

A Multicast IPTV Bandwidth Saving Method

Mohamed Moughit
National School of Applied
Sciences, Univ Hassan I, IR2M
Laboratory, Khouribga, Morocco

Abdelmajid Badri
LEEATI Laboratory FSTM,
Mohammedia Univ Hassan II
Mohammedia Morocco

Aicha Sahel
LEEATI Laboratory FSTM
Mohammedia Univ Hassan II
Mohammedia Morocco

ABSTRACT

IPTV services delivered traditional television channels via IP to customers. IGMP protocol is the control mechanism used to control the delivery of multicast traffic to interested and authorized users. IGMP commands notify the upstream equipment to stop sending (“leave”) one channel or begin sending (“join”) another channel. Depending on the architectural choices, this process occurs in the DSLAM, an aggregation switch, or at an edge router. All channels are sent by a multicast source to DSLAM even if no user in the DSLAM has requested it. This leads to sub-optimal use of bandwidth.

This paper studies and investigates the performance of IPTV controlled by CGMP Protocol to save bandwidth using OPNET package. It shows that when CGMP is enabled on edge routers and switches, hosts receive only the channels demanded and therefore the bandwidth is optimized and also the queuing delay is reduced.

Keywords:

IPTV, PIM-SM, IGMP, CGMP, Bandwidth, Simulation, OPNET.

1. INTRODUCTION

The growth of high speed Internet and the development of terminal devices capable of playing multimedia had lead to a fast development of multimedia services. Internet Protocol Television (IPTV) is such an example. This service grows fast in recent years. According to Frost & Sullivan's report in 2009, there were about 40 million users at the end of 2009, and about 140 million in 2012[8].

ITU-T defines IPTV as multimedia services (TV, video, audio, text, graphics, data ...) delivered on a broadband network using the IP protocol. In IPTV system, TV programs are first collected from video sources, compressed, converted to IP packets through IP streaming and delivered through IP networks[1,3]. IPTV utilizes the reachability and high transmission efficiency of IP networks to provide the required level of quality of service, security, interactivity and reliability.

In an IPTV network, each broadcast television channel is an IP multicast group[3]. The subscriber changes the channel by LEAVE-ing one group and JOINing a different group using IGMP (Internet Group Management Protocol) protocol[1]. All channels are delivered to the DSLAM (Digital Subscriber Line Access Multiplexer) by IPTV head-end even if no one

requests it[10]. As IPTV requires large bandwidth (typically 4 Mbps per channel [8]) and bandwidth is limited, lot of papers proposes to compress multimedia data before their transmissions. In this case, source coding methods for Multimedia Data are widely used[5]. This paper shows that if IPTV channels are forwarded only to those subscribers currently viewing them, a great amount of bandwidth will be saved. Thus, it proposes the protocol CGMP as a smart solution to control and motorizes traffic sent by the head-end. In fact, CGMP works in conjunction with IGMP messages to dynamically configure switch ports so that IP multicast traffic is forwarded only to those ports associated with IP multicast hosts.

OPNET [16] Simulator is used to show amount of bandwidth saved when CGMP is implemented.

2. IPTV COMPONENTS

2.1 IPTV Hardware

IPTV service refers to television service deployed on the broadband network. It provides programs and information, such as broadcasting, video on demand, etc. IPTV service provides to users a high quality video and audio in WEB mode under operating modes of traditional televisions.

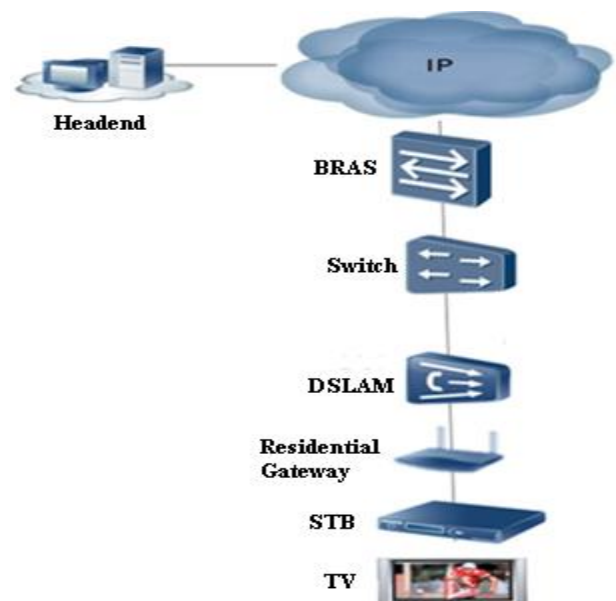


Figure 1: IPTV Equipments

The network architecture [10] offering IPTV service is illustrated in Figure 1. There are up to four network elements involved: The set-top box (STB), the routing gateway (RG),

DSLAM, the Broadband Remote Access Server (BSR), an aggregation switch and the Head-end.

2.1.1 Head-end

The IPTV head-end is where content such as television channels or Video on Demand movies is received and prepared for transmission in multicast across the operator's private IP network.

2.1.2 BRAS

The BRAS (Broadband Remote Access Server) is the aggregation point for the subscriber traffic. It also authenticates the subscriber's credentials, validates the users access policies, controls the QoS, assigns IP address and routes channels and queries to its respective destinations.

2.1.3 DSLAM

The DSLAM is the first convergence point in the network where subscribers of a specific area terminate. It aggregates traffic from multiple subscribers. BRAS and DSLAMs may be connected directly through a SDH or PDH based fiber optic transmission network or via an aggregation switch, while subscribers are connected to the DSLAM through copper cables. There are three categories of DSLAM:

- Layer 2 DSLAMs primarily convert xDSL to Ethernet (or ATM), providing little additional function. This type of DSLAM is essentially a Layer 2 switch, with some relevant enhancements. Layer 2 DSLAMs cannot interpret IGMP, so they cannot selectively replicate IPTV channels.
- IP-aware DSLAMs understand and can respond to IGMP traffic. To support IPTV applications, these DSLAMs interpret IGMP requests and replicate channels based on received requests
- IP DSLAMs add extensive IP intelligence, possibly including IP routing and advanced queuing based on DiffServ markings.

2.1.4 STB

STB (Set Top Box) is the end host used to receive IPTV video. The main function of STB is to receive multimedia streams from IP network, and decode, to transfer to the televisions, and to make users to be able to enjoy IPTV service.

2.1.5 RP

An RP (Rendezvous Point) is a router that has been configured to be used as the root of the non-source-specific distribution tree for a multicast group. Join messages from receivers for a group are sent towards the RP, and data from senders is sent to the RP so that receivers can discover who the senders are and start to receive traffic destined for the group.

2.2 IPTV Protocols

2.2.1 IP Multicast system

Multicast is the delivery of data to a group of destination host simultaneously in a single transmission from the source. It scales to a larger receiver population by not requiring prior knowledge of who or how many receivers there are. Multicasting has two major benefits compared to unicasting in one-to-many and many-to-many applications. It reduces the bandwidth that is required by the application and it reduces the load on the sending server. Thus, it's widely used in IPTV transmission [1,4].

2.2.2 PIM Protocol

PIM (Protocol Independent Multicast) is a multicast routing protocol for delivery multicast in a routed environment. It's widely used in multicast routing. It has a major role in constructing a distribution tree to forward multicast packets. The basic approaches in most multicast protocols for building distribution trees are Sparse Mode (SM) and Dense Mode (DM) [1].

PIM-SM is a multicast routing protocol that can use the underlying unicast routing information base or a separate multicast routing information base. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) per group, and optionally creates shortest path trees per source.

PIM-DM is a multicast routing protocol that uses the underlying unicast routing information base to flood multicast datagrams to all multicast routers. Prune messages are used to prevent future messages from propagating to routers without group membership information.

2.2.3 IGMP Protocol

IGMP is the control mechanism used to control the delivery of multicast traffic to interested and authorized users [2].

Basic IGMP operation involves two devices:

IGMP host which issues messages to join or leave a multicast group.

IGMP router, which responds to the join and leave messages to determine if multicast groups should be forwarded out an interface.

IGMP provides three basic functions for IP multicast networks [4]:

JOIN: An IGMP host indicates that it wants to receive information from ("become a member of") a multicast group.

LEAVE: An IGMP host indicates that it no longer wishes to receive information from a multicast group.

QUERY: An IGMP router can ask the hosts which groups they are members of. This is done to verify a JOIN/LEAVE request or to look for error conditions.

2.2.4 IGMP Snooping

IGMP Snooping is a multicast control mechanism that operates in Layer 2 [13]. It assigns Layer 3 capabilities to a switch. Indeed, the switch with this feature analyzes all IGMP traffic between the hosts and the multicast router and performs different operations depending on the type of traffic. If the message is "host membership report to the multicast router", the switch will add to his list the multicast port number of the host. Therefore, multicast traffic will be sent only to this host and not to all hosts attached to the switch. This allows a bandwidth saving in networks equipped with multicast groups.

The snooping agent can stop sending multicast traffic when a leave is received. The snooping agent must also keep some state regarding general "Membership Query Maximum Response Time" timers in the event a LEAVE message is not issued from an IGMP client.

2.2.5 CGMP protocol

CGMP (Cisco Group Management Protocol) is a Cisco developed group management protocol that limits the forwarding of IP multicast packets to only those ports associated with IP multicast clients [13]. CGMP works in conjunction with IGMP messages to dynamically configure Cisco Catalyst switch ports so that IP multicast traffic is forwarded only to those ports associated with IP multicast hosts. Thus, it saves network bandwidth on user segments by not propagating unnecessary IP multicast traffic.

3. IPTV OPNET SIMULATION

OPNET (Optimized Network Engineering Tools) [14] is a discrete event simulation tool, which provides a comprehensive development environment supporting the modeling and simulation of communication networks and which contains data collection and data analysis utilities. OPNET allows a various numbers of closely spaced events in a sizeable network to be represented accurately. It uses a modeling approach where networks are built of nodes interconnected by links. Each node's behavior is characterized by the constituent components and these components are modeled as a state-transition diagram

OPNET Simulator is used to compare bandwidth utilization when CGMP protocol is activated on switches.

The simulation model for the IPTV is illustrated in Figure 2.

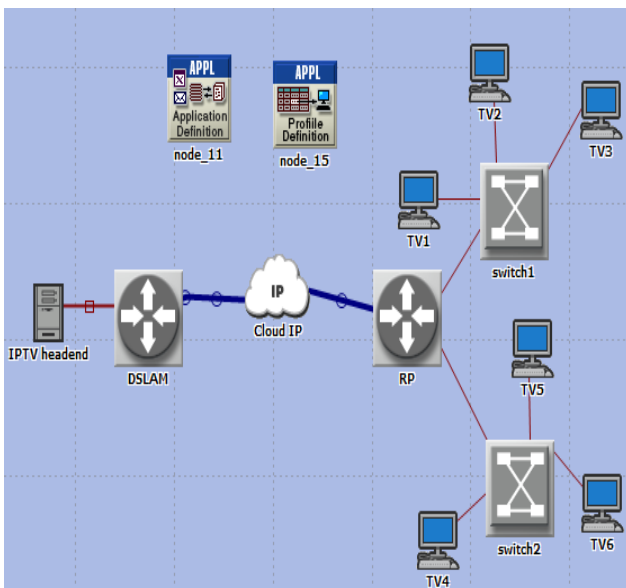


Figure 2 : IPTV model

Application definition contains three application types: FTP Application, video1_multicast and video2_multicast.

Video1_application modeled a TV channel with a resolution of 300x240 pixel transmitted at the rate of 30 frames per second while video2_application modeled a TV channel with a resolution of 128x240 pixels at frame rate 15frames per second.

In the profile definition, three profiles are defined: profil FTP, profil_video1 and profil_video2. Figure 3 shows the detail of IPTV profile definition. Profil_video1 and profil_video2 are attributed to the IPTV head-end only.

Two multicast group are defined: one group with 224.233.24.231 as multicast address associated to video1_application. The second group has 224.233.24.232 as multicast address associated to video2_application.

As protocol PIM-SM consumes less bandwidth, resulting in lower link occupancy rate [15], it is enabled on DSLAM and RP (figure 4) to perform IPTV bandwidth save.

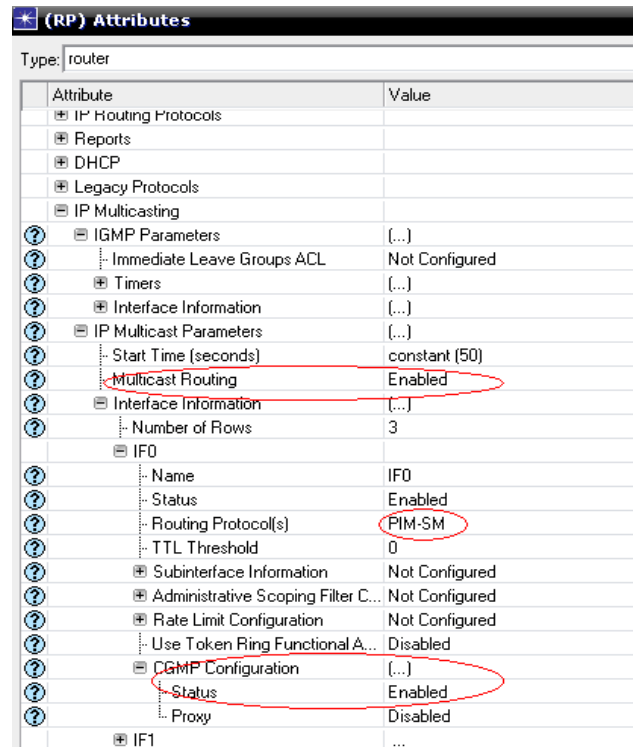


Figure 4 :RP Configuration

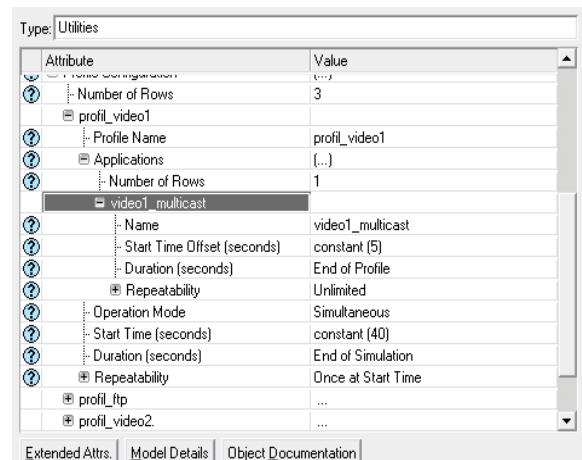


Figure 3: IPTV Profil definition

4. RESULTS AND DISCUSSIONS

4.1 Scenario 1: CGMP is not activated on RP

Before enabling CGMP on Rendezvous Point (RP), the Switch distributes multicast traffic to all member of multicast group connected to the switch even if there's no demand from these hosts. In this scenario TV1 demand video1_application. But we note that TV2 receive also this traffic (figure 5).

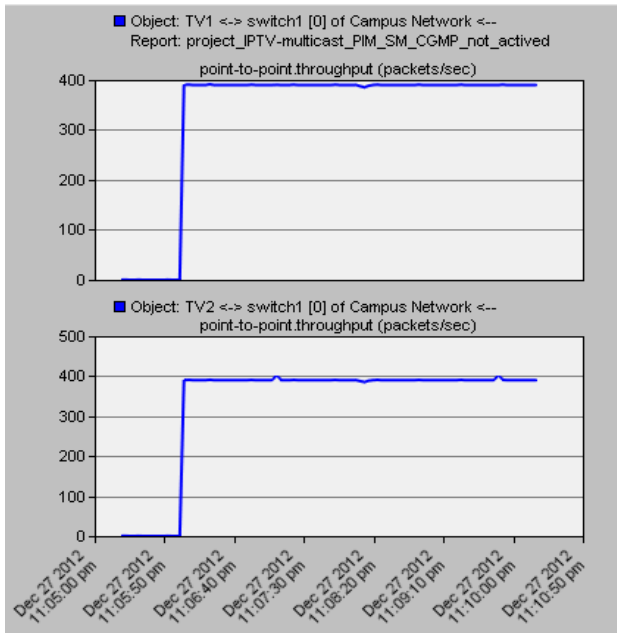


Figure5: Received traffic by hosts, CGGP not activated

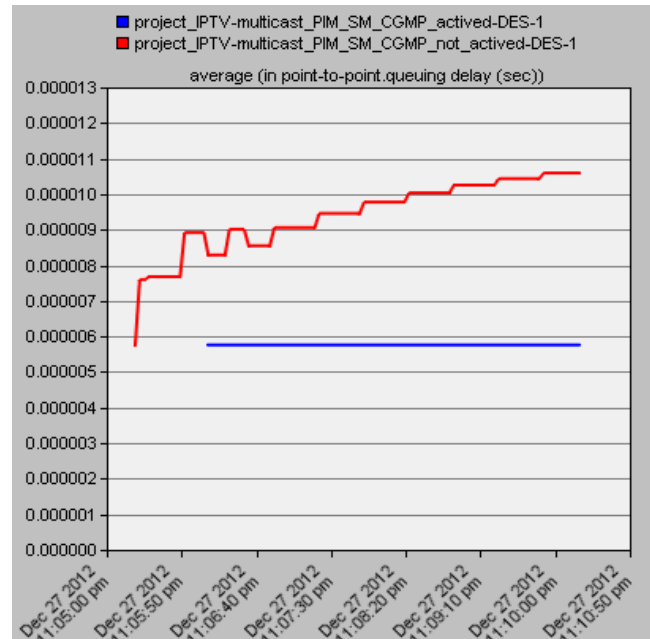


Figure7: Queuing delay

4.2 Scenario 2: CGMP is activated on RP

In this case, only TV1 receives traffic as if it is unicast transmission. The figure 6 shows that TV2 receives any traffic even if it belongs to the same group as the host TV1.

Also, the queuing delay becomes constant and very small compared to the case where the CGMP isn't enabled on the RP (Figure 7).

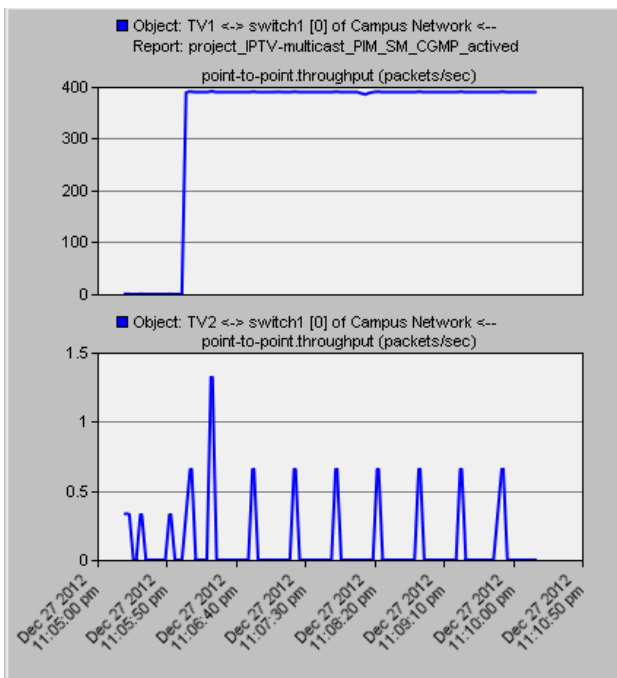


Figure6: Received traffic by hosts, CGGP activated

5- Conclusion

IPTV service delivers digital video using an IP network infrastructure. IP multicast protocols and IGMP protocols are used to enable efficient distribution of video streams to a large population. A critical factor in multicasting is bandwidth efficiency in the transport network. In fact, channels may be delivered to all STB connected to the DSLAM even if they don't demand any channel. To overcome this problem, the present paper has proposed to deploy layer 2 switches and edge routers with CGMP protocol in order to avoid flooding multicasts to all switchports and therefore save bandwidth and minimize transmission delay to permit the telecom operators to provide more channels to customers with high quality.

6- REFERENCES

- [1] Daniel Minoli by John Wiley & Sons, IP MULTICAST WITH APPLICATIONS TO IPTV AND MOBILE DVB-H, 2008
- [2] Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service Layer Requirements to integrate NGN Services and IPTV Doc. Nb. TS 181 016 Ver. 3.3.1 Ref. RTS/TISPAN-01059-NGN-R3, ITU-T, 2009
- [4] Scott Shoaf, Marc Bernstein (2006) Introduction to IGMP for IPTV Networks, Juniper Networks, Inc.
- [5] Abhik Majumdar, Daniel Grobe Sachs, "Multicast and Unicast Real-Time Video Streaming Over Wireless LANs", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 12, NO. 6, JUNE 2002
- [6] Ibrahim Khider, Salah Elfaki, MOHAMED ELHASSAN, MONA SIDDIQ, "Evaluate the performance of Internet Protocol Television", Electrical and Control Engineering (ICECE), 2011 International Conference.

- [7] Sibel Malko, ErdemUçar and Rafet Akdeniz “Improving QoE in multicast IPTV systems: Channel zapping times”, *Scientific Research and Essays Vol. 7(35)*, pp. 3107-3113, 6 September, 2012
- [8] Huawei Technologies Co., Ltd.(2010), Technical White Paper for HDTV Bearer Networks
- [9] Johan Hjelm, “Why IPTV? Interactivity, Technologies and Services”, A John Wiley and Sons, Ltd, Publication (2008)
- [10] Shahbaz Rahmanian, Huawei , December, 2008 , IPTV Network Infrastructure
- [11] Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem Architecture Doc. Nb. TS 182 028 Ver. 3.3.1 Ref. RTS/TISPAN-02074-NGNR3, ITU-T, 2009
- [12] Zhang J, Wang Y, Rong B (2009). QoS/QoE Techniques for IPTV Transmissions. *IEEE Int. Symp. on Broadband Multimedia Sys.* pp. 1-6.
- [13] Power Connect Application Note #18 February 2004DELL “Understanding IGMP Snooping”
- [14] Computer Networks A system Approach, Larry L.Peterson and Bruce S.Davie, April 2003
- [15] Libing Wu, Shengchao Ding, Chanle Wu, Dan Wu, Bo Chen “The Research and Emulation on PIM-SM” *Protocol High Performance Computing and Applications Lecture Notes in Computer Science Volume 5938*, 2010, pp 465-472
- [16] OPNET Users' Manual, OPNET Architecture, OV.415.<http://forums.opnet.com>