自动发现及注册流程

10G EPON 系统中 OLT 和 ONU 必须完成自动发现和注册过程才能进行正常通信。自动发现和注册过程包括的主要功能有：10G EPON 网络在系统复位或上电后，OLT 端能够自动发现请求加入系统的 ONU，给新加入的 ONU 分配唯一确定的身份标识 LLID，并协商出 ONU 的相关参数，具体过程如图 2-6 所示。

1） EPON 网络初始化过程中，OLT 开始向所有的未注册 ONU 广播发送自动发现帧（DISCOVERY GATE），告知 ONU 授权时间窗口长度、发送请求的开始时间和结束时间等相关信息；

2）各 ONU 收到 DISCOVERY GATE 帧后，会在规定的时间窗口内通过竞争的方式

向 OLT 发送注册请求帧（REGISTER_REQ）；

3）当 OLT 接收到 ONU 发送的 REGISTER_REQ 帧后，首先对帧进行验证，如果通过就给 ONU 发送注册帧（REGISTER）。该帧主要包括 OLT 端分配给目的 ONU 的 LLID 和一些功能和物理参数等；

4）ONU 收到 REGISTER 帧后，不会立刻进行下一步工作，而是等待 OLT 继续发送 GATE 帧，告知带宽分配等授权信息；

5） 一旦 ONU 收到 OLT 发送的 GATE 帧，便开始进行授权认证，通过即给 OLT 发送注册应答帧（REGISTER_ACK），告知 OLT 注册已完成。这样，OLT 和 ONU 就建立了连接，可以开始传输数据了。

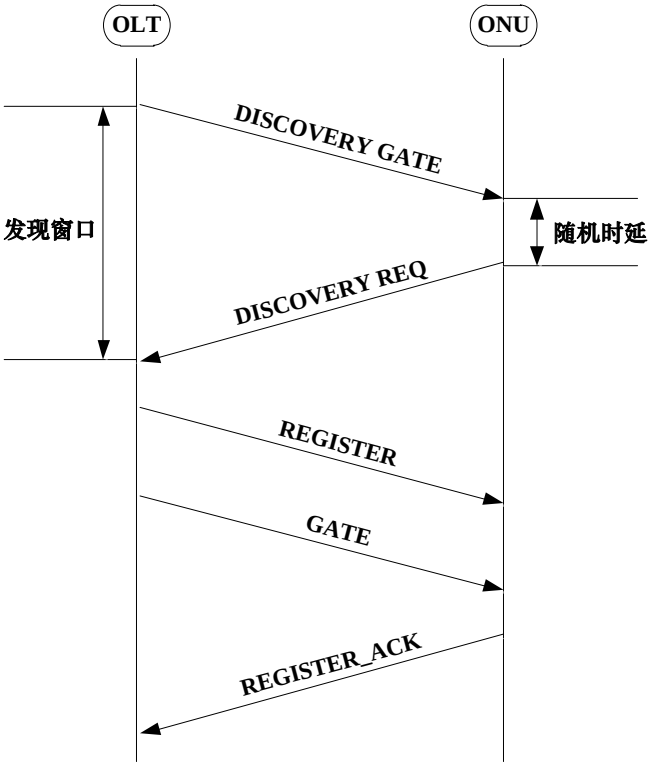

图 2-6 EPON 注册过程

Fig.2-6 EPON Register Process

（3）GATE/REPORT 机制

EPON 网络中 MPCP 协议帧最基本的通信操作就是 GATE/REPORT 机制，其中系统测距和带宽分配就是 GATE 帧和 REPORT 帧协同完成的。如图 2-7 所示，用户请求的数据首先发送给与之连接的 ONU，然后 ONU 将这些数据通过 REPORT 帧上传报告给 OLT，OLT 接收到该帧后，开始给 ONU 分配请求带宽，通过 GATE 帧发送给 ONU。其中，OLT 端通过分析 ONU 的 REPORT 帧完成系统测距，并根据 ONU 的状态再发出 GATE 授权帧的，最终实现 OLT 和 ONU 的数据传输连接。

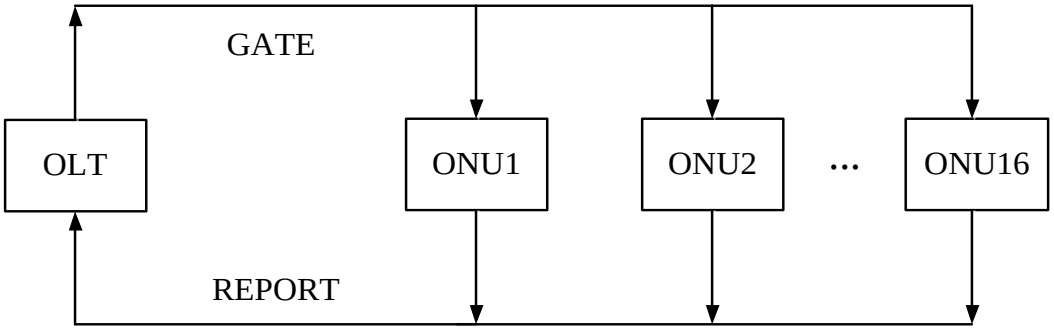

图 2-7　EPON 网络系统 GATE/REPORT 机制
Fig.2-7　GATE/REPORT Mechanism of EPON Network

2.1.3 EPON 系统存在的安全威胁

1、系统安全威胁

EPON 网络系统由传统的 Ethernet 技术和 PON 技术结合形成的，因此具有 PON 网络和 Ethernet 技术的双重特性[26]。由于 EPON 网络继承了 PON 网络点到多点的树形拓扑传输方式，在安全方面存在很大威胁，主要包含以下三种[26]。

（1）窃听

EPON 网络系统下行采用广播的方式向所有 ONU 发送数据，每个 ONU 收到数据包后，会依据 EPON 帧前导码中的身份标识 LLID 字段来进行过滤匹配，只接收属于自己的信息。这种过滤机制操作简单方便，但是存在很大安全隐患。

我们知道，在以太网中，数据过滤是依据 MAC 地址，以太网的网卡能够设置成“混杂”模式，而 EPON 的下行数据过滤机制与以太网过滤机制类似。因此，当非法用户把 ONU 也设置成“混杂”模式时，LLID 过滤机制规则将失效，所有的 ONU 都能接收到 OLT 发送的数据包内容。另外，EPON 网络在传输通道中都是封装好的标准以太网数据包，帧的格式完全公开，恶意用户只需要使用一个带有光口的以太网探测工具，就能接收到 OLT 发送给目的 ONU 的所有下行数据信息。这些下行数据中包含从 EPON 系统的 MAC 客户层传下来的高层数据，以及 PON 网络内部产生的一些重要控制信息。一旦被窃听，这两部分的数据将完全暴露。

（2）拒绝服务攻击

通常，拒绝服务攻击指的是，当非法用户窃听到下行数据时，会根据这些重要身份信息伪装成合法用户，然后伪造 REPORT 帧向系统发送大量数据请求，消耗系统的可用带宽和网络资源，使这些资源无法被合法用户所访问和申请，大大降低合法用户的服务质量，影响整个 EPON 网络的性能。恶意用户一般通过以下三种方式对系统实施拒绝服务攻击：

（a）系统的有限资源不断地被消耗，如分配的带宽、CPU 时间等。

（b）系统当中的一些重要配置信息被破坏，如网络设备的 MAC 地址、身份字段

LLID，以及 VLAN 标识等。

（c）物理层上网络连通性的破坏，如恶意用户在 EPON 网络上行传输方向上随意发送一个很强的光信号，当 OLT 端接收到该信号，网络设备便瘫痪，其它合法用户无法连接网络。

（3） 假装

IEEE 802.3ah 标准只定义了 EPON 网络系统的自动发现和注册过程，对于未注册的 ONU 和重新加载上电的 ONU 都可以通过该过程加入到系统中来。然而，该标准却没有对网络中的 OLT 和 ONU 的身份认证进行定义，所有的 ONU 只要发送注册请求，就可以在 OLT 端分配到 LLID，完成注册过程。这样，恶意用户只要获得一个光接入点，向 OLT 发送注册请求，就可以加入到 EPON 网络中去。然后，非法用户窃听其它 ONU 的相关信息，修改自己的 MPCP 数据帧，伪装成该合法 ONU，向 OLT 发送业务请求，获得大量网络资源，而费用却由该合法 ONU 承担。因此，在系统中添加身份认证机制，使 OLT 根据 ONU 的身份合法性来确定是否添加该用户很有必要。

2、系统认证对象选择

正是由于 EPON 网络系统存在伪装、窃听、拒绝服务攻击等安全威胁，因此对系统进行身份验证非常有必要。而认证过程一般需要涉及到验证方，被验证方和认证协议。其中，认证协议的设计过程中，首先要考虑的就是认证对象。EPON 网络系统中包括 OLT 端和 ONU 端两个部分，下面具体讨论。

在实际的网络应用中，ONU 可以连接一个或多个用户，而 EPON 网络系统进行身份认证的目的是为了防止恶意 ONU 在自动发现和注册中获得其它 ONU 分配的 LLID，因此 OLT 选择的认证对象应该是 ONU 而不是 ONU 所携带的用户。另外，由 EFM 指定的标准可以知道，ONU 可以支持一个或多个 LLID，即对于网络中的任何一个 ONU 来说，OLT 端能够分配 8 个以下 LLID 的点到点逻辑链路，ONU 可以利用这些 LLID 连接不同的业务。因而，需要进一步确定认证的对象是 ONU 还是分配给 ONU 的 LLID。在 EPON 网络系统中，ONU 是 LLID 的载体，OLT 也是根据 ONU 目的地址来发送 LLID。因此，当成功验证 ONU 的身份，再由系统决定分配一个还是多个 LLID 给该 ONU，更有针对性。所以，选择 ONU 作为认证对象。

此外，恶意用户可以通过窃听的方式获得下行发送数据，分析出上行数据的发送时隙，然后伪装成合法 ONU 向 OLT 发送请求数据。当 OLT 发送资源时，非法用户便开始分析 OLT 的相关重要配置信息，再次假装成合法 OLT，截取上行数据，更改 EPON 系统的重要配置信息和一些物理参数，使整个系统造成不可修复的破坏。因而，不仅对 ONU 的身份需要认证，对 OLT 的身份同样需要认证。

3、系统认证时机的选择

系统认证时机指的是 EPON 系统中开始执行认证过程的开始时间，主要有 2 个选择，一个是在注册完成之前，一个是在注册完成之后。

当选择在注册完成之后进行认证，即先不验证 ONU 身份的合法性，等注册结束，OLT 分配给 ONU 身份标识 LLID 后再进行认证。如果 ONU 未能通过身份验证，则 OLT 会释放与 ONU 刚建立的通道链接，标记分配的 LLID 为无效。该认证过程中，密钥传输是个很大的难题，需要重新设计额外的认证协议。此外，系统之前建立的 OLT 和 ONU 的数据传输链路有可能因为 ONU 身份认证失败而被取消，造成系统资源不必要的浪费。另外，OLT 分配 LLID 的方式采用的是优先编码，如果非法 ONU 通过窃听方式最终入侵系统，即使认证不能通过，得到的 LLID 再次被收回，但是系统分配 LLID 的规则已被恶意 ONU 获知，严重影响其安全性。因此，本文将选择在注册完成之前进行 OLT 和 ONU 的双重身份验证，OLT 确保 ONU 身份合法才分配 LLID，ONU 验证 OLT 安全可靠才建立链路。

2.2 NTRUsign 认证算法

在 2.1.3 节中我们介绍了 EPON 的安全研究现状及其存在的安全问题，重点分析了认证对于 EPON 系统的重要性，指出了双向认证的必要性。本节将重点介绍当前比较新颖的签名认证算法 NTRUsign，并准备将该认证算法嵌入到 EPON 系统的注册阶段，解决 OLT 和 ONU 的双向身份安全问题，为 EPON 承载多业务提供安全环境，具体方案设计见第三章。

NTRUSign 是基于 NTRU 格的签名算法[27]，与传统的认证算法相比，如 ECC、RSA 等，不论在运算速度，还是在同等密钥长度的安全性方面都更加具有优势[28]。算法的安全性是基于近似最近向量问题，利用私钥对信息进行签名获得一个近似最近向量，攻击者因无法获知私钥，因而很难找到这个近似最近向量，从而保证安全。

NTRUsign 签名认证算法的所有基本操作都是位于 N-1 维的多项式环 $R = Z[X]/(X^N-1)$ 中。其中，Z 是整数环，$Z_q[X]/(X^N-1)$ 是 Z 的商环。NTRUsign 签名算法有三个相关的整数参数(N; q; NormBound)，N 是素数，q 是 2 的阶数，NormBound 是用于验证签名值的边界值。在本文中，我们设置(N; q; NormBound)=（251；128；310）。多项式 w 是一个 N 维的矢量，记作 $w = (w_0; w_1; w_2; \ldots; w_{N-1})$。进行模 q 操作的区间为[-q/2,+q/2]。NTRUsign 签名算法的公钥含有一个 N-1 维度的多项式 h，私钥有两个很小的系数 f 和 g，且满足 $f*h=g$。其中，多项式 f, g 和 h 都是 $Z_q[X]/(X^N-1)$ 中的元素。L（n）表示对在环 $R = Z[X]/(X^N-1)$ 内的所有多项式进行设置，即 n 个系数为 1，其它所有系数为 0。对于多项式 A，$A \in Z[X]/(X^N-1)$ 表示靠近 A 的最近整数多项式。此身份认证算法主要包括密钥生成、信息签名和验证 3 个过程，具体过程如下：

1.密钥生成阶段：此阶段主要是为了获得公钥与私钥。

（1）随机选择两个多项式 $f \in L(65)$ and $g \in L(61)$，然后检测 f 是否可逆。如果 f 可

逆，则令 $f_q=f^{-1}$；否则，重新选择一个 f。

（2）求得另外两个短向量 $F,G\in R$，满足

$$\mathrm{f}*\mathrm{G}-\mathrm{F}*\mathrm{g}=\mathrm{q} \tag{2-1}$$

其中，

$$\|\mathrm{F}\|\approx\|\mathrm{f}\|\sqrt{\mathrm{N}/12},\qquad \|\mathrm{G}\|\approx\|\mathrm{g}\|\sqrt{\mathrm{N}/12} \tag{2-2}$$

（3）计算公钥 h，

$$h=\left\{f_q*g\right\}(\mathrm{mod}\,q) \tag{2-3}$$

公开公钥 h，保存私钥 (f,g,F,G)。

2. 签名阶段: 此阶段主要完成对消息 D 的签名。

（1）输入待签名的数字消息 D，计算哈希函数

$$m=h(D) \tag{2-4}$$

由公式（2-4），对 m 进行模 q 运算

$$(m_1,m_2)=m(mod\ q) \tag{2-5}$$

（2）计算：

$$G*m_1-F*m_2=A+q*B \tag{2-6}$$

$$-g*m_1+f*m_2=a+q*b \tag{2-7}$$

$$B=\left[\frac{-F*m}{q}\right]\qquad b=\left[\frac{f*m}{q}\right] \tag{2-8}$$

且 a 和 A 的各项系数在 $(-q/2,q/2)$ 内。

（3）计算签名信息：

$$s=(f*B+F*b)(modq) \tag{2-9}$$

则数字消息 D 的签名即是 (D,s)。

3. 验证阶段：此阶段完成签名信息的判断。

（1）输入签名信息 (D,s) 和公钥 h。

（2）令：

$$m=h(D) \tag{2-10}$$

$$(m_1, m_2) = m(mod q) \tag{2-11}$$

$$t = s * h(mod q) \tag{2-12}$$

（3）如果

$$\| m_1 - s \| + \| m_2 - t \| \le NormBound \tag{2-13}$$

成立，则表明所生成的签名是有效的，否则判定为无效签名，验证失败。

2.3 EPON 承载 IPTV 业务

2.3.1 IPTV 业务概述

IPTV 即交互式网络电视，是一种利用宽带接入网的设施，以机顶盒加上家用电视机作为主要接收终端，应用多媒体、互联网、通信等多种技术，通过网络 IP 协议向用户提供广告、插件、微博等多种交互式服务。IPTV 音视频流媒体业务通常采用高效的视频压缩技术，当视频流传输带宽达到 800Kb/s 时即等同于 3M/s 的 DVD 观赏效果，对当前急需开展的网络视频直播、高清节目源录制与制作、超远距离视频实时点播等业务来说，具有很强的优势[29]。

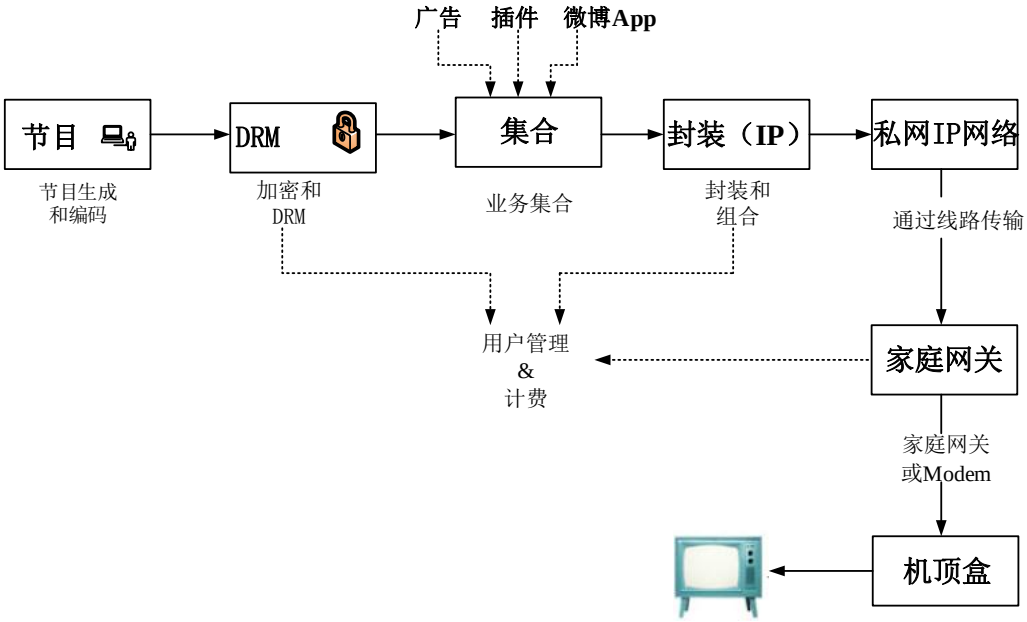

图 2-8 当前 IPTV 业务配置

Fig.2-8 Current IPTV deployments

图 2-8 为当前 IPTV 业务配置信息，主要由四个部分组成，包括节目生成与制作系统、节目互动指南系统、数字业务管理系统和机顶盒客户端配置系统[30]。这些系统所能实现的功能包含：基于 IP 协议的视频业务流单播与组播技术、数字证书加密与解密技

术、终端用户管理和收费技术、音频及视频存储阵列服务等。同时，根据不同的接入方式，IPTV 业务的应用系统还会涉及各种宽带接入网络技术，例如 Ethernet 技术、xDSL 技术、HFC Cable MODEM 技术、WLAN/WMAN 技术、3G/4G 技术、FTTH 技术和 FTTHx+LAN 技术等等[31]。这些相关的系统技术为 IP 视频节目实现端到端的精确分发服务提供一套完整的技术支持，能够保证音视频流媒体业务经媒体中心分发后，通过骨干网络、核心网络和 EPON/GPON 宽带接入网传输，最终被用户接收。

而随着电子技术和软件行业的发展，进行跨平台的业务交换成为可能，例如在 AppleTV，Mac，PCs，iPhone 和 iPod 都可以进行 iTunes 业务浏览和下载。另外，随处可见的 Android 系统将可能代替当前的浏览器平台，产生通用平台，从而 IPTV 可以在传统的机顶盒之外选择手机、电脑等终端设备进行业务订购，用户在家中即可以享受三种 IPTV 服务：⑴个人 PC；⑵网络机顶盒+普通电视机；⑶各类便捷式移动终端设备，例如 iPhone 等。图 2-9 描述的就是这样的一个 IPTV 系统并且有望在不久的将来就能进行配置，它主要依靠业务融合设备独立中间件来连接家庭网络的大量终端设备，完成相关 IPTV 业务选择，实现用户业务体验。

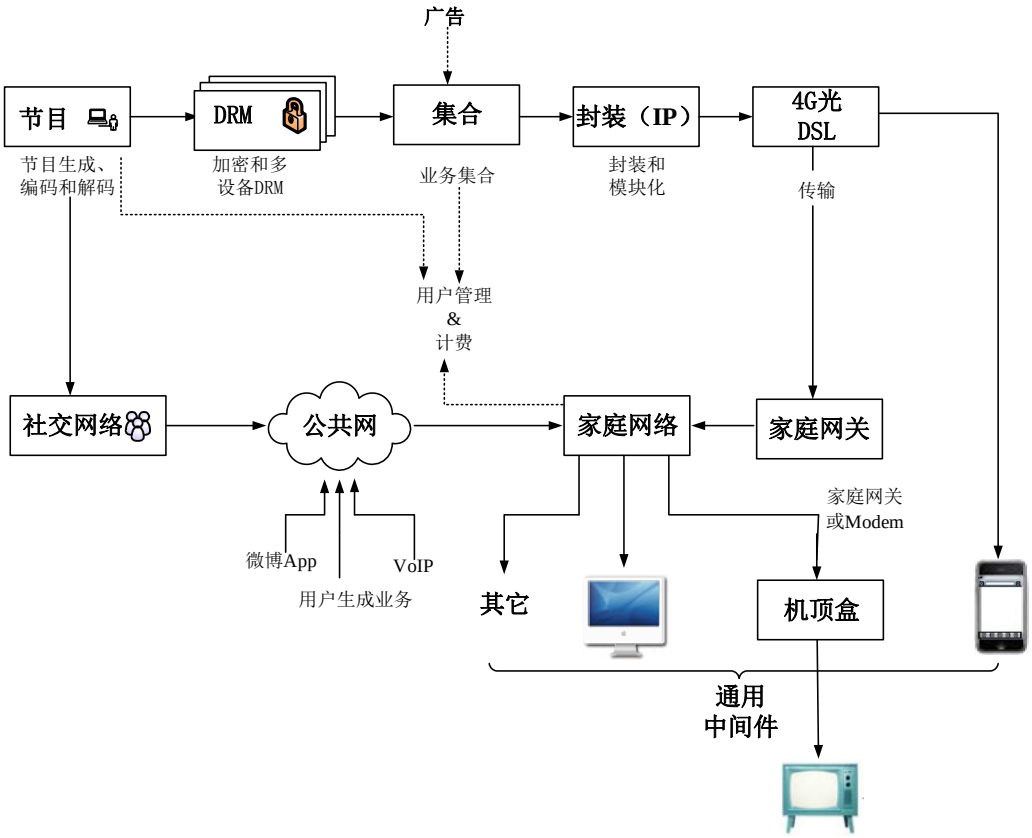

图 2-9 未来 IPTV 业务配置

Fig.2-9 Future deployments of IPTV

2.3.2 EPON 承载 IPTV 业务分析

EPON 系统能够提供 1Gbps 的上下行带宽，采用与 IP 协议兼容的以太网帧结构，

无需协议转换，而且 EPON 系统可以满足与任何视频压缩格式的视频业务传送需求，能在传输过程中提供较高的 QoS 保证，所以在承载 IPTV 业务方面，EPON 技术比传统的 xDSL 技术具有更大的优势。

图 2-10 为一般的 IPTV 系统结构图[32]。基本工作原理是 SHO（Super Hub Office，超级中心站）从 IPTV 视频内容提供商获取节目，对原始的视频数据进行编码后，转化成 IP 协议数据包形式发送给所有的 VHO（Video Hub Office，视频中心站），每个 VHO 负责一个城域网的业务。其中，长途 IPTV 骨干网包括 SHO 和 VHO 之间的路由器以及传输链路。VHO 中的路由器或者交换机携带业务流通过 MIO（Metro Intermediate Office，城市中间站）转发给 VSO（Video Serving Office，视频服务中心），VSO 为 DSLAM（Digital Subscriber Line Access Multiplexer）提供服务，经由 RG（Residential Gateway，家庭网关）最终达到用户终端，经过数据解码后，通过电视机或 PC 机播放出来。DSLAM 一般配置在户外，能够为 100-200 个 RG 提供正常服务。为了有效地传输 DSLAM 和 RG 之间的数据，各类接入技术都被使用，而当前优势明显的 10G EPON 最为受到关注。本论文将利用 10G EPON 承载多业务，并在保证用户喜爱的 IPTV 业务不受带宽分配的影响下，其它各种订购业务也能正常得到服务。

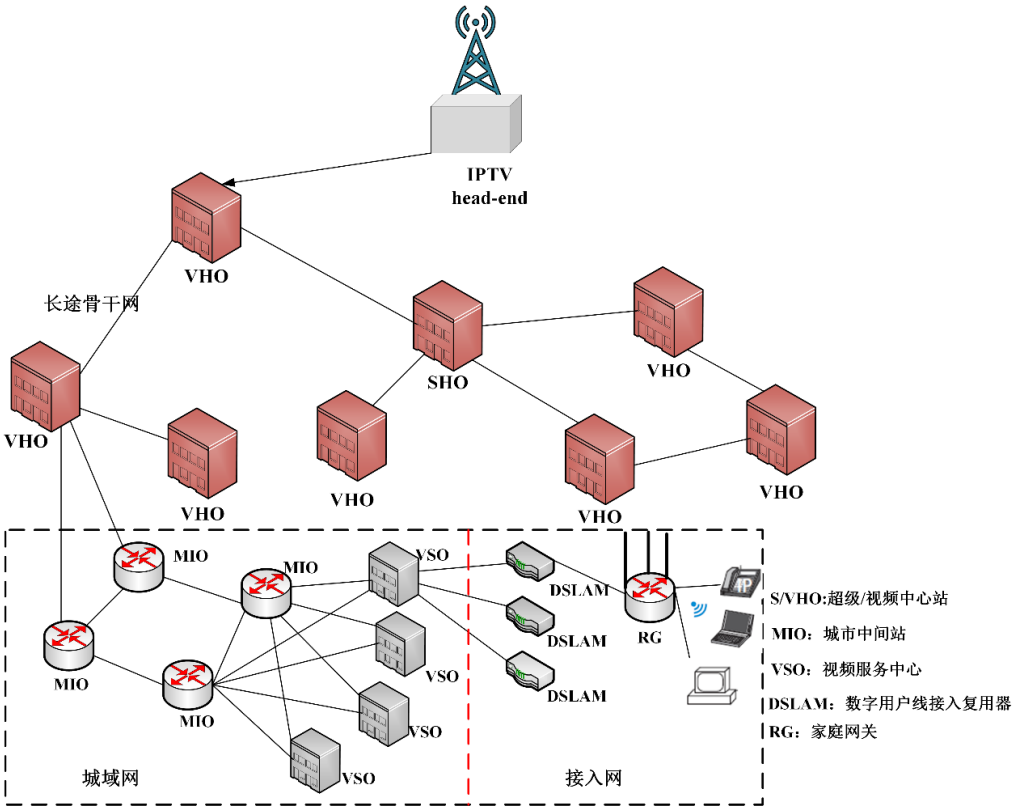

图 2-10 通用 IPTV 结构图

Fig.2-10 General IPTV architecture

2.3.3 EPON 承载 IPTV 组播技术

（1）实现组播技术的必要性

EPON 网络系统为一点对多点的树形分支拓扑结构，OLT 与 ONU 进行下行数据通信通常采用单播和广播两种方式。当 EPON 工作在单播方式时，即“一对一”的通讯模式， OLT 向 N 个 ONU 发送相同的数据时需要进行 N 次包的复制。当 N 数值较大时，OLT 传送的次数也就随之增多，这样将会占用大量的下行带宽。当 EPON 工作在广播方式时，即“一对所有”的通讯模式，OLT 发送的下行数据将通过无源分配器广播给所有的 ONU，不管 ONU 是否愿意或者需要接收该数据，容易引起系统拥塞。

组播技术是将源节点的数据传送到多个目的节点[33,34]，即“一对一组”的通讯模式，只有预先设定在组播组中的成员才能接收到，其它的成员不必处理，高效地利用网络带宽，解决不同业务的分离问题，被广泛应用于承载 IPTV 业务中。然而，当前的 EPON 标准中并没有考虑组播支持和管理问题，组播数据一律是按广播方式发送出去，所以实现 EPON 组播技术非常有必要[35]。

（2）EPON 实现组播技术分析

EPON 系统在下行方向是个共享的网络，只要进行合理的改进，EPON 系统就可以实现组播传输，但是要解决以下三个问题：第一，OLT 怎样创建和管理组播组；第二，ONU 怎样对组播数据进行过滤;第三,用户怎样加入或者离开一个组播组[36]。根据 EPON 系统的特点，组播数据的过滤仍然在 RS 子层实现，而且一般采用二层组播协议中的 IGMP Snooping（IGMP 侦听）协议或者 IGMP Proxy（IGMP 代理）协议解决用户加入或者离开组播组的问题[37]。

IGMP Snooping 机制是交换机设备通过侦听用户发送路由器的 IGMP 报文。IGMP 报文是封装在 IP 数据报中，且在 IP 数据报中的协议域值为 0x20，其报文格式如图 2-11 所示[38]。交换机根据 IGMP 报文中加入或者离开的信息来建立本地组播表，并且形成组成员和端口的对应关系，然后交换机根据该对应关系将接收到的组播数据帧只发送给内部端口，不向其它端口扩散，从而实现用户加入和退出组播组功能。

1byte	1byte	2byte	4byte
类型	最大响应时间	校验和	组地址（D类IP地址）

图 2-11 IGMP 报文格式

Fig.2-11 The Format of IGMP Message

1. 类型：0x12/ox16 为加入报文，用户主机申请加入某个组；0x17 为离开包围，即不接收该组的组播数据。

2. 最大响应时间：缺省为 10 秒，规定在发送回应报告之前的最大延迟时间。

3. 校验和：报文校验值。

4. 组地址（Group Address）：为 D 类 IP 地址，即是用户想加入或离开的组播地址。

IGMP Proxy 实现的功能和 IGMP Snooping 基本相同，但是 IGMP Proxy 机制更加智能。IGMP Snooping 只是通过侦听 IGMP 报文来获取相关信息，并不能处理 IGMP 报文，IGMP 报文会继续往上层转发；而 IGMP Proxy 不但可以侦听 IGMP 报文获取信息，而且会判断要不要将报文继续转发，实质上代替了路由器处理组播协议。例如，当有用户发送一个加入某组播组的请求时，如果执行 IGMP Proxy 机制的设备发现本地组播表中已经存在该组播项，设备就不再向上层路由器转发该请求报文，减轻路由器的负担。

2.3.4 EPON 承载 IPTV 业务分类规则

当前数据包的分类规则一般使用两类方法，一种是基于 VLAN 帧中的 802.1p 优先级[39,40]，另一种是基于 IP 报文头的 ToS（Type of Service，服务类型）字段的优先级位[41]。分类主要是完成数据包的优先级排列，在传输过程中的交换机会根据这些优先级的值执行相应的 QoS 行为。而 VLAN 帧一般在二层帧中使用，本文利用 EPON 系统承载 IPTV 属于三层帧，因此分类规则优选 IP 报文的 ToS 字段方法。

1．ToS 字段的 IP 优先级

在前期的 RFC 791 标准当中，数据的优先级主要是通过 IP 数据包的 ToS（Type of Service，服务类型）字段来标识。ToS 是 IP 数据包中的 IP 报头中的一个字段（共 1 个字节），用来指定 IP 包的优先级，设备会优先转发 ToS 值高的数据包。

ToS 字段共一个字节（8 位），包括三个部分：0~2 共三位用来定义数据包的 IP 优先级（IP Precedence）、ToS 和最后一个固定为 0 的位，如图 2-12 所示。

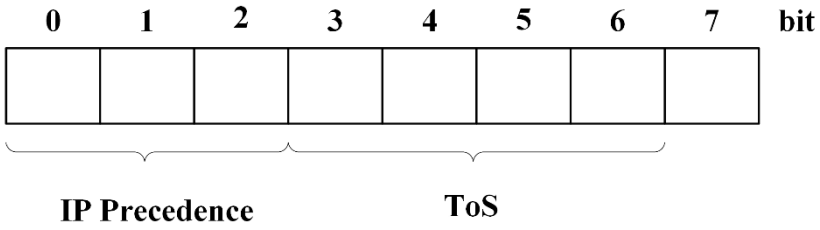

图 2-12 IP 包头中的 ToS 字段结构

Fig.2-12 ToS field structure of IP Packet Header

（1）IP Precedence 部分

IP 优先级部分共三位，取值范围为 0~7（值越大，优先级越高）。用名称表示时，这 8 个取值分别为 routine（普通，值为 000）、priority（优先，值为 001）、immediate（快速，值为 010）、flash（闪速，值为 011）、flash-override（急速，值为 100）、critical（关键，值为 101）、internetwork control （网间控制，值为 110）和 network control（网络控制，值为 111），分别对应于数字 0~7。

（2）ToS 部分

在 IP 包头的 ToS 字段中紧接着 IP 优先级字段后面的四位是 ToS 部分，代表需要为

对应报文提供的服务类型（标识报文所注重的特性要求）。一开始，在 RFC 791 中是只用到了第 3~5 位，分别代表 IP 包在 Delay（延时），Throughput（吞吐量），Reliability（可靠性）这三方面的特性要求（每个报文在这三位中只有一位可能置 1，此时表示 IP 包在对应方面有特别要求）。后来在 RFC1349 标准中又扩展到第 6 位，表示 IP 包在路径开销（cost）方面的特性要求。

2. DS 字段的 DSCP 优先级和 PHB

在后来的 RFC 2474 标准中，重新定义了原来 IP 包头部的 ToS 字段，并改称之为 DS（Differentiated Services，差分服务）字段[42]，也是共一个字节（8 位）。总的来说，第 0~5 位（共六位）用来表示 DSCP（Differentiated Services Code Point，差分服务代码点）优先级[43,44]，取值范围为 0~63，共能标识出 64 个优先级值（值越大，优先级越高），最后两位保留，用于显示拥塞通知（Explicit Congestion Notification，ECN），如图 2-13 所示。

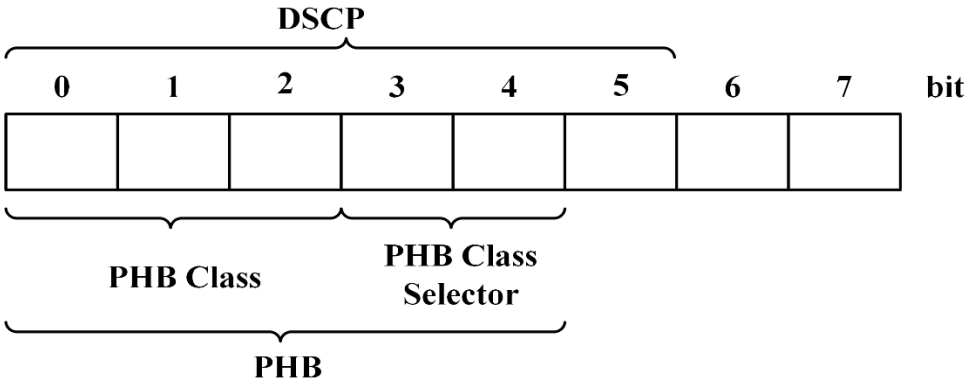

图 2-13 IP 包头中的 DS 字段结构

Fig.2-13 DS field structure of IP Packet Header

在 IETF RFC 2597 标准中定义了 PHB（Per-Hop Behavior，逐跳行为），通过 PHB 值可以确定在网关处对 IP 包的转发行为[45]。这个 PHB 值是通过前面介绍 DSCP 优先级部分的第 0~4 位来标识的，其中第 0~2 位用来标识 PHB 类别（PHB Class）值，共 8 个值，对应表示为 CS0~CS7，对应在 RFC 791 定义的 8 个 IP 优先级值，而第 3~4 位用来标识 PHB 类别选择（PHB Class Selector）值，参见图 2-11。PHB 类别值和 PHB 类别选择值共同组成 PHB 值。DSCP 值是由 PHB 的五位再加上第 5 位（固定为 0），但在 PHB 类别中的三位不能全为 0。

在 RFC 2597 中定义了四种确保转发（Assured Forwarding，AF）PHB 组（称之为 AF PHB）。它使用了 DS 字段中的第 0~2 位定义 PHB 类别，而使用 DS 字段中的第 3 和 4 位代表报文的“丢弃优先级”，用 AF（x,y）表示，其中 x 表示流分类，y 表示对应的丢弃优先级。

在 AF 的 PHB 中，定义了四种 PHB 类别（也即“流分类”），它们的值分别为 001、

010、011 和 100（对应 CS1~CS4），它们本身代表了流的不同优先级（值越大转发优先级越高），然后通过第 3 和 4 位的丢弃优先级值（取非 0 的三个值，分别为 01、10 和 11，值越大丢弃优先级越高）进一步区分同一类流不同 IP 包的丢弃优先级。

再后来在 RFC 3246 标准中，又定义一个加速转发（Expedited Forwarding，EF）PHB，对应 CS5，即在 DS 字段中的第 0~2 位取值为 101，第 3~4 位取值固定为 11，第 5 位固定为 0，这样一来对应的 DSCP 值就为 46（101110）。EF PHB 具有低延时、低开销和低抖动特性，适用于语音、视频和其他实时服务，一般具有比其他通信类型更加优先的队列。

除了前面介绍的 AF 和 EF 外，还有一个缺省的 PHB，那就是尽力服务类型，它所对应的 DSCP 值为 000000，即十进制的 0。另外还定义了 CS6 和 CS7，CS6 用于网间控制，对应的 DSCP 为 110000，即十进制的 48；CS7 用于网内控制，对应的 DSCP 值为 111000，即十进制的 56。

2.4 本章小结

本章概述了 EPON 的体系结构和工作原理，介绍了多点控制协议帧结构及其功能，就 EPON 系统存在的安全威胁作重点阐述，指出双向身份认证的必要性，并分析了认证对象、认证时机和认证算法的选择问题。然后概述性的介绍了本文选用的身份认证算法 NTRUsign 及其工作原理。最后介绍了 IPTV 业务，分析了多业务情形下 EPON 承载 IPTV 业务的可行性，以及组播技术和区分服务模型使用的必要性。

第三章 基于 NTRUsign 的双向认证系统方案设计

在第二章中我们介绍了 EPON 系统面临的安全威胁，详细地分析了 OLT 和 ONU 双向身份认证的必要性，并对系统认证对象选择，系统认证时间选择做了重点阐述。本章将根据 EPON 系统特性，把 NTRUsign 签名认证算法嵌入到注册阶段中的 MPCP 协议帧中去，在 OLT 和 ONU 间进行传送。当注册结束，OLT 和 ONU 的双向身份认证过程也随之完成，并协商出额外的会话密钥，可以为后续数据加密使用。

3.1 基于 NTRUSign 双向身份认证方案设计

3.1.1 方案整体流程概述

如图 3-1 所示，本方案中注册认证过程主要分为两个阶段，即初始化阶段和 OLT 与 ONU 的双向认证阶段。在初始化阶段，OLT 与 ONU 各自利用 DISCOVERY_GATE 帧和 REGISTER_REQ 帧生成敏感信息，包括证书、公钥、私钥和随机值等。在认证阶段，ONU 首先验证由 CERTIFICATION_GATE 帧携带的 OLT 的证书 C_{OLT}。如果合法，则 ONU 向 OLT 发送自己的签名值 S_{ONU} 来验证自己的身份。最后，OLT 同样向 ONU 发送自己的签名值 S_{OLT} 来验证自己的身份。其中，S_{ONU} 帧由 ONU_SIGNATURE 帧携带，S_{OLT} 帧由 OLT_SIGNATURE 帧携带。

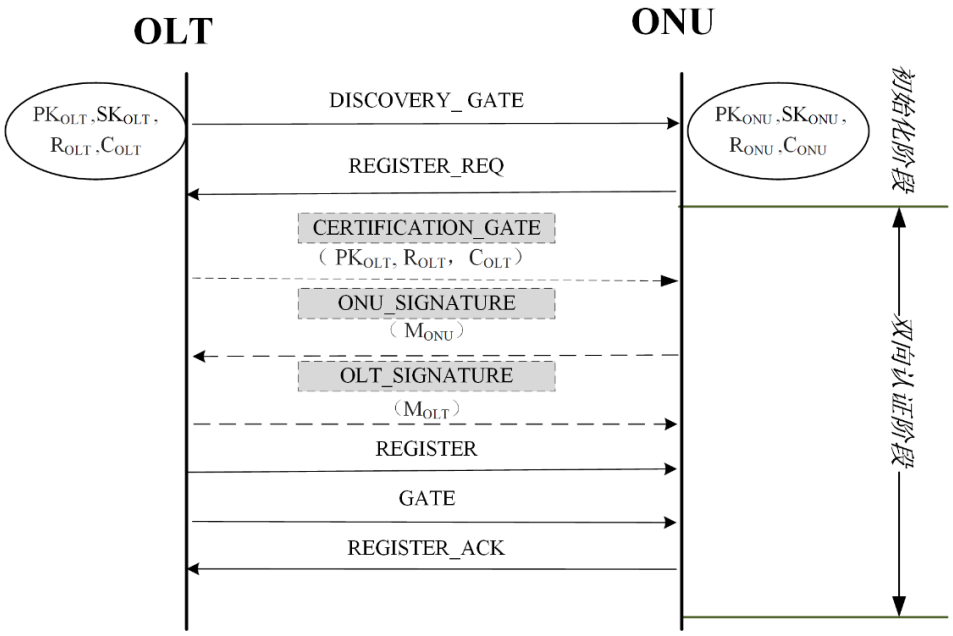

图 3-1 OLT 和 ONU 端双向认证过程

Fig.3-1 The authentication process of OLT and ONU

3.1.2 方案具体实现过程

在这一部分，我们将详细地描述在 EPON 系统注册期内 OLT 和 ONU 端基于

NTRUsign 签名算法的双向身份验证方案。值得注意的是，OLT 和 ONU 端相互传输并用于验证身份的八个帧，有五个是 EPON 系统当中固有的 MPCP 控制帧，其它三个帧，CERTIFICATION_GATE 帧、ONU_SIGNATURE 帧和 OLT_SIGNATURE 帧根据通用的 MPCP 帧格式重新定义。这三个帧结构将在 3.1.3 中具体介绍。表 3-1 是本方案中使用的符号及意义。

表 3-1 本方案中使用的符号及含义

符号名称	意义
PSK	预共享密钥
KD-HMAC-SHA256	密钥导出算法
K	临时加密密钥
E(x, y)	用密钥 *x* 加密 *y*
D(x, y)	用密钥 *x* 解密 *y*
r_1	ONU 生成的一个随机参数
a||b	*a* 和 *b* 串联起来
PK_X	*X* 的签名公钥
SK_X	*X* 的签名私钥
K_{XY}	*X* 和 *Y* 的会话密钥
R_X	*X* 产生的随机值
s_X	NTRUSign 算法中 *X* 的签名
h(X)	*X* 的哈希函数
C_X	*X* 的证书

（1）ONU 和 OLT 端的初始化

如图 3-1 所示，EPON 系统当中固有五个 MPCP 帧。OLT 周期性地产生时间窗口，向所有的 ONU 传送发现帧（DISCOVERY_GATE），告知 ONU 发现时隙的开始时间和长度。在此时间内， OLT 随机选取两个多项式 $f_{OLT}\in L_f$ 和 $g_{OLT}\in Lg$，然后根据 NTRUSign 数字签名算法公式（2-1）~(2-3)生成自己的公钥与私钥，其中公钥为 PK_{OLT}，私钥 SK_{OLT} 为 $(f_{OLT},g_{OLT},F_{OLT},G_{OLT})$。OLT 证书 C_{OLT} 定义为：

$$C_{OLT}=(f_{OLT}*B+F_{OLT}*b)(\mathrm{mod}\,q) \tag{3-1}$$

其中，系数对 B 和 b 通过公式（2-4）和（2-8）计算如下：

$$m=h(PK_{OLT}\,\|\,R_{OLT}) \tag{3-2}$$

$$B=\left[\frac{-F_{OLT}*m}{q}\right],\qquad b=\left[\frac{f_{OLT}*m}{q}\right] \tag{3-3}$$

随机值 R_{OLT} 是 OLT 在注册期内选取的随机值。不同的注册期内，R_{OLT} 值也是不同

的，即该值是动态变化的。

当 ONU 收到 DISCOVERY_GATE 帧后，将会等待一个随机时间，然后向 OLT 传输请求帧（REGISTER_REQ）。在该时间内，ONU 端也同样进行初始化过程，生成自己的公钥 PK_{ONU}，私钥 SK_{ONU}：(f_{OLT},g_{OLT},F_{OLT},G_{OLT})，证书 C_{ONU} 以及随机值 R_{ONU}，并储存公私钥对。

(2)双向认证及秘钥协商阶段

当初始化完成之后，则进行双向认证和密钥协商。具体步骤如图 3-1 所示：

步骤 1: 当 OLT 收到 ONU 发送的 REGISTER_REQ 帧后，开始向 ONU 发送 CERTIFICATION_GATE 帧，其中包括了 OLT 在初始化过程中生成的公钥 PK_{OLT}，随机值 R_{OLT}，证书 C_{OLT}。

步骤 2:在收到步骤 1 所发送的信息后，ONU 将获得 OLT 初始化时生成的证书 C_{OLT}，公钥 PK_{OLT} 和随机值 R_{OLT}。然后开始利用 NTRUSign 数字签名算法的验证算法核对 OLT 证书的有效性，即验证 C_{OLT} 的合法性，具体过程如下：

$$m = h(PK_{OLT} \| R_{OLT}) \quad (3\text{-}4)$$

$$(m_1, m_2) = m(mod q) \quad (3\text{-}5)$$

$$t = C_{OLT} * PK_{OLT}(mod\ q) \quad (3\text{-}6)$$

$$\| m_1 - C_{OLT} \| + \| m_2 - t \| \le NormBound \quad (3\text{-}7)$$

不等式(3-7)是关于参数(m_1, m_2), C_{OLT} 和 t 的函数。如果这些参数不满足（3-7）成立，则认为 C_{OLT} 不正确，即 OLT 身份是非法的。那么，ONU 将不会进行剩下的注册和认证过程，需要等待下一个注册时间窗口重新进行所有操作。反之，认为 OLT 是合法发送用户，则开始验证双方的签名有效性。需要注意的是，C_{OLT} 通过验证并不表示 OLT 就是合法的，只是代表 OLT 不是恶意用户。真正的身份认证是在 C_{OLT} 验证通过后开始。

ONU 随后选取一个随机值 r_1 用于生成签名值。令 $Q_{ONU}=R_{OLT}||r_1$，替换等式（3-2）中的 R_{OLT}，则等式（3-2）和等式（3-3）转变为

$$m = h(PK_{ONU} \| Q_{ONU}) \quad (3\text{-}8)$$

$$B = \left[\frac{-F_{ONU} * m}{q} \right], \qquad b = \left[\frac{f_{ONU} * m}{q} \right] \quad (3\text{-}9)$$

由等式（3-8），（3-9）和 SK_{ONU} 可以计算出 ONU 的签名值 S_{ONU} 如下

$$s_{ONU} = (f_{ONU} * B + F_{ONU} * b)(mod\, q) \quad (3\text{-}10)$$

我们知道，当 ONU 以明文的方式向 OLT 上行传输这些机密信息，如 S_{ONU}，PK_{ONU}, R_{ONU}, C_{ONU}, r_1，容易遭受到已经明文等攻击。因此，对这些信息进行加密操作很有必要。令密文为 M_{ONU}，计算为

$$M_{ONU} = E(K, PK_{ONU}, R_{ONU}, C_{ONU}, s_{ONU}, r_1) \quad (3\text{-}11)$$

其中 K 为临时加密密钥，由文献[46]可得

$$K = KD\text{-}HMAC\text{-}SHA256(PSK, R_{OLT}) \quad (3\text{-}12)$$

最后，密文 M_{ONU} 嵌入到 ONU_SIGNATURE 帧中，然后发送给 OLT。

步骤 3：OLT 收到 M_{ONU} 信息后，先用密钥导出算法计算得到临时加密密钥 K=KD-HMAC-SHA256(PSK,R_{OLT})，然后解密收到的密文信息 M_{ONU} 获得 ONU 的证书 C_{ONU}，ONU 的签名 s_{ONU} 等信息。然后 OLT 根据等式（3-4）~（3-7）来验证 ONU 证书的合法性。其中，使用 PK_{OLT}, R_{OLT}, C_{OLT} 替换 PK_{ONU}, $R_{OLT}||r_1$, S_{ONU},可得

$$m = h(PK_{ONU} \| r_1 \| R_{OLT}) \quad (3\text{-}13)$$

$$(m_1, m_2) = m(mod q) \quad (3\text{-}14)$$

$$t = S_{ONU} * PK_{ONU}(mod\ q) \quad (3\text{-}15)$$

$$\| m_1 - S_{ONU} \| + \| m_2 - t \| \le NormBound \quad (3\text{-}16)$$

如果不等式（3-16）成立，则 ONU 是合法用户。下一步，将验证 OLT 的身份合法性。

在等式（3-8）和（3-9）中，用 R_{ONU},（$f_{OLT}, g_{OLT}, F_{OLT}, G_{OLT}$）代替 $PK_{ONU}||R_{ONU}$,（$f_{ONU}, g_{ONU}, F_{ONU}, G_{ONU}$），得到 OLT 的 签名 S_{OLT} 如下：

$$s_{OLT} = (f_{OLT} * B + F_{OLT} * b)(\mathrm{mod}\, q) \quad (3\text{-}17)$$

为了保护签名值 S_{OLT} 在下行传输方向的安全性，OLT 将使用相同的密钥 K 进行加密。从而，密文 M_{OLT} 为

$$M_{OLT} = E(K, s_{OLT}) \quad (3\text{-}18)$$

最后，M_{OLT} 嵌入到 OLT_SIGNATURE 帧中，同 GATE 帧和 REGISTER 帧一起传送给目的 ONU。这里，GATE 帧给每个 ONU 分配唯一身份标识 LLID，REGISTER 帧给每个 ONU 分配带宽。

步骤 4：ONU 收到 OLT 发送的密文信息 M_{OLT} 后，将计算 D(K,M_{OLT})解密密文获得 OLT 的签名信息 s_{OLT}。然后同验证 CERTIFICATION_GATE 帧携带的 OLT 证书 C_{OLT} 一样，根据等式(3-4)~(3-7)验证签名值 S_{OLT}，判断 OLT 签名的有效性。如果通过了，则表明 OLT 是合法的。则双向认证成功，确保了 ONU 与 OLT 双方均是合法的。

步骤 5：当双向认证成功之后，ONU 向 OLT 发送注册确认帧（REGISTER _ACK），告知身份合法性验证结果。 OLT 与 ONU 同时也进入密钥协商阶段生成会话密钥，分别计算 K_{OLTONU}=h(R_{ONU}||R_{OLT}||r_1)作为它们双方共享的会话密钥。该会话密钥可以用于后续数据的加密，保证了数据传输的安全。

3.1.3 认证帧、ONU 签名帧和 OLT 签名帧的设计

MPCP 是一种信令协议，主要用于 ONU 的注册和动态带宽分配等过程中，为 ONU

分配传输时隙，保证 OLT 与 ONU 正确合理的传输信息。MPCP 设计了 5 个帧：授权（GATE）帧、报告（REPORT）帧、发现帧（DISCOVERY_GATE）、注册（REGISTER）和注册确认（REGISTER_ACK）帧。以上 5 个控制帧其字节长度都是 64 字节，与标准的以太网 MAC 帧是相同的。

在本方案中，根据图 2-2 通用 MPCP 协议帧自定义了 3 个帧：认证帧(CERTIFICATION_GATE)，ONU 签名帧（ONU_SIGNATURE）、OLT 签名帧（OLT_SIGNATURE），具体如下所述：

（1）认证帧(CERTIFICATION_GATE)

如图 3-2（a）所示，认证帧 Op-code 为 00-07，包含证书 C_{OLT}，公钥 PK_{OLT}，随机值 R_{OLT}。认证帧用于对要加入 EPON 系统的 ONU 发起认证过程，当 ONU 收到此信息后，则开始认证。

（2）ONU 签名帧（ONU_SIGNATURE）

图 3-2（b）为 ONU_SIGNATURE 帧，操作码 Op-code 为 00-08，包含信息 M_{ONU} 和保留域。当 OLT 收到 ONU 发送的 ONU_SIGNATURE 帧时，会立刻使用密钥 K 来解密该帧，获得 ONU 的签名值 S_{ONU}。如果 OLT 验证 S_{ONU} 通过，则请求注册的 ONU 被认为是合法用户。否则，其余的注册和认证过程将不再进行，ONU 需要等待下一个时间窗口重新进行该过程。

（3）OLT 签名帧（OLT_SIGNATURE）

图 3-2（c）为 OLT_SIGNATURE 帧，操作码 Op-code 为 00-09，包含信息 M_{OLT} 和保留域。当 ONU 收到该帧，同样利用密钥 K 解析出 OLT 的签名值 S_{OLT}。如果 S_{OLT} 通过认证，则 OLT 为合法用户。从而，双向认证过程全部结束，OLT 和 ONU 之间可以进行安全数据传输。

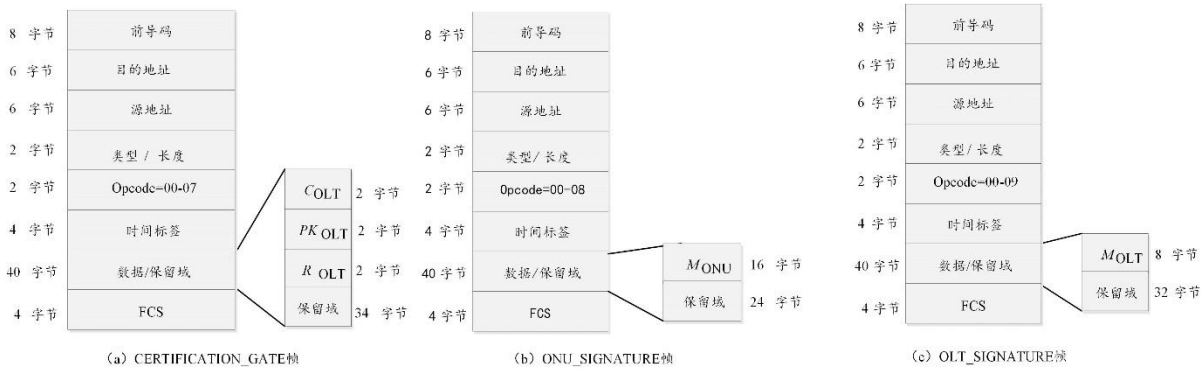

图 3-2 根据通用 MPCP 帧结构设计的三个自定义帧结构和具体字节：（a）CERTIFICATION_GATE 帧；（b）ONU_SIGNATURE 帧；（c）OLT_SIGNATURE 帧

Fig 3-2 Three Self-defined Frame Based on Universal MPCP Frame and Detailed Byte Design: (a) CERTIFICATION_GATE Frame；（b）ONU_SIGNATURE Frame；（c）OLT_SIGNATURE Frame

3.2 基于 NTRUsign 的身份认证方案性能分析

3.2.1 抵抗攻击的能力

本节重点分析方案的抵抗攻击能力，主要有以下几个方面：

1）中间人攻击。中间人攻击指的是 EPON 网络中恶意用户利用 OLT 无法判断 ONU 的实体身份而进行的攻击。在本设计方案中，即使攻击者截获 OLT 与 ONU 之间发送的信息，也无法对系统实施攻击，因为非法用户无法知道临时加密密钥 K，不能解密 ONU 发送给 OLT 的信息 M_{ONU}，从而得到重要的系统机密信息。数据传输过程中生成的临时加密密钥是由密钥导出算法 $KD-HMAC-SHA256$ 计算得出，预共享密钥 PSK 只被系统中的 OLT 和目的 ONU 所知，并且随机值 R_{OLT} 也是 OLT 随机产生的，所以最终生成的会话密钥是动态变化的，攻击者不能够通过上次数据传输得到的临时加密密钥来破解当前正在发送的信息，因此无法构造出合法的签名，中间人攻击无效。

2）伪装攻击。EPON 网络中伪装攻击指的是非法用户假装成合法 ONU 向 OLT 申请资源或者恶意用户假装成合法 OLT 更改系统信息。在本设计方案中，即使攻击者在注册开始阶段通过设置网卡为“混杂”模式窃取到 OLT 发送的 CERTIFICATION_GATE 证书，也无法获得 OLT 初始化的信息，因为 NTRUsign 签名算法是基于最近向量的难解性，非法用户无法从公钥推出隐藏的私钥，不能伪造 CERTIFICATION_GATE 帧，通不过 ONU 的验证。所以，这种攻击是失败的。

3）重放攻击。假设目的 ONU 泄露了一些敏感信息如 PK_{OLT}, R_{OLT} 和 C_{OLT}，攻击者可以用来使 LLID 过滤规则无效。重放攻击指的是攻击者利用这些截获的信息再次发送给目的 ONU，获得密文 M_{ONU}。然而，目的 ONU 在接收到 CERTIFICATION_GATE 帧后会立刻选取一个随机值 r_1，使 M_{ONU} 在不同的时间窗口是动态变化的，从而使重放攻击无效。

4）已知会话密钥攻击。由等式 $K_{OLTONU}=h(R_{ONU}||R_{OLT}||r_1)$可知，会话密钥是在双向认证完成后生成，用于加密 ONU 和 OLT 之间发送的数据。假如恶意用户得到了上次会话结束后获得的会话密钥，依然无法通过分析该密钥来获得当前数据链接得到的会话密钥，因为在本协议中每次认证结束 OLT 和 ONU 都会独自生成密钥，其中 ONU 生成的随机值 R_{ONU} 与随机参数 r_1 均是被保密的，而且每次会话 ONU 生成的这两个值均是不同的，会使得会话密钥也不断改变，因此已知会话密钥攻击无法成功。

3.2.2 注册效率的影响

IEEE802.3ah 在“一公里以太网”（Ethernet in the first mile，EFM）中为 EPON 系统定义了自动发现和注册过程，但是没有给出相应的身份认证机制。因此，在 OLT 和 ONU 之间添加认证算法，无疑会带来传输和处理延迟。同时，能成功注册链接上 OLT 的 ONU 数目也会出现下降趋势。为了更好地了解 EPON 系统的注册输出情况，我们使用基于 C++的 OPNET 仿真软件[47]，对本双向身份认证方案进行模拟，EPON 网络系统的注册

流程如图 3-3 所示。整个系统结合了当前正在使用的 1G EPON 系统原型和八个 MPCP 协议帧。这里通过软件设置 ONU 和 OLT 仿真器件，一个 OLT 可以携带 160 个 ONU[48]。另外，当 ONU 和 OLT 收到速率或者帧请求时，便会根据 NTRUsign 签名算法生成敏感信息，然后通过八个帧进行相互传送并进行身份认证。假设光参数的保护时隙为 1 μs，OLT 到最远 ONU 的最大单向传输时间 Q 为 100 μs，L 为八个控制帧的长度，D 为发现时隙的开始时间。我们以 GEPON 为例[49]，L=2.528 μs，发现窗口=2Q+ω+L，D=ω+L。最大等待时间 ω 将在下面讨论。

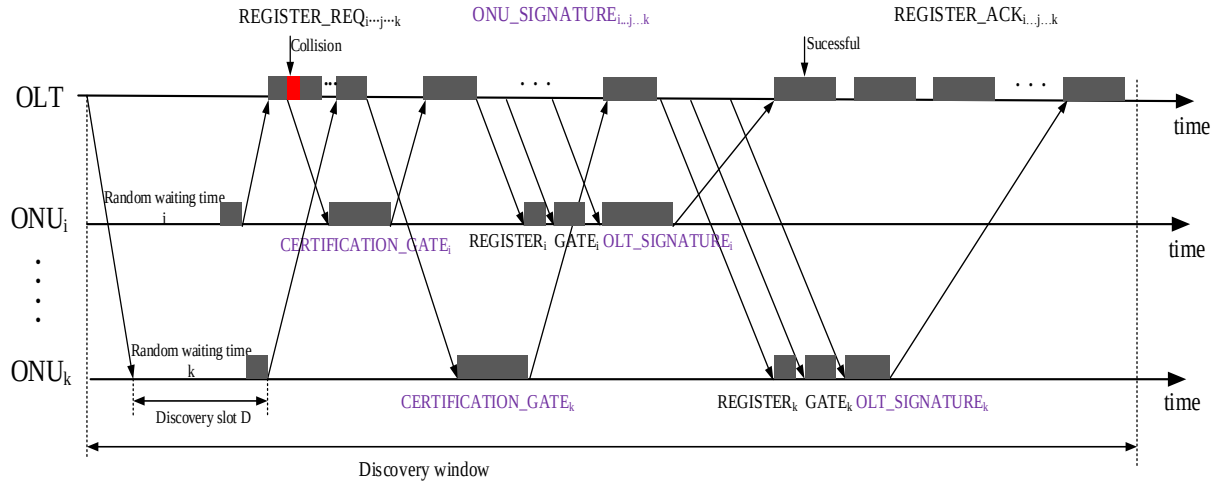

图 3-3 EPON 网络系统注册过程

Fig.3-3 Registration process in the EPON system

首先，通过改变加入 EPON 系统的注册 ONU 数目来测定数据包的传输延时。为了使结果更加清晰，没有嵌入认证算法的原始注册过程作为参照，已有的基于 ECC，MD5 和 GMAC 的认证方法作为对比。从图 3-4 可以看出，所有的曲线都是先平稳上升，一旦达到最大 ONU 的注册数目便成指数倍增加。造成此情况的原因如下。基于 MD5 和 GMAC 的认证机制需要额外的第三方认证服务器帮助，即 ONU 发送给 OLT 的认证信息不是直接由 OLT 处理，而是先转发给远程认证服务器进行处理然后返回给 OLT，造成严重的时间延时。参考文献 18 通过 EPON 系统当中固有的五个 MPCP 帧达到系统注册输出和安全认证的一个平衡。同时，为了保证数据的安全交换，该文献还使用了基于 ECC 的密钥交换协议，带来更多的额外操作，造成时延影响。在本论文中，我们利用 EPON 系统的固有的五个帧和自己定义的三个 MPCP 帧，结合 NTRUsign 认证算法，完成 OLT 和 ONU 的双向身份认证。系统当中唯一的延时就是 ONU 和 OLT 间相互传输三个自定义帧的时间 3L。从图 3-4 可以看出，当注册 ONU 的数目小于 128 个时，没有嵌入认证算法和添加 NTRUsign 认证算法的 EPON 注册过程的平均时延分别为 4.4ms 和 4.5ms。当注册 ONU 的数目大于 128 个时，原始注册过程在时延和抖动方面比基于 NTRUsign 认证过程呈现一个小的跳动。另一方面，基于 GMAC，ECC 和 MD5 的注册认证过程在时延方面都比 NTRUsign 注册认证过程高，因为它们都需要更多的时间处理

数据帧。当注册 ONU 的数目分别达到它们最大允许数目 96,80,62 时，时延都开始增加。结果显示，时延的大小取决于注册 ONU 数目和 ONU 的数据处理能力。在图 3-4 中可知，当注册 ONU 的数目小于 128 个时，本文的注册认证过程既有低时延的优势，又能保证 OLT 和 ONU 的身份安全。

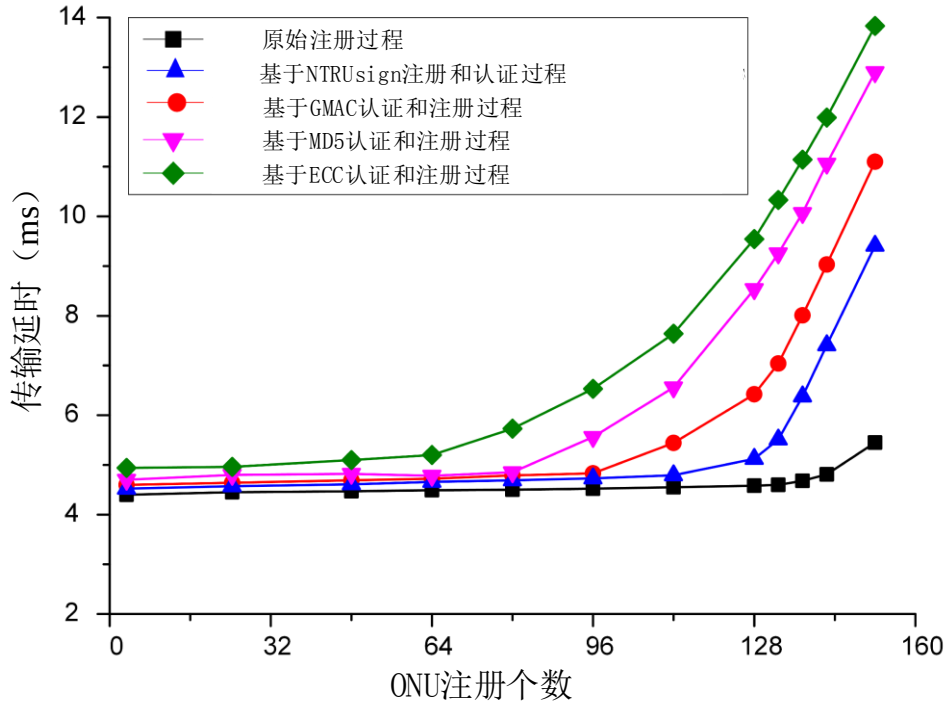

图 3-4 四种不同认证方案在不同 ONU 注册个数下的数据时延

Fig.3-4 Packet delay based on four different authentication scheme by changing ONUs

另外，我们对不同最大等待时间 ω 下，预注册 ONU 的数目 G 和实际注册输出 ONU 个数 λ_{out} 进行了测试。从图 3-5 中可以看出，注册输出 λ_{out} 先呈指数倍的上升，当最大允许注册 ONU 的个数 G=G*时，λ_{out} 达到最大输出 λ_{max} ，然后开始下降。G*代表在 EPON 系统中能够在一个时间窗口内成功注册的最大 ONU 数目。当 G<G*时，预加入 EPON 系统的 ONU 数目不多，发现窗口没有被完全利用，注册输出一直递增。当 G>G*时，大量的 ONU 同时加入注册通道，发现窗口过小，容易造成 ONU 之间碰撞，影响系统输出。根据参考文献 49 的输入与输出比 ξ，可得以下等式：

$$\xi=\lambda_{max}/G* \qquad (3\text{-}19)$$

$$\omega=\omega^{*}=LG+\sqrt{L^{2}G^{2}+2LG(2Q+L)} \qquad (3\text{-}20)$$

其中，$\omega=\omega^{*}$ 为 G=G* 时，ONU 的最大等待时间。

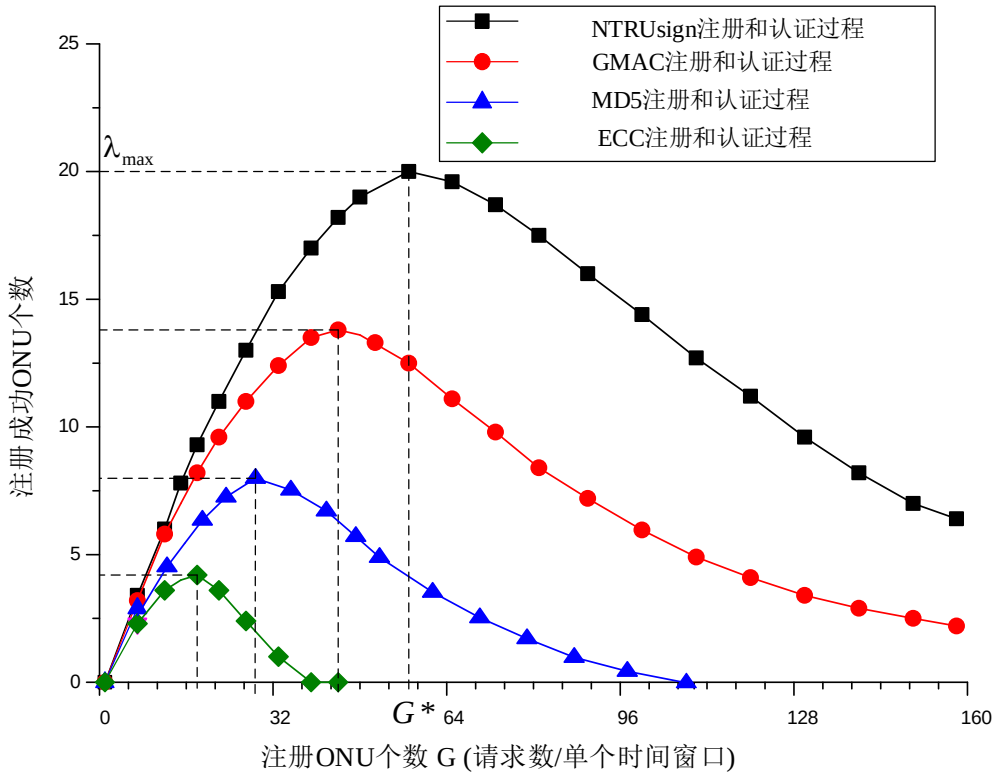

图 3-5 四种不同注册认证算法在不同 ONU 个数下成功注册 ONU 个数

Fig.3-5 successfully Registered ONUs versus different registered ONUs of four different authentication algorithm

从图 3-5 的曲线簇可以可知，四种不同认证方案的输出 λ_{out} 都是与 G 相关。ONU 的最大注册数 G*从下到上分别为 17.35, 27.23, 42.72, 57.25，相应的最大注册输出 λ_{max} 为 4.32, 8.04, 13.84 和 20.00。因此，由等式（3-19）可得到 ξ 分别为 0.2490, 0.2953, 0.3240 和 0.3493，表明在 EPON 系统中加入 NTRUsign 算法来验证 OLT 和 ONU 身份合法性的方案获得最大输出效率。结果显示，当 OLT 根据等式（3-20）选择 $\omega^* = 426.81\mu s$ 和 G=G*=57.25 时，能够得到最大效率比 ξ。与文献 27 的最大注册效率 36%相比，只要 ω 选择合适，本方案对注册效率影响极小。

3.3 本章小结

本章首先概述了基于 NTRUSign 签名算法的 EPON 系统 OLT 和 ONU 双向身份认证方案的流程，然后详细描述了双向认证方案的实现过程，并给出了论文中基于 MPCP 协议自定义的三个帧。最后对本方案抵抗攻击能力和注册效率影响进行了详细的分析。

第四章 EPON 承载多业务下的 IPTV QoS 保障

第三章主要解决了 EPON 网络系统中固有的身份安全问题，为多业务的传输提供了一个安全的传送通道。近年来，IPTV 业务在各类业务中尤为受广大用户的欢迎，订购数目成几何倍的增长，在接入网中占据的带宽也越来越大，给其它业务带来冲击，造成网络使用高峰期拥塞，多业务的 QoS 得不到保障。为了解决该问题，本章将提出一种 EPON 承载多业务情形下 IPTV 业务调度算法，满足不同用户对业务的需求。

4.1 EPON 承载 IPTV 业务的关键问题解决

EPON 网络承载 IPTV 业务实现首先需要解决两个方面的难点[50]：（1）如何正确地寻找一个模型来代表 IPTV 业务并快速生成数据流量。（2）如何将流量模型与 10G EPON 接入网进行结合。下面将分别介绍。

（1）IPTV 模型

生成一个 IPTV 的模型是非常困难的，因为每个视频都是完全不同的，且不同视频的统计特性也是变化的[51]。另外，即使是相同的视频流，也是时空变化的，或者说是随机变化的。例如，一个视频包含不同的画面，它们都随着时间和运动而时刻变化，同一视频中一组 GOP（Group of Pictures，图片组）与另外一组 GOP 通常都不一样。此外，在同一组 GOP 中，有大量的 I 帧，B 帧和 P 帧，每一个帧编码都不同，表现出差异很大的统计特性。如果只是抓住这些特性，是远远不够建立 IPTV 模型的，因为一个画面与另一个画面的帧的大小是强相关的，因此找到不同画面及它们的相关性尤为重要[52]。

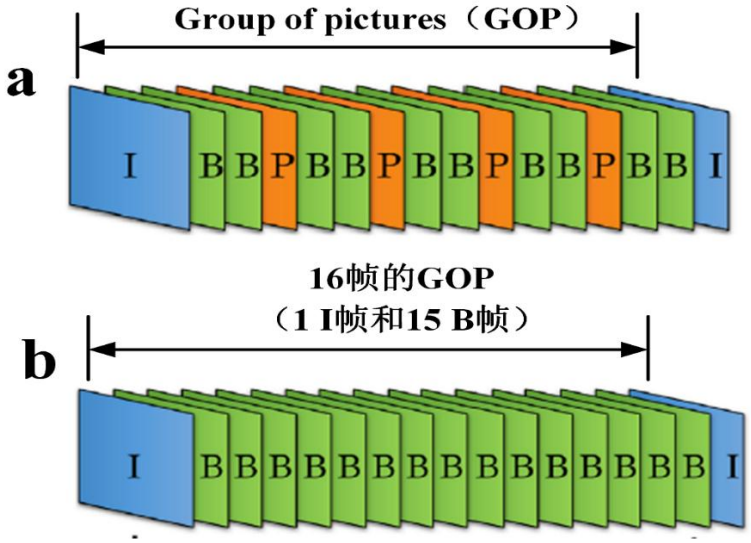

图 4-1 视频压缩模式：（a）典型视频流帧分布（b）单层 H.264 SVC 高压缩比的编码视频流帧分布.

Fig.4-1 Video compression patterns:(a)Frames in a typical video stream (b)frames in a single-layer H.264 SVC coded video at hignest compression.

建立 IPTV 的模型有许多选择，主要分为三类。第一类试图通过建立一个独立模型来代表 IPTV 业务。通常，这些模型都是多维的，通过变化时间和运动，以 GOP 为单位，观察信息变化情况。同时，还详细地给出了每个 GOP 内三个帧的变化情形。这些模型能够根据既定的编码算法就能产生理想的合成视频流业务，且容易分类。然而，精确的模型意味着复杂，成本过高，与接入网进行结合异常困难。如果简化模型，则无法准确地捕捉视频流的特点。

第二类试图利用视频追踪文件建立模型。当前，许多视频追踪技术都是可以公开使用的，它们能够创建正确的编排格式来生成视频流，且能够适应不同接入网平台。然而，该模型有两个方面的缺陷：（1）需要文件 I/O，使得与接入网结合时进行性能评估处理速度缓慢。（2）额外添加的追踪文件使系统产生更多的冗余操作。

第三类是一个混合方案，通过以往的视频特性来产生合成视频流。这种方法需要利用以往的数据进行已知分布（例如对数正太分布）比较，其中能够提供最优特性的分布将用来产生视频流业务。这种混合方案编码简单，遵循视频的统计特性，且能够克服其它两类方法的诸多不足。然而，因为每个视频都是不同的且拥有的统计特性不一样，因此合成视频流也面临着几个方面的挑战，包括如何对 I 帧和 B 帧的大小分布进行建模，怎样获得一个 GOP 内和多个 GOP 间的相关特性，以及怎样获取一个视频的总体统计特性。实际中，一个动作电影的视频同一个新闻报道视频肯定是不同的，它们必须根据不同的类型来选择相应的模型。生活中的一般视频种类包括运动、新闻、动作电影等。

本论文旨在建立一个足够准确的视频流模型，同时要求模型简单易编码。因此，选择第三类混合模型来生成合成视频流。在视频流生成阶段，数据压缩模式如图 4-1（b）所示。

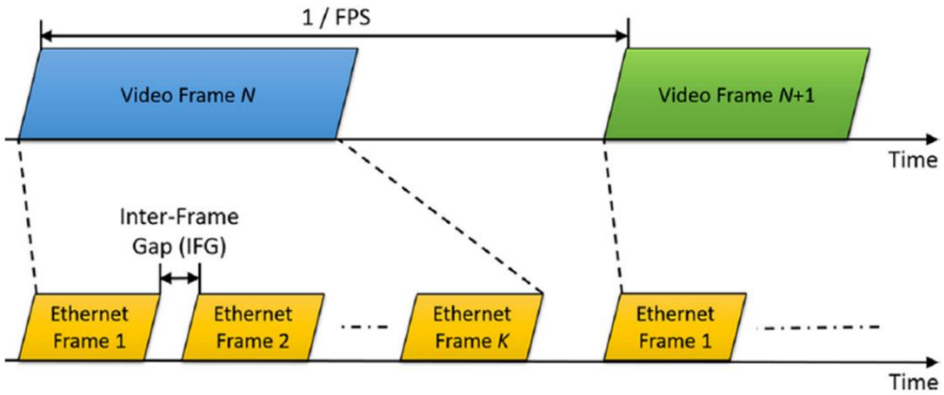

图 4-2 视频帧转换为以太网帧

Fig.4-2 Conversion of a Video Frame to Ethernet Frame

（2）流量模型与 EPON 网络结合

以太网是当今最流行的接入网技术，如何将 IPTV 流量模型转换为以太网帧格式，从而实现接入网（本论文选用 10G EPON 网络）性能评估是一大难题。合成视频流生成

器根据精确的帧速率 FPS（Frames Per Second，每秒帧数）来产生大小不一的视频帧。通常视频帧都比较大，根据它的大小，每个视频帧被封装成许多个连续的以太网帧，每个以太网帧之间要留有一个最小帧间隔（12 比特）。从而，合成视频流生成器能够转换成一个视频流量生成器，根据 FPS 能够在规定的时间间隔内生成视频帧，且对于每个视频帧，所有相应的以太网帧将连续到达。因此，取决于相应的视频帧大小，视频流量生成器将会有一个周期性的以太网帧突发。图 4-2 展示了视频帧如何转换成以太网帧。

4.2 EPON 承载 IPTV 业务的 QoS 整体方案设计

图 4-3 为 EPON 承载多业务情形下分级调度的总体设计方案。业务流从上游的多业务中心服务器（如文本服务器，流媒体服务器）发送给 VSO，经 DSLAM 达到接入层的 OLT 端。在 OLT 内部，各业务首先通过分类器各自进入缓存队列，包括两种缓存队列，单播缓存队列和组播缓存队列。组播缓存队列用于存储组播通信量，如 IPTV 业务流，本文包括高级接收队列、中级接收队列和低级接收队列。单播缓存队列用于存储单播通信量，如 e-mail 和 BE（Best Effort，尽力到达）业务（一般包括 Internet 访问数据）。然后调度模块根据相关调度算法给各队列分配合理带宽。最终，各业务队列通过 RG 到达订购用户端。该方案实现主要包括四个部分：单/组播划分模块、分类模块、调度模块、输入输出模块。

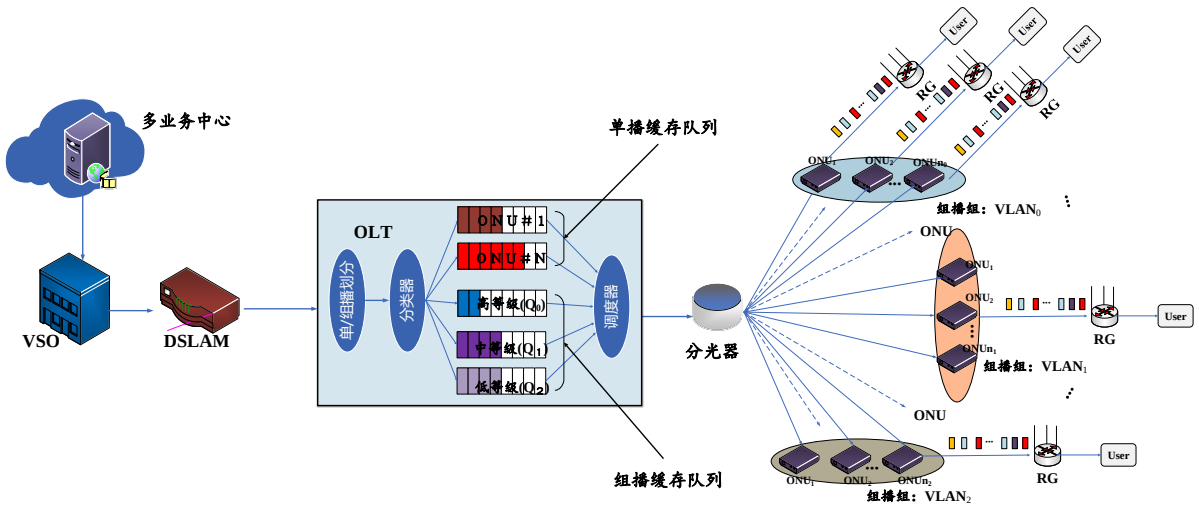

图 4-3 EPON 承载多业务下的分级调度

Fig.4-3 Hierarchical Scheduling of Multi-service under EPON Network

4.3 方案各模块设计

4.3.1 多业务单/组播划分模块

用户订购的多业务进入 OLT 端时，首先会根据带宽大小和用户的喜爱程度进行单/组播划分。LLID 是 EPON 网络系统当中分配给 ONU 用于点到点的身份标识，具有唯一性，所以本文采用 LLID 来定义 VLAN，实现组播功能。

（1）VLAN 方案定义

图 4-4 为本文重新定义的 LLID 字段，使它在保留原有的广播、点播功能标识的基础上，具有 VLAN 标识作用，从而实现组播功能。

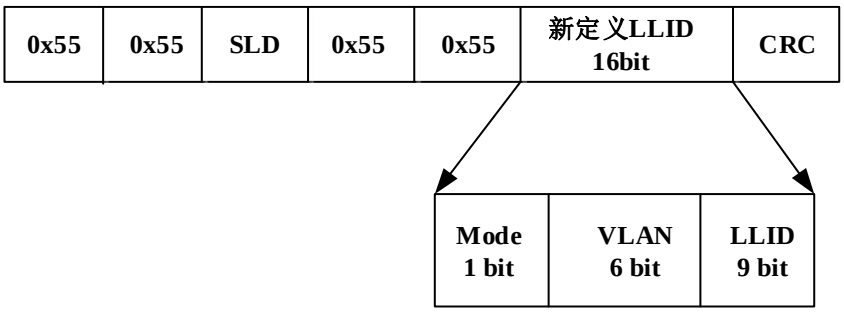

图 4-4 重新划分的 LLID 帧格式

Fig.4-4 The Frame Format of the Redefined LLID

1. Mode：模式位。用于区分不同数据类型：“0”代表单播数据帧，“1”代表广播或者组播数据帧。

2. VLID 字段：虚拟局域网标识字段（VLAN ID）。VLID 字段最大值（0x3f）代表最大的局域网，用来实现单播和广播功能，其余比特组合代表不同大小的局域网，用来实现组播功能。由于 1G EPON 系统分光比最大为 64，即使 1G EPON 向 10G EPON 平滑过渡，最大分光比也只能达到 256，再加上一个广播数据表示，有 9 个比特位（29=512）的 LLID 足够 OLT 分配给不同的 ONU 起身份标识作用。

3. LLID 字段：逻辑链路标识字段。LLID 字段除了最大值（0x1ff）作为广播或者组播数据标志外，其余比特组合是在 ONU 自动发现与注册过程中，OLT 分配给 ONU 起身份标识作用。

可以看出重新定义的 LLID 能标识出下行数据是广播、单播还是组播数据，组播数据的模式位和 LLID 字段跟广播数据一样，但是虚拟局域网标识不一样，组播数据的 VLID 只是代表一组特定的 ONU 能接收到，而广播数据的 VLID 代表所有的 ONU 都能接收到，从而实现 RS 子层也能过滤组播数据的能力。而且广播数据标识仍然使 0xffff；单播数据最高位也仍然为 0，只不过紧跟着的后 6 位都为 1，主要利用最后 9 位来标识是哪个 ONU 的单播数据，很好的做到与原先协议兼容。

（2）VLAN 标识操作

1. VLAN 分配

在 ONU 自动发现与注册过程中，OLT 为每个成功注册的 ONU 分配相同的 VLID 值（0x3f）和不同的 LLID 值，实现原理跟原先的 ONU 的自动发现与注册过程一样，如图 4-5 所示，只不过分配的前 6 位值都为 1，使所有成功注册的 ONU 都是最大局域网中的成员，能实现 EPON 系统原有的单播和广播功能。

但是每个 ONU 的 VLID 值是可以再分配的，在这里需要每个 OLT 维护一张相同的组播地址跟 VLID 值（GIP-VLID）的映射表，其中一个 VLID 值可以对应一个节目频道或多个节目频道的组播地址，这张映射表可以由网管软件建立和维护。这样每个 OLT 可以根据下行用户退订组播业务情况发送一个注册帧 REGISTER，对用户上端的 ONU 的 VLID 值进行再次分配更新，但是 LLID 值是不会变的，然后 ONU 对该 VLID 进行更新保存，这样就能把那些拥有相同组播业务的 ONU 预先划到同一个 VLAN 中，而且一个 ONU 可能在多个 VLAN 中，成为不同的组播成员，从而解决 OLT 创建和管理组播组的问题。

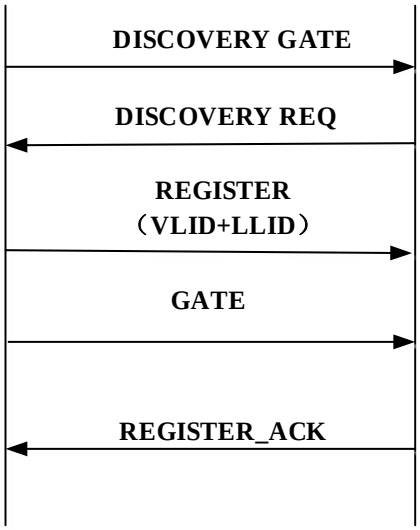

图 4-5 EPON 网络中 VLID 分配

Fig.4-5 The Allocation of VLID in EPON Network

2. VLID 帧的转发

在 OLT 端向下行方向转发数据帧时，OLT 解析数据帧的目的地址 DA 值，如果 DA 值是某一 ONU 的 MAC 地址，表明是单播数据，则前导码中 Mode 位为 0，VLID 字段等于 6’0x3f，LLID 为该 ONU 一开始注册时分配的 LLID 值；如果 DA 值为组播 MAC 地址，表明是组播数据，则 Mode 为 1，VLID 字段为 GIP-VLID 映射表中对应的 VLID 值，LLID 字段以及 LLID 字段合并起来（Mode&VLID&LLID）等于 16’0xffff。

3. VLID 帧的过滤

当下行数据到达 ONU 端时，RS 子层根据表 4-1 所示的过滤规则对数据进行选择性的接收过滤；当帧中 Mode 位为 0，说明必是单播数据，则只有 LLID 值匹配时 ONU 才能接收，否则表明是不属于自己的单播数据则直接丢弃；当帧中 Mode 位为 1，可能是

组播数据或者广播数据，则只有 VLID 值匹配时 ONU 才能接收，否则说明 ONU 不是该组成员，不能接收此数据。其实广播数据也可以看成组播数据，只不过下行 ONU 都是该组成员，都可以接收到该数据。

表 4-1 VLID 帧过滤规则

帧标记			接收状态
Mode	VLID	LLID	RS 层
0	0X3F	匹配	接收
		其它	丢弃
1	匹配	0X1FF	接收
		其它	丢弃
	其它	----	丢弃

4.3.2 分类模块

多业务通过单/组播划分模块后会分别进入缓存队列。其中，单播业务直接通过分类模块进入单播缓存队列，而 IPTV 组播业务种类多，用户需求各异，需要分类模块进行重新划分。本文根据区分服务模型思想，利用 DSCP 字段值将不同等级需求的 IPTV 业务划分到对应三个队列。

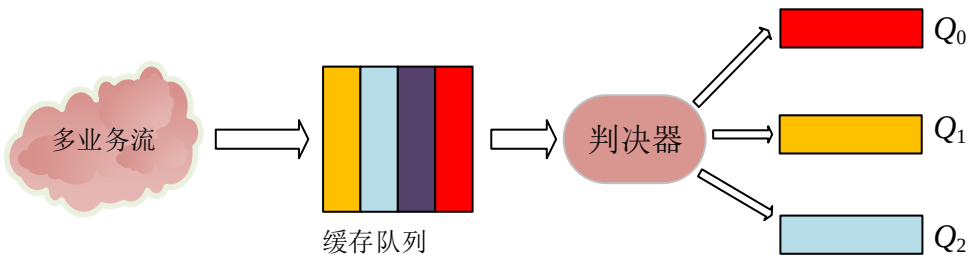

图 4-6 IPTV 队列分类模块图

Fig. 4-6 Queue Classification Module of IPTV

(1) 高等级缓存队列 Q_0:这类队列主要为音频和视频等流媒体数据，产生的网络数据量较大，对时延要求高，对数据完整性要求一般。

(2) 中等级缓存队列 Q_1：这类队列主要为图片和文件等一般数据信息，占用的网络资源较小。与流媒体业务相比，对数据在传输过程中的实时性要求不高，对数据完整性要求中等。

(3) 低等级缓存队列 Q_2：这类队列主要为机密数据，例如个人账户、系统配置信息和网络物理参数等，产生的数据流量同其它业务相比最小，时延要求低，但是对数据在传输过程中的安全性要求最高。

三个不同等级的队列划分主要依靠判决器，其工作原理根据 2.3.4 节介绍的区分服务模型。按照分组 DSCP 的字段值，队列划分为 EF、AF 和 BE。当工作在 AF 模式下时，本文将根据 DSCP 值的 0-5bit 将队列划分为三类，如表 4-2 所示。其中，0-2bit 的值按照 001、010 和 011 的顺序增加缓存大小，3-5bit 的值根据 010、100 和 110 由低到高的顺序来划分丢弃优先级。由表所示，组播 IPTV 业务中的流媒体数据对应 DSCP 值为 011010，一般数据数据对应 DSCP 值为 010100，关键加密 DSCP 值为 001110。

表 4-2 DSCP 组合表

DSCP值 3-5bit / DSCP值 0-2bit		丢弃级别依次递增 →		
		010	100	110
缓存空间依次递增 ↓	001	未定义	未定义	001110 关键数据业务Q_2
	010	未定义	010100 一般数据业务Q_1	未定义
	011	011010 流媒体数据业务Q_0	未定义	未定义

4.3.3 调度模块

调度模块主要取决于选取的调度算法，本文将采用时延保障和队列分配公平性兼顾的加权轮询调度算法 WRR 来对组播 IPTV 队列进行调度[53]。WRR 算法遍历所有业务队列，并根据队列的优先权分配相应的带宽，并且低优先级的业务也一直在工作，保证了队列调度的公平性。同时，WRR 算法根据队列分组大小和时延敏感性来具体分配调度资源，对于分组队列数较多、时延敏感的数据将分配较大的网络带宽，而分组队列较少、时延敏感一般的数据分配较少带宽，这样既控制了分组调度速率不会过快，又保障了时延。

图 4-7 为 WRR 调度过程图，所有队列通过分类模块后，WRR 算法根据优先级不同计算权值 W_i（i=0、1、2、…、N, N 为整数），权值所占的比例大小代表获取的网络资源。权值 W_i 表示分配给某一队列的带宽，计算公式如下：

$$W_i = \sqrt{q_i \sum_{j=1}^{k_i} n_{ij} \Big/ k_i} \tag{4-1}$$

其中 n_{ij} 表示第 j 个队列当中第 i 个数据流的分组数，k_i 表示第 i 个队列中数据流的个数，q_i 表示服务优先级，可以根据实际网络情况做出调整。三类业务中流媒体数据的

数据流量最大且对时延的要求最严格，其次是一般数据业务，最后是关键数据业务。根据对时延要求，这里我们为 q_i 赋初始值为 9、4、1（i=1、2、3），即流媒体的调度优先级大于一般数据业务，而关键机密数据业务优先级最低。

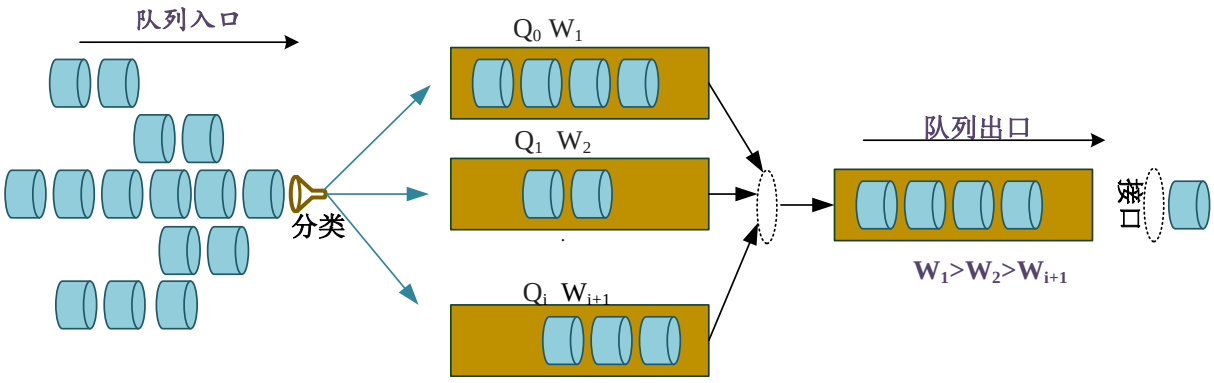

图 4-7　WRR 调度图

Fig.4-7　Figure of WRR Scheduling

4.3.4 输入输出模块

各类业务分组经过单/组播划分后进入输出队列，其排列顺序发生了变化，需要重新划分顺序。本文输出队列采用先到先服务FCFS 队列，如图 4-8 所示，在这种调度策略下，分组进入队列的顺序与被发送的顺序相同，与缓存队列的待发分组长度无关。将所有的到达分组统一缓存的一个队列当中，按照到达时间排队，系统首先发送排在队列最前的分组。

FCFC 队列算法实现容易，管理简单，数据达到接收端后不需要重新进行排序，并且队列的最大延时能够根据最大队列深度和发送速率来进行调节，非常适合高速接入网中使用。

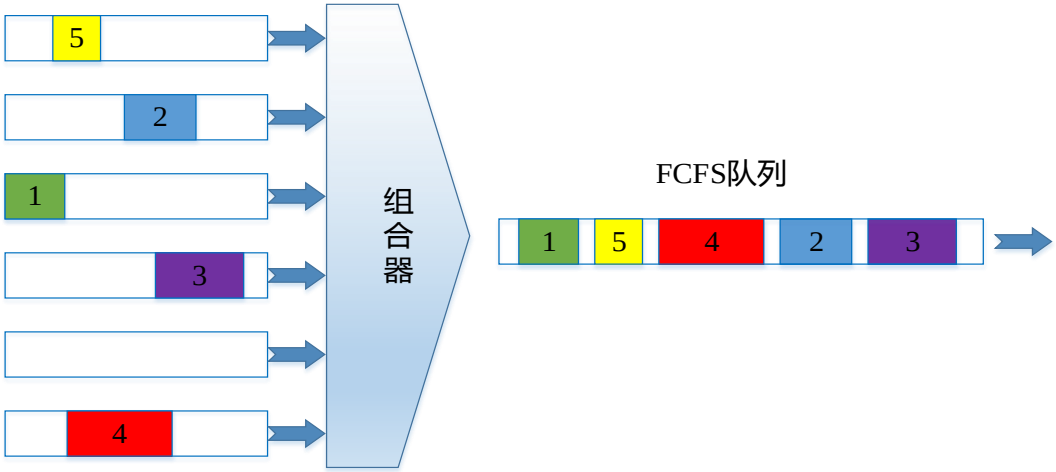

图 4-8 FCFS 队列调度图

Fig.4-8　Queue Scheduling of FCFS

4.4 承载 IPTV 业务实现流程

本节利用基于 ONU 的 VLAN 技术方案在 EPON 系统中承载 IPTV 业务实现流程，主要介绍通过在 OLT 和 ONU 端分别部署执行因特网组管理协议代理（IGMP Proxy）和帧听（IGMP Snooping）机制对组播成员用户进行管理，控制节目频道的加入和离开。

4.4.1 IPTV 节目授权过程

IPTV 用户机顶盒 STB（Set Top Box）或 PC 机开始注册时先发送 DHCP（动态主机配置协议）报文从服务器获得一个 IP 地址，然后 BRAS 服务器对 IPTV 用户名和密码进行认证。认证成功后，用户将使用所获得的 IP 地址信息和 IPTV 内容服务器进行通信，首先 IPTV 服务器通过 OLT 发给关于该用户的一张电子节目单 EPG（Electronic Program Guide），EPG 包括各种 IPTV 业务的索引及导航，用户可以利用这张 EPG 提供的菜单，选择自己喜欢的组播频道、点播自己喜欢的视频节目以及订购或退订其他节目。然后 OLT 根据用户授权的节目频道，查找 GIP-VLID 映射表，给 ONU 分配一个相应的 VLID 值，把 ONU 划分到相应的组播成员里面。整个注册过程如图 4-9 所示。

当用户注册成功后，如果用户想订购其他节目频道时，会发出一个订购请求来给视频服务器，则视频服务器更新该用户的授权节目单发给 OLT，OLT 同样根据 GIP-VLID 映射表对该 ONU 的 VLID 值进行更新，如图 4-9 所示。用户退订节目过程跟订购过程类似，所以 OLT 可以做到集中管理每个用户的节目表，并依此给 ONU 动态分配 VLID 值。

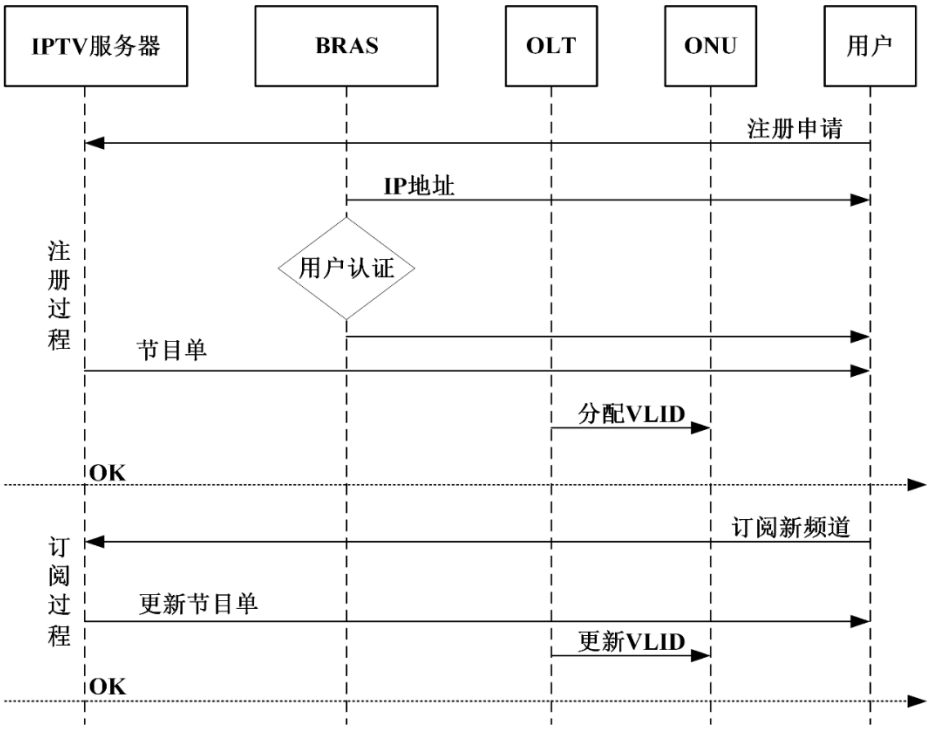

图 4-9 IPTV 节目授权过程

Fig.4-9 IPTV Program Impowers Process

4.4.2 IPTV 节目频道加入过程

每个用户经过 IPTV 节目授权过程后，都有自己的业务权限，用户只能观看已经授权的节目频道。而且 OLT 已经根据用户的组业务情况为它所属的 ONU 分配好 VLID 值，把 ONU 预先划分到相应的组播成员中。下面介绍用户怎样加入收看某一组播节目频道，整个过程如图 4-10 所示。

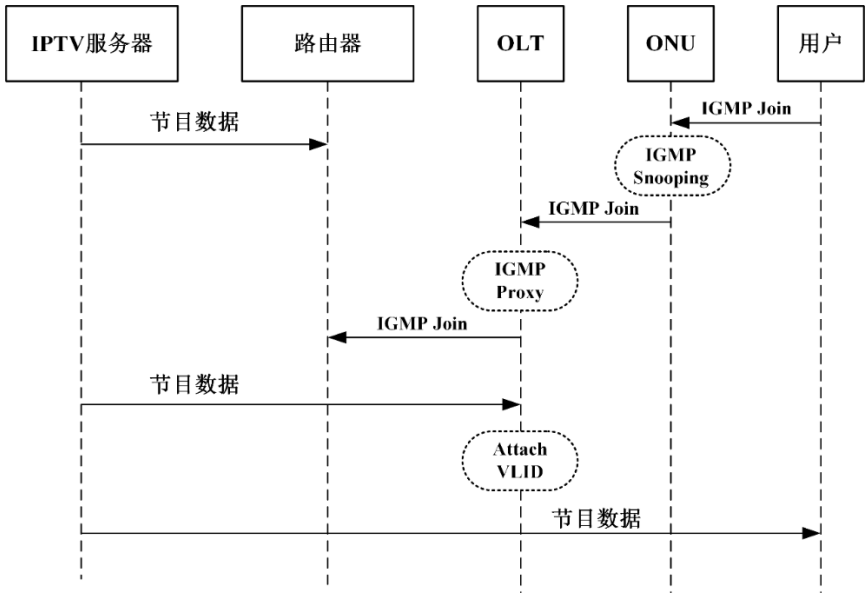

图 4-10 IPTV 节目频道加入过程

Fig.4-10 The Process of Jion IPTV Channel

当用户通过 EPG 菜单选择观看某个特定的额组播节目频道时，STB 会发出一个加入该频道的 IGMP 请求报文（IGMP Join）。此时 ONU 执行 IGMP Snooping 机制，将报文继续往 OLT 转发并且倾听该 IGMP 报文内容信息[55]，根据倾听到的信息创建维护本地组播表（组播地址与端口的关系），如表 4-3 所示，这里把端口直接对应用户。如果本地组播表中没有该组播项，则在组播表中添加组播地址和端口；如果本地组播表中已经存在该组播项，则只需要该组播项中添加申请端口。这样 ONU 就可以将接收到的组播数据帧只转发给内部端口，不向其他端口扩散。

表 4-3 ONU 端组播表

组播 IP 地址---端口			
组播地址	GIP1	GIP2	GIP3
端口	User1 User2	User3	User4

当 IGMP Join 报文传送到 OLT 端时，OLT 执行 IGMP Proxy 机制，倾听该 IGMP 报文信息并根据 OLT 的本地组播表（组播地址和 ONU 的关系），如表 4-4 所示，判断是不是新的组播数据申请。如果组播表中还没有此组播地址项，表明该用户申请的节目数

据流是 OLT 中还没有的，则在 OLT 组播表中添加该组播地址和 ONU 组播成员，并将 IGMP Join 报文继续往上层路由器转发，使路由器建立组播映射表，这样路由器才会将该组播数据下发到 OLT 上；如果组播表中已经存在此组播地址项，说明不是新的组播数据申请，用户选中的节目数据在 OLT 已经存在，则直接将 IGMP Join 报文丢弃，不再向路由器发送。

表 4-4 OLT 端组播表

组播 IP 地址---端口			
组播地址	GIP1	GIP2	GIP3
ONU	ONU_1 ONU_2 ONU_3	ONU_1 ONU_2	ONU_1

当节目数据流到达 OLT 时，OLT 会根据组播地址和 VLID 值的映射表在数据前导码中插入对应的 VLID 值，然后转发给下行的 ONU，这时只有该组播成员的 ONU 才能接收到该组播数据，接着组播成员的 ONU 再根据本地的组播表将接收到的组播数据帧只转发到给请求的数据用户，最后用户观看到节目。假如表 4-3 是 ONU1 端的组播表，则可以看出 ONU1 能收到三个组播地址 GIP1、GIP2 以及 GIP3 对应的组播数据，但是 ONU1 只将 GIP1 的组播数据转发给用户 1 和用户 2，将 GIP2 的组播数据转发给用户 3，而 GIP3 的组播数据只转发给用户 4。

4.4.3 IPTV 节目频道切换过程

用户可以在自己的授权节目频道中从一个频道切换到另一个频道，频道切换的流程如图 4-11 所示。当用户切换频道时，STB 首先发送一个关于原先频道的 IGMP 离开报文（IGMP Leave），ONU 执行 IGMP Snooping 机制，倾听 IGMP Leave 报文更新维护自己的本地组播表：把请求离开的端口从原来组播项中删除，同时，如果该组播项里面刚好也没有其他端口时，则把该组播项直接从组播表中删除。OLT 端执行 IGMP Proxy 机制，同样根据 IGMP Leave 报文更新本地组播表并且将 IGMP Leave 报文直接丢弃，不再往上层路由器转发。随后 STB 发出关于加入新频道的 IGMP Join 报文，后面的过程跟前面 IPTV 节目频道加入过程一样，最终实现节目频道的切换。可以看出在 EPON 系统部署执行基于 ONU 的 VLAN 技术和 IGMP Snooping 机制来承载 IPTV 业务，可以很好的为用户提供不同的、安全的电视频道服务，而且缩短了 IPTV 节目频道切换的时间，更好的满足用户的需求。

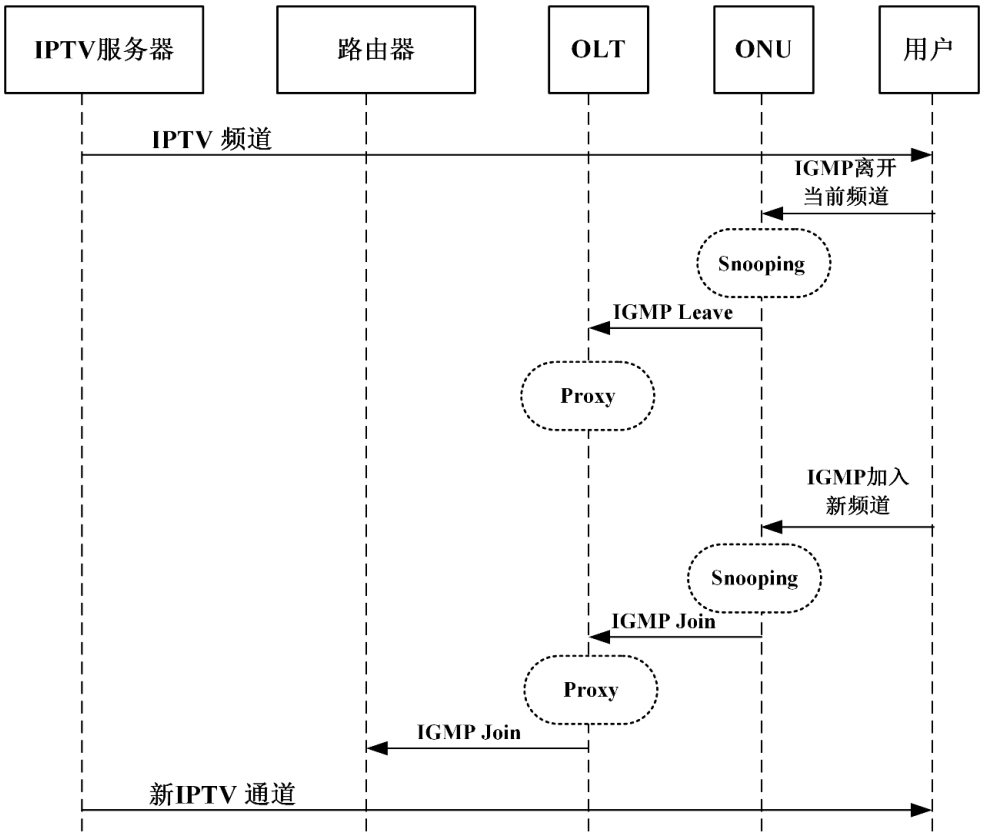

图 4-11 IPTV 节目频道切换过程

Fig.4-11 The Process of Transition IPTV Channel

4.5 本章小结

本章首先介绍了 EPON 承载 IPTV 需要解决的两个关键问题，即如何正确地寻找一个模型来代表 IPTV 业务并快速生成数据流量；如何将流量模型与 10G EPON 接入网进行结合。然后详细的介绍了多业务情形下 EPON 承载组播 IPTV 的分级调度算法设计，把多业务分为一般业务和组播 IPTV 类业务，缓存到对应队列中去。其中，组播 IPTV 队列根据 WRR 算法进行低级、中级、高级区分分配带宽。最后，介绍了 IPTV 业务的注册授权、用户加入节目频道过程和离开节目频道的过程。

第五章 承载 IPTV 业务技术方案的 FPGA 设计

5.1 OLT 控制模块的 FPGA 设计

针对基于 ONU 的 VLAN 设计实现 EPON 系统承载 IPTV 业务，OLT 端完成的主要功能有：完成 ONU 的自动加入与注册、对多业务的单/组播划分、对队列的调度、对 ONU 的 VLID 的分配更新、对用户发往路由器的 IGMP 报文倾听以及对数据帧的传输控制。由于 OLT 端的数据分为上行数据和下行数据，下行数据是从网络层传输到 OLT 端，而上行数据是从 ONU 上传到 OLT 端，因此 OLT 端控制模块 OLT_Block 的 FPGA 设计结构框图如图 5-1 所示。

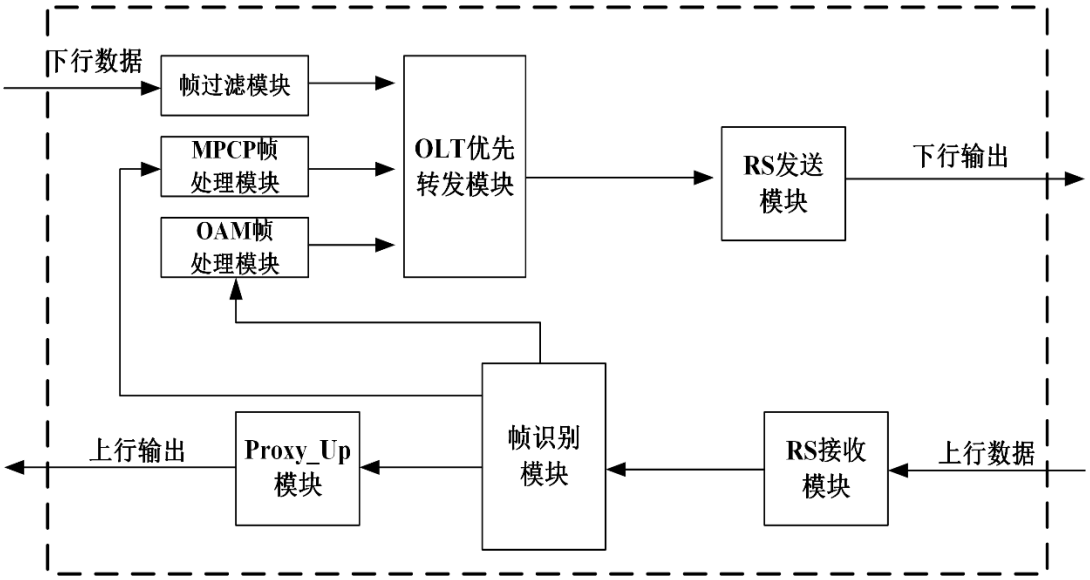

图 5-1 OLT 端模块设计图

Fig. 5-1 Module Design Diagram of OLT

OLT_Block 主要包括 7 个模块：帧过滤模块 Frame_Filter、MPCP 帧处理模块 OLT_MPCP_Block、OAM 帧处理模块 OLT_OAM_Block、OLT 优先转发模块 OLT_Scheduling、RS 模块（包括下行 RS 发送模块 OLT_RS_Send 和上行 RS 接收模块 OLT_RS_Receive）、帧识别模块 Frame_Identify 以及上行数据侦听模块 Proxy_Up。其中，OLT_OAM_Block 模块和 OLT_MPCP_Block 模块操作方式类似，Frame_Identify 模块设计简单，所以下面重点介绍其它 5 个模块的设计。

5.1.1 Frame_Filter 模块设计

1.模块功能介绍

Frame_Filter 模块的主要功能是对异常帧进行过滤，对来自上层的普通以太报文数据进行字节长度检查，过滤掉那些不符合协议的超长或者残余的报文数据。因为根据协议规定，以太网数据帧长度范围是 64 到 1518 个字节之间，所以本文利用 Frame_Filter

模块只接收符合标准的数据帧，丢弃那些字节长度小于 64 的残余帧或大于 1518 的超长帧。Frame_Filter 模块的接口信号如图 5-2 所示。

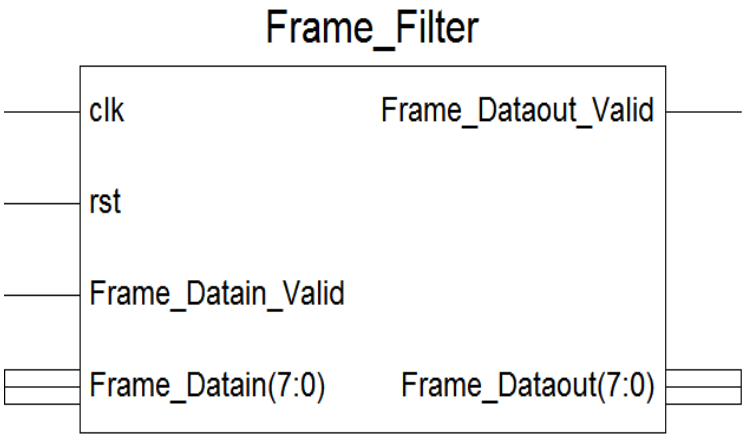

图 5-2 Frame_Filter 模块接口图

Fig. 5-2 Interface Signal Chart of Frame_Filter

Frame_Filter 模块的信号接口定义如表 5-1 所示。

表 5-1 Frame_Filter 模块接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
Din(7:0)	I	帧输入信号
Din_Valid	I	帧输入有效信号
Dout_Valid	O	帧输出有效信号
Dout(7:0)	O	帧输出信号

2.模块具体设计

Frame_Filter 模块的设计流程如图 5-3 所示，模块复位开始后，准备接收上层数据帧。协议规定数据帧的发送方式为连续发送，中间不能有间断，但帧与帧之间需等待一个帧间隙时间（interframe gap,IFG），作为帧接收之间的恢复时间。如果检测到 Frame_Datain_Valid 为高电平，说明有数据到来，则模块开始接收存储数据并对该数据帧的字节计数。当计数完成，Frame_Datain_Valid 恢复为低电平时，说明此数据帧传输完成。接着判断数据帧的字节大小，如果字节数在 64—1518 范围之内，则拉高 Frame_Datain_Valid 信号，数据帧从 Frame_Dataout 信号接口向后续模块转发，否则直接丢弃该数据帧。

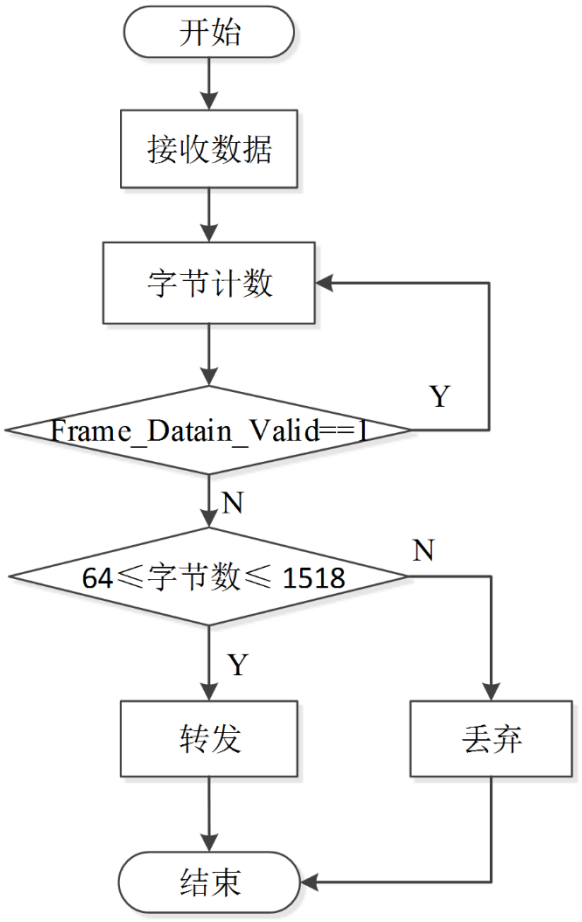

图 5-3 Frame_Filter 模块工作流程图

Fig.5-3 Flow Chat of Frame_Filter

5.1.2 OLT_MPCP_Block 模块设计

1.模块功能介绍

OLT_MPCP_Block 模块是 OLT 端重要控制模块，主要完成 ONU 的发现、注册以及三个自定义 MPCP 帧的设计，给未注册的 ONU 分配初始 VLID 值（6'0x3f）和唯一 LLID 值，并根据 8 个 MPCP 帧进行 OLT 和 ONU 的双向身份验证。ONU 的注册过程都是从 OLT 端周期产生并发送的广播注册 DISCOVERY_GATE 帧开始的，连同其它 4 个 EPON 系统中原有的 MPCP 帧和 3 个自定义的 MPCP 帧完成身份验证，实现成功注册。过程中，为了方便调试和观察，本文设计了一个注册控制引脚 Register_Contor 信号。当 Register_Contor 为高电平时，OLT_MPCP_Block 模块发送 DISCOVERY_GATE 帧，启动一轮 ONU 的注册过程，否则 ONU 一直等待注册。另外，本文还增加了一个注册成功指示信号 Register_Success，当 ONU 成功注册则拉高此信号。OLT_MPCP_Block 模块的接口信号图如图 5-4 所示。

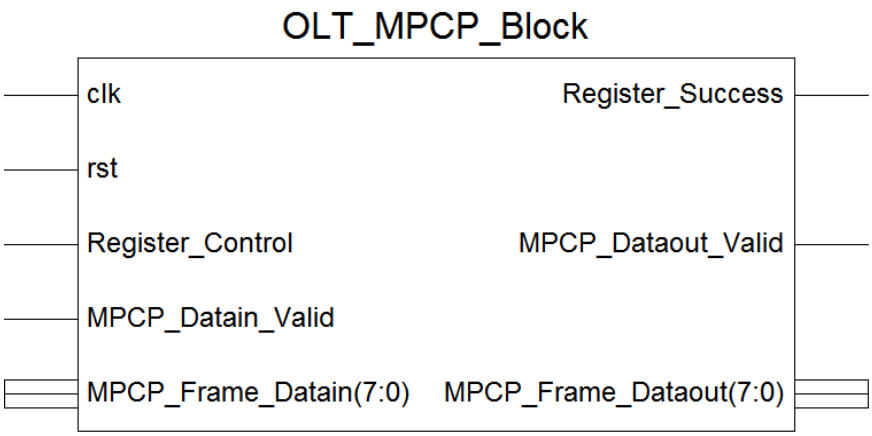

图 5-4 OLT_ MPCP_Block 模块接口图

Fig. 5-4 Interface Signal Chart of OLT_ MPCP_Block

OLT_MPCP_Block 模块的信号接口定义如表 5-2 所示。

表 5-2 OLT_MPCP_Block 接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
Register_Control	I	注册控制信号
MPCP_Datain_Valid	I	MPCP控制帧输入有效信号
MPCP_Frame_Datain(7:0)	I	MPCP控制帧输入信号
Register_Success	O	注册成功指示信号
MPCP_Dataout_Valid	O	MPCP控制帧输出有效信号
MPCP_Frame_Dataout(7:0)	O	MPCP控制帧输出信号

2. 模块具体设计

OLT_MPCP_Block 模块的设计流程图如图 5-5 所示，OLT_MPCP_Block 模块复位后，手动给 Register_Contor 信号赋一个高电平，开始一轮 ONU 的注册，则模块随即准备接收 OUN 发送来的 MPCP 控制帧。当检测到 MPCP_Datain_Valid 为高电平时，表明有 ONU 发来 MPCP 控制帧，则接收并存储此控制帧。然后解析判断 MPCP 控制帧中操作码字段 Opcode。如果 Opcode 值为 0x0004,说明接收到的是注册请求帧 REGISTER_REQ,并且同时验证 Opcode=16'h007,16'h008,16h009 三个自定义的 MPCP 帧，如果都通过,则 ONU 和 OLT 的双向身份认证成功,模块开始发送一个注册帧 REGISTER（内容有 VLID=6'0x3f 和一个 LLID 值）。当 REGISTER 帧输出完后发送一个普通 GATE 帧 NORMAL_GATE 给该 ONU 授权,当 NORMAL_GATE 帧输出完毕后转到结束状态。如果 Opcode 值为 0x0006，说明接收到的是注册确认帧 REGISTER_ACK，表明注册成功，拉高 Register_Success 信号，然后转到结束状态。否则直接结束，ONU 注册失败，

等待下一轮注册。

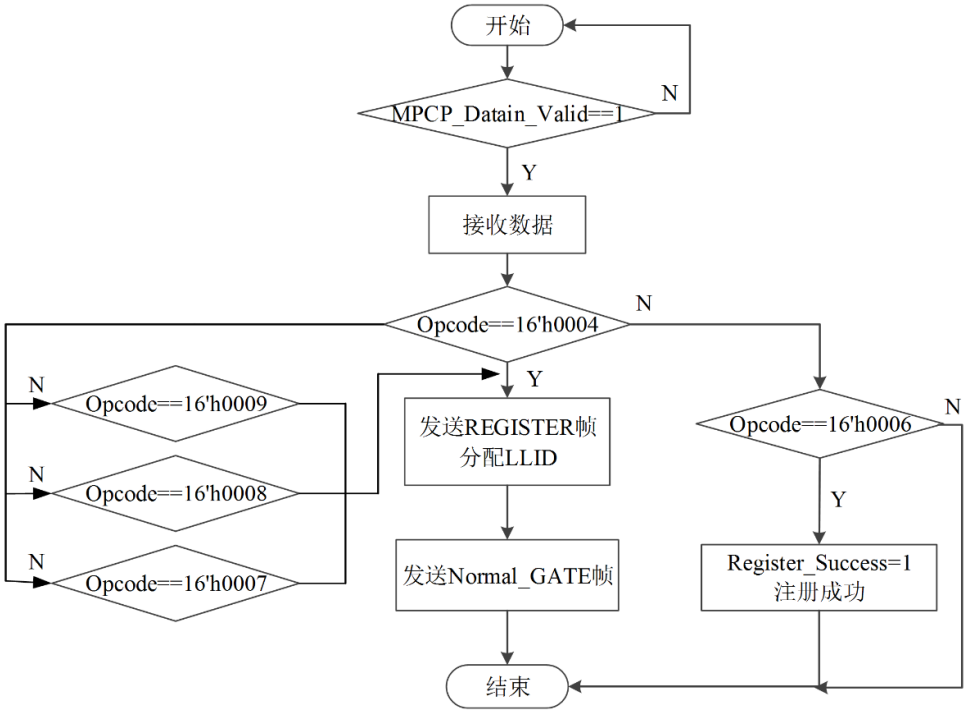

图 5-5 OLT_MPCP_Block 工作流程图

Fig. 5-5 Flow Chat of OLT_MPCP_Block

5.1.3 OLT_Scheduling 模块

1.模块功能介绍

OLT_Scheduling 模块主要实现对来自 Frame_Filter 模块的普通以太报文数据、OLT_MPCP_Block 模块的 MPCP 控制帧以及 OLT_MPCP_Block 模块的 OAM 帧的优先发送控制，转发的优先顺序为：MPCP 控制帧最高，OAM 帧其次，普通以太报文数据帧最低。其中，普通以太网报文多业务数据根据 WRR 调度优先级来决定如何调度低级缓存、中级缓存、高级缓存三种业务。OLT_Scheduling 模块的接口信号图如图 5-6 所示。

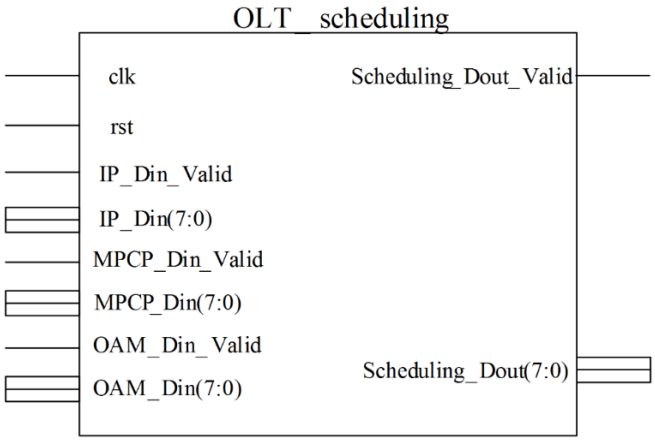

图 5-6 OLT_Scheduling 模块接口信号图

Fig.5-6 Interface Signal Chart of OLT_Scheduling

OLT_Scheduling 模块的信号接口定义如表 5-3 所示。

表 5-3 OLT_Scheduling 模块接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
IP_Din_Valid	I	IP 数据输入有效信号
IP_Din(7:0)	I	IP 数据输入信号
MPCP_Din_Valid	I	MPCP 帧数据输入有效信号
MPCP_Din(7:0)	I	MPCP 帧数据输入信号
OAM_Din_Valid	I	OAM 帧数据输入有效信号
OAM _Din(7:0)	I	OAM 帧数据输入信号
Scheduling_Dout_Valid	I	帧输出有效信号
Scheduling_Dout (7:0)	I	帧输出信号

2.模块具体设计

OLT_Scheduling 模块采用三个 FIFO（First In First Out）存储器和一个优先控制模块来实现，如图 5-7 所示。其中三个 FIFO 存储器分别接收存储来自 OLT_MPCP_Block 模块的 MPCP 控制帧、OLT_OAM_Block 的 OAM 帧和 Frame_Filter 模块的普通以太网报文数据帧。三种帧数据再经过优先控制模块进行数据优先转发，转发原则是：优先转发 MPCP 控制帧和 OAM 帧，对于以太网业务分组，划分为一般业务和组播业务，并对组播业务根据按照公式 4-1 分别计算三类业务的权值，然后按照相应的权值发送数据分组。

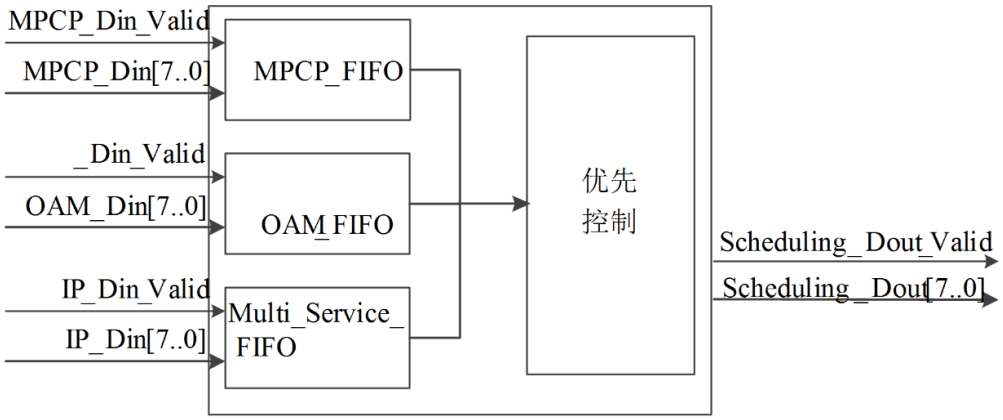

图 5-7 OLT_Scheduling 模块组成

Fig.5-7 The Compostion of OLT_Scheduling Block

5.1.4 OLT_RS_Send 模块设计

1. 模块功能介绍

OLT_RS_Send 主要实现 ONU 的数据选择功能，只接收属于自己的数据，丢弃其它数据，通过在 EPON 网络下行数据的前导码字段来插入相应的值，这些值主要包括：

MODE 位、虚拟局域网标识字段 VLID 以及逻辑链路标识 LLID。然后对前导码中第 3 个字节到第 7 个字节进行 CRC-8 校验并将校验码添加在前导码的第 8 个字节上，最终形成完整的 EPON 帧向下行 ONU 发送出去。OLT_RS_Send 模块的接口信号图如图 5-8 所示。

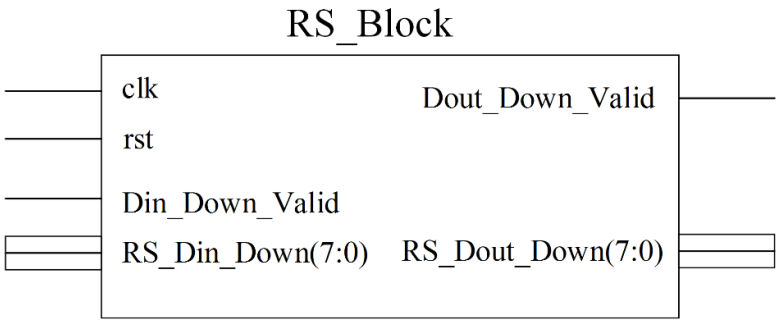

图 5-8 RS 模块接口图

Fig. 5-8 Interface Signal Chart of RS

模块接口定义如表 5-4 所示。

表 5-4 OLT_RS 模块接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
RS_Din_Down(7:0)	I	RS下行帧输入信号
Din_Down_Valid	I	下行帧输入有效信号
Dout_Down_Valid	O	下行帧输出有效信号
RS_Dout_Down(7:0)	O	RS下行帧输出信号

2.模块具体设计

OLT_RS_Send 模块的设计流程图如图 5-9 所示，详细地介绍了如何根据下行帧中目的地址字段 DA 值插入相应的 Mode 位、VLID 字段值和 LLID 字段值来形成完整的前导码过程。当 OLT_RS_Send 模块复位开始后，模块准备接收数据。当检测到 Din_Down_Valid 为高电平时，表明 OLT 端有数据要发送，便接收存储此数据帧。然后解析帧中目的地址 DA 值，如果为广播地址（48’0xff-ff-ff-ff-ff-ff），则 Mode&VLID&LLID 为 16’0xffff；如果为某个 ONU 的 MAC 地址值，则 Mode 为 0，VLID 值等于 6’0x3f，LLID 值为该 ONU 注册时分配的 LLID 值；如果为组播 MAC 地址，则 Mode 为 1，VLID 值为该组播地址对应的 VLID 值，LLID 等于 9’0x1ff，这三种类型的数据都将通过 CRC-8 电路计算出前导码的 CRC8 检验值，并添加在前导码的第 8 个字节上，最终形成完整的 EPON 下行帧结构，随即拉高 Dataout_Dowm_Valid 信号并将完整的下行帧从

RS_Dataout_Down 接口发送出去。否则直接丢弃结束。

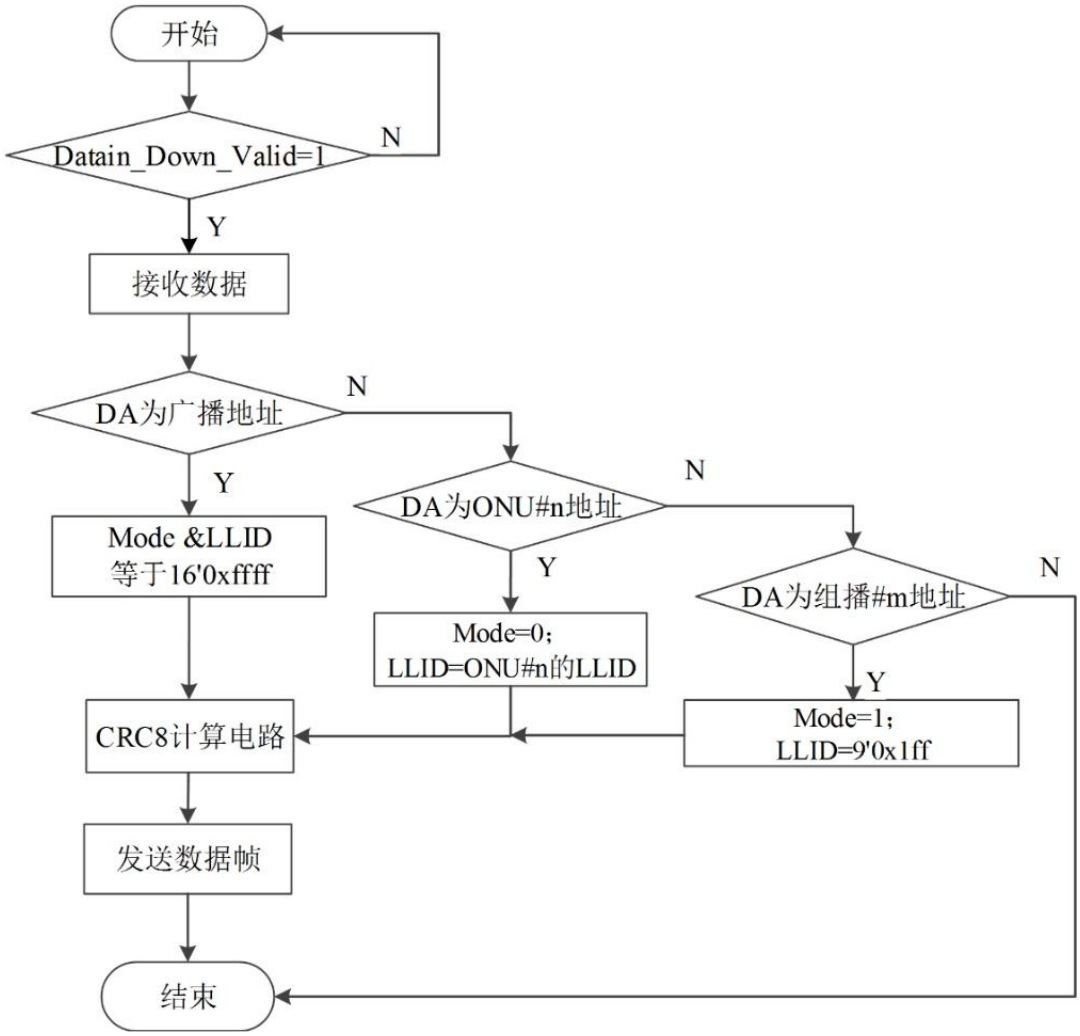

图 5-9 RS 模块流程图

Fig. 5-9 Flow Chat of RS

5.1.5 Proxy_Up 模块设计

1. 模块功能介绍

Proxy_Up 模块的功能是实现 OLT 执行 IGMP Proxy 机制。在本文设计方案中 Proxy_Up 模块通过倾听来至 Frame_Identify 模块的 IP 数据帧，判断是不是 IGMP 报文数据。如果不是说明仅仅是普通的 IP 业务数据，则直接向上层转发出去；如果是 IGMP 报文则继续解析 IGMP 报文中的信息内容来建立维护 OLT 端的组播表。Proxy_Up 模块的接口信号图如图 5-10 所示。

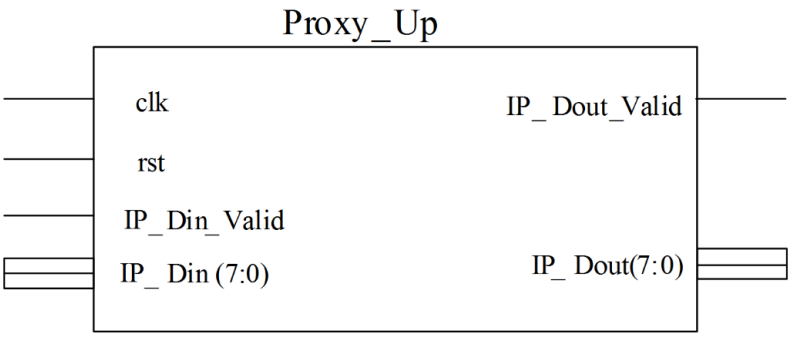

图 5-10 Proxy_Up 模块接口信号图

Fig.5-10 Interface Signal Chart of Proxy_Up

Proxy_Up 模块的信号接口定义如表 5-5 所示。

表 5-5 Proxy_Up 模块信号接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
IP_ Din_ Valid	I	IP帧输入有效信号
IP_ Din(7:0)	I	IP帧输入信号
IP_ Dout_Valid	O	IP帧输出有效信号
IP_ Dout(7:0)	O	IP帧输出信号

2. 模块具体设计

Proxy_Up 模块的设计流程图如图 5-11 所示。当 Proxy_Up 模块复位开始后，准备接收上行数据。当检测到 IP_Dn_Valid 为高电平时，说明有 IP 数据帧到来，则接收此数据。然后存下帧中的源地址 SA 并解析 IP 报文的协议字段 Protocol。如果 Protocol 值不是 0x02,则说明不是 IGMP 报文数据，则拉高 IP_Dout_Valid 信号，将此数据直接向上层转发。若 Protocol 值等于 0x02，则说明是 IGMP 报文，进一步解析 IGMP 报文类型字段 type 和组播地址字段 GIP。如果 type 只等于 0x12 或者 0x16，说明该数据是用户申请加入 GIP 对应节目频道的报文，随即判断 GIP 是不是新的组播地址，如果是，说明该用户申请加入的组播数据流在 OLT 中没有记录，则添加此组播地址项 GIP 和源地址 SA，并拉高 IP_Dout_Valid 信号将 IGMP 报文继续向上层路由器传送，使路由器建立组播映射表，这样上层路由器才能把该组播数据下发到 OLT；如果 GIP 不是新的组播地址，表明该 GIP 对应的节目数据在 OLT 已经存在，则直接将此 IGMP 请求报文丢弃，不再向路由器转发。若 type 值是 0x17 代表是用户离开节目频道申请，则将 OLT 组播表中该 GIP 组播项下的源地址 SA 删除，而且不再将报文往路由器转发。

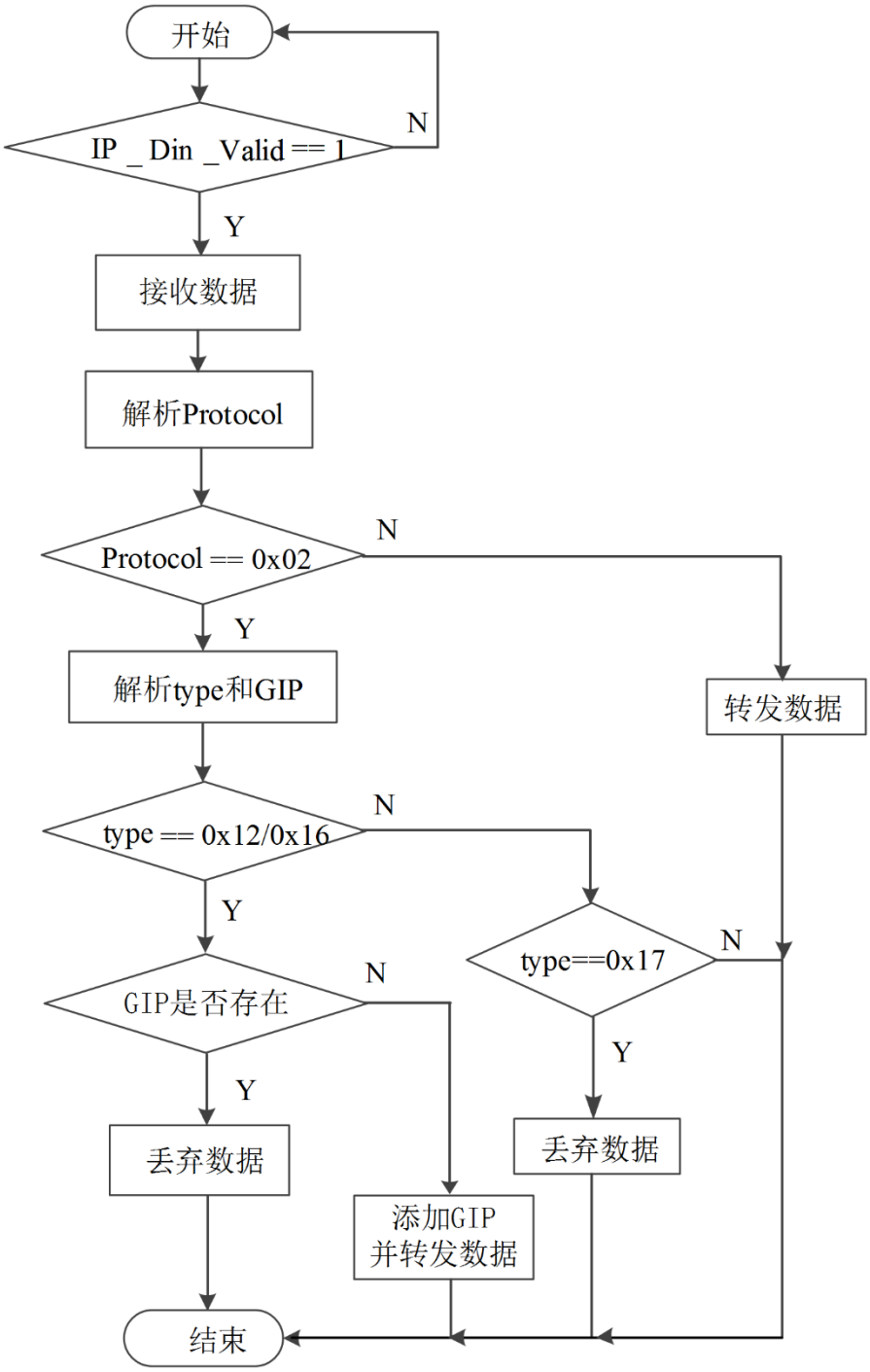

图 5-11 Proxy_Up 模块流程图

Fig.5-11 Flow Chat of Proxy_Up Block

5.2 ONU 控制模块的 FPGA 设计

针对本文设计方案，ONU 端的完成的主要功能有：配合 OLT 完成自己的注册过程；对用户发往路由器的 IGMP 报文倾听以及对业务数据帧接收转发控制。由于 ONU 端的数据也分为上行数据和下行数据：下行数据是 OLT 的数据下发到 ONU，上行数据是用户的数据上传到 ONU，因此 ONU 端控制模块 ONU_Block 的 FPGA 设计结构框图如图

5-12 所示。

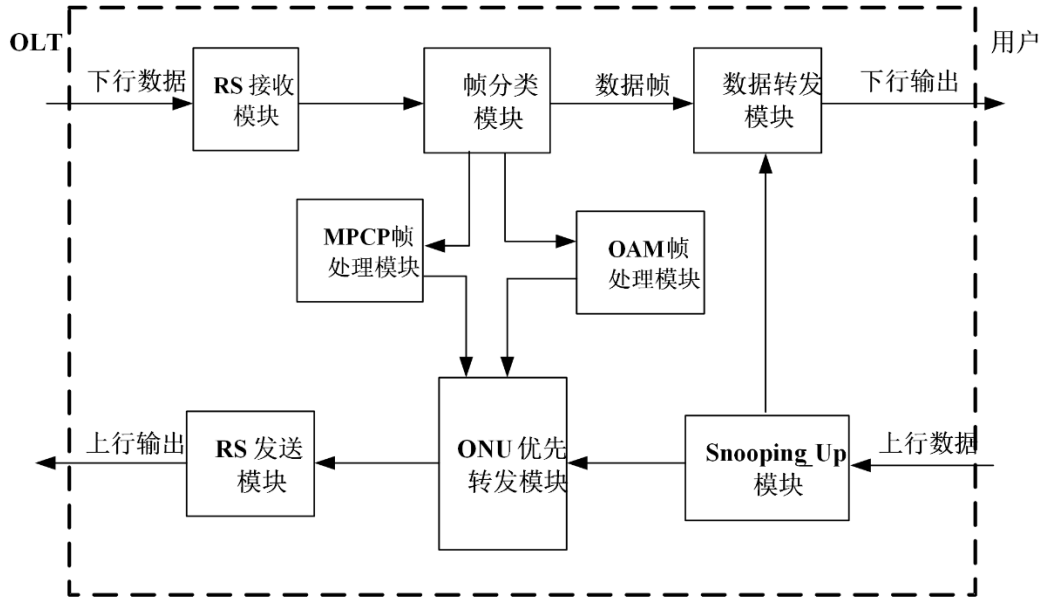

图 5-12 ONU_Block 模块结构框图

Fig.5-12 Structure Diagram of ONU_Block

下行数据经过 ONU_RS_Receive 模块过滤和 ONU_FCS_Check 模块校验后，ONU 只接收属于自己的有效数据。然后通过 Frame_Classify 模块区分出数据类型：普通 IP 数据帧、MPCP 控制帧以及 OAM 帧。OAM 帧送入 ONU_OAM_Block 模块处理、MPCP 控制帧送入 ONU_MPCP_Block 模块进行处理，而普通数据帧在 Data_Transmit 模块控制下向用户端转发。上行数据经过 Snooping_Up 模块后，MPCP 控制帧、OAM 帧和多业务请求数据在 ONU_Scheduling 模块的控制下实现优先转发，输出数据再通过 ONU_RS_Send 模块发往 OLT 端。

由于本文 ONU 端的 FCS 模块跟 OLT 端的 FCS 模块设计原理相同，Frame_Classify 跟 OLT 端帧的识别模块 Frame_Identify 相似，ONU 优先转发控制模块跟 OLT 优先转发模块相同，所以下面只详细介绍其他子模块的设计。

5.2.1 ONU_RS_Receive 模块设计

1. 模块功能设计

ONU_RS_Receive 模块主要实现 ONU 端 RS 子层接收过滤数据的功能，本文方案中主要包括：VLID、LLID 的过滤以及前导码中 CRC8 的检验功能，将那些 VLID、LLID 不匹配或者 CRC8 检验错误的下行数据直接丢弃处理，实现 RS 子层对单播、组播以及广播数据的接收过滤。ONU_RS_Receive 模块的接口信号图如图 5-13 所示。

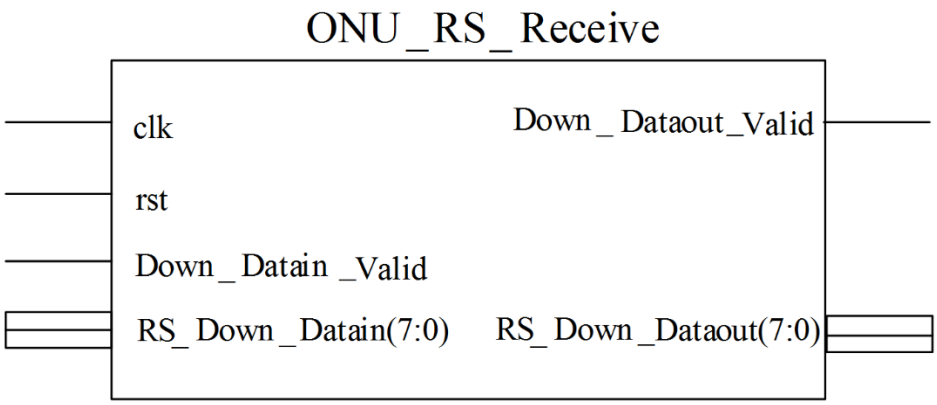

图 5-13 ONU_RS_Receive 模块杰克卢信号图

Fig.5-13 Interface Signal Chart of ONU_RS_Receive

ONU_RS_Receive 模块的信号接口定义如表 5-6 所示。

表 5-6 ONU_RS_Receive 模块信号接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
RS_ Down _Datain(7:0)	I	RS下行数据输入信号
Down _ Datain _Valid	I	下行数据输入有效信号
Down _ Dataout_Valid	O	下行数据输出有效信号
RS_ Down _Dataout(7:0)	O	RS下行数据输出信号

2. 模块具体设计

ONU_RS_Receive 模块的设计流程图如图 5-14 所示。当 ONU_RS_Receive 模块复位后，准备接收下行数据。当检测到 Down_Datain_Valid 为高电平时，说明有下行数据帧到来，则 ONU_RS_Receive 模块接收并存储此数据。然后解析帧前导码中 CRC8 检验值，如果 CRC8 检验值错误，则直接求其该数据帧结束。如果 CRC8 检验值正确，则继续解析前导码中模式位 Mode、VLID 字段以及 LLID 字段。如果 Mode&VLID&LLID 为 16’0xffff，说明该下行数据帧为广播数据，则拉高 Down_Dataout_Valid 信号并将该数据转发给后续模块处理；如果 Mode 为 1，VLID 与 ONU 的 VLID 值匹配，而且 LLID 等于 9’0x1ff，说明该下行数据帧属于自己的组播数据，则拉高 Down_Dataout_Valid 信号并将数据转发；如果 Mode 为 0，VLID 值等于 6’0x3f，LLID 与该 ONU 的 LLID 值匹配，说明该数据帧是属于自己的单播数据，则拉高 Down_Dataout_Valid 信号也将该下行数据转发出去；否则丢弃此下行数据结束。

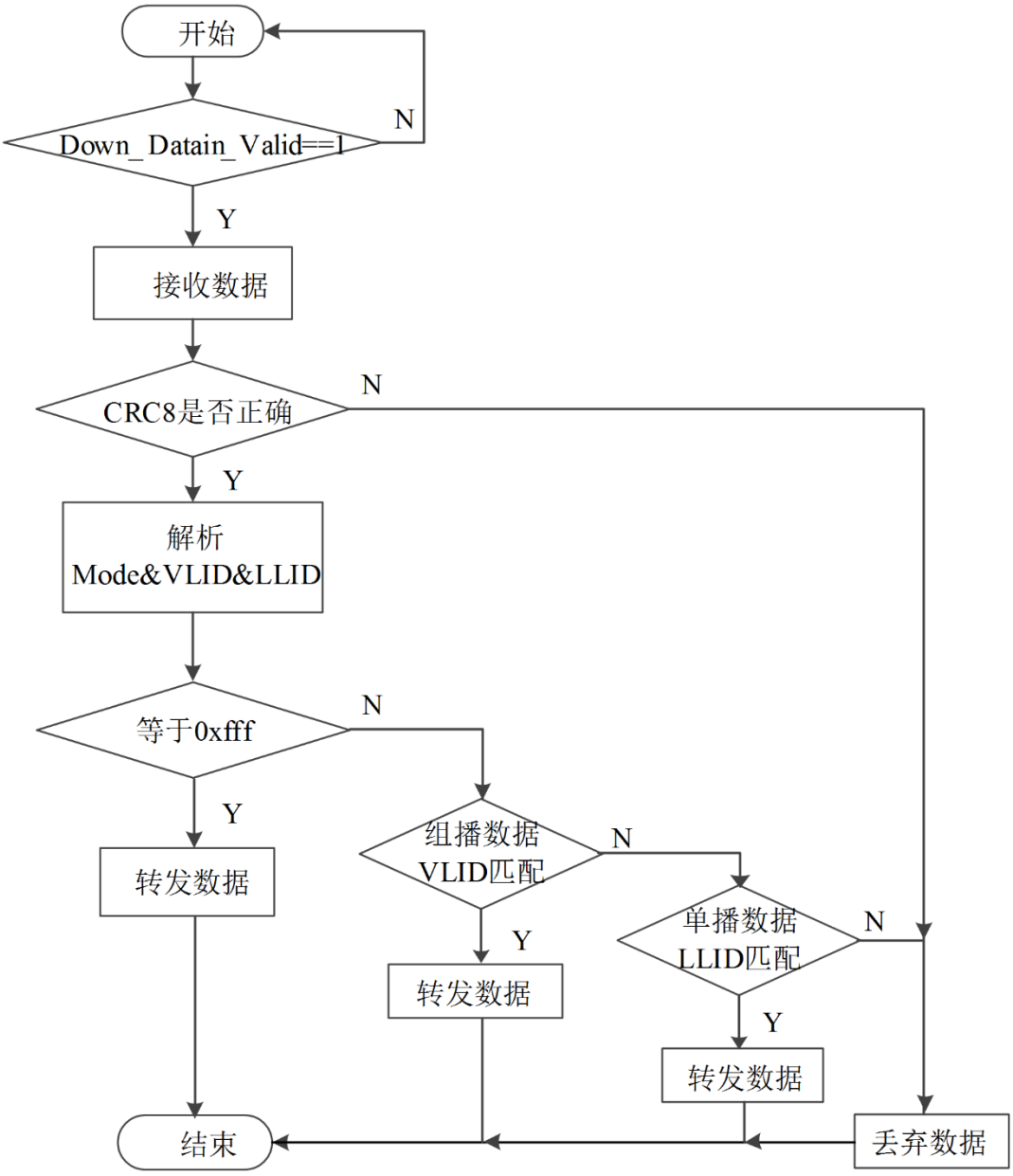

图 5-14 ONU_RS_Receive 模块流程图

Fig.5-14 Flow Chat of ONU_RS_Receive Block

5.2.2 ONU_MPCP_Block 模块设计

1. 模块功能介绍

ONU_MPCP_Block 模块是 ONU 端重要控制模块，在本文方案设计中其主要功能是通过配合相应 OLT_Block 模块发送过来的各种 MPCP 控制帧，完成自己的注册过程，从而得到自己的身份标识 LLID 以及 VLID 的更新内容。另外，本文在设计中还添加了 LLID 和 VLID 字段输出信号，方便在测试中观察值的变化情况。ONU_MPCP_Block 模块的接口信号图如图 5-15 所示。

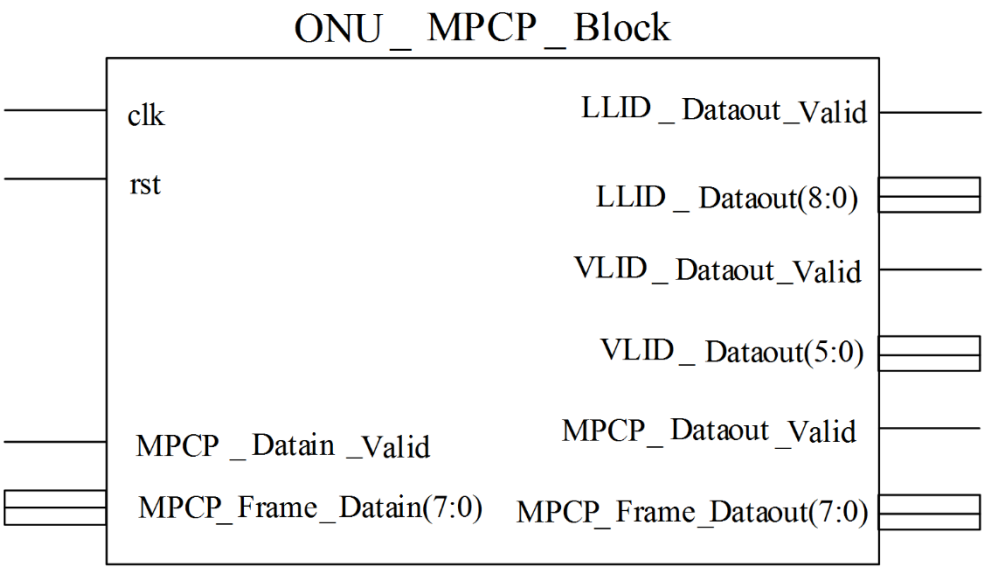

图 5-15 ONU_MPCP_Block 模块接口信号图

Fig.5-15 Interface Signal Chart of ONU_MPCP_Block

ONU_MPCP_Block 模块的信号接口定义如表 5-7 所示。

表 5-7 ONU_MPCP_Block 模块信号接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
MPCP _ Datain _Valid	I	MPCP控制帧输入有效信号
MPCP_ Frame_ Datain(7:0)	I	MPCP控制帧输入信号
LLID _ Dataout_Valid	O	LLID值输出有效信号
LLID _ Dataout(8:0)	O	LLID值输出信号
VLID _ Dataout_Valid	O	VLID值输出有效信号
VLID _ Dataout(5:0)	O	VLID值输出信号
MPCP_ Dataout _Valid	O	MPCP控制帧输出有效信号
MPCP_ Frame_Dataout(7:0)	O	MPCP控制帧输出信号

2. 模块具体设计

ONU_MPCP_Block 模块的设计流程图如图 5-16 所示，ONU_MPCP_Block 模块复位开始后，准备接收数据。当检测到 MPCP_Datain_Valid 为高电平时，说明有 MPCP 控制帧输入，则 ONU_MPCP_Block 模块开始接收并存储该控制帧，然后解析 MPCP 控制帧中操作码字段 Opcode 的值。如果 Opcode 值为 0x0002，说明接收到的控制帧是启动注册 GATE 帧，判断 LLID_Dataout_Valid 的值，如果 LLID_Dataout_Valid 为高电平，说

明该 ONU 已经注册，则忽略该 GATE 帧直接结束，如果 LLID_Dataout_Valid 为低电平，则发送 REGISTER_REQ 帧请求注册，当 REGISTER_REQ 帧输出完毕后转到结束状态；如果 Opcode 值为 0x0004，说明接收到的是 REGISTER 帧，则拉高 VLID_Dataout_Valid 和 LLID_Dataout_Valid 信号，并根据该 REGISTER 帧中的信息内容给 VLID_Dataout 和 LLID_Dataout 信号赋值，同时发送一个注册确认帧 REGISTER_ACK 告诉 OLT 注册成功；否则直接结束。

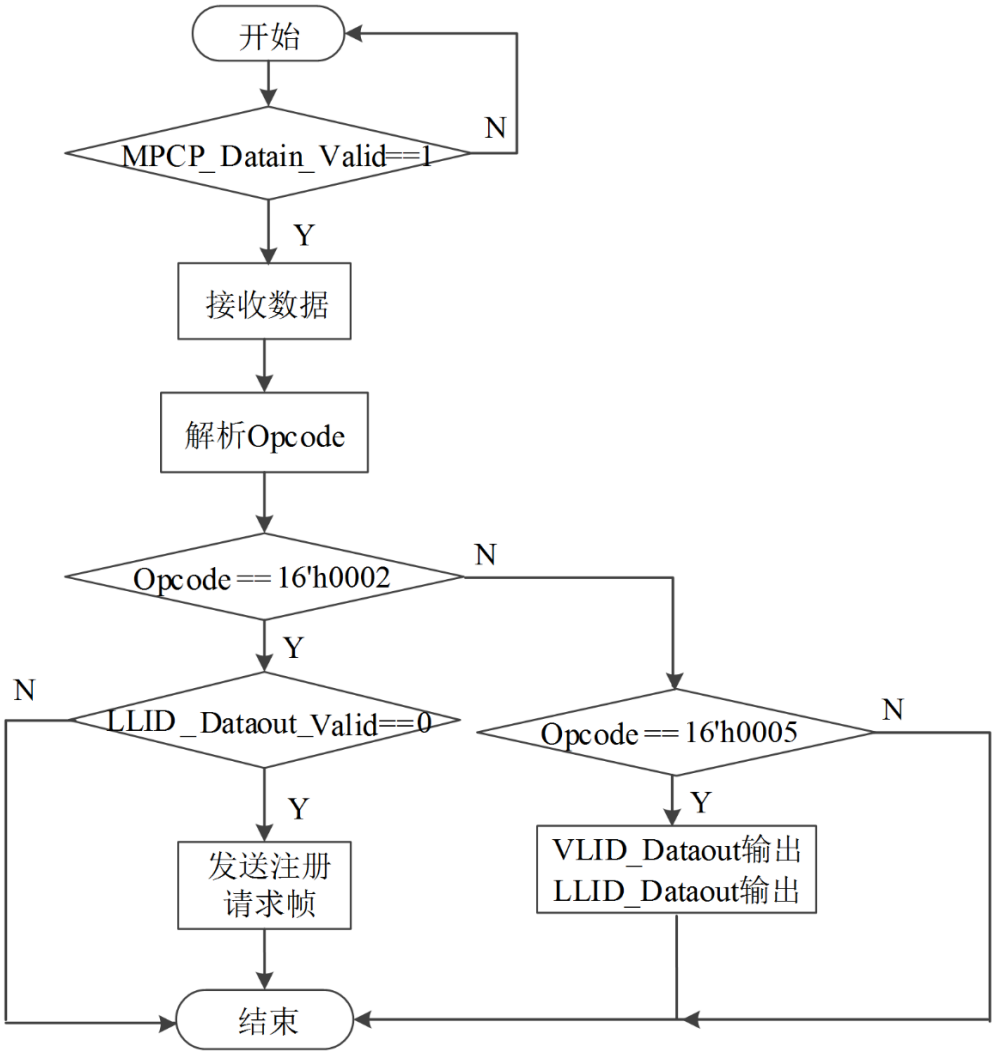

图 5-16 ONU_MPCP_Block 模块流程图

Fig.5-16 Flow Chat of ONU_MPCP_Block

5.2.3 Snooping_Up 模块设计

1. 模块功能介绍

Snooping_Up 模块的功能类似于 OLT 端 Proxy_Up 模块，都是倾听上行 IGMP 报文来获取用户相关信息。但是 Snooping_Up 模块只是倾听信息，并不具备 Proxy_Up 模块的代理路由去处理 IGMP 报文数据的功能，所以上行数据达到 Snooping_Up 模块时，数据都将往上层转发。Snooping_Up 模块的接口信号图如图 5-17 所示。

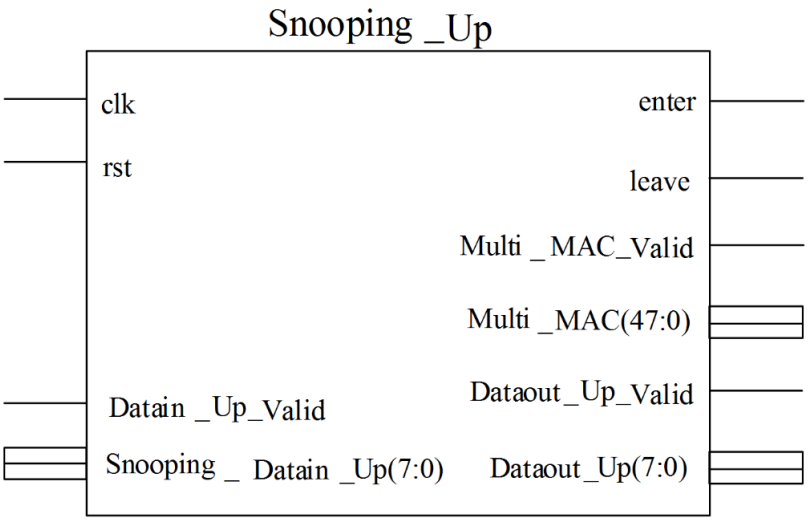

图 5-17 Snooping_Up 模块接口信号图

Fig.5-17 Interface Signal Chart of Snooping_Up

Snooping_Up 模块的信号接口定义如表 5-8 所示。

表 5-8 Snooping_Up 模块的信号接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
Datain _Up_Valid	I	上行数据输入有效信号
Snooping _ Datain _Up(7:0)	I	倾听上行数据输入信号
enter	O	加入标识信号
leave	O	离开标识信号
Multi _MAC_Valid	O	组播MAC地址输出有效信号
Multi _MAC(47:0)	O	组播MAC地址输出信号
Dataout_Up_Valid	O	上行数据输出有效信号
Dataout_Up(7:0)	O	上行数据输出信号

2. 模块具体设计

Snooping_Up 模块的设计流程图如图 5-18 所示。Snooping_Up 模块复位开始后，准备接收上行数据。当检测到 Datain_Up_Valid 为高电平时，表明有数据到来，则模块接收存储该数据并且拉高 Dataout_Up_Valid 信号，将数据直接往上行转发。解析数据帧中 IP 报文的协议字段 Protocol,如果 Protocol 值不是 0x02，则说明只是普通 IP 报文数据，则直接结束倾听；如果 Protocol 值等于 0x02，说明是 IGMP 报文数据，进一步解析 IGMP 报文中类型 type 值和组播地址字段 GIP。如果 type 值等于 0x12 或 0x16，则代表该数据

是下行用户申请加入节目频道报文，则拉高 enter 信号和 Multi_MAC_Valid 信号，并且将 GIP 对应的组播 MAC 地址输出；若 type 值是 0x17，则代表该数据是下行用户离开节目频道信息，则拉高 leave 信息和 Multi_MAC_Valid 信号，并且将 GIP 对应的组播 MAC 地址输出。

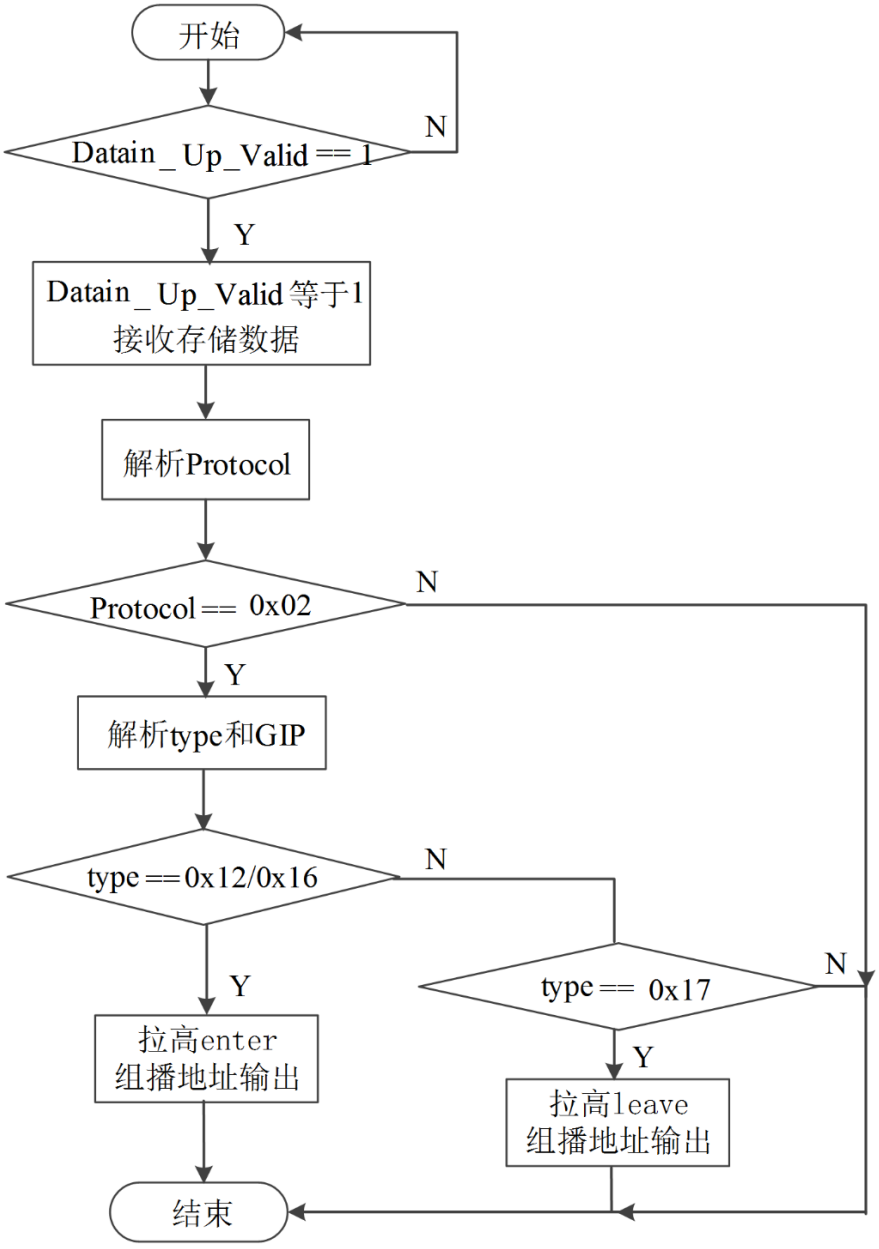

图 5-18 Snooping_Up 模块流程图

Fig.5-18 Flow Chat of Snooping_Up_Block

5.2.4 Data_Transmit 模块设计

1. 模块功能介绍

Data_Transmit 模块的主要功能是根据 Snooping_Up 模块倾听到的用户加入或者离开组播节目频道信息对组播数据进行选择性的转发，只转发下行用户加入的频道数据，

而没有用户加入的节目数据直接丢弃处理，但是对单播、广播数据直接向下行转发不做任何处理。Data_Transmit 模块的接口信号图如图 5-19 所示。

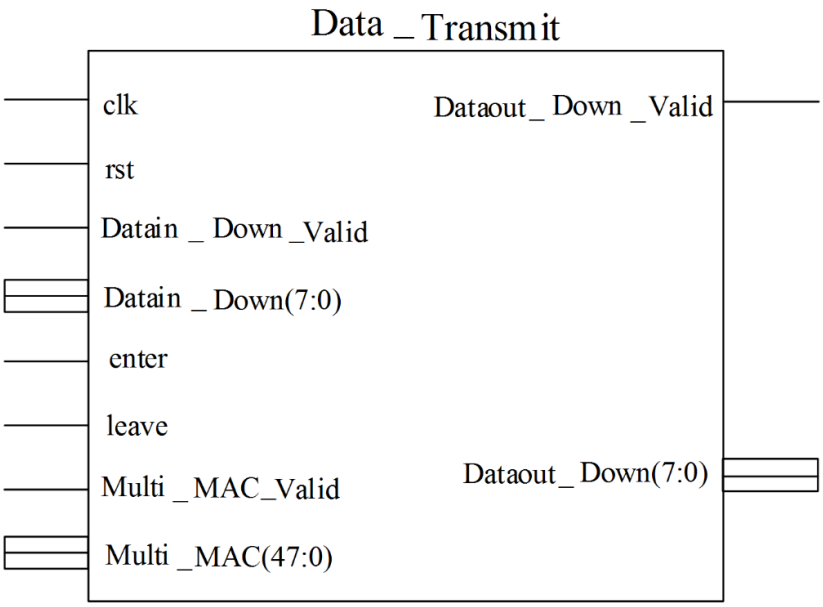

图 5-19 Data_Transmit 模块接口信号图

Fig.5-19 Interface Signal Chart of Data_Transmit

Data_Transmit 模块的信号接口定义如表 5-9 所示。

表 5-9 Data_Transmit 模块信号接口定义

信号名	I/O	功能描述
rst	I	复位信号
clk	I	时钟信号
Datain _ Down _Valid	I	下行数据输入有效信号
Datain _ Down(7:0)	I	下行数据输入信号
enter	O	加入标识信号
leave	O	离开标识信号
Multi _ MAC_Valid	O	组播MAC地址输入有效信号
Multi _MAC(47:0)	O	组播MAC地址输入信号
Dataout_ Down _Valid	O	下行数据输出有效信号
Dataout_ Down(7:0)	O	下行数据输出信号

2. 模块具体设计

Data_Transmit 模块的具体设计流程图如图 5-20 所示。Data_Transmit 模块复位后，模块准备接收来自 Frame_Classify 模块分类出来的普通业务数据帧。当检测到

Datain_Down_Valid 为低电平时，说明有下行数据到来，则模块开始接收并存储数据。解析数据帧中的目的地址 DA 值，如果 DA 的值为组播地址，则判断该组播地址是否存在，如果存在说明有用户申请加入该组播数据，则发送该组播数据帧；如果不存在说明没有用户申请该组播数据，则直接丢弃数据结束。如果 DA 的值不是组播地址，说明该下行数据是广播或者单播数据，则直接将数据向下行用户转发。

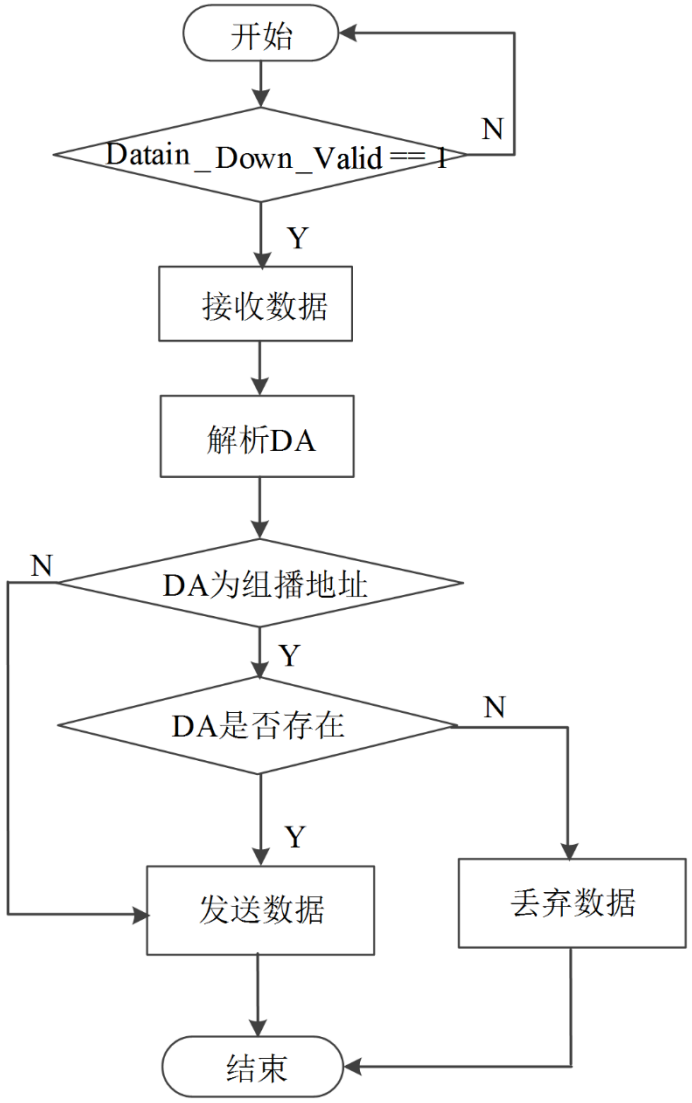

图 5-20 Data_Transmit 模块流程图

Fig.5-20 Flow Chat of Data_Transmit_Block

5.3 本章小结

本章首先简要概述了 OLT 和 ONU 控制端的 FPGA 设计流程，然后详细的给出了 10G EPON 网络系统安全承载多业务下组播 IPTV 业务队列调度方案的 FPGA 硬件设计，包括 OLT 端的 MPCP 控制、Frame 过滤、RS 发送、Proxy_Up 侦听和 OLT 分类调度五个模块，

以及 ONU 端的 RS 接收、MPCP 控制、Snooping_Up 侦听和下行数据传输四个模块，初步实现了硬件设计。

第六章 总结

6.1 本文总结

随着信息技术的不断发展，视频广播、多画面分割、时移窄播、IPTV 等各种新业务的涌现，对接入带宽、系统成本、功耗提出了很大的要求，而当前的主流 10G EPON 无疑被看作是最好的解决方案。

然而 10G EPON 承载这些业务，尤其是用户最为喜爱的 IPTV 业务，需要解决两个方面的问题，一个是 10G EPON 固有的身份安全问题，一个是如何保证当前用户喜爱的 IPTV 业务与其它新业务的带宽合理分配问题。针对这两个问题，本文所做的工作为：

（1）介绍了 10G EPON 网络系统的基本结构和工作原理，以及 MPCP 帧结构和 ONU 的自动发现与注册过程，分析了其点到多点的网络拓扑结构带来的安全威胁，提出了 OLT 和 ONU 双向认证的必要。

（2）提出了一种基于 NTRUSign 的双向认证方案。该方案利用 NTRUsign 签名算法，嵌入到 10G EPON 网络系统的注册过程中，完成了 ONU 和 OLT 的身份验证，并且协商出了会话密钥，可以作为后续 OLT 与 ONU 数据传输的加密密钥。方案中的双向身份认证过程都是基于 ONU 的注册过程，无需再重新设计认证协议。方案的安全性理论分析显示本方案能够抵抗多种安全攻击，同时仿真表明方案对注册效率影响极小。

（3）在 10G EPON 网络系统的双向认证过程中，有 8 个 MPCP 协议帧，其中有三个信息帧是根据 MPCP 通用帧格式自定义的，即认证帧 Certification，信息帧 M_{ONU} 和信息帧 M_{OLT}。

（4）10G EPON 的身份安全保障下，本文研究 10G EPON 承载多业务，首先对一般业务和 IPTV 业务进行单组播划分，然后再对组播 IPTV 进行等级划分，根据 WRR 算法分配带宽。

（5）对上述方案进行了 FPGA 硬件设计，给出了 OLT 端和 ONU 端各个子模块的具体功能介绍和流程图设计。

6.2 工作展望

由于经验不足，本文虽然有了一定的进展，但还有很多地方需要进行完善，下一步的研究工作主要从以下几个方面进行展开：

（1）用于身份验证的NTRUSign签名算法进行参数优化，可以从密钥生成方面进行分析，整体优化算法运算量，从而改善系统延时的影响。另外，可以寻找更为有效和前沿的认证算法来保障身份安全，如当前根据量子技术提出的量子签名技术。

（2）本文设计的基于NTRUSign的10G EPON网络双向身份认证方案只进行了理论分

析和仿真，下一步可以考虑通过软件实现，嵌入到实际运行的设备中去，从而更全面的测试本方案的可行性。

（3）本文只给出了 OLT 和 ONU 的硬件模块设计，并没有在硬件平台上实验。下一步可以使用 verilog 语言进行编程，在平台上进行调试，验证方案的正确性和可靠性。

参考文献

[1] Ling Leng, Lin Wang.The Current Status and Development Prospect of 10G PON Technology [J]. Applied Mechanics and Materials, 2014, 543-547:3431-3434.

[2] Kolotouros D M, Baron S, Soos C, et al. A TTC upgrade proposal using bidirectional 10G-PON FTTH technology [J]. Journal of Instrumentation, 2015, 10:C04001-C04001.

[3]张喜云, 左利钦. 关于三网融合中的FTTH网络设计探讨[J]. 硅谷, 2015(4):157-158.

[4] 庞雪莲. 基于EPON平台的三网融合业务的实现[J]. 数字技术与应用, 2015(7):29-31.

[5] 梁鸿超, 殷爱菡, 陈冬,等. 基于签密算法的EPON认证方案研究[J]. 光通信技术, 2015, 39(4).

[6] Bhaumik P, Reaz A S, Murayama D, et al. IPTV over EPON: Synthetic traffic generation and performance evaluation[J]. Optical Switching & Networking, 2014, 18:180-190.

[7] 徐梅香, 陈亮. 高带宽业务需求下有线宽带提速升级方案研究[J]. 电信工程技术与标准化, 2016(1).

[8] 朱春志. EPON技术的发展与介绍[J]. 中国新通信, 2016(1).

[9] 刁兴玲. 中兴戴驰:10G EPON FTTH将于2017年迎来规模部署[J]. 通信世界, 2015(32).

[10] 陈海霞. 国内外FTTH发展状况[J]. 有线电视技术, 2009, 16(1):26-28.

[11] Transparency Market Research Company.IPTV Market：Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2014-2020. From http://www.transparencymarketresearch.com/

[12] Barz H W, Bassett G A. 11. High-End IPTV [M]// Multimedia Networks: Protocols, Design, and Applications. John Wiley & Sons, Ltd, 2016.

[13]Implementing Next-Generation Passive Optical Network Design with FPGAs [White Papar].//www.altera.com.

[14] 顾建国, 何宁. 《广播电视安全播出管理规定》之IPTV集成播控平台、网络广播电视台实施细则修订解析[J]. 广播与电视技术, 2015, 42(8):48-52.

[15] 鲁义轩. 2016年国内4G用户规模有望破6亿[J]. 通信世界, 2016(1).

[16] Jin, D, Kartalopoulos, SV, Verma, PK. Analysis of Security Vulnerabilities and Countermeasures of Ethernet Passive Optical Network (EPON) [J]. CHINA COMMUNICATIONS, 2007, 4(3):17-29.

[17] Zi-yi Fu, and Li Zong-jie.Study of authentication and encryption scheme in EPON. Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops (*Proc. ISECS*), 2010: 176-178.

[18] Wu W, Gao H. Method, equipment, and system for detecting and authenticating terminal in passive optical network. U.S. Patent 8,406,628[P], 2013.

[19] Kim, Young-Seok, Su-Hyung Kim, and Yun-Je Oh. Authentication method and apparatus in EPON. U.S.Patent.20040179521, 2004.

[20] Chen, Xianghua et al. Encryption and Authentication Mechanism of 10G EPON Systems Based on GCM. *e-Business and Information System Security (EBISS), 2010 2nd International Conference on*. IEEE, 2010: 1-4.

[21] 白松, 雷为民, 林镜华,等. 一种双通道的 IMS-based IPTV 频道快速切换方法[J]. 小型微型计算机系统, 2011, 32(4):713-716.

[22] 魏云峰, 王有先. 转发组播业务的方法和系统、ONU 和 OLT: , CN104378303A[P]. 2015.

[23] 许双朋. EPON 系统互通性研究与实现[D]. 北京邮电大学, 2008.

[24] Lai J R, Chen W P. High utilization dynamic bandwidth allocation algorithm based on sorting report messages with additive-polling thresholds in EPONs [J]. Optical Switching & Networking, 2015, 18:81-95.
[25] Diab W W, Frazier H M. 9. EPON Multipoint Control Protocol [M]// Ethernet in the First Mile: Access for Everyone. John Wiley & Sons, Inc., 2011:271-293.
[26] Marek Hajduczenia, Pedro R. M. Inacio, Henrique J.A. Da Silva et al. ON EPON SECURITY ISSUES. Communications Surveys and Tutorials [J], 2007, 9(1):68-83(2007).
[27] Surhone L M, Timpledon M T, Marseken S F. NTRUSign [M]. Betascript Publishing, 2010.
[28] 朱明. 基于 NTRUSign 算法的双向认证协议研究[D]. 华东交通大学, 2014.
[29] Barz H W, Bassett G A. 11. High-End IPTV [M]// Multimedia Networks: Protocols, Design, and Applications. John Wiley & Sons, Ltd, 2016.
[30] Montpetit M J, Klym N, Mirlacher T. The future of IPTV[J]. Multimedia Tools & Applications, 2011, 53(3):519-532.
[31] Kawamori M. 5. Current Status of the Discussion on IPTV Accessibility Technology at ITU-T(Accessibility for Image Information Media)[J]. Journal of the Institute of Image Information & Television Engineers, 2015, 69.
[32] Hwang I S, Nikoukar A A, Chen K C, et al. QoS Enhancement of Live IPTV Using an Extended Real-Time Streaming Protocol in Ethernet Passive Optical Networks[J]. Journal of Optical Communications & Networking, 2014, 6(8):695-704.
[33] Chang R I, Wei T T, Wang C H. A cost-effective key distribution of P2P IPTV DRM over opportunistic multicast overlay for e-commerce systems[J]. Electronic Commerce Research, 2015, 15(1):49-71.
[34] 钟宇霆, 房靖基, 陈嘉. IPTV 中组播冗余的应用[J]. 广播与电视技术, 2015, 42(1).
[35] 张伟, 张傲, 何岩. EPON 系统中多播技术实现方案[J]. 光通信技术, 2004, 28(6):54-56.
[36] Wang Y. Research on Implementation of IPTV Controllable Multicast Based on 10 G EPON[J]. Video Engineering, 2011.
[37]田绍东. IGMP Snooping 在 IPTV 业务二层设备上的实现研究[J]. 计算机光盘软件与应用, 2014(5):289-289.
[38] Wang J, Sun L, Jiang X, et al. IGMP snooping: a VLAN-based multicast protocol[C]// High Speed Networks and Multimedia Communications 5th IEEE International Conference on. IEEE, 2002:335-340.
[39] 石恒华, 许鑫, 张娜,等. 基于 Packet Tracer 的 VLAN 和 802.1Q 研究[C]// 2011 年亚太信息网络与数字内容安全会议(APCID2011). 2011.
[40] 李海芸, 周文勤. VLAN 间路由的几种解决方案研究[J]. 自动化与仪器仪表, 2015(8).
[41] Paul Ferguson. Simple Differential Services:IP TOS and Precedence, Delay Indication, and Drop Preference[Internet Draft]// http://tools.ietf.org/html/draft-ferguson-delay-drop-02.
[42] Liu Y, Lu G, Zhang W, et al. A DSCP-Based Method of QoS Class Mapping between WLAN and EPS Network[M]// Algorithms and Architectures for Parallel Processing. Springer International Publishing, 2014:204-213.
[43] Passas N. A DIFFSERV-BASED CLASSIFICATION SCHEME FOR INTERNET TRAFFIC OVER WIRELESS LINKS [J]. PCARMD Book Series (Philippines), 2015.
[44] Bouras C, Primpas D, Sevasti A, et al. Enhancing the DiffServ architecture of a simulation environment[J]. Critique of Anthropology, 2015, 35(5):17-59.
[45] Kim Y, Kim C. QoS-Guaranteed DiffServ-Aware-MPLS Traffic Engineering with Controlled Bandwidth Borrowing [M]// Software Engineering Research and Applications. Springer Berlin Heidelberg, 2004:253-265.
[46] Frankel S. Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec [J]. Information on Rfc, 2007.

[47] Peng Z W, Radcliffe P J. Study on Dynamic Bandwidth Allocation Algorithms Based on EPON [J]. Advanced Materials Research, 2012, 433-440:5243-5249.
[48] M. Hajduczenia, H. J. A da Silva. Discovery process for emerging 10 Gb/s EPONs. IEEE Communication Magazine, 2008(11): 82-90.
[49] S. Bhatia, R. Bartos. Closed-form expression for the collision probability in the IEEE EPON registration scheme. Journal of Optical Networks.,2006,5(1):1-14.
[50] Bhaumik P, Reaz A S, Murayama D, et al. IPTV over EPON: Synthetic traffic generation and performance evaluation[J]. Optical Switching & Networking, 2014, 18:180-190.
[51] 闫飞燕, 张丽娟. IPTV 系统中的 QoS 性能优化[J]. 电视技术, 2015, 39(z1).
[52] Zhang G, Xuepeng F U, She F, et al. Analysis on IPTV Video Transmission Quality[J]. Radio & Tv Broadcast Engineering, 2014.
[53] 野田,翔, 山岡,克式. WRR Weight Distribution Method to Maximize the Number of Processing Packets in Allowable Delay[J]. 电子情报通信学会技术研究報告 = IEICE technical report : 信学技报, 2015, 114:179-184.
[54] Choi J K, Sang G J, Kwon Y H, et al. A Weighted Scheduling Mechanism to Reduce Multicast Packet Loss in IPTV Service over EPON[J]. Etri Journal, 2009, 31(4):469-471.
[55] 石鹏程, 周昭荣. 组播技术在 EPON 系统中的应用[J]. 电信科学, 2007, 23(10):92-95.

个人简历　在读期间发表的学术论文

个人简历：

丁以胜，男，1989 年 2 月生。

2013 年 7 月毕业于安徽滁州学院电子信息工程专业，获学士学位。

2013 年 9 月入华东交通大学就读硕士研究生。

已发表论文：

[1] Yin A, Ding Y. Design of a mutual authentication based on NTRUsign with a perturbation and inherent multipoint control protocol frames in an Ethernet-based passive optical network [J]. Optical Engineering, 2014, 53(11):115101-115101.（SCI 收录）.

[2] Yin A, Ding Y, Xiong L. Design and analysis of a photonic crystal fiber with four-hole unit [J]. Optik - International Journal for Light and Electron Optics, 2014, 125(23):7068-7071.（SCI 收录）.

[3] Yin A, Chen D, Ding Y. An efficient and secure authentication scheme based on NTRU for 10G ethernet passive optical [J]. Optik - International Journal for Light and Electron Optics, 2014, 125(24):7207-7210.（SCI 收录）.

[4] Yin A, Ding Y. A novel dynamic multi-service multi-grade encryption scheme used in EPON [J]. Optik - International Journal for Light and Electron Optics, 2015, 126(21):2809-2813 (SCI 收录).

致谢

首先需要感谢我的导师，感谢殷老师这三年来一直对我的指导和关怀，让我从一个什么都不懂的少年慢慢变得成熟懂事！

时间过的飞快，转眼在华东交通大学的三年研究生生活就要结束了，在这三年当中，我从一个知识面泛泛的本科生进行了一次次蜕变，专业技能和专业知识得到很大提高，学习也更精细、更有深度，对我今后的生活产生莫大的裨益。而这一切，都是源自于我的老师的谆谆教诲，让我铭记于心。在科研上，老师对我们要求严厉，说话直言不讳，直截了当的告诉我们错在哪里，应该做什么，不该做什么，指导我们快速的进入科研状态，紧紧的把握在校的科研时间点，让我们从不落后于其他同学;在学业上,老师严肃而不刻板,指导我们学习要讲究方法，灵活而不偷懒；在平时的生活中，老师是我们的长辈，时刻告诫我们要团结实验室的师兄弟，能敏锐的察觉我们的情绪波动，与我们进行心对心的交谈，并且定期组织我们户外活动，促进同学之间的关系。在这临近毕业之际，我要衷心的祝愿老师身体健康，天天开心，工作顺利！

我还要感谢实验室的各位小伙伴,感谢陪伴我一起走过三年研究生生活的李强、梁洪超、陈冬，因为有你们，我的生活才变得更加丰富多彩；其次要感谢实验室的师兄朱明、郭建伟和王胜凯，我之所以能获得现在的一点成绩，很大程度上要感谢你们细心的辅导，你们的铺垫才成就了现在的我们；再感谢实验室的师弟们，祝你们科研有成，能够出更多的成果，为实验室增光添彩。

在此还要谢谢我的父母，感谢你们多年来对我的培养和支持，在我生命的十字路口上你们都一直尊重我的选择，一直都是引导，而不是强加干涉。我的父亲母亲，祝福你们身体健康，生活开心。

最后衷心感谢对论文进行评审的各位老师们，你们辛苦了，感谢你们。