JPPI Vol 10 No 1 (2020) 59 - 72

Jurnal Penelitian Pos dan Informatika

32a/E/KPT/2017

e-ISSN 2476-9266
p-ISSN: 2088-9402

Doi:10.17933/jppi.2020.100105

Development of Multicast Service Standardization Regulation for the XG-PON OLT Equipment

Pengembangan Regulasi Standarisasi Layanan Multicast untuk Perangkat OLT XG-PON

Nomarhinta Solihah[1], Muhammad Imam Nashiruddin[2]

Infrastructure Assurance, Digital Business Directorate, PT. Telekomunikasi Indonesia, Bandung, 40113, Indonesia[1]
Center for Regulation & Management of Telecommunication, School of Electrical Engineering, Telkom University
Bandung, 40257, Indonesia[2]

rhinta@telkom.co.id[1]

Received: 3 March 2019; Received in revised from: 27 August 2020; Accepted: 3 September 2020

Abstract

The deployment of Fiber-To-The-x (FTTx) technology is developing rapidly in various regions of Indonesia. One of the most implemented technologies is the XG-Passive Optical Network (XG-PON). It offers high-speed internet access of 10 Gbps downstream/upstream directions and is able to pass numerous services at once, such as data, voice, to video multicast (IPTV) services. However, the technical requirements standardization regulation for multicast services in Indonesia does not include this new technology. Therefore, a reference test must be done to update the current regulation. In this study, the testing of Optical Line Termination (OLT) devices is conducted by using five kinds of scenarios; the ability to pass IGMP version 2, then followed by passing IGMP version 3, afterward to assist IGMP Snooping, subsequently supporting the IGMP proxy, and lastly the capacity in moving several IGMP multicasts groups. The test results indicate that the tested OLT XG-PON device shows suitability between IGMP message format version 2 with the RFC 2236 standard and IGMP version 3 with the RFC 3376 Standard. Whereas in IGMP proxy testing traffic, the IP address source of the OLT equipment is 0.0.0.0, which complies with the RFC 4541 standard for the Reporting proxy process. The OLT XG-PON device tested was also capable of passing 1,024 IGMP multicast groups within the addresses range from 239.1.1.1 to 239.1.5.1.

Keywords: multicast service, XG-PON, OLT, standardization regulation, telecommunication management
.

INTRODUCTION

Nowadays, people use various broadband services to support their daily activities. One aspect of supporting broadband services in providing ease of use is the internet. As part of a broadband infrastructure network, the internet can pass on multiple services such as data, voice, and video. The global internet growth trend is the key to digital transformation with increased internet users, interconnected devices, broadband service speeds, and video service users.

Based on We Are Social and Hootsuite, internet users had reached 4.388 billion globally in 2019. As a big country with a large population, Indonesia contributes 150 million internet usage (We Are Social and Hootsuite, 2019). It becomes the main driving force for Indonesian telecommunications providers to offer triple-play services on broadband infrastructure, including Passive Optical Network (PON).

Optical network technologies, such as PON, offer various advantages such as high throughput, flexibility, scalability, and energy efficiency (Dalamagkas et al., 2018). PON represents the optical distribution network (ODN) between the Optical Line Termination (OLT) and the Optical Network Unit (ONU). PON does not contain active electronic devices but instead uses an optical connector and splitter to direct individual wavelength signals to end-users (Huszaník et al., 2018). One PON technology that promises to provide quality service for its users is the 10-gigabit-capable PON (XG-PON) technology.

In the past decade, a large number of telecommunication operators had implemented fiber-to-the-x (FTTx) technology. Especially in large cities, where fiber is taken directly to end-users such as Fiber To The Home (FTTH) or very close to users like in Fiber to The Neighborhood/Curb (FTTN/C), which then ends with a cable (Hernandez et al., 2019).

The International Telecommunication Union (ITU) has presented recommendations for XG-PON standardization in 2010, by offering 10 Gbps downstream and 2.5 Gbps upstream. As an enhancement to GPON, XG-PON inherits the framing and management from GPON. XG-PON provides full-service operations four times higher and twice as large to support PON network structures (Batagelj et al., 2012).

XG-PON channels a variety of packet-based services with high-quality service and bit-rate capabilities. Some services that can be distributed by XG-PON include voice services such as VoIP and POTS, video services such as Internet Protocol Television (IPTV) and Digital TV broadcasting, and data services such as high-speed internet access. IPTV, which is one of the benefits of XG-PON, continues to grow from year to year. Based on a study conducted by Research and Markets (Research and Markets, 2019), the global IPTV service market is expected to grow at a CAGR of around 15% during 2019-2024. It has become a driving factor for IPTV service providers who use XG-PON technology, especially in Indonesia, to maintain the quality of video services that served to customers.

In terms of standardization regulations, the Indonesian government has regulates the technical requirements of PON based telecommunication tool and device access with Regulation of Director General of Posts and Telecommunications Number 257/DIRJEN/2008 (Department of Communications and Informatics, 2008). However, PON technology, which is the scope of this regulation, is still limited to G-PON and E-PON. This regulation governs various technical aspects, such as electrical requirements, performance, network management systems, and EMC. For video services distributed by PON technology, restriction is made by the government by expecting the device to carry at least 256 multicast groups and run well on each ODN interface.

With the increase of the internet, especially IPTV, the multicast service regulations on PON devices should be updated. Thus, this study comes as a reference for regulators and service providers when determining the ability of XG-PON OLT multicast service. Furthermore, this study's testing technique can be used as a reference in applying equipment certification conducted by telecommunication testing institutions in Indonesia.

This study is done to develop two previous studies relating to multicast service. A research conducted by Mamun and Motalab (2011) has made observations with various audio and video file compression techniques. The only lacking of this research is that it is conducted on a laboratory scale and mostly on the router side. The result showed a detailed packet through the IPTV lab, such as User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), Protocol-Independent Multicast (PIM), and the Cisco Group Management Protocol (CGMP) (Mamun & Motalab, 2011).

Other studies were also conducted (Khider et al., 2011), which has analyzed the performance of the simulation results of IPTV services. However, it is limited to the Digital Subscriber Line (DSL) network and only examined the packets sent and received. Khider et al., (2011) analyze the traffic rate of the IPTV model simulation. The result indicates that over 150 packets were sent in one second, though there was a packet delay; otherwise, it freezes or makes the system slow.

Therefore, to extend the previous research above, this study presents a testing scenario and analysis of IPTV multicast services' ability and performance on the XG-PON network both on a laboratory and operational scale. Several methods tested in OLT XG-PON multicast service are IGMP version 2 and 3, IGMP Snooping, IGMP proxy, static IGMP, IGMP fast leave, and the number of 1024 IGMP multicast groups

OLT XG-PON

XG-PON is a development from the previous technology, namely G-PON, by adopting GPON point-to-multipoint network architecture and being able to support various access such as fiber to the home (FTTH), fiber to the cell (FTTCell), fiber to the building (FTTB), fiber to the curb (FTTCurb), and fiber to the cabinet (FTTCabinet). XG-PON was recommended by ITU in G.987 in 2010 using the Time-Division Multiplexing (TDM) method for the downstream direction and the Time Division Multiple Access (TDMA) for the upstream direction to increase the speed of data in XG-PON. Furthermore, one of the advantages of XG-PON compared to G-PON is improved security capability.

In XG-PON, the PON system needs to support robust reciprocation authentication options to protect the integrity of PON management messages and PON encryption keys (Effenberger, 2011). Every PON technology, including XG-PON, has a typical network structure consisting of three critical components, namely Optical Line Termination (OLT), Optical Network Terminal (ONT), and

Optical Distribution Network (ODN). In its architecture, OLT is placed in the Central Office (CO), connected to the Optical Network Terminal (ONT) via PON with fiber cables, splitters, and other passive components.

Based on ITU-T G.987 as shown in Figure 1, OLT is a network element in an optical access network based on ODN that terminates the root of at least one ODN (downlink) and provides an interface to the service node (uplink). The primary function of OLT is to control information that crosses ODN to various ONTs. OLT also converts electrical signals originating from service provider devices to optical fiber signals and frames supported by the PON system (Gupta et al., 2018). Moreover, OLT has the management and maintenance functions for ODN and ONT. The OLT is compulsory to deliver voice, data, and video services from service providers to customers with high-speed access.

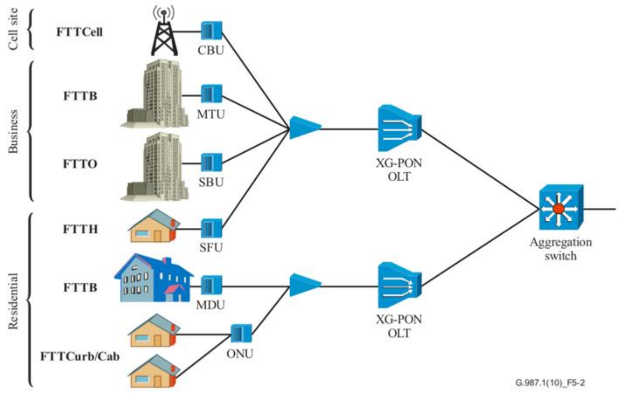


Figure 1. XG-PON Network Scenarios
Source: (International Telecommunication Union, 2016)

Internet Protocol Television (IPTV)

IPTV is a technology in which digital television services such as channels and video programs are sent to television devices or smartphones via a broadband connection, rather than sent via conventional cable or broadcast settings. The IPTV delivers similar content as broadcast or cable TV, consisting of a vast number of live channels (pre-recorded videos or shows can be provided too), on a privately owned and operated network (Al-zoubi et al., 2016). Most of the IPTV service providers are large telecommunications service providers that already have their network infrastructure (Sardju, 2016).

Users can watch internet TV on a computer screen, a television screen (with the set-top box installed), or mobile devices such as smartphones or tablets. The video stream is encoded as a series of the internet protocol packet, and these packets travel through the public internet that are received by any user who has a set-top box (STB) and subscribes to the service (Vasanthi & Chidambaram, 2014).

IPTV uses several protocols to deliver services to customers. Hypertext Transfer Protocol (HTTP) used in the Web Browser. Real-time Streaming Protocol (RSTP) is used to transmit Video on Demand services, and Internet Group Management Protocol (IGMP), which is used to connect the television with multicast TV programs.

The work process of IPTV on optical networks can be divided into three processes, namely the process of IPTV service providers, the distribution process, and the process of service users. IPTV service providers store video content that will distribute to customers on IPTV video servers. Video content such as live broadcasts is broadcast in real-time, whereas previously recorded programs and film videos need to store in such a way that they can be selected and streamed on-demand.

Also, there is a Head End where content such as television channels or Video on Demand is received and prepared for transmission in multicast throughout the operator's private Internet Protocol (IP) network (Moughit et al., 2013). In this section, the video content goes through the encoding process before finally being transmitted to the IP network. The method of transmitting IPTV services through optical media has the advantage of carrying thousands of audio and video streams for long-distance services. There is a set-top box that functions to receive streaming video from the network and decode it on the service user side. Set-top box software works as middleware by performing many operations on the set-top box.

This software also manages various details, such as determining the channel packet the user can access, customer details, and providing Video on Demand (VOD). Also, there is an Electronic Program Guide (EPG) which provides presentations to service users to enable users to view programs and navigate within the subscription channel.

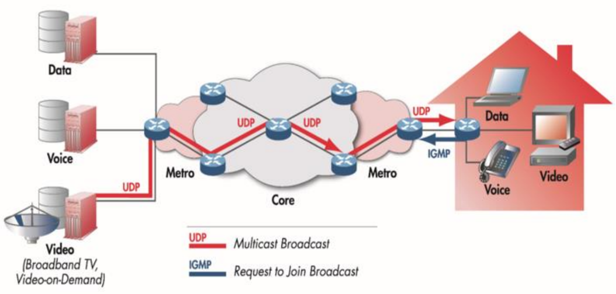


Figure 2. IPTV Broadcast Information Flow
Source: (IXIA, 2017)

IPTV supports television broadcast services with multicast delivery techniques and VOD with unicast delivery techniques. The multicast delivery technique on IP networks is a one-to-many service model that sends video content to many users simultaneously, like television broadcasts, as shown in Figure 2. In contrast, the unicast technique is a one-to-one service model that addresses video content specifically for every use. Physical and Link layers should have the capability for multicasting to support the IP multicasting.

Multicast Services

One service model on IPTV uses the multicast technique. Multicast is a technique of sending data from a source to a group of destination hosts simultaneously in one transmission. This delivery is carried out to a larger recipient population-scale without requiring prior knowledge of who or how many recipients there are (Moughit et al., 2013). All customers receive the same signal at the same time.

IP multicast works by utilizing service users while receiving data packets with specific IP addresses used explicitly for multicasting purposes. To receive multicast packets from specific servers, the receiving device instructs the Ethernet Card to accept the packet with that particular IP address. The Internet Engineering Task Force (IETF) has established an IP addressing scheme for multicasting in Class D with a range of addresses from 224.0.0.0 to 239.255.255.255.

Multicast has two main benefits: efficient use of network bandwidth and reducing the sender's traffic burden since it only sends one information to a multicast group. The bandwidth distributed by the server using the multicast method shows significant bandwidth savings compared to the unicast method (Ridwan et al., 2019). Routing in multicast uses unique methods, namely dense mode, and sparse mode. Dense mode floods all network branches with multicast data packets. The dense mode distance is limited by the TTL (Time to Live) of the data packet. The sparse mode is used by applications whose data receivers are geographically spread out in many areas to not cause congestion on the network (Anwar & Chamid, 2018).

A multicast group is a set of service users, both queries and hosts, with appropriate group membership criteria, or a set of group-owned rules that allow multicast-based services and applications. To form multicast groups, hosts and routers on IPv4 networks use the Internet Group Management Protocol (IGMP).

ITU-T G.987.1 defines the requirements for multicast services, as shown in Figure 3. Figure 3 shows the service logic that is usually provided with the User-Network Interface on an Ethernet network. The multicast signaling interaction on XG-PON refers to IETF IGMP, version 2, or 3 for IPv4 and MLDPv2 for IPv6. Multicast service management consists of the feasibility of the User-Network Interface (UNI) for receiving multicast traffic, XG-PON ports containing multicast, and interconnection traffic is defined in ITU-T G.988.

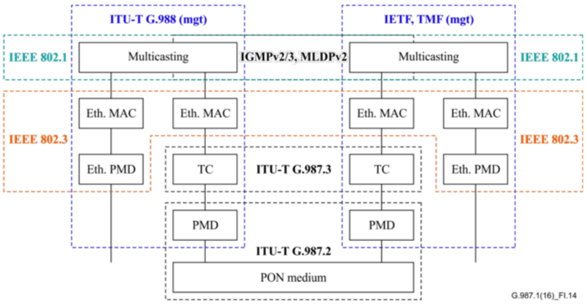


Figure 3. Multicast Services Configuration
Source: (ITU-T G.987.1, 2016)

For layer 2 devices such as OLT, the primary measure of IP multicast scalability is group capacity or the number of IGMP protocols traced by that device. ITU-T does not define IP multicast scalability capabilities that must be fulfilled by OLT devices. However, of the four OLT brands, namely Nokia, Fiberhome, Huawei, and ZTE, it has 1024 IGMP IPv4 multicast group capabilities.

METHODS

This research is conducted by using a quantitative data approach through optical device testing laboratory testing at Telkom DDS Bandung. The object of research is the OLT XG-PON device. The card tested was the XG-PON service card only, considering that this study would solely focus on the XG-PON technology capabilities. The flow of this research is presented in Figure 4.

Quantitative data collection is done by designing the test scenario, carrying out the testing process, and collecting traffic and packet data. Tests are carried out on several multicast service specifications such as IGMP version, IGMP Snooping, IGMP proxy, and IGMP multicast group. The capability measurements of the IGMP version, IGMP snooping, and IGMP proxy are conducted using live IPTV traffic. At the same time, the IGMP Multicast Group is tested using a traffic generator and analyzer.

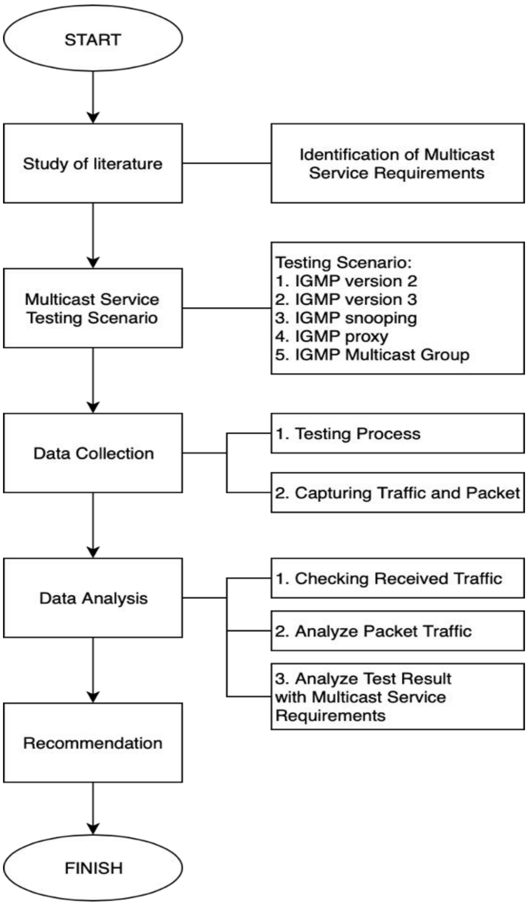

START
Study of literature
Identification of Multicast Service Requirements
Multicast Service Testing Scenario
Testing Scenario:
1. IGMP version 2
2. IGMP version 3
3. IGMP snooping
4. IGMP proxy
5. IGMP Multicast Group
Data Collection
1. Testing Process
2. Capturing Traffic and Packet
Data Analysis
1. Checking Received Traffic
2. Analyze Packet Traffic
3. Analyze Test Result with Multicast Service Requirements
Recommendation
FINISH

Figure 4. Research Flow

Data is obtained from several testing to see the ability of multicast service in OLT XG-PON. The analysis process is done by monitoring the IPTV traffic packet using Wireshark software. Wireshark is a tool used to analyze data packets in network performance. Wireshark can capture data packets or information that are on the network. Wireshark has supervision for data packet in real-time. Wireshark application can be accessed free of charge and run on several platforms such as Linux, Mac, and Windows (Afrida & Rahmatia, 2018). The study results are expected to become a reference for regulators and providers of XG-PON IPTV technology in ensuring quality while deploying the XG-PON OLT equipment.

Multicast Service Testing Scenario

This study involves several devices, namely OLT, ONT, STB, TV, Telkom IPTV network, traffic generator, and laptop as an instrument for analysis, as shown in Figure 5 and Figure 6.

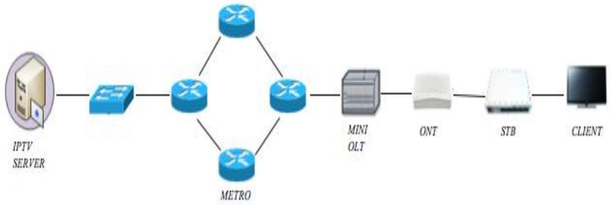


Figure 5. IGMP, IGMP Proxy, and IGMP Snooping Testing Configuration

Figure 5 is used to prove that the OLT XG-PON device supports IGMP version 2, IGMP version 3, IGMP Snooping, and IGMP proxy. The OLT device's uplink port is connected to Telkom's operational IPTV network, and the OLT service port connected to the ONT is already associated with ONT, STB, and Television. It is necessary to ensure that the IPTV service is functioning prior to testing. In order to obtain test results, the OLT is connected to a laptop with Wireshark software installed to obtain data on packet traffic flowing in OLT.

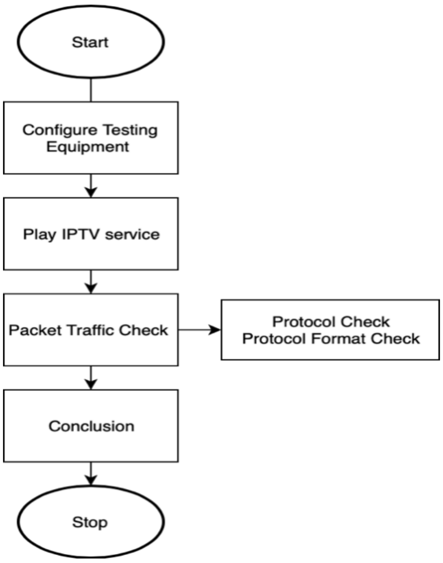


Figure 6. IGMP Version Testing Flowchart

IGMP version testing is done based on the flow in Figure 6. After all the equipment sets and IPTV service work, data is retrieved using Wireshark. Data, which is packet traffic, is checked by protocol and format. The results is analyzed based on the IGMP version theory.

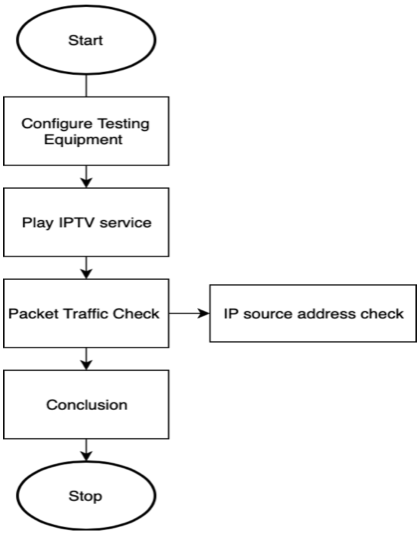


Figure 7. IGMP Snooping and Proxy Testing Flowchart

Figure 7 shows how IGMP snooping and proxy is done. First, OLT and ONT are set as IGMP snooping and IGMP proxy mode. After that, the IPTV service has to work correctly. IGMP snooping and IGMP proxy function is monitored from packet traffic Wireshark. The IP source address is checked to know whether OLT in IGMP snooping or IGMP proxy mode.

Figure 8 and Figure 9 are used to ascertain the ability of the IGMP multicast group number in OLT XG-PON devices. As shown in Figures 8 and 9, 1024, IGMP multicast groups have been configured in OLT and ONT devices connected to a traffic generator and analyzer. In the traffic generator and analyzer, traffic flow is made between OLT and ONT with 1 Gbps bandwidth. The downstream direction port is set as UDP traffic, while the upstream direction port creates 1024 IGMP multicast groups.

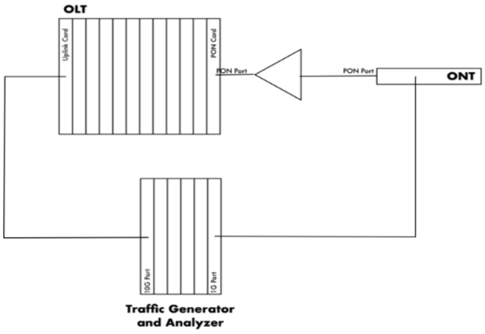


Figure 8. IGMP Group Multicast Testing Configuration

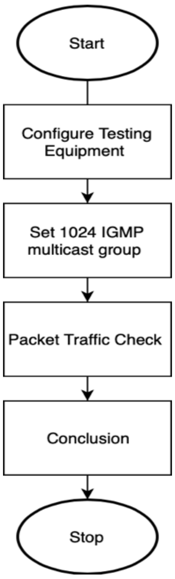


Figure 9. IGMP Group Multicast Testing Flowchart

After everything is configured in such a way, the measuring devices deliver traffic from OLT and ONT. The test results obtained by ensuring that traffic is generally running without frame loss and analyzing the traffic flowing on OLT to get the ability of IGMP multicast group OLT.

RESULTS AND DISCUSSION

The following are the results of testing of multicast service specifications such as IGMP version, IGMP Snooping, IGMP proxy, and IGMP Multicast Group. The multicast service testing in this study used a specific research object, which is XG-PON OLT. The data obtained worked on live IPTV networks compare to another previous research.

IGMP Testing (Version 2 and Version 3)

On IPTV networks, television broadcasts are sent via IP multicast using a particular protocol, namely IGMP. IGMP controls and limits multicast traffic flow across the network by using specific multicast queries and hosts. Query messages are sent by network devices such as routers to determine which network devices are members of the multicast group. The host is the recipient who sends report messages in response to request messages (Shohag & Mozammel-Bin-Motalab, 2011). Hosts representing end-users are organized into groups; each host can join or leave one or more groups, and this means choosing whether to receive data sent to each group or not. A router is a network device that provides multicast traffic and maintains records of subscription hosts (Humar & Podnar, 2013).

IGMP has several versions namely IGMP version 1 (RFC 1112), IGMP version 2 (RFC 2236), and IGMP version 3 (3376). IGMP version 2 adds support for "low leave latency" compared to IGMP version 1. Unlike IGMP version 2, a new feature is added in IGMP version 3 that is knowns as the "source filtering" to support Source-Specific Multicast (SSM). It allows the hosts to determine the source of where it wants to receive multicast traffic, or from all specific source addresses, sent to specific multicast addresses. IGMP version 3 implementation must also pay attention to compatibility with IGMP version 2 and IGMP version 1 (Tian & Roger, 2012).

The two primary devices in IGMP operations are IGMP Host (client) and IGMP Router (multicast router). The IGMP hosts issues the IGMP Report/Join message, and the IGMP leave a multicast group. On this client device, it responds to queries (questions) from multicast routers. A set-top box is an example of an IGMP host.

The IGMP router is the part that responds to the IGMP Join, and IGMP Leave messages to be able to determine if the multicast group should or should not receive multicast data to the interface. The IGMP router accepts multicast groups through multicast protocols such as PIM or via IGMP messages. This section is the termination point for IGMP messages. On IP multicast networks, IGMP has the IGMP Message form in the format shown in Figure 10 below.

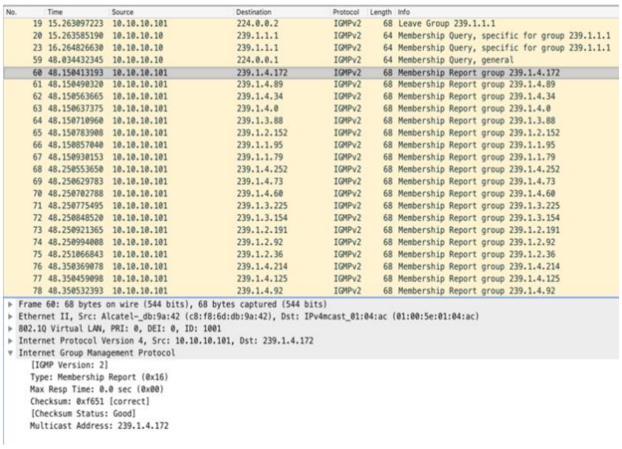
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     | Max Resp Time |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Group Address                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 10. IGMP Message Format
Source: (Fenner, 1997)

Type is the type of IGMP message associated with the interaction between host and router, namely Membership Report/Join Group and Leave Group on IGMP host and Membership Query on IGMP Query. The message Membership Report/Join Group indicates that the host wants to receive multicast information data or become a multicast group member. In IGMP version 2, the IGMP message format is 0x16, while in IGMP version 3, it is 0x22 (Cain et al., 2002).

The Leave Group message with the format IGMP message 0x17 indicates that the host is no longer interested in the services/channels received from the multicast group (switching television channels). The Membership Query Message provides questions to the host about the host group's membership; the purpose is to support IGMP Join/Leave messages or identify any errors. The question can be in the form of a Specific Query to ask whether a host is affiliated with a particular multicast group, and General Query asks which host belongs to the multicast group. The IGMP message format for Membership Queries is 0x11.

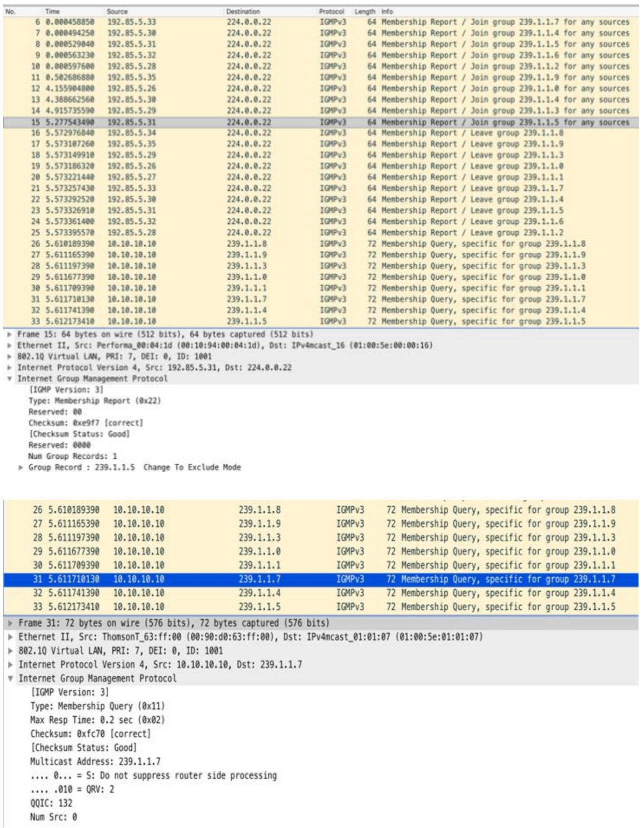
The IGMP Version 2 testing results in Figure 11shows that OLT XGPON can pass IGMP traffic version 2. It can be seen from several types of messages that are readable on Wireshark, including the message Membership Query, Membership Report, and Leave Group. The package also shows the membership report format of the IGMP protocol is 0x16 or IGMP version 2.



```
No.   Time          Source          Destination    Protocol  Length Info
   19 15.263097223  10.10.10.101    224.0.0.2      IGMPv2      68 Leave Group 239.1.1.1
   20 15.263585190  10.10.10.10     239.1.1.1      IGMPv2      64 Membership Query, specific for group 239.1.1.1
   23 16.264826630  10.10.10.10     239.1.1.1      IGMPv2      64 Membership Query, specific for group 239.1.1.1
   59 48.034432345  10.10.10.10     224.0.0.1      IGMPv2      64 Membership Query, general
   60 48.150413193  10.10.10.101    239.1.4.172    IGMPv2      68 Membership Report group 239.1.4.172
   61 48.150490320  10.10.10.101    239.1.4.89     IGMPv2      68 Membership Report group 239.1.4.89
   62 48.150563665  10.10.10.101    239.1.4.34     IGMPv2      68 Membership Report group 239.1.4.34
   63 48.150637375  10.10.10.101    239.1.4.0      IGMPv2      68 Membership Report group 239.1.4.0
   64 48.150710960  10.10.10.101    239.1.3.88     IGMPv2      68 Membership Report group 239.1.3.88
   65 48.150783908  10.10.10.101    239.1.2.152    IGMPv2      68 Membership Report group 239.1.2.152
   66 48.150857040  10.10.10.101    239.1.1.95     IGMPv2      68 Membership Report group 239.1.1.95
   67 48.150930153  10.10.10.101    239.1.1.79     IGMPv2      68 Membership Report group 239.1.1.79
   68 48.250553650  10.10.10.101    239.1.4.252    IGMPv2      68 Membership Report group 239.1.4.252
   69 48.250629783  10.10.10.101    239.1.4.73     IGMPv2      68 Membership Report group 239.1.4.73
   70 48.250702788  10.10.10.101    239.1.4.60     IGMPv2      68 Membership Report group 239.1.4.60
   71 48.250775495  10.10.10.101    239.1.3.225    IGMPv2      68 Membership Report group 239.1.3.225
   72 48.250848520  10.10.10.101    239.1.3.154    IGMPv2      68 Membership Report group 239.1.3.154
   73 48.250921365  10.10.10.101    239.1.2.191    IGMPv2      68 Membership Report group 239.1.2.191
   74 48.250994008  10.10.10.101    239.1.2.92     IGMPv2      68 Membership Report group 239.1.2.92
   75 48.251066843  10.10.10.101    239.1.2.36     IGMPv2      68 Membership Report group 239.1.2.36
   76 48.350369078  10.10.10.101    239.1.4.214    IGMPv2      68 Membership Report group 239.1.4.214
   77 48.350459098  10.10.10.101    239.1.4.125    IGMPv2      68 Membership Report group 239.1.4.125
   78 48.350532393  10.10.10.101    239.1.4.92     IGMPv2      68 Membership Report group 239.1.4.92
▶ Frame 60: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
▶ Ethernet II, Src: Alcatel-_db:9a:42 (c8:f8:6d:db:9a:42), Dst: IPv4mcast_01:04:ac (01:00:5e:01:04:ac)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
▶ Internet Protocol Version 4, Src: 10.10.10.101, Dst: 239.1.4.172
▼ Internet Group Management Protocol
    [IGMP Version: 2]
    Type: Membership Report (0x16)
    Max Resp Time: 0.0 sec (0x00)
    Checksum: 0xf651 [correct]
    [Checksum Status: Good]
    Multicast Address: 239.1.4.172
```

Figure 11. Testing Results of IGMP Version 2 Package

However, based on the IGMP Version 3 test results in Figure 12, it shows that OLT XGPON can stream IGMP traffic version 3. From Wireshark software captured, there are several types of messages, including the Membership Query, Membership, and Membership Report messages. The packet also shows the membership report format of the IGMP protocol is 0x22 or IGMP version 3.



```
No.   Time          Source          Destination   Protocol  Length  Info
    6 0.000458850   192.85.5.33     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.7 for any sources
    7 0.000494250   192.85.5.30     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.4 for any sources
    8 0.000529040   192.85.5.31     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.5 for any sources
    9 0.000563230   192.85.5.32     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.6 for any sources
   10 0.000597600   192.85.5.28     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.2 for any sources
   11 0.502686880   192.85.5.35     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.9 for any sources
   12 4.155904800   192.85.5.26     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.0 for any sources
   13 4.388662560   192.85.5.30     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.4 for any sources
   14 4.915735590   192.85.5.29     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.3 for any sources
   15 5.277543490   192.85.5.31     224.0.0.22    IGMPv3    64 Membership Report / Join group 239.1.1.5 for any sources
   16 5.572976840   192.85.5.34     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.8
   17 5.573107260   192.85.5.35     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.9
   18 5.573149910   192.85.5.29     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.3
   19 5.573186320   192.85.5.26     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.0
   20 5.573221440   192.85.5.27     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.1
   21 5.573257430   192.85.5.33     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.7
   22 5.573292520   192.85.5.30     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.4
   23 5.573326910   192.85.5.31     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.5
   24 5.573361400   192.85.5.32     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.6
   25 5.573395570   192.85.5.28     224.0.0.22    IGMPv3    64 Membership Report / Leave group 239.1.1.2
   26 5.610189390   10.10.10.10     239.1.1.8     IGMPv3    72 Membership Query, specific for group 239.1.1.8
   27 5.611165390   10.10.10.10     239.1.1.9     IGMPv3    72 Membership Query, specific for group 239.1.1.9
   28 5.611197390   10.10.10.10     239.1.1.3     IGMPv3    72 Membership Query, specific for group 239.1.1.3
   29 5.611677390   10.10.10.10     239.1.1.0     IGMPv3    72 Membership Query, specific for group 239.1.1.0
   30 5.611709390   10.10.10.10     239.1.1.1     IGMPv3    72 Membership Query, specific for group 239.1.1.1
   31 5.611710130   10.10.10.10     239.1.1.7     IGMPv3    72 Membership Query, specific for group 239.1.1.7
   32 5.611741390   10.10.10.10     239.1.1.4     IGMPv3    72 Membership Query, specific for group 239.1.1.4
   33 5.612173410   10.10.10.10     239.1.1.5     IGMPv3    72 Membership Query, specific for group 239.1.1.5
▶ Frame 15: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
▶ Ethernet II, Src: Performa_00:04:1d (00:10:94:00:04:1d), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
▶ 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 1001
▶ Internet Protocol Version 4, Src: 192.85.5.31, Dst: 224.0.0.22
▼ Internet Group Management Protocol
    [IGMP Version: 3]
    Type: Membership Report (0x22)
    Reserved: 00
    Checksum: 0xe9f7 [correct]
    [Checksum Status: Good]
    Reserved: 0000
    Num Group Records: 1
  ▶ Group Record : 239.1.1.5  Change To Exclude Mode
```

```
   26 5.610189390   10.10.10.10     239.1.1.8     IGMPv3    72 Membership Query, specific for group 239.1.1.8
   27 5.611165390   10.10.10.10     239.1.1.9     IGMPv3    72 Membership Query, specific for group 239.1.1.9
   28 5.611197390   10.10.10.10     239.1.1.3     IGMPv3    72 Membership Query, specific for group 239.1.1.3
   29 5.611677390   10.10.10.10     239.1.1.0     IGMPv3    72 Membership Query, specific for group 239.1.1.0
   30 5.611709390   10.10.10.10     239.1.1.1     IGMPv3    72 Membership Query, specific for group 239.1.1.1
   31 5.611710130   10.10.10.10     239.1.1.7     IGMPv3    72 Membership Query, specific for group 239.1.1.7
   32 5.611741390   10.10.10.10     239.1.1.4     IGMPv3    72 Membership Query, specific for group 239.1.1.4
   33 5.612173410   10.10.10.10     239.1.1.5     IGMPv3    72 Membership Query, specific for group 239.1.1.5
▶ Frame 31: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
▶ Ethernet II, Src: ThomsonT_63:ff:00 (00:90:d0:63:ff:00), Dst: IPv4mcast_01:01:07 (01:00:5e:01:01:07)
▶ 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 1001
▶ Internet Protocol Version 4, Src: 10.10.10.10, Dst: 239.1.1.7
▼ Internet Group Management Protocol
    [IGMP Version: 3]
    Type: Membership Query (0x11)
    Max Resp Time: 0.2 sec (0x02)
    Checksum: 0xfc70 [correct]
    [Checksum Status: Good]
    Multicast Address: 239.1.1.7
    .... 0... = S: Do not suppress router side processing
    .... .010 = QRV: 2
    QQIC: 132
    Num Src: 0
```

Figure 12. Testing Results of IGMP Version 3 Package

IGMP Snooping Testing

IGMP Snooping works at layer 2 as a multicast control mechanism. The goal is to monitor and check IGMP messages between the host and the multicast router. IGMP Snooping provides the advantage of saving bandwidth usage on network segments by looking at the presence or absence of hosts who express interest in receiving multicast packets sent to the group address. IGMP snooping brings more benefits to the usage and conservation of bandwidth (Fariss et al., 2018).

Figure 13 shows the IGMP Snooping switch between the IGMP host and the router. IGMP Snooping checks IGMP membership Reports and IGMP Leave Group and forwards only if necessary, to the connected IGMP router. Through IETF, IEEE has issued Request for Comment (RFC) 4541, which discusses the IGMP Snooping switch.

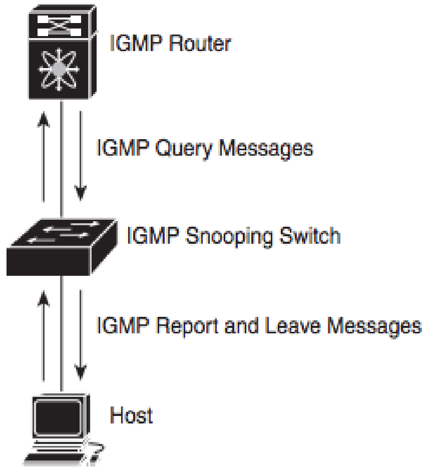
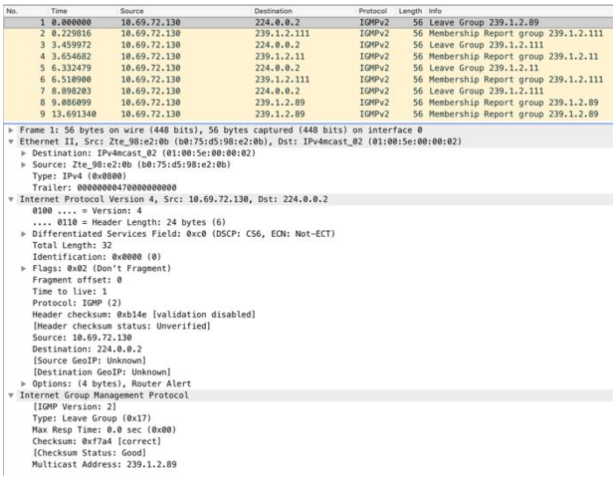


Figure 13. IGMP *Snooping*
Source: (Cisco, 2017)

Moreover, IGMP has a forwarding setting which arrange membership report for a group address a host may put interest in, upon receipt by a host. In this case, the host is not required to send another membership report (report suppression) message to the same group. If the snooping switch does not accept the host's membership reports, the host will not receive multicast data.

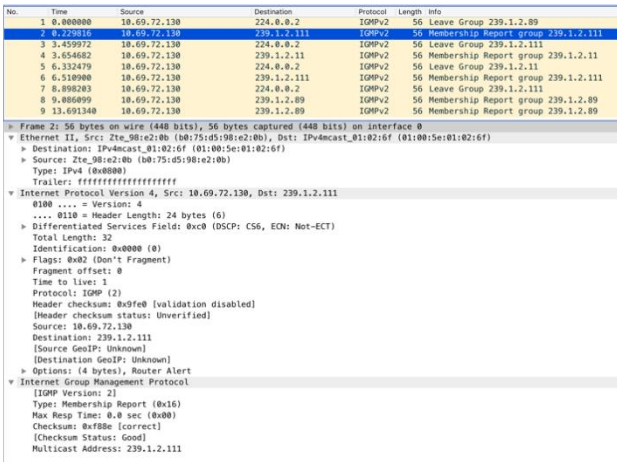
A Snooping switch that can implement IGMP is required to maintain a list of the ports that are connected to that switch. In IGMP Snooping, IGMP queries sent by multicast routers do not originate from the IP address 0.0.0.0 (Christensen et al., 2006).

Based on packet traffic from the IGMP Snooping test results shown in Figures 14 and 15, the OLT XGPON supports IGMP Snooping functions. From the packet, it has been discovered that the source IP for IGMP Snooping was 10.69.72.130. It follows the RFC 4541 (IGMP Snooping), where the IP source address for the Membership Query message on switches that have IGMP Snooping capability is an IP address other than 0.0.0.0. OLT acts as a Snooping switch by forwarding the multicast packets from the multicast router to the ONT. The snooping ability in OLT aims to identify and send multicast packets to the involved hosts only.



```
No.     Time        Source          Destination    Protocol  Length  Info
      1 0.000000    10.69.72.130    224.0.0.2      IGMPv2       56   Leave Group 239.1.2.89
      2 0.229816    10.69.72.130    239.1.2.111    IGMPv2       56   Membership Report group 239.1.2.111
      3 3.459972    10.69.72.130    224.0.0.2      IGMPv2       56   Leave Group 239.1.2.111
      4 3.654682    10.69.72.130    239.1.2.11     IGMPv2       56   Membership Report group 239.1.2.11
      5 6.332479    10.69.72.130    224.0.0.2      IGMPv2       56   Leave Group 239.1.2.11
      6 6.510900    10.69.72.130    239.1.2.111    IGMPv2       56   Membership Report group 239.1.2.111
      7 8.898203    10.69.72.130    224.0.0.2      IGMPv2       56   Leave Group 239.1.2.111
      8 9.086099    10.69.72.130    239.1.2.89     IGMPv2       56   Membership Report group 239.1.2.89
      9 13.691340   10.69.72.130    239.1.2.89     IGMPv2       56   Membership Report group 239.1.2.89
▶ Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▼ Ethernet II, Src: Zte_98:e2:0b (b0:75:d5:98:e2:0b), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
  ▶ Destination: IPv4mcast_02 (01:00:5e:00:00:02)
  ▶ Source: Zte_98:e2:0b (b0:75:d5:98:e2:0b)
    Type: IPv4 (0x0800)
    Trailer: 00000000470000000000
▼ Internet Protocol Version 4, Src: 10.69.72.130, Dst: 224.0.0.2
    0100 .... = Version: 4
    .... 0110 = Header Length: 24 bytes (6)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 32
    Identification: 0x0000 (0)
  ▶ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 1
    Protocol: IGMP (2)
    Header checksum: 0xb14e [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.69.72.130
    Destination: 224.0.0.2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▶ Options: (4 bytes), Router Alert
▼ Internet Group Management Protocol
    [IGMP Version: 2]
    Type: Leave Group (0x17)
    Max Resp Time: 0.0 sec (0x00)
    Checksum: 0xf7a4 [correct]
    [Checksum Status: Good]
    Multicast Address: 239.1.2.89
```

Figure 14. Testing Results of IGMP Snooping (Leave Group Message)



```
No.     Time        Source          Destination    Protocol  Length  Info
      1 0.000000    10.69.72.130    224.0.0.2      IGMPv2       56   Leave Group 239.1.2.89
      2 0.229816    10.69.72.130    239.1.2.111    IGMPv2       56   Membership Report group 239.1.2.111
      3 3.459972    10.69.72.130    224.0.0.2      IGMPv2       56   Leave Group 239.1.2.111
      4 3.654682    10.69.72.130    239.1.2.11     IGMPv2       56   Membership Report group 239.1.2.11
      5 6.332479    10.69.72.130    224.0.0.2      IGMPv2       56   Leave Group 239.1.2.11
      6 6.510900    10.69.72.130    239.1.2.111    IGMPv2       56   Membership Report group 239.1.2.111
      7 8.898203    10.69.72.130    224.0.0.2      IGMPv2       56   Leave Group 239.1.2.111
      8 9.086099    10.69.72.130    239.1.2.89     IGMPv2       56   Membership Report group 239.1.2.89
      9 13.691340   10.69.72.130    239.1.2.89     IGMPv2       56   Membership Report group 239.1.2.89
▶ Frame 2: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▼ Ethernet II, Src: Zte_98:e2:0b (b0:75:d5:98:e2:0b), Dst: IPv4mcast_01:02:6f (01:00:5e:01:02:6f)
  ▶ Destination: IPv4mcast_01:02:6f (01:00:5e:01:02:6f)
  ▶ Source: Zte_98:e2:0b (b0:75:d5:98:e2:0b)
    Type: IPv4 (0x0800)
    Trailer: ffffffffffffffffffff
▼ Internet Protocol Version 4, Src: 10.69.72.130, Dst: 239.1.2.111
    0100 .... = Version: 4
    .... 0110 = Header Length: 24 bytes (6)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 32
    Identification: 0x0000 (0)
  ▶ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 1
    Protocol: IGMP (2)
    Header checksum: 0x9fe0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.69.72.130
    Destination: 239.1.2.111
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▶ Options: (4 bytes), Router Alert
▼ Internet Group Management Protocol
    [IGMP Version: 2]
    Type: Membership Report (0x16)
    Max Resp Time: 0.0 sec (0x00)
    Checksum: 0xf88e [correct]
    [Checksum Status: Good]
    Multicast Address: 239.1.2.111
```

Figure 15. Testing Results of IGMP Snooping (Membership Report Message)

IGMP Proxy Testing

IGMP Proxy is used on Layer 2 devices between routers and hosts. Therefore, Layer 2 devices act as proxy servers (IGMP proxy agents), as shown in Figure 16 below. The IGMP proxy agent sends the IGMP request packet to the host and processes the IGMP response packet sent from the host.

Additionally, IGMP proxy agents respond to query packets sent from routers, summarize messages sent by hosts to join or leave multicast groups, and notify routers about host activity. For the host, the IGMP proxy agent functions as a router, while for the router, the IGMP proxy agent functions as the host. A forwarding entry was created to implement Layer 2 multicast (Huawei Technologies, 2011).

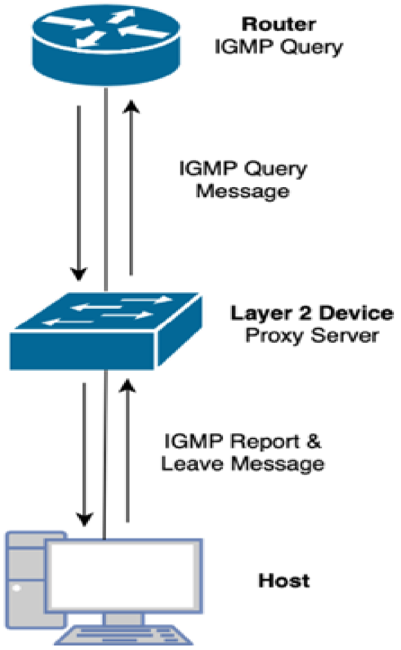
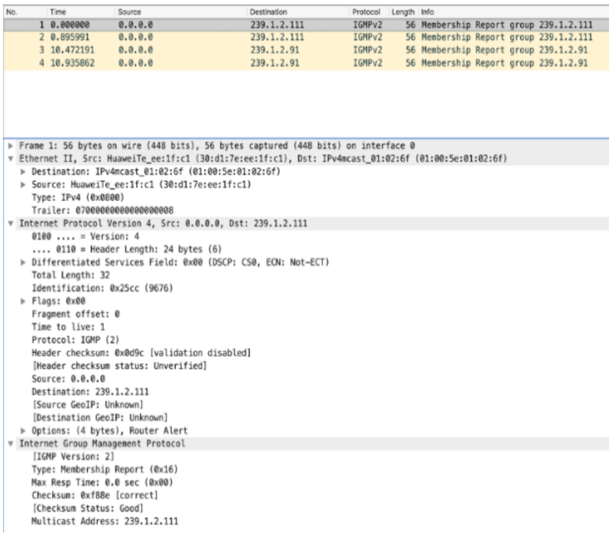


Figure 16. IGMP *Proxy*

The IGMP proxy aims to enable multicast routers to learn the multicast group's membership information and forward the multicast packets based on group membership information. RFC 4541 states that the IGMP network has a proxy reporting capability where the messages received come from downstream hosts that are used to establish membership status internally. Proxy reporting uses the source IP address 0.0.0.0 when sending it to the upstream section.

The test result in Figure 17 shows that OLT XGPON supports the IGMP Proxy function. It identifies 0.0.0.0 as the source IP address on IGMP Proxy traffic. The IP address 0.0.0.0 indicates that the message received by the Snooping switch device is doing the Reporting proxy (RFC 4541).



```
No.   Time        Source     Destination   Protocol  Length  Info
    1 0.000000    0.0.0.0    239.1.2.111   IGMPv2        56  Membership Report group 239.1.2.111
    2 0.895991    0.0.0.0    239.1.2.111   IGMPv2        56  Membership Report group 239.1.2.111
    3 10.472191   0.0.0.0    239.1.2.91    IGMPv2        56  Membership Report group 239.1.2.91
    4 10.935862   0.0.0.0    239.1.2.91    IGMPv2        56  Membership Report group 239.1.2.91
```

```
▶ Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▼ Ethernet II, Src: HuaweiTe_ee:1f:c1 (30:d1:7e:ee:1f:c1), Dst: IPv4mcast_01:02:6f (01:00:5e:01:02:6f)
  ▶ Destination: IPv4mcast_01:02:6f (01:00:5e:01:02:6f)
  ▶ Source: HuaweiTe_ee:1f:c1 (30:d1:7e:ee:1f:c1)
    Type: IPv4 (0x0800)
    Trailer: 07000000000000000008
▼ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 239.1.2.111
    0100 .... = Version: 4
    .... 0110 = Header Length: 24 bytes (6)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 32
    Identification: 0x25cc (9676)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: IGMP (2)
    Header checksum: 0x0d9c [validation disabled]
    [Header checksum status: Unverified]
    Source: 0.0.0.0
    Destination: 239.1.2.111
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▶ Options: (4 bytes), Router Alert
▼ Internet Group Management Protocol
    [IGMP Version: 2]
    Type: Membership Report (0x16)
    Max Resp Time: 0.0 sec (0x00)
    Checksum: 0xf88e [correct]
    [Checksum Status: Good]
    Multicast Address: 239.1.2.111
```

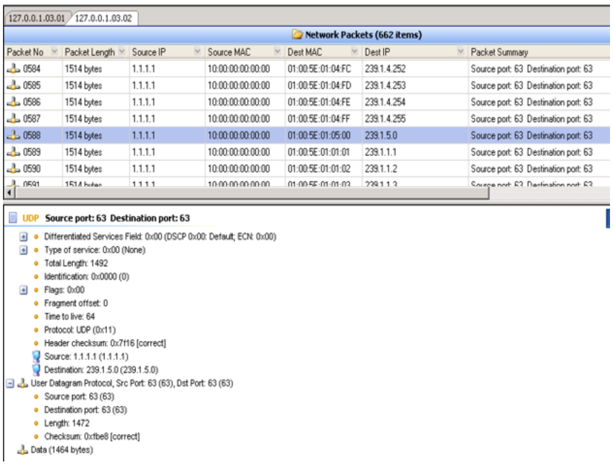
Figure 17. Testing Results of IGMP Proxy

IGMP Multicast Group Capabilities Testing

Multicasting is a process of data delivery to a group of destination hosts simultaneously in a single transmission from the source. Internet Engineering Task Force (IETF) developed four multicasts addressing schemes, one of which is reserved for multicasting traffic. Class D is reserved for multicasting traffic groups and identified with IP addresses in the range from 224.0.0.0 to 239.255.255.255.

Multicast traffic travels through the IP network to a subset of nodes called a multicast group. The basic concept of IP multicast is that the source host sends only one copy of data to a multicast group addresses. All receivers in the multicast group acquire the same data copy. The hosts in the multicast group receive the data while the other hosts on the network cannot receive the data.

Based on the test results shown in Figure 18, the XGPON OLT device tested was able to pass 1024 IGMP multicast groups on an IPv4 network. A total of 1024 multicast group OLT device capabilities proved to serve multicast services.



```
Packet No  Packet Length  Source IP  Source MAC         Dest MAC           Dest IP     Packet Summary
0584       1514 bytes     1.1.1.1    10:00:00:00:00:00  01:00:5E:01:04:FC  239.1.4.252  Source port: 63  Destination port: 63
0585       1514 bytes     1.1.1.1    10:00:00:00:00:00  01:00:5E:01:04:FD  239.1.4.253  Source port: 63  Destination port: 63
0586       1514 bytes     1.1.1.1    10:00:00:00:00:00  01:00:5E:01:04:FE  239.1.4.254  Source port: 63  Destination port: 63
0587       1514 bytes     1.1.1.1    10:00:00:00:00:00  01:00:5E:01:04:FF  239.1.4.255  Source port: 63  Destination port: 63
0588       1514 bytes     1.1.1.1    10:00:00:00:00:00  01:00:5E:01:05:00  239.1.5.0    Source port: 63  Destination port: 63
0589       1514 bytes     1.1.1.1    10:00:00:00:00:00  01:00:5E:01:01:01  239.1.1.1    Source port: 63  Destination port: 63
0590       1514 bytes     1.1.1.1    10:00:00:00:00:00  01:00:5E:01:01:02  239.1.1.2    Source port: 63  Destination port: 63
0591       1514 bytes     1.1.1.1    10:00:00:00:00:00  01:00:5E:01:01:03  239.1.1.3    Source port: 63  Destination port: 63
```

```
UDP  Source port: 63  Destination port: 63
  ⊞ • Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  ⊞ • Type of service: 0x00 (None)
    • Total Length: 1492
    • Identification: 0x0000 (0)
  ⊞ • Flags: 0x00
    • Fragment offset: 0
    • Time to live: 64
    • Protocol: UDP (0x11)
    • Header checksum: 0x7f16 [correct]
      Source: 1.1.1.1 (1.1.1.1)
      Destination: 239.1.5.0 (239.1.5.0)
⊟ User Datagram Protocol, Src Port: 63 (63), Dst Port: 63 (63)
    • Source port: 63 (63)
    • Destination port: 63 (63)
    • Length: 1472
    • Checksum: 0xfbe8 [correct]
  Data (1464 bytes)
```

Figure 18. Traffic Package Test Results for IGMP Multicast Group Capabilities

In this test, 1024 multicast groups were generated with IP addresses from 239.1.1.1 to 239.1.5.0. With the following range of addressing, it can be concluded that the OLT device has a total of 1024 multicast groups.

CONCLUSIONS

This research produces technical requirements and testing scenario alternatives for multicast services that are expected to be used as a reference for regulators and telecommunications operators that provide IPTV services. The technical specifications requires the OLT XG-PON to pass the IGMP protocol version 2 and 3 traffic in accordance with the ITU-T G.987.1 recommendations.

Another requirement that can be used as a reference is the ability of OLT to support IGMP

Snooping and Proxy. IGMP Snooping has the advantage of saving bandwidth usage on network segments. At the same time, the IGMP proxies can learn multicast group's membership information and forward the multicast packets based on group membership information.

Furthermore, regulators and IPTV service providers can develop technical requirements for IGMP multicast groups. Based on the test result, since OLT XG-PON is capable of passing 1024 IGMP multicast groups, the requirements for IGMP multicast groups shall be set to 1024 multicast groups.

Given the network testing in this study which uses the IPv4, it is recommended for further research to measure the performance of multicast services on the IPv6 XG-PON network. The use of IPv6 systems in the future is expected to become natural. Therefore, extensive research is needed to assess its performance, especially on optical access networks.

Additionally, further research can also develop multicast service testing on FTTx networks using other PON technologies that are not regulated in Regulation of Director General of Posts and Telecomunications No. 257 of 2008, such as XGS-PON and WDM-PON.

ACKNOWLEDGMENTS

The authors granted a high appreciation to the Digital Service Division of PT. Telekomunikasi Indonesia, Postgraduate Program in Regulation & Management of Telecommunication, School of Electrical Engineering, Telkom University, and our colleague: Muhammad Adam Anugeraha, for their support of this study.

REFERENCES

Afrida, F. A., & Rahmatia, S. (2018). Analisis Internet Group Management Protocol (IGMP) Menggunakan Software Wireshark dalam Layanan Live Streaming IPTV pada Multi Service Access Network (MSAN) di Area Darmo, Surabaya. *Jurnal AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, *4*(4), 176–181.

Al-zoubi, H., Halloush, M., & Al-qudah, Z. (2016). A Survey on Recent Advances In IPTV. *Jordanian Journal of Computers and Information Technology (JJCIT)*, *2*(2), 86–106.

Anwar, N. A., & Chamid, N. (2018). Perancangan Layanan Real Time Mobile Tv Pada Jaringan Wlan Menggunakan Protokol Multicast. *NJCA (Nusantara Journal of Computers and Its Applications)*, *3*(2). https://doi.org/10.36564/njca.v3i2.71

Batagelj, B., Erzen, V., Tratnik, J., Naglic, L., Bagan, V., Ignatov, Y., & Antonenko, M. (2012). Optical Access Network Migration from GPON to XG-PON. *ACCESS 2012: The Third International Conference on Access Networks*, 62–67.

Cain, B., Deering, S., Kouvelas, I., Fenner, B., & Thyagarajan, A. (2002). *Internet Group Management Protocol, Version 3* (RFC 3376; Issue 57).

Christensen, M., Kimball, K., & Solensky, F. (2006). *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches* (RFC 4541).

Cisco. (2017). Cisco Visual Networking Index: Forecast and Methodology Cisco Visual Networking Index: Cisco Visual Networking Index: Forecast and Methodology. *Forecast and Methodology*, 2015–2020.

Dalamagkas, C., Sarigiannidis, P., Moscholios, I., Lagkas, T. D., & Obaidat, M. (2018). PAS : A Fair Game-Driven DBA Scheme for XG-PON Systems. *2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), July*, 1–6. https://doi.org/10.1109/CSNDSP.2018.8471787

DEPKOMINFO. (2008). *Persyaratan Teknis Alat dan Perangkat Telekomunikasi Akses Berbasis Passive Optical Network (PON) (257/DIRJEN/2008)*. Departemen Komunikasi dan Informatika RI.

Effenberger, F. J. (2011). The XG-PON System : Cost-Effective 10 Gb / s Access. *Journal of Lightwave Technology*, *29*(4), 403–409. https://doi.org/https://doi: 10.1109/JLT.2010.2084989

Fariss, M., Allali, N. El, & Asaidi, H. (2018). Review of Ontology-Based Approaches for Web Service Discovery : Methods and Protocols Review of Ontology-Based Approaches for Web Service Discovery. *International Conference on Advanced Information Technology, Services, and Systems* (Issue October). Springer International Publishing. https://doi.org/10.1007/978-3-030-11914-0

Fenner, W. (1997). *Internet Group Management Protocol, Version 2 Status* (RFC 2236; Vol. 21, Issue 3).

G.9807.1. (2016). G.9807.1 : the 10-Gigabit-capable symmetric passive optical network (XGS-PON). *Itu-T G-Series Recommendations*.

Gupta, H., Gupta, P., Kumar, P., Gupta, A. K., & Mathur, P. K. (2018). Passive Optical Networks : Review and Road Ahead. *Proceedings of TENCON 2018 - 2018 IEEE Region 10 Conference*, *October*, 28–31. https://doi.org/https:// doi: 10.1109/TENCON.2018.8650204

Hernandez, J. A., Sanchez, R., Martin, I., & Larrabeiti, D. (2019). Meeting the Traffic Requirements of Residential Users in the Next Decade with Current FTTH Standards: How Much? How Long? *IEEE Communications Magazine*, *57*(6), 120–125. https://doi.org/10.1109/MCOM.2018.1800173

Huawei Technologies. (2011). *Multicast Technology White Paper*.

Humar, I., & Podnar, M. (2013). Implementation and performance evaluation of IGMP snooping supporting multicast functionality on Linux-based Ethernet switches. *Telecommunication Systems*, *52*(3), 1559–1572. https://doi.org/10.1007/s11235-011-9523-3

Huszaník, T., Turán, J., & Ovseník, Ľ. (2018). Simulation of Downlink of 10G-PON FTTH in the city of Košice. *Carpathian Journal of Electronic and Computer Engineering*, *11*(1), 33–39. https://doi.org/10.2478/cjece-2018-0006

International Telecommunication Union. (2016). ITU-T G.987.1. In *10-Gigabit-capable passive optical networks (XG-PON): General requirements: Vol. 2.0*.

IXIA. (2017). *Black Book - Video over IP*. Keysight Technologies.

Khider, I., Elfaki, S., Elhassan, M., & Siddig, M. (2011). Evaluate the performance of Internet Protocol Television. *2011 International Conference on Electrical and Control Engineering, ICECE 2011 - Proceedings*, 5902–5905. https://doi.org/10.1109/ICECENG.2011.6057450

Mamun, S. S. Al, & Motalab, M. Bin. (2011). An Observation and Analysis of IPTV and Multicasting Traffic. *International Journal of Computer Application*, *30*(1), 1–6.

Moughit, M., Badri, A., & Sahel, A. (2013). A Multicast IPTV Bandwidth Saving Method. *International Journal of Computer Applications*, *64*(14), 22–26. https://doi.org/10.5120/10702-5611

Research and Markets. (2019). *IPTV Market: Global Industry Trends, Share, Size, Growth, Opportunity, and Forecast 2019-2024*.

Ridwan, M., Sutabri, T., & Nandi. (2019). *Analisis Pendistribusian Bandwidth Pada Video Streaming Dengan Metode Unicast Dan Multicast Pada Teknologi Gigabit Passive*. *5*(1), 78–87.

Sardju, A. P. (2016). Implementasi IPTV (Internet Protocol Television) Berbasis Web Pada Jaringan Wireless. *PROtek : Jurnal Ilmiah Teknik Elektro*, *3*(2). https://doi.org/10.33387/protk.v3i2.155

Shohag, S. A. M., & Mozammel-Bin-Motalab. (2011). An Observation and Analysis of IPTV and Multicasting Traffic. *International Journal of Computer Application*, *30*(1), 1–6.

Tian, Y., & Roger, H. (2012). A resolution for IGMP V3 protocol using a finite state machine. *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, *2*, 517–520. https://doi.org/10.1109/ICCSEE.2012.124

Vasanthi, V., & Chidambaram, M. (2014). *Internet Protocol Television (IPTV) and its Security Threats - An Overview*. *2*(4), 172–175.

We Are Social and Hootsuite. (2019). Digital 2019: Indonesia. In *Kepios Pte. Ltd., We Are Social Ltd., Hootsuite Inc*.