UNIVERSITI TEKNIKAL MALAYSIA MELAKA

A STUDY OF MULTICAST PROTOCOL EFFICIENCY IN A CAMPUS NETWORK ENVIRONMENT USING eNSP

This report is submitted in accordance with the requirement of the Universiti Teknikal Malaysia Melaka (UTeM) for the Bachelor of Electronics Engineering Technology (Telecommunications) with Honours.

by

UMI ATIKAH BINTI ISMAIL

FACULTY OF ELECTRICAL AND ELECTRONIC ENGINEERING TECHNOLOGY

2021

DECLARATION

I hereby, declared this report entitled A STUDY OF MULTICAST PROTOCOL EFFICIENCY IN A CAMPUS NETWORK ENVIRONMENT USING eNSP is the results of my own research except as cited in references.

Signature: 

Author : UMI ATIKAH BINTI ISMAIL

Date: 14/02/2021

APPROVAL

This report is submitted to the Faculty of Electrical and Electronic Engineering Technology of Universiti Teknikal Malaysia Melaka (UTeM) as a partial fulfilment of the requirements for the degree of Bachelor of Electronics Engineering Technology (Telecommunications) with Honours. The member of the supervisory is as follow:

Signature: ……

Supervisor: Ts. FAKHRULLAH BIN IDRIS

Signature: ……

Co-supervisor: Ts. GLORIA RAYMOND TANNY

ABSTRAK

Dalam era digitalisasi ini, rangkaian komputer memainkan peranan penting dalam kehidupan kita. Ini membolehkan pengguna di rangkaian berkongsi maklumat atau sumber dan berhubung antara satu sama lain. Dengan teknologi multicast, setiap reka bentuk komunikasi rangkaian yang melibatkan penghantaran maklumat kepada beberapa penerima dapat memanfaatkan kecekapan lebar jalurnya. Walau bagaimanapun, tujuan projek ini adalah untuk menerapkan protokol multicast dalam topologi rangkaian kampus dengan menggunakan eNSP dan mengkaji kecekapannya. Projek ini akan diuji melalui proses penstriman video yang dihantar dari satu pelayan ke beberapa pelanggan. Selain itu, projek ini tidak akan menggunakan apa-apa pelaksanaan perkakasan dan ini hanya termasuk pada simulasi. Protokol multicast yang digunakan terutamanya dalam projek ini adalah Protokol Multicast Dense Mode (PIM-DM) dan Protokol Independent Sparse Mode (PIM-SM) selain daripada Open Shortest Path First (OSPF) dan Internet Group Management Protocol (IGMP). Pelaksanaan perisian tersebut merangkumi simulator rangkaian Huawei eNSP dan penganalisis rangkaian Wireshark. Projek ini dapat mengurangkan kos dan menjimatkan masa kerana hanya berlaku dalam simulasi. Walaupun hanya dalam simulasi, penyelidik akan dapat melihat bagaimana ia berfungsi dalam realiti proses penstriman video.

ABSTRACT

In this era of digitalization, the computer network plays a crucial role in our lives. It lets users on the network to share information or resources and connect with each other. With multicast technology, any design of network communication that involve the transmission of one message from a source to multiple receivers will have the efficiency benefits of its bandwidth. However, the purpose of this project is to apply multicast protocol in a campus network topology by using eNSP and to study their efficiency. This project will be tested through a delivered video streaming process from one server to multiple clients. Besides, this project will not use any hardware implementation and it is including only on the simulation. The multicast protocol mainly used in this project are Protocol Independent Multicast-Dense Mode (PIM-DM) and Protocol Independent-Sparse Mode (PIM-SM) other that Open Shortest Path First (OSPF) and Internet Group Management Protocol (IGMP). The software implementation is including Huawei eNSP network simulator and Wireshark network analyzer. This project is able to reduce costs and save time as it only happens in simulation. Although only in simulation, the researcher will be managed to see how it works in the reality of the video streaming process.

DEDICATION

This project is especially dedicated to my beloved parents, Allahyarham Ismail Bin Mat Isa and Siti Mariam Binti Md Zain, my supervisor and co-supervisor, Ts. Fakhrullah Bin Idris and Ts. Gloria Raymond Tanny, my siblings, my friends, and my lecturers.

ACKNOWLEDGEMENTS

First and foremost, I would like to have my gratitude and thanks toward Allah S.W.T for giving this opportunity to breathing and completing this final year project 1 and final year project 2. Throughout the hardship I have endured and giving me endless strength to face the project.

However, I also want to give my gratitude to my supervisor Ts. Fakhrullah bin Idris and my co-supervisor Ts. Gloria Raymond Tanny for patience, motivation and gave full commitment by helping me to completing this final year project 1 and final year project 2.

Furthermore, I would like to give my biggest gratitude toward my family especially my parents, Allahyarham Ismail Bin Mat Isa and Siti Mariam Binti Md Zain for giving me endless moral motivation and support of money and love for me.

Finally, my sincere gratitude toward all my friends who helped me during process of completing this project and on my writing report. Thank you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, SYMBOLS AND NOMENCLATURES

eNSP	-	Enterprise Network Simulation Platform
GNS3	-	Graphical System Simulator
IGMP	-	Internet Group Management Protocols
IP	-	Internet Protocols
IPTV	-	Internet Protocol television
IPV4	-	Internet Protocols Version 4
IPV6	-	Internet Protocols Version 6
LAN	-	Local Area Network
LTE	-	Long Term Evolution
MOSPF	-	Multicast Open Shortest Path First
MTRSA	-	Multi-Tree Routing State Assignment
OSPF	-	Open Shortest Path First
PC	-	Personal Computer

PIM-SM	-	Protocols Independent Multicast Sparse Mode
PIM-DM	-	Protocols Independent Multicast Dense Mode
RP	-	Rendezvous Point
RIP	-	Routing Information Protocols
SDN	-	Software Define Networking
SMTE	-	Scalable Multicast Traffic Engineering
UDP	-	User Datagram Protocol
VLC	-	Video LAN Client
VRP	-	Versatile Routing Platform
WLAN	-	Wireless Local Area Network

CHAPTER 1

INTRODUCTION

1.1 Project Background

These days, the computer network plays a crucial role in our lives. It lets users on the network to share information or resources and connect with each other. However, in multicast technology, any design of network communication that involve the transmission of one message from a source to multiple receivers will have the benefits of bandwidth reduction. Besides, the simulation will be used for the purpose of this project. In this project, the Network Simulator would apply the Huawei eNSP software.

According to (Golecha, A., Karanje, S., and Abraham, J., 2017) proposed that there should be one multicast source and one or more network destinations. At least one participant of the team is involved in obtaining a datagram of multicast from the source. The address of the group will identify the members of the group. Multicasting explores its use in applications such as radio or video broadcasts, video conferencing, and so on, which send the same data to several recipients at once. The paper mentions that the Protocol Independent Multicast Dense Mode (PIM DM) and Protocol Independent Multicast Sparse Mode (PIM SM) are the multicasting routing protocols that perform better and more effectively than the other protocols.

Subsequently, an article proposed by (Li, X. and Jiang, T., 2014) states that the network resources with centralization features is the main features of the campus network in according to different patterns of geographical distribution. The campus network covers a wide geographical area, the size of the network is diverse, and the multi-administrative campus network is used to

measure requirement of computing in the specific large scale. Typically, campus network operates on CERNET architecture that is high demand for network connection and can cause certain constraints. The implementation is not very complex in terms of the principle of logical design.

However, the article proposed by (Chen, J. *et al*., 2019) addressed that the Enterprise Network Simulation Platform (eNSP) is a freeware and scalability software provided by Huawei. It is mainly to simulate router, switch, firewall, WLAN, and any others of equipment on the enterprise network. It is also friendly interface and provides a real of equipment to support the networking in large scale. This software can able the users for design the enterprise network even if does not have any equipment for real life.

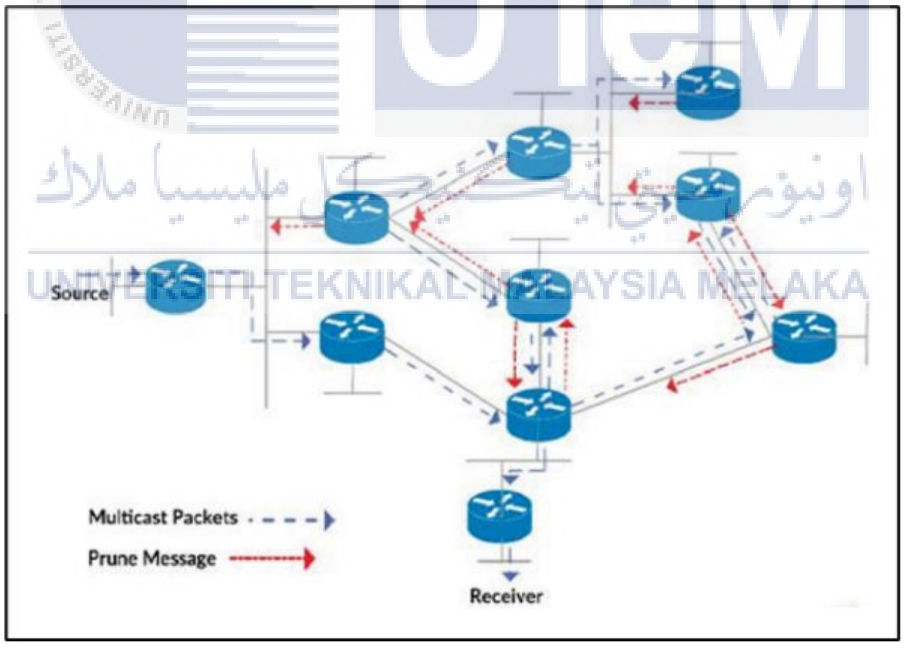


Figure 1.1: Multicast in PIM-DM. (Golecha, A., Karanje, S., and Abraham, J., 2017)

1.2 Objectives of Project

There are several objectives for this project:

1. To design the network topology of campus network and able to deliver video streaming to the clients using eNSP.
2. To compare the different types of multicast protocols implementation that mainly used Protocol Independent Multicast-Dense Mode (PIM-DM).
3. To study the efficiency of multicast protocols configuration on similar campus network topology.

1.3 Scope of Project

Even so, the scope of this project ultimately encompasses a whole university or campus. But for this research, it comprises several networking equipment which are most important to be used in the design of the campus network such as network switches, routers, and clients. The number of network elements used are as following; four routers, eight switches and sixteen clients. Moreover, fibre optic and copper will be link to all equipment in the transmission media for this project. There are also two software of eNSP and Wireshark that will be implemented to execute this project. Thus, to reinforce this campus network design, we will implement the multicast protocols with different types of configuration and study their efficiency.

1.4 Problem Statement

Unlimited access to the networking world beyond the campus is one of the biggest purposes for building a campus network for all faculties, students, and staff. The worldwide electronic environment also has on-campus access to services and resources such as e-mail use, involvement in web forums, access to bibliographic and full text document content and information sharing. All these teachers, students and staff will easier able to work if they are able to access the Internet from their device. Indeed, many of the advantages, such as the web's potential for instructional use or as a campus-wide information system "intranet," that can only be noticed if everybody on campus provides exposure to it.

Most Internet operation requires fairly slow transmission of characters or text files. The development of Web usage for graphics, audio, and full motion video are leading higher demand for campus network efficiency. Before to design a campus network, we should predict the increasing demand for more network usable capacity, as well as stronger security, fidelity and optimized the service quality.

However, such excessive multicast streams would cause the cache and connection bandwidth of the switches to be wasted. But the cache and link bandwidth are necessary for transmitting application streams with less packet loss, latency, and jitter. Besides, the packets data are will likely happen duplicated at an exponential rate, it also will be leading to extremely bandwidth requirements and overhead of routing.

In addition, simulation of the eNSP network software is rarely used and known whether in the field of education or in the field of work. This means that eNSP software need to be more explore and we can figure out the best functionality of this network simulation compared to any other network simulations such as GNS3 and Cisco Packet Tracer. eNSP software encompasses of

an actual network equipment in the simulation. This would let the users to understanding and easy to manage the function and setup of related equipment in real life.

1.5 Thesis Arrangement

The first chapter introduces the probability of this project to be promptly clarified. The project background emphasized about the multicast technology, multicast protocols, campus network and eNSP software. This chapter also will explain the objectives, scope of project, problem statement and thesis arrangement of this project.

The second chapter is about the study of literature from previous researches that gather the information, techniques, and several features of the multicast technology. This chapter consists of multicast routing and protocol, campus network, eNSP software and Wireshark software that related and can be develop in this project. This chapter also based on articles, journals, and international research sources.

The third chapter will be exploring the different approaches to information-gathering. This chapter is a method that should be taken, and comprehensive studies reports that would be conducted to achieve this project's aim or objective. This section also determines the methods used to complete the mission, as well as details the project progress.

The fourth chapter will produce the expected results of this project. This chapter will analyze and observe all the output data from the implemented software.

The fifth chapter is the last chapter that will consists of the conclusion from all of this project. This chapter will be related the objectives of this project and provides some recommendations for the future research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this section is a vital part of the project before starting any project as it provides all the relevant and related project to gain the knowledge. This chapter emphasis on the information and methods from the previous researches that equivalent to this project Multicast Protocol Efficiency in a Campus Network Environment using eNSP. In order to reinforce this project, some studies and research as part of the literature will be carried out.

2.2 Multicast Routing and Protocols

The total bandwidth costs can be minimized by Multicast Technique. This article (Huang L. *et al*., 2016) proposed to discuss the issue of minimizing total cost of bandwidth by using the SMTE (Scalable Multicast Traffic Engineering) formula in compliance with connection and capacity node limitations in Software-defined networking (SDN) for multiple trees. The studies have observed that no ration can be used for SMTE. The MTRSA (Multi-Tree Routing and State Assignment Algorithm) has been recommended to support SMTE. They also simulate the multicast trees routing and attribution of nodes state branch with YouTube Traffic that will reduce overall bandwidth costs and the time of computation create several different trees to appropriate with practical SDNs. They use HP Procurve 5406zl OpenFlow experimental SDN to test the MTRSA in current environments. The multiple transmission rules of SDN-FEs are installed via Floodlight. They create multicast group information in a group table and create multicast, multi-physical port mapping. MTRSA operates at the top of Floodlight. The total bandwidth use during playback is

shown in Figure 2.1. They average the use of bandwidth every 40 seconds. Results show that MTRSA bandwidth is 35% and 46% less than SPT or ST, respectively. SDN Multicast Traffic Engineering will also be supported by MTRSA. Finally, since MTRSA's tree is not constrained by delays, the authors conclude that they expanded it to enable QoS multiple transmissions in future investigations.

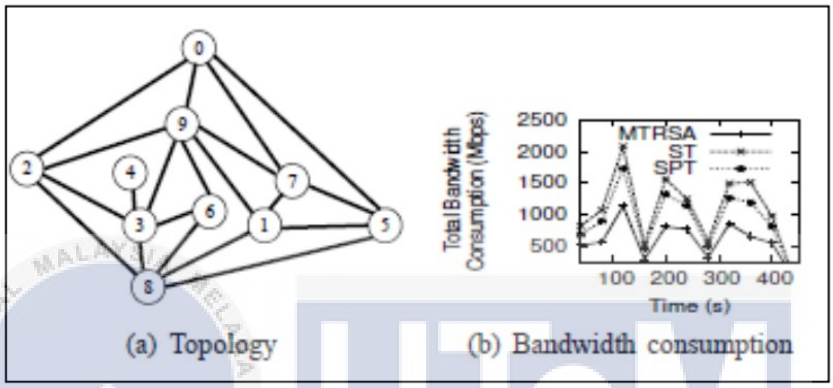


Figure 2.1: SDN Experimental Implementation Results. (Huang L. *et al*., 2016)

According to this article discussed by (Choi, J., Reaz, A. S., and Mukherjee, B., 2012). This paper explores provider's way to save multicast streaming systems with bandwidth and video-on-demand (VoD). The author also addresses streaming methods for saving bandwidth, including encoding, patching, batching, mixing, information user interface and multicast streaming method. The author observes and compare the multicast streaming technology for each device. They also analyze the main technology of multi-cast streaming, which is a hybrid architecture that uses multiple multi-cast streaming methods to enhance performance. The authors then study the capacity of these interactive VCR streaming technologies. In continuous VCR operations, it identifies VCR interactivity and sets scales for multiple streaming schemes. In addition, various multicast streaming schemes have been checked with the VCR support instruments. The authors conclude

that they are also exploring a variety of ways to boost resource performance, for example by reducing the bandwidth for Multicast streaming systems.

Multicast streaming offers a one-to-one content infrastructure to guarantee satisfactory data quality. Although multi-cast streaming demand is progressively increasing, bandwidth demand is also increasing. To maintain the quality of service for the expected bandwidth is challengeable. A solution incorporating SDN, CDR and PIM technologies is offered in this previous article (Yen, L. *et al*. 2018). The preliminary assessment performance results are presented. The following factors make the provision of a multi-cast service for a wide geographic area difficult. A network area managed by a unique SDN controller or SDN domain is a restricted element physically. The wide network is commonly divided to different management or policy consideration of SDN domain. For the single multi-cast service, therefore, a frame between SDN domains in an extensive range would be attractive. Next, SDN is not ready for all network domain. The backwards compatible system is needed for network domain of SDN and non-SDN to provide a multicast service. The authors take the SDN and non-SDN network fields on Kuang-Fu campus and Boai campus at NCTU in Hsinchu. They take out 4 different types of the multicast structure such as intra-domain, inter-domain (intra-campus), inter-campus multicast and internet multicast as shown as in Table 2.2. Finally, the authors conclude that SDN technology helps to control the growth of dynamic bandwidth and multicast trees. To enables the fast architecture of CORD fabric and versatile sharing of information between differently SDN domains. By using Protocol Independent Multicast (PIM), the conventional IS network can be connected. The CORD overlay segment and PSM would be introduced in future, as well as could be used in CORD operations.

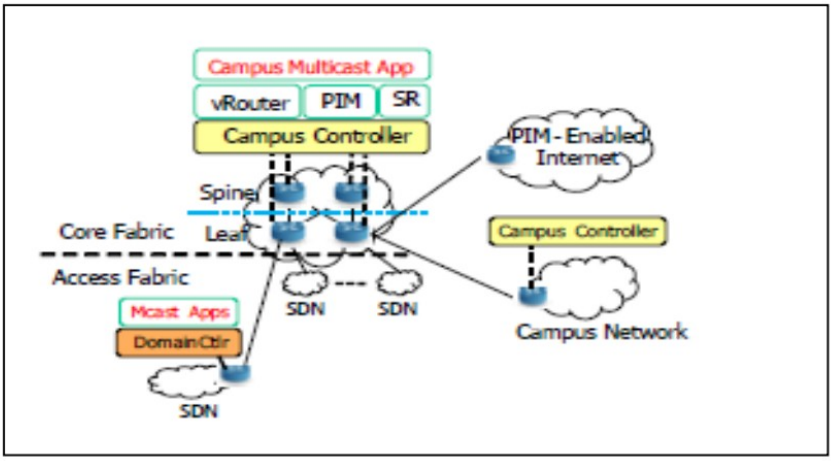


Figure 2.2: The Campus Network Architecture of NCT. (Yen, L. *et al*., 2018)

Table 2.1: Comparison between Different Types of Multicast. (Yen, L. *et al*., 2018)

Types of multicast	Relative Locations (Source and Client)	Methods
Intra-domain	The client and source in the same SDN domain.	SDN based and conventional multicast L2 solutions for the network SDN and non-SDN.
Intra-campus	The client and source in dissimilar SDN domain but the same campus network.	Central Office Re-Architected as a data center (CORD) by using leaf-spine switching architecture with virtual router (vRouter).
Inter-campus	The client and source in dissimilar campus network.	Central Office Re-Architected as a data center (CORD) by using leaf-spine switching architecture with virtual router (vRouter).

Internet multicast	The client is in campus network and the source is at outside.	Protocol Independent Multicast (PIM) offering conventional IP network with backward compatible.

Table 2.2: The Diversity of Utilization in Multicasting

Author	Study Aim	Method/Solution
Huang, L. *et al*., (2016)	Minimize the total bandwidth cost.	Using SMTE (Scalable Multicast Traffic Engineering) formula and MTRSA (Multi-Tree Routing State Assignment) altgorithm.
Choi, J., Reaz, A. S., and Mukherjee, B., (2012)	Video-on-demand (VoD)	Video streaming on VoD and reducing the usage of bandwidth usage.
Yen, L. *et al.*, (2018)	SDN technology helps to control dynamic bandwidth and multicast tree development.	To integrates the technologies of SDN, CORD and PIM.

2.3 The difference of Multicast Routing Protocol

The effective multicast routing protocol ad-hoc configuration, this article (Vodnala, D., Phani, S., and Auvala, S., 2014) also includes main issues like constant updating delivery paths, the dynamic membership of the group and little information from the state. Five features that should have a good multicast routing protocol are analyzed by the author. Efficiency, overhead control,

service quality, unicast routing protocol dependence and resource management are included. In order to view its scalable performance difference, they were also classified into four kinds of topology, like Tree Based, Mesh Based, Hybrid Based and Zone Based. These protocols must be drawn up and the very short operating mechanisms discussed. The authors also conclude that no protocol has been developed to solve all ad-hoc network problems. There are also possible problems with the multi-routing protocol, which will optimize protocols for efficient multi-casting in the future.

Protocol	Multicast Topology	Loop Free	Dependence on Unicast Protocol	QoS Support	Perio -dic Msg
MAODV	Tree	Y	Yes	No	Yes
PIM	Tree	Y	No	No	Yes
MOSPF	Tree	Y	Yes	No	Yes
AMRIS	Tree	Y	No	No	Yes
ODMRP	Mesh	Y	No	No	Yes
PUMA	Mesh	Y	Yes	No	Yes
CAMP	Mesh	Y	Yes	No	Yes
EIGRP	Hybrid	Y	Yes	Yes	Yes
AMRoute	Hybrid	N	Yes	No	Yes
MCEDAR	Hybrid	Y	Yes	Yes	Yes
HARP	Zone	Y	Yes	Yes	Yes
ZRP	Zone	Y	No	Yes	Yes
ZHLS	Zone	Y	Yes	No	Yes
RSGM	Zone	Y	No	Yes	Yes
MZRP	Zone	Y	No	Yes	Yes

Table 2.3: Comparison of Multicast Routing Protocols. (Vodnala, D., Phani, S., and Auvala, S., 2014)

Next paper recommended by (Fan, Y. and Li-Zhen, Z., 2017) that addresses IP protocols for multicasting. Therefore, because of the lack of a practical Network Engineering program, IP Multicasting Technology is identified as part of research based on a simulation approach for the eNSP Network to implement IP Multicasting Framework in conjunction with protocols of IGMP, PIM-SM, and OSPF into the topology.

Another article by (Oliveira, P., Silva, A., and Valadas, R., 2016) proposes multicast routing protocol which is considered as hard-state to the PIM-DM, (HPIM-DM). The author states the HPIM-DM solves a range of PIM-DM problems, which leads to a weak integration and makes PIM-DM unsuitable for high-speed networks. The concept of upstream neighbors, i.e. neighbors capable of supplying multi-cast traffic from the source, mechanisms ensuring reliable messages transmission and sequences and a synchronizing process allowing the router to join in the network to receive immediate information on active multi-cast tree systems have made these improvements possible. Thus, no periodic control messages need to be transmitted (for state update) and the protocol immediately reacts to events that change the multicast tree configuration. Furthermore, the protocol has been optimized to resist repetition attacks. HPIM-DM's accuracy was evaluated with logical justification and model controls. In Python, the author also performs entirely HPIM-DM and conducts extensive tests to verify that the protocol is correct.

This paper describes the performance assessment of the two-multicast protocol: the PIM-SMv4 and the PIM-SMv6 based on QoS methodologies, such as throughput, jitter, datagram loss and the collected data, according to this article (Chihab, S. S., and Mohamed, I. J. 2017). The author used the GNS3 simulator and JPERF to evaluate this performance. In addition, reports from several IPv4 and IPv6 PIM-SM-performance studies have shown PIM-SMv6 to be highly effective in comparison to PIM-SMv4. The data collected for PIM-SMv6 is much more than PIM-SMv4. The

IPv4 jitter is higher than IPv6. The loss of IPv6 datagram is less than the loss of IPv4. Measurement of both protocols based on UDP traffic. Figure 2.3 shows the IPv6/IPv4 multicast network topology performance.

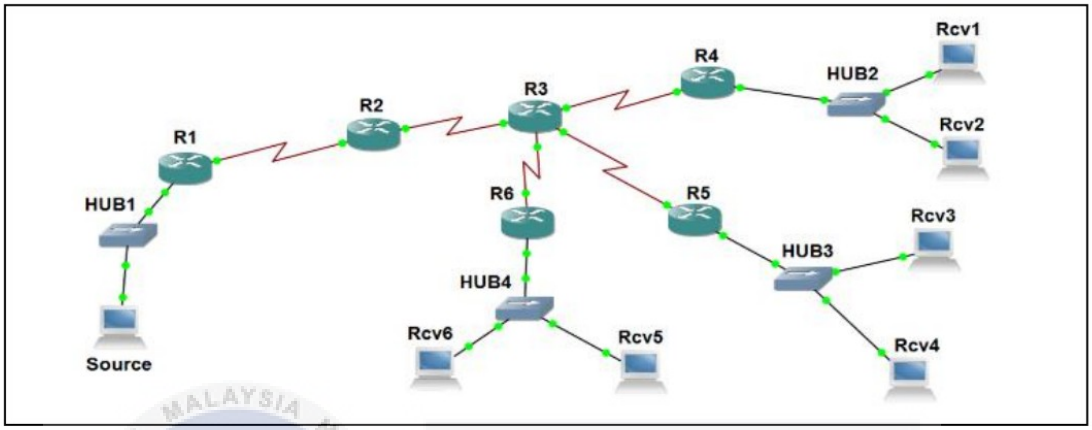


Figure 2.3: IPv6/IPv4 Multicast Network Topology Performance. (Shihab, S. S., and Mohamed, I. J., 2017)

However, this article proposed by (Ko, J., Park, S., and Lee, E., 2010) addressed how the PIM-Sparse Mode protocol proposed to be extended would be to help eliminate excessive PIM-SM protocol processes. These approaches are also used for transportation of multi-cast packets directly to the SPT without having to use the RPT in an IPTV service environment in real time and the RPT (RP Tree) to SPT (Shortest Path Tree) switching. A simulation is used to validate the proposed expanded PIM-SM Protocol. The results from the simulation, the recently developed protocol of PIM-SM that can decrease the use of RPs in IPTV services compared to conventional PIM-SM protocol. As well as, since the RP router presumed to be Edge-routers, the suggested enlarged protocol of PIM- SM is expected to be used with different access network architectures. For an integrated solution, processing time and delay in a similar network with real-network are required for the suggested extended the protocol of PIM-SM. Currently, time delay is a matter of

considerable importance. The Figure 2.4 shows the simulation of network configuration by using OPNET Modeler and Figure 2.5 shows the blue solid line speeds up since the RP has to reveal multicast packets data and change per subscriber demand of RPT to SPT while the red solid line decreasingly since the RP use the improved protocol of PIM-SM.

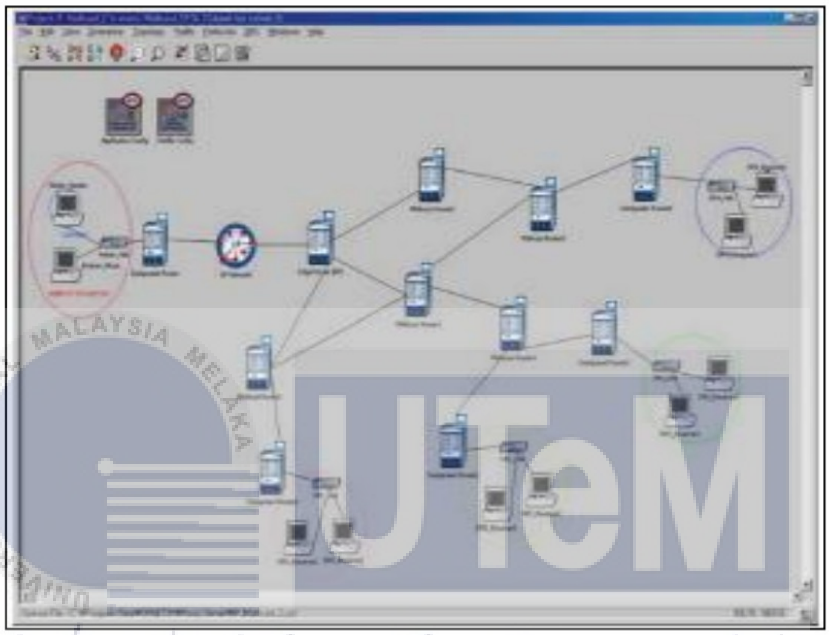


Figure 2.4: The Network Configuration by using OPNET Modeler. (Ko, J., Park, S., and Lee, E., 2010)

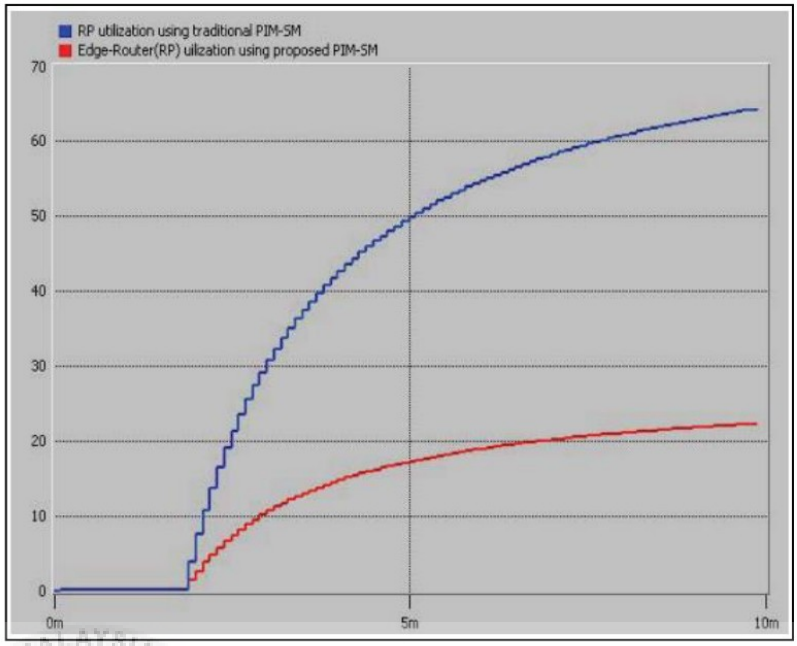


Figure 2.5: The usage of RP for The Conventional of PIM-SM and The Extended of PIM-SM. (Ko, J., Park, S., and Lee, E., 2010)

Other than that, the article discussed by (Papan, J. *et al*., 2016). They presented the new mechanism of IPFRR using the typical multicast protocol which is PIM-SM. The IPFRR PIM-SM as mentioned is intended to keep specified unicast data flows. The main idea of IPFRR PIM-SM is from a specific RP router that use IPFRR terminology. They can create an alternative disjoint path by optimizing the position of RP and D routers on PIM-SM, which is useful for restoring affected contact after failure detection. There are two operational modes in the proposed PIM-SM IPFRR mechanism. Second, the first contents impacted communications, which means they use the tunnel to establish alternate disjoint route, after failure detection with the new IP header. This method is also employed using common tunneling technology in the existing mechanism of IPFRR. The second approach developed for the new IPFRR PIM-SM is a packet destination IP adjustment and router D in conversion table to make sure the packets must be restored correctly to the place of origin. This mechanism has the major benefit of not encapsulating additional headers for involved

packets because of a default. However, the MTU has not been reduced in the comparison of the first method and other existed mechanism of IPFRR. Figure 2.6 shows the new PM-SM for mechanism of IPFRR.

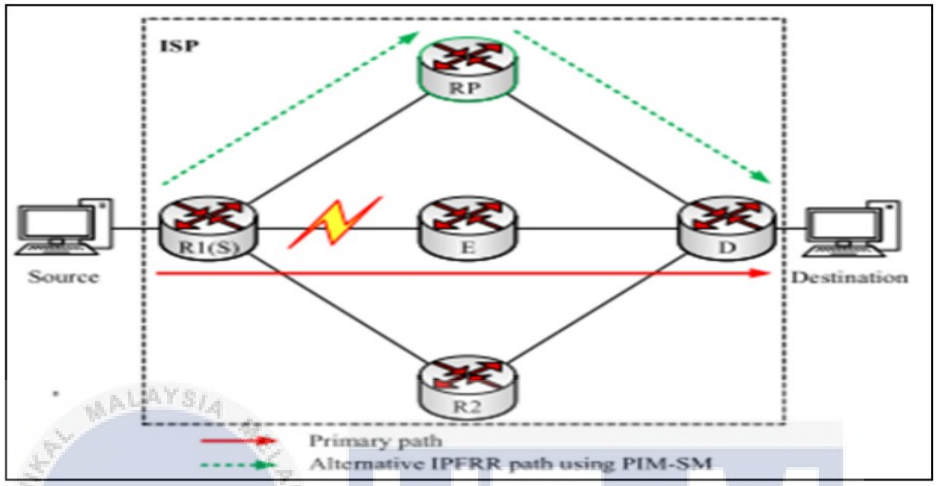


Figure 2.6: The IPFRR Mechanism with The New of PIM-SM. (Papan, J. *et al.*, 2016)

Table 2.4: The Difference of Multicast Protocol

Author	Protocol	Study Aim
Vodnala, D., Phani, S., and Auvala, S., (2014)	MAODV, PIM,MOSPF, AMRIS, ODMRP, PUMA, CAMP,EIGRP, AMRoute, MCEDAR, HARP, ZRP, ZHLS, RSGM, MZRP	Development of ad-hoc networks using multicast routing protocol.
Fan, Y., and Li-Zhen, Z., (2017)	IGMP, PIM-SM, OSPF protocols	Streaming video
Oliveira, P., Silva, A., and Valadas, R., (2016)	Hard-state Protocol Independent Multicast -	To resolved a selection of PIM-DM issues, resulting

	Dense Mode (HPIM-DM)	in weak integration and rendering PIM-DM unappropriated for high-speed networks.
Shihab, S. S., and Mohamed, I. J., (2017)	PIM-SMv4 and the PIM-SMv6	Used the GNS3 simulator and JPERF to evaluate IPv6/IPv4 in multicast network performance.
Ko, J., Park, S., and Lee, E., (2010)	Extended protocol PIM-Sparse Mode	To eliminate excessive the conventional PIM-SM protocol processes.
Papan, J. *et al*., (2016)	PIM-SM	To keep the specified unicast data flow of the IPFRR technology.

2.4 Campus Network

According to (Zhao, Q., and Ding, G. Z., 2017), the author concise an overview of the 'Triple Play" framework in the development of telecommunication technology. The triple play is including radio network, television network and computer network. It can be beneficial in the future network platform in terms of exchanging resources, prevent the overlapping architecture, reduce the usage of bandwidth and so on. But there is a considerable need to be integrate between the potential growth of the university campus network with the current situation of continual reform, modification, and enhancement. However, the author has described with some characteristics to make the network campus be more efficient. There is system of wireless telephone, service systems of mobile video, and scalability framework of data center. Figure 2.7 shows the logic diagram of university campus network.

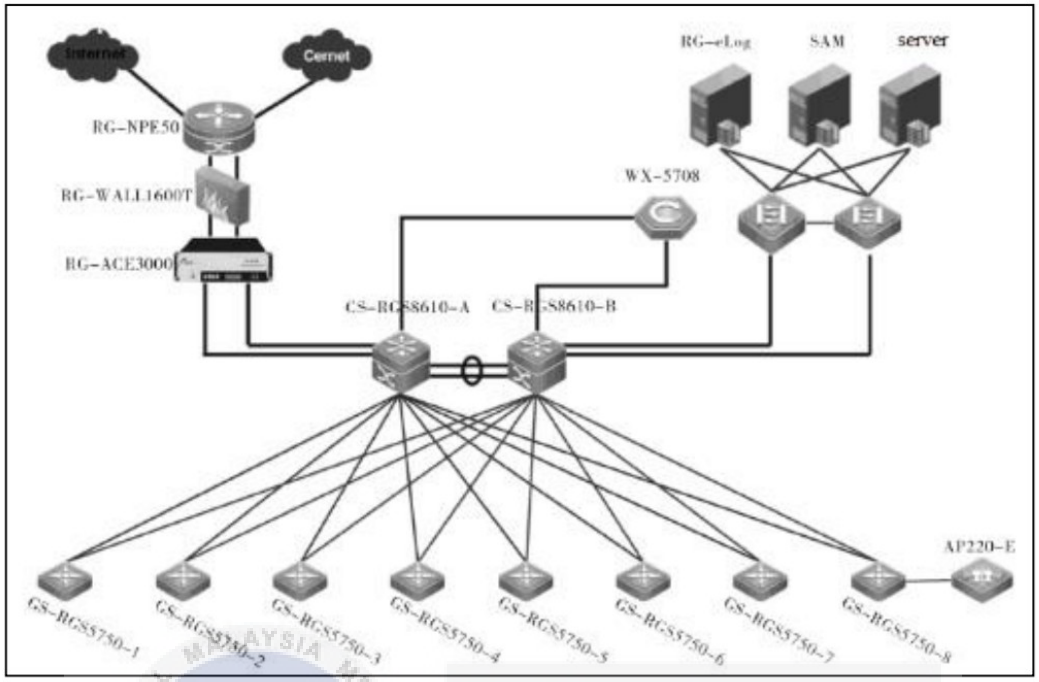


Figure 2.7: Backbone Logic Diagram of University Campus Network. (Zhao, Q., and Ding, G. Z., 2017)

In short, a united log storage infrastructure can be installed into the college campus network by selecting an integrated technological scheme. This article proposed by (Zhou, D., 2017) that discussed about the necessary of research on log collection and analysis for operation and maintenance, safety management of campus network. The author reviews the source analysis of campus network log in campus infrastructure, source of network log, network equipment, system log and application service log. Then, they identify the technologies of log collection. The processing of logs relies on the technology and facilities of the campus network. Standard equipment can enforce the log record program, which ensures that the log can be documented as needed. The protocol of log source includes Syslog, SNMP (Simple Network Management Protocol) and Windows log files. After that, for log storage includes file format storage, database

mode storage, Hadoop storage and elasticsearch storage. For the technologies of log analysis, they use traditional single-machine log analysis and large-scale distributed log analysis.

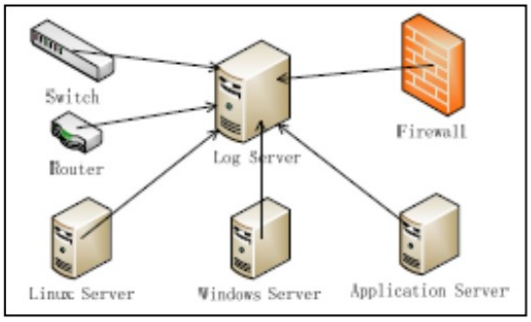


Figure 2.8: Distributed Deployment of Log Collection. (Zhou, D., 2017)

Then, move to this journal by (Ma, H., Lv, G., and Wu, C., 2018) that provides an overview of the architecture of campus network and the network construction process diagram. This journal addressed the purpose of campus network design, network technology selection, network equipment selection, etc. They therefore explain how to prepare for the development of the campus network effectively and securely. The author said that the hierarchical model will be implemented in the design of the network. As the building has 6 levels, the center room could be placed at the training building, for example from two to five floors on a layer depending on the distribution of the buildings between the schools. Most of the systems have a central fiber switch. The campus building needs to support long-distance single mode and multi-mode fiber transmission that uses 1000 BASE-LX to connect each cable from one floor to the next. The Gigabit Ethernet switching network uses the campus network. The main switch and secondary switches should be configured. For every switch can support the expansion ports of fiber with extension module of slots. After that, campus network can support the Gigabit, quick on-site sharing, can provide fast and seamless protection for all users while at the same time requesting for services, play the full role of

multimedia school teaching, while also ensuring that all users and a campus network operate more smoothly. However, the network center configures 2 dedicated servers, which are network device and switch, to process the application server and web server. The backbone of the campus network with WLAN and Wi-Fi is the form of the network center. Finally, the author conclude that the concept of network design involves the design of the network and construction of the campus network, maintenance and campus security, campus resources and the efficient operation of the campus network and other three connections.

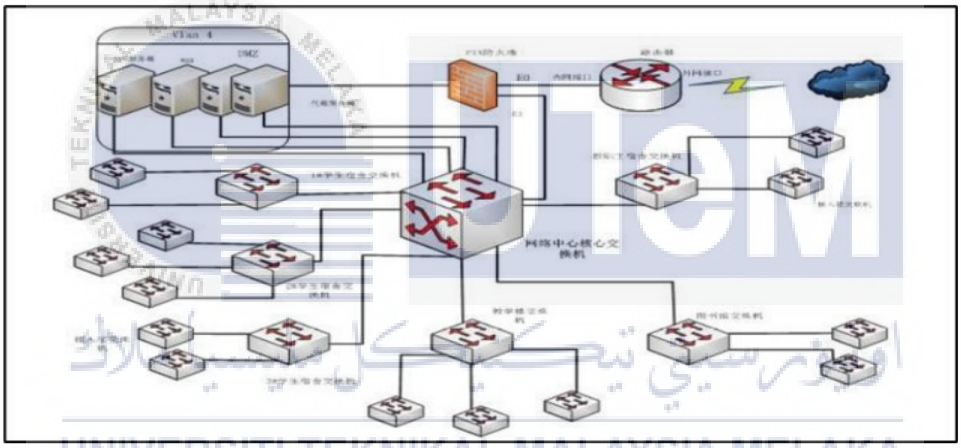


Figure 2.9: Topology of Campus Network. (Ma, H., Lv, G., and Wu, C., 2018)

After that, this article proposed by (Yu, Z., Xu, X., and Wu, X., 2010) discussed the implementation and architecture of wireless mesh network in the campus network. However, in the field of education, wireless network has been widely used, playing an increasingly important role in education. One of the main innovations of the digital campus is the wireless campus network. With the continuing improvement of the protocol standards in the wireless network and the cost performance ratio improving the products in recent years, the wireless mesh network has rapidly been deployed on campus and has an increasingly important role on campus. This architecture will

have the greatest advantage if the data will automatically be re-enrolled to a neighboring node with smaller communication traffic for transmission by the nearest AP because of heavy network traffic congestion. As well as, according to network conditions, data packets can also carry on to the nearest node until they reach the end destination. This method of this access is multi-hop access. Figure 2.10 shows the architecture of mesh terminal and router.

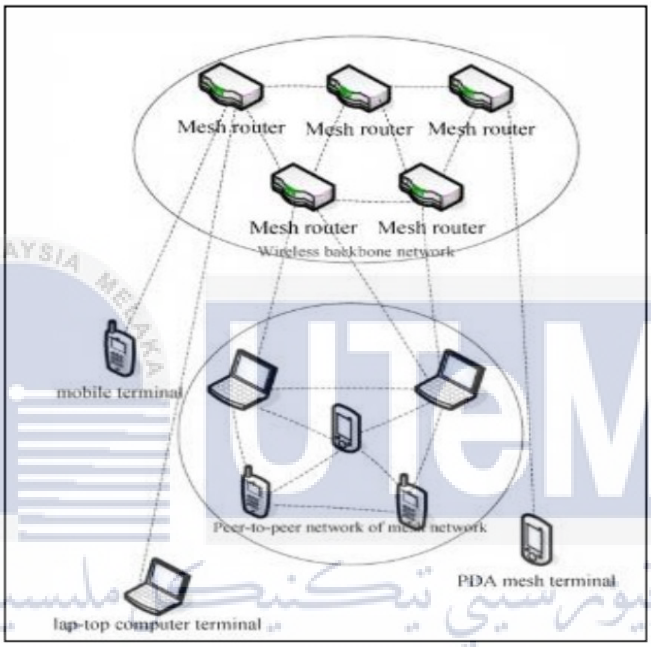


Figure 2.10: Mesh Terminal and Routers of the Networking Systems. (Yu, Z., Xu, X., and Wu, X., 2010).

Table 2.5: The comparison of Campus Network

Author	Study Aim	Method/Solution
Zhao, Q., and Ding, G. Z., (2017)	To build an efficient of university campus network.	Suggested Triple Play framework.
Zhou, D., (2017)	Research on log collection and analysis for operation and maintanance, safety management of campus network.	Syslog, SNMP (Simple Network Management Protocol and Windows log files.
Ma, H., Lv, G., and Wu, C., (2018)	The purpose of campus network design, network technology and equipment selection.	1000 BASE-LX and Gigabit Ethernet. (Network device and Switch)
Yu, Z., Xu, X., and Wu, X., (2010).	To improve the application of wireless in education.	Wireless Mesh Network.

2.5 Huawei eNSP Network Simulation

According an article proposed by (Fan, Y., and Li-Zhen, Z., 2017) discussed about the normal operation of the device can simulate the servers to the receivers and able to check all forms of multicast packets data on the network simulator in terms of their fundamental qualities. The test results have checked the accuracy of the functionality on this technique. During this project, the author describes the fundamental principle of multicasting innovation IP, combined with network engineering operations, which advances the basic structure of the IP scenario. Therefore, the

possible links between the transmissions of data between the IP multicasting networks can be evaluated and tested in order to acknowledge the operating simulation below the eNSP Network structure scenario, which can validate further the transmission by the IP multicasting packet as well. Multicasting of sources of information and other forms of daily data. This approach and this case can therefore be used as a guideline for students in network engineering learning research to better understand multicast technology and to use multicast IP addresses in operation.

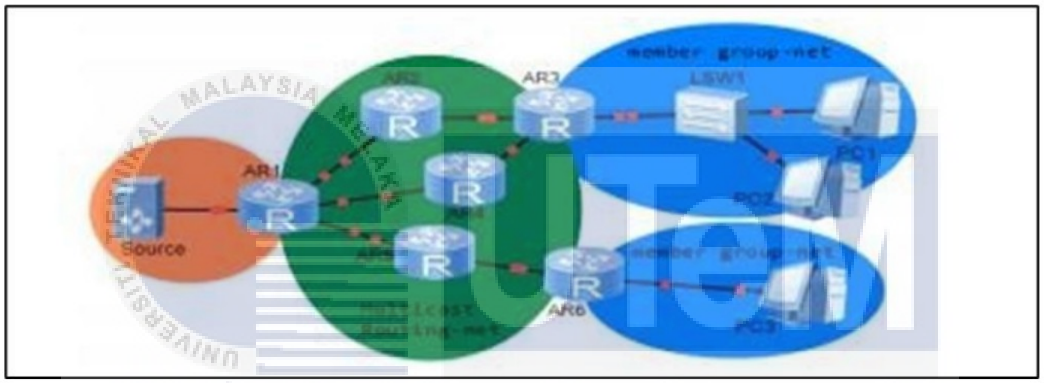


Figure 2.11: Network Topology with IP Multicasting Implementation. (Fan, Y., and Li-Zhen, Z., 2017)

Next, this journal proposed by (Chen, J. *et al.*, 2019) discussed about the WLAN experimental design by using the eNSP software, development of an exploratory environment, configuration of AC and AP network interconnection, and allows mobile clients to navigate the wireless signal in the area coverage. Simultaneously, they utilize Wireshark software to capture data packets, evaluate the configuration protocol and principle of wireless access point control, and demonstrate the wireless terminal roaming process. For this experiment simulation, the students

can understand the basic WLAN principles and the process of Establishment CAPWAP Session, disciple the AC method configuration and the simple WLAN switched, and able to understand the mobile clients roaming status. They have prepared the education and staff department for AP AP2050 and management for AC AC6005. The two of APs are added to the switch S3700 access layer and connected to the switch S5700 convergence layer. The same VLAN and the mobile clients roaming access must be realized to connect to the wireless access point. It is necessary to set up topology of network, AC configuration, switch convergence layer configuration and switch access layer configuration, and allocate the DHCP with AP address for the navigation of mobile clients and different Aps switches. Figure 2.12 shows the topology of WLAN network and Table 2.6 shows the equipment address.

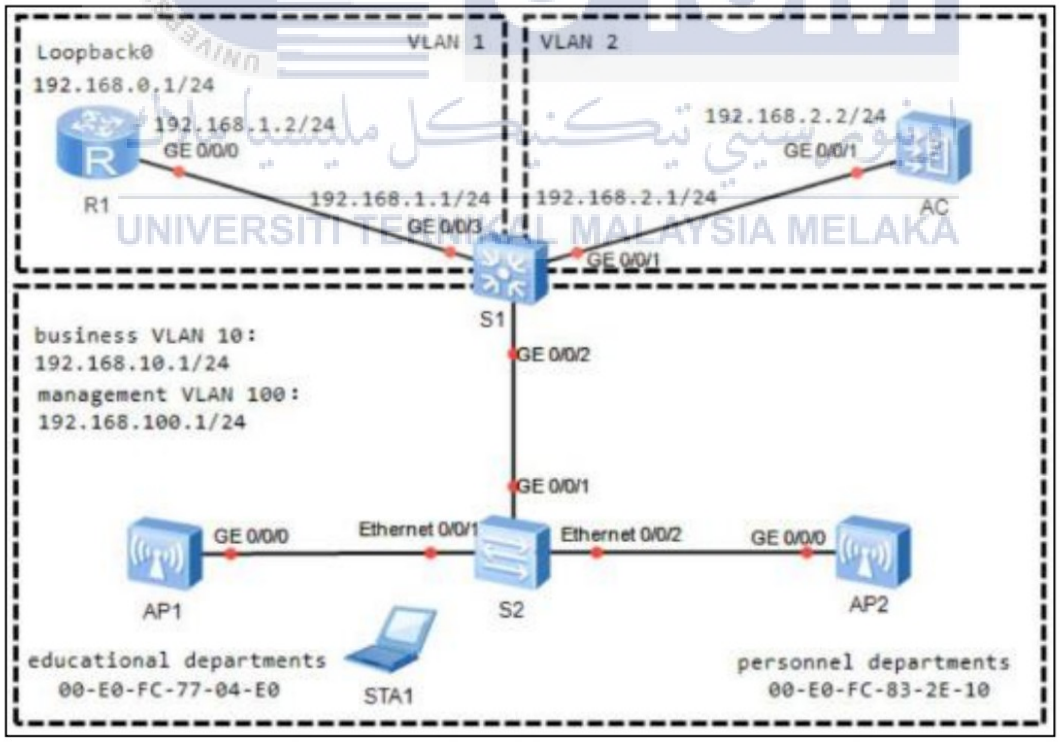


Figure 2.12: WLAN Topology. (Chen, J. *et al.*, 2019)

Table 2.6: The Equipment Address. (Chen, J. *et al*., 2019)

Equipment	Interface /VLAN	IP address	Subnet mask
S1(S5700)	GE0/0/1, VLAN 2	192.168.2.1	255.255.255.0
	GE0/0/2, VLAN 10	192.168.10.1	255.255.255.0
	GE0/0/3, VLAN 1	192.168.1.1	255.255.255.0
	VLAN100	192.168.100.1	255.255.255.0
AC1(AC6005)	GE0/0/1, VLAN 2	192.168.2.2	255.255.255.0
R1(AR1220)	GE0/0/0, VLAN 1	192.168.1.2	255.255.255.0
	Loopback0	192.168.0.1	255.255.255.0

This article presented by (Zhang, Y., and Wang, Q., 2017) states that eNSP and Cisco Packet Tracer can be used for the design of experiment simulation and computer network. The authors address the implementation of experiment simulation for the data communication Curriculum and the computer networks. It is frequently used by users for education motive. The network simulators are easily to use and fast to understand. A simple network simulation with devices almost identical to the real hardware is eNSP and Cisco Packet Tracer. This helps them to simulate and build a topology network and to apply it to hardware equipment. The author also performs a research project on data communication, computing, and computer networking.

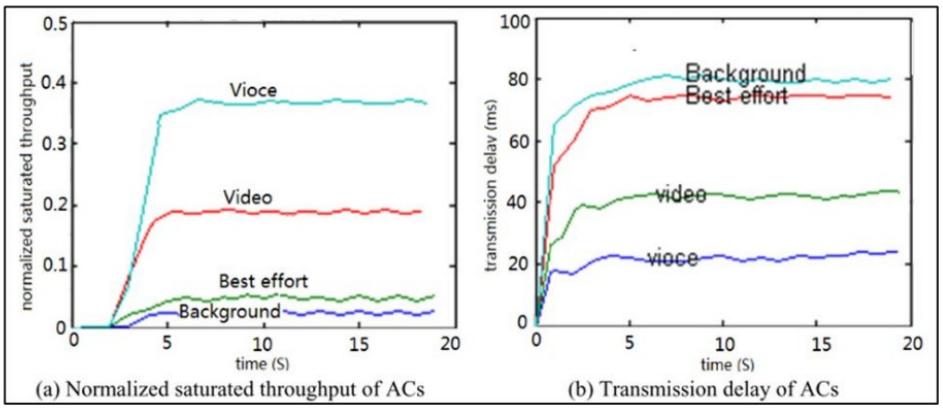


Figure 2.13: Performance of EDCA Simulation Experiment Analysis Results. (Zhang, Y., and Wang, Q., 2017)

According an article proposed by (Suntu, S. L., 2017) discussed the simulation tools such as the Enterprise Network Simulation Platform (eNSP) and Cisco Packet Tracer are widely used in networking field. After that, this can also implement in the network topology virtual environment design, efficiency, and security to conform to the actual hardware. To test the efficiency regarding to nearby customer roaming transmission, the simulation can be performed based on the MAC layer. The OMNet++ use multiple access point to obtain the roles transfer latency between the session keys transmission and the access points to enable Aps credential extraction.

Table 2.7: The Difference Usage of Huawei eNSP

Author	Study Aim	Method/Solution
Fan, Y., and Li-Zhen, Z., (2017)	To simulate behavior ordinary system between the receivers, and multicast servers and study the basic multicasting packets basic qualities on the network simulation.	Huawei eNSP
Chen, J. *et al*., (2019)	To build the WLAN experimental scheme on the eNSP simulation platform, create an experimental environment, recognize network interconnection by AC and AP configuration, and enable mobile clientss to access the wireless signal	Huawei eNSP and Wireshark.

	of area coverage.	
Zhang, Y., and Wang, Q., (2017)	Developing simulation projects for the data processing and computer networking curriculum.	Huawei eNSP and Cisco Packet Tracer.
Suntu, S. L., (2017)	To check the efficiency of simulation on the MAC layer regarding the switch to a nearby roaming customer.	Huawei eNSP and Cisco Packet Tracer.

2.6 Wireshark Network Analyzer

The composition and role of Wireshark and the design and development method for Wireshark analysis parsers is described in this article (CUI, X., and SHEN, Q., 2018). The Wireshark structure consists of GTK 1/2, with the graphical window tool that controls all user interfaces and outputs, Epan, where the Wireshark Protocol Analyzer is located, Capture in which the packet capture engine is based on the underlying library of Winpcap / libpcap and Where the wiretap The author resumes the parsing principle of a protocol that sends protocol data back to the bottom, based on the OSI model of seven-layer protocols and reverses protocol parsing, which requires bottom-up. Wireshark analyzes a log tree to analyze packet data. First, after a protocol identifies a network layer, Wireshark reduces the group packet and then removes the network laying protocol header and provides analysis of the data inside the transport layer. The framework layer

was included. They also briefly develop protocol parsing, in which two ways can be implemented: integrated and plugin, to incorporate a Wireshark protocol parser. The plug-in form is a plug-in recorded in the main system of parsing (for example, shared library (DLL)). The built-in form consists of a browser module compiled in the main program that is always open. The results of the parsing are shown in Figure 2.14, which confirms the success of the foo protocol parser and can be scanned accordingly. In order to obtain accurate protocol package information, a more detailed and accurate work and implementation can be done.

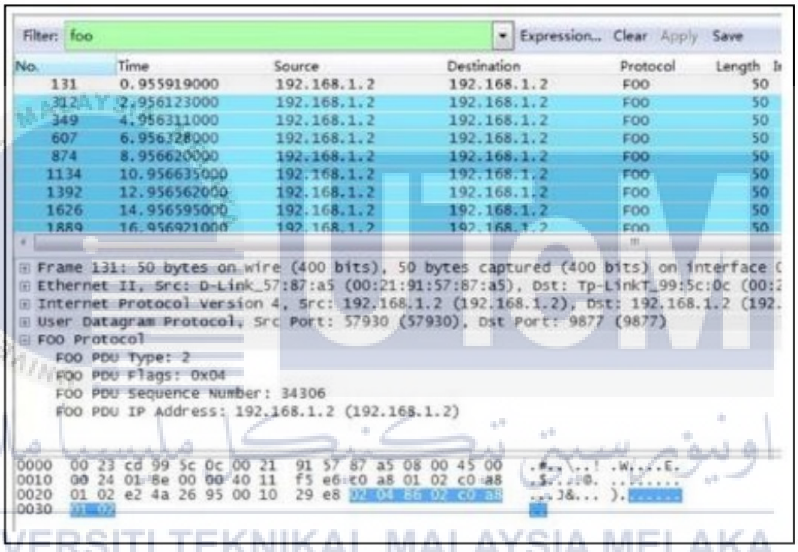


Figure 2.14: Result diagram of Protocol Analysis. (CUI, X., and SHEN, Q., 2018)

In this article, the improvement of the Wireshark capacity as a tool to detect intrusions in Denial of Service (DoS) attacks is discussed (Pavithirakini, S. *et al*. 2016). The author identifies certain problems which Wireshark is not a system of intrusion. In reality, Wireshark can help you understand what works when weird things happen. Wireshark will not control anything in the network. Components are the calculation. Wireshark does not send or run any network packets.

Wireshark is not in support of centralized and long-term monitoring systems. Instead, when using the trackback feature, Wireshark method. Managing the network is very helpful. The attacker also uses a variety of techniques to hide his true identity. Steppingstones intermediate host for a zombie machine used commonly for DoS attacks between attackers as shown as in Figure 2.15. The new Wireshark 2.0 version is only tested if IP packets enter the network. It does not involve network protection. This is a major drawback for Wireshark when an attacker enters the network. In this article, therefore, the mechanism of traceback was added. The network is secured by this mechanism. For hacking, most attackers have used the spoofed IP address. If the Wireshark is attached to a traceback mechanism, it will identify the address of the true source packets causing the attack. With a single packet, Traceback will track the attacker. They implement the logging classification in Wireshark tool; the ICMP-trackback and the packet marking algorithms. Use Logging to begin tracking packets when you click on this button in the Wireshark tool. The attacker's path is determined by the packet crossing during the attack time. When the packet takes time to get not all packets, ICMP is implemented as an add-on option in Wireshark. Generate if the packet is from the same location where a message is delivered to the packet destination. The instruction of the attack is reconstructed. Wireshark used the Algorithm labeling packet, marks packets at time and is a single ID for a specific destination. This makes Wireshark take this as their priorities Wireshark acts like the mechanism for protection against intrusion.

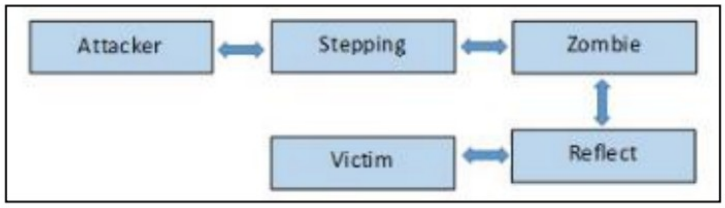


Figure 2.15: Process of Attacks. (Pavithirakini, S. *et al*., 2016)

This journal proposed by (Musa, A. *et al.*, 2019) that discussed an analysis network security of peer-to-peer using Wireshark. In order to prevent future threats for the network peer-to- peer, the author suggested some strategy to improve the network security of peer-to-peer by using simulation based experimental studies and the current methodology. They have set up an experiment to use the BitTorrent and Wireshark of uTorrent application to show how a packet sniffing device can track a P2P. UTorrent is an application for the BitTorrent system. It is one of BitTorrent's most common and classic examples. This allow to connect with another Bittorent customers, files exchange with another active peers and any peer who would like to upload a file must be the same as BitTorrent. The implementation is involved the DHT (distributed hash table) as part of the standard client functionality of uTorrent. DHT allows several of active peers to be managed by using the relevant file and each client. Lastly, for pattern recognition and further analysis can be used the results of captured data files. Some network security measures the needed due to the sensitivity of the data shared via the P2P network in an extremely responsive to the network environment. Figure 2.17 shows the process flow chart and the data recording processes for their proposed experimental setup.

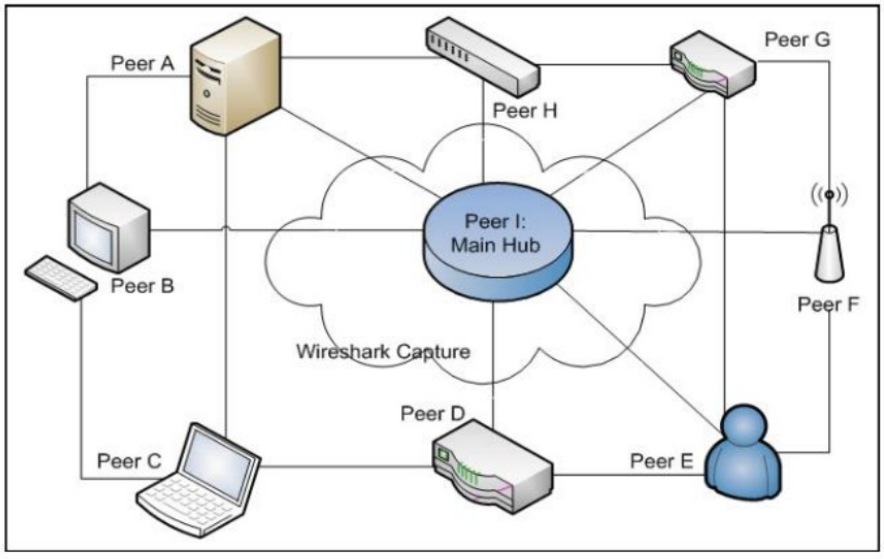


Figure 2.16: Peer-To-Peer Security Diagram. (Musa, A. *et al*., 2019)

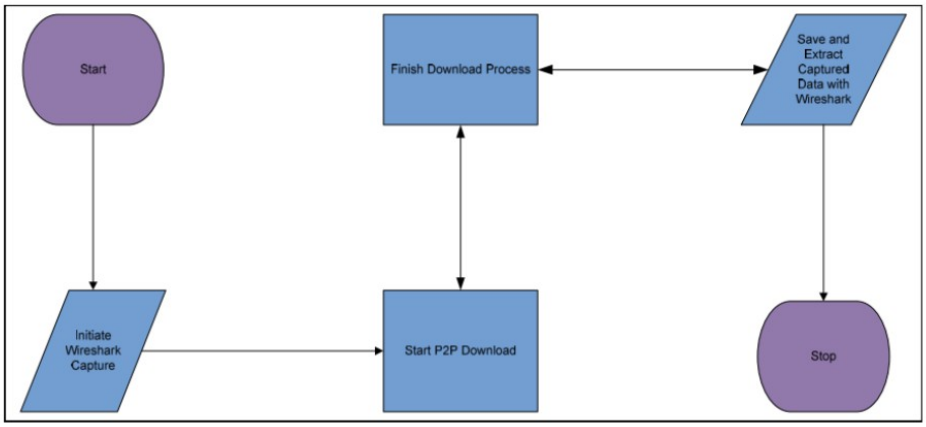


Figure 2.17: Flowchart of Capture P2P Data by Wireshark. (Musa, A. *et al*., 2019)

After that, following with this article proposed by (Kim, H., Lee, H., and Lim, H., 2020). In this article, the author compared the packets were collected and analyzed using software (Wireshark) and hardware (Observer). In addition, they also compared and analyzed each packet collections using Wireshark, while the Observer need to check the performance of their work. In environments where large amounts of data are used, Viavi Corp. operates the Observer platform with greater efficiency than Wireshark. The Observer Analyzer can collect and record data for a lengthy time by using Viavi GigaStor to retrieve information from TCP's session such as HTTP's website, IM, FTP / Telnet and prevent the use of network forensics for encrypted packets, allowing the forensics to help Sarbanes Oxley or HIPPA requirements. Many mobile network managers use the benefits of free wires, scalability through plug-ins and almost any operating system. Figure 2.18 shows how the hardware of Viavi Corp. look like is.

Figure 2.18: Viavi Corp. Hardware as an Observer. (Kim, H., Lee, H., and Lim, H., 2020)

Table 2.8: The Comparison the Usage of Wireshark Software

Author	Study Aim	Method/Solution
CUI, X. and SHEN, Q., (2018)	To obtain accurate protocol package information, detailed and accurate work implementation.	Wireshark.
Pavithirakini, S. *et al*., (2016)	To improve the Wireshark capacity as a tool to detect intrusions in Denial of Service (DoS) attacks.	Wireshark used the Algorithm labeling packet, marks packets at time and is a single ID for a specific destination.
(Musa, A. *et al*., 2019)	To avoid any future threats in the peer to peer networks.	Wireshark.
Kim, H., Lee, H., and Lim, H., (2020)	To compare the packets data were collected and analyzed using software (Wireshark) and hardware (Observer).	Wireshark and Viavi Corp.

2.7 Summary of the Chapter 2

At the end of this chapter, twenty-one articles have been observed. We were acknowledged that there are so many methods and techniques can be exampled to be used in the implementation of this project Multicast Protocol Efficiency in a Campus Network Environment using eNSP. By studying this chapter, we have known that the use of multicast is significantly efficient compared to broadcast and unicast.

However, with multicast routing protocols, we can use to transmit audio and streaming video to the multiple users. In this project we will apply three multicast protocols such as Open Shortest Path First (OSPF), Internet Group Management Protocol (IGMP) and Protocol Independent Multicast-Dense Mode (PIM-DM) and Protocol Independent Multicast-Sparse Mode (PIM-SM) since they are very useful in the multicast network traffic. We will implement these multicast protocols to define the efficiency of video streaming in the campus network design.

Other than that, campus network is a wide network range. As stated in the 2.4 subtopic, there are have a lot of ways to improve the organization of the campus network. In this research, we will design the campus network in the simulation by using eNSP software. eNSP is a Huawei product software that can be used to create and construct network topology. From the previous researches, most of them used this software for education motive.

Nevertheless, Wireshark is one of the network protocol analyzers most widely implemented today. We can capture packet data in real time from our network and read the data that have been captured from the packet. For viewing the captured packets, only by click on the packet list pane that will show the selected packet in the tree view and byte view panes. This software can be run

on Windows and many other platforms, including IEEE 802.10, PPP, loopback, and captures the network traffic with an operating system capture library.

CHAPTER 3

METHODOLOGY

3.1 Introduction

In this section will be focused on the process and the design project of Multicast Protocol Efficiency in Campus Network Environment. The software required to develop routers, switches, and clients in this project design by using eNSP. Nevertheless, this project is not using any hardware implementation and it is including only on the simulation.

3.2 Progress of Projek Sarjana Muda 1 (PSM 1)

One of the compulsory subjects for second semester of the third year of study is Projek Sarjana Muda 1(PSM 1). This section shows the following flowchart regarding the circulation of Projek Sarjana Muda 1 (PSM 1). This flowchart as shown in Figure 3.1 comprises from to find the supervisor and co-supervisor, selection the PSM title project which is A Study of Multicast Protocol Efficiency in a Campus Network Environment, content of project report progression (Chapter 1, 2 and 3) and lastly the presentation of PSM 1 is done by live streaming session. All this progression happened as planned from week 1 to week 15 in the Gantt chart as shown in Table 3.1.

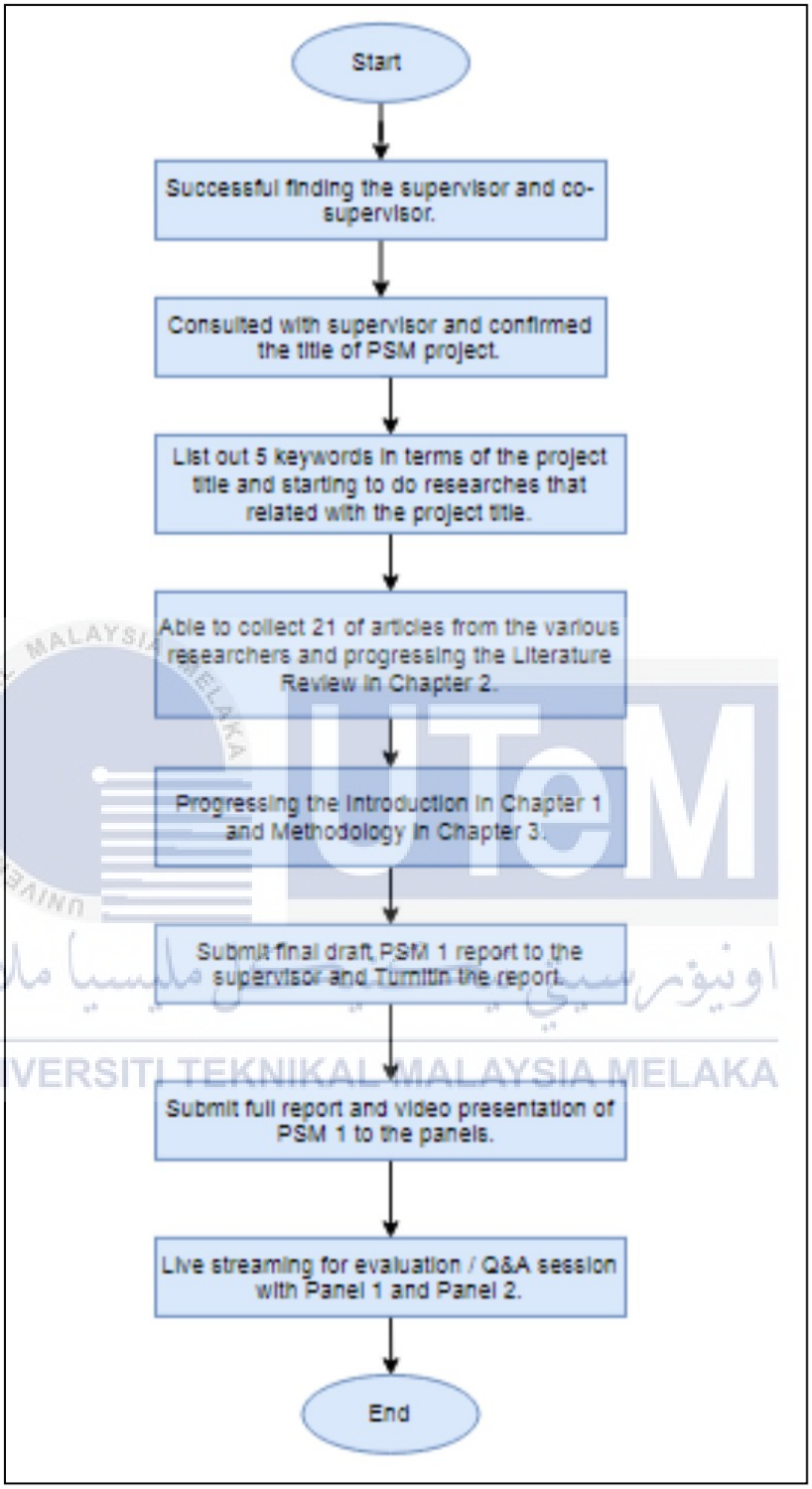


Figure 3.1: Flowchart of PSM 1 Progress

3.3 Gantt Chart

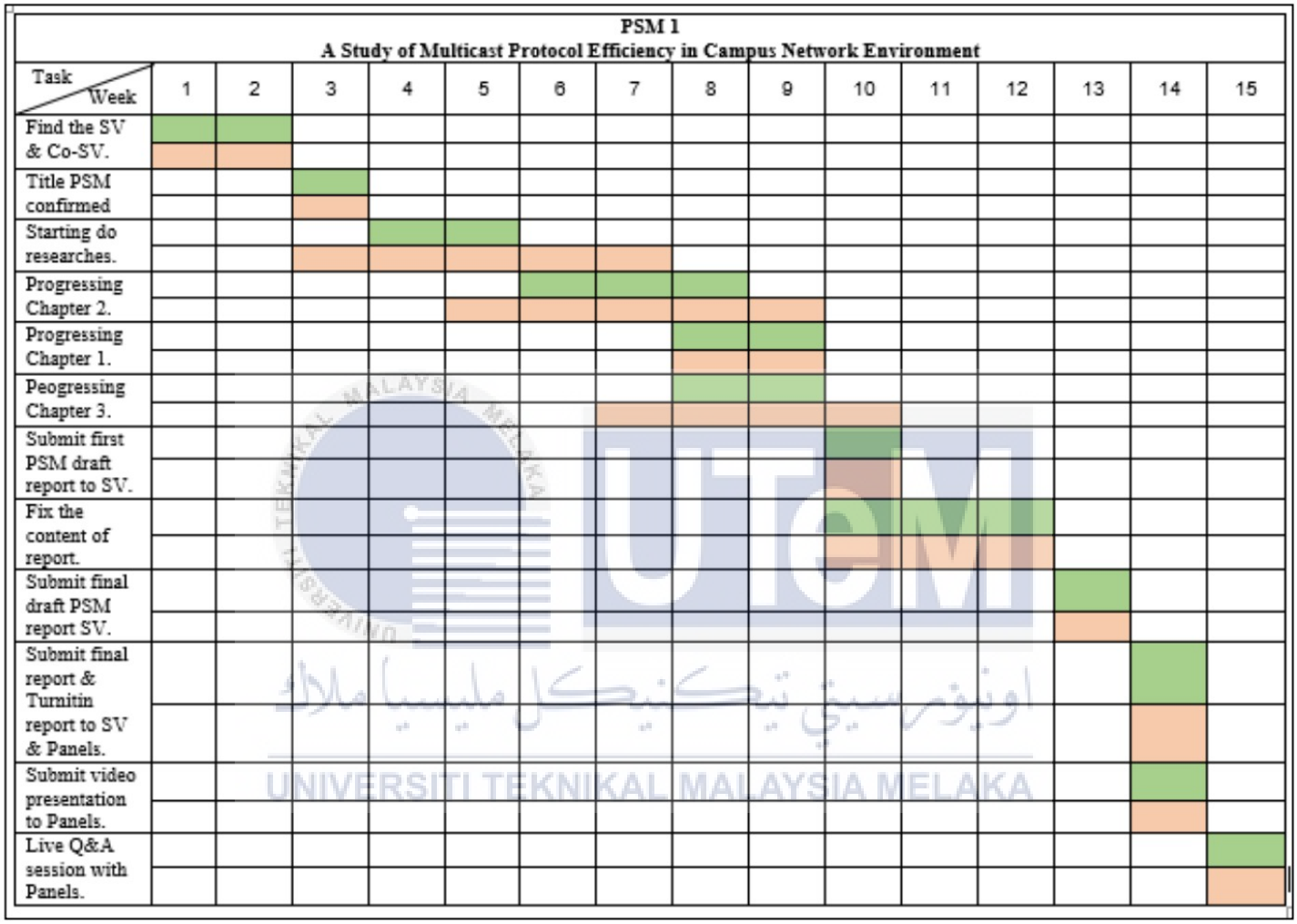


Table 3.1: Projek Sarjana Muda 1 (PSM 1) Gantt Chart

3.4 Equipment Implementation

This section will explore and explain the equipment and the features that used in the Multicast Protocol Efficiency in a Campus Network Environment using eNSP for simulation of network topology.

3.4.1 Router AR1220

Figure 3.2: Router AR1220 in Simulation

AR1220 is a Huawei router based on the Various Routing Platform (VRP) copyrights of the Huawei. In order to offer industrially leading efficiency and reliability to meet current and prospective demands, they develop on their leadership role in data communications and networking. The AR1220 includes functions such as routing, switching, voice, security, 3-G service, and WLAN. The AR1220 features an effective hardware authentication mechanism and offers a voice enhancement for a digital signal processor (DSP). Also, firewalls, processing call and voicemail security are provided by the router. Wireless communication modes can be supported, for example E1 / T1, xDSL, xPON, wi-fi, 3 G and more. The characteristics of this router interfaces are fixed 8FE, one CON/AUX, two fixed GE, one Mini USB and two USB.

3.4.2 Switch S3700

Figure 3.3: Switch S3700 in Simulation

The company switch of S3700 series is a switch layer three save-energy of the future networking era. In order to provide high-performance connectivity and convergence to the company campus network the S3700 uses advanced hardware and software from Versatile Routing platform (VRP) Huawei. The S3700 of switch can be easily installed and maintained. The S3700 allows business users to develop the networks of the next era with their scalable VLAN distribution, PoE functions, extensive features of the routing and the potentiality to relocate to an IPv6 network. Furthermore, the switch of S3700 utilizes advanced stacking, VRRP and RRPP stability technologies to improve efficiency and flexibility in the network. The S3700 is a 1U high box component. The standard edition (SI) is available as well as an improved (EI) edition. Layer 2 features and basic layer 3 features are supported in version SI. The EI version supports complex protocol routing and provides more functionality than those provided in the SI version.

3.4.3 End Device

Figure 3.4: PC as a Client in Simulation

A client is an end device that has installed software that allows it to request and display the information obtained from a server. It is a PC simulator and has one Ethernet interface. However, a web browser such as Internet Explorer, is one example of client applications. The server and the client use the network as a method to be connected and communicate from each other. Likewise, when the clients want to express to their server, the client will use the network to deliver and accept the communication or requests over their order. After that, the server will utilize the request to make sure that request is logical or illogical. If the whole checks out are well, the server will recover the requests and the client service. However, the server can produce a client to request too. It might to check the client's status, or ask if it has received any security patches, or if it still needs server resources. If not receive any, the connection will be close immediately to release the network traffic.

3.4.4 Multicast Source (MCS)

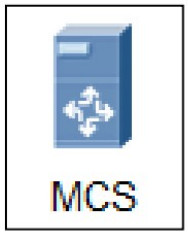


Figure 3.5: Multicast Source (MCS) in Simulation

Multicast Source (MCS) will be as a server for this campus network design project. It is consisting of one Ethernet interface. The function of this server is to send multicast packet to the PC simulators through the switches.

3.5 Multicast Protocols Implementation

Multicast Protocols is a method that one-to-one and many-to-many in the real-time of communication application on an Internet Protocol (IP) network framework. In this project, we will execute the three of multicast protocols. There are Open Shortest Path First (OSPF), Internet Group Management (IGMP) and Protocol Independent Multicast-Dense Mode (PIM-DM) and Protocol Independent-Sparse Mode (PIM-SM). But mainly used in this project are protocols of PIM-SM and PIM-DM.

3.5.1 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a routing protocol that use in the IP network. It is utilizing a Link State Routing (LSR) algorithm which slots to the Interior Gateway Protocol (IGP) group and works in one alternative structure. For wide enterprise networks, OSPF is usually used the IGP.

3.5.2 Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) operates in the middle of routers and hosts of the LAN to monitor and identify the multicast group where these hosts and routers are group members.

3.5.3 Protocol Independent-Dense Mode (PIM-DM)

PIM-Dense Mode (PIM-DM) includes a multicast flood pushing model at each network intersection. This push model provides data to recipients without requested data by the recipients. This technique is successful in some implementations in which recipients are involved on each network subnet. A router will presume all other routers would like to forward packets for a party in this dense mode. When a router receives a packet with multi-channels but there is no nearby participant have been connected directly, the packets will be sent back to the source. This router on this trimmed branch should not be overwhelmed by the following multicast packets. PIM develops distribution trees on a source-based basis.

3.5.4 Protocol Independent-Sparse Mode (PIM-SM)

PIM-sparse mode (PIM-SM) utilizes a multi-cast traffic pull model. The traffic is available only to active users who specifically ask for content in the network elements. Contrary to dense mode interfaces, the multicast routing table is enabled with spacious interfaces only if a directly attached participant is disabled or a daily message from descending routers are received. Sparse-mode operation occurs if an RP is identified by the group when it is in forwarding from a LAN. If the RP is identified for the group, the transmission from the LAN result obtained in a sparse mode

operation. So then, the packets would be enclosed and submitted to the RP. If no RP is known, it will fill the packet densely.

3.6 Software Implementation

In this project, Huawei eNSP software and Wireshark software will be used in the Multicast Protocol Efficiency in a Campus Network Environment project. This section will briefly explain about the features and how it is working.

3.6.1 eNSP Software

Figure 3.6: eNSP Network Simulator Software

Enterprise Network Simulation Platform (eNSP) is a simulation tool for the graphical network. It is a network simulation software provided by Huawei. Huawei eNSP is a free open-source software that can be install at Huawei website. However, this software needed certain additional software such as WinPcap, Wireshark and VirtualBox to work cooperatively. It mainly

simulates routers, switches, firewalls, WLANs, and other devices on the enterprise network. Huawei eNSP is encompasses of an actual network equipment in the simulation and support large scale networking. This would let the users to understanding and easy to manage the function and setup of related equipment in real life. Hence, we will apply this network simulator to design the campus network topology for this project.

3.6.2 Wireshark Software

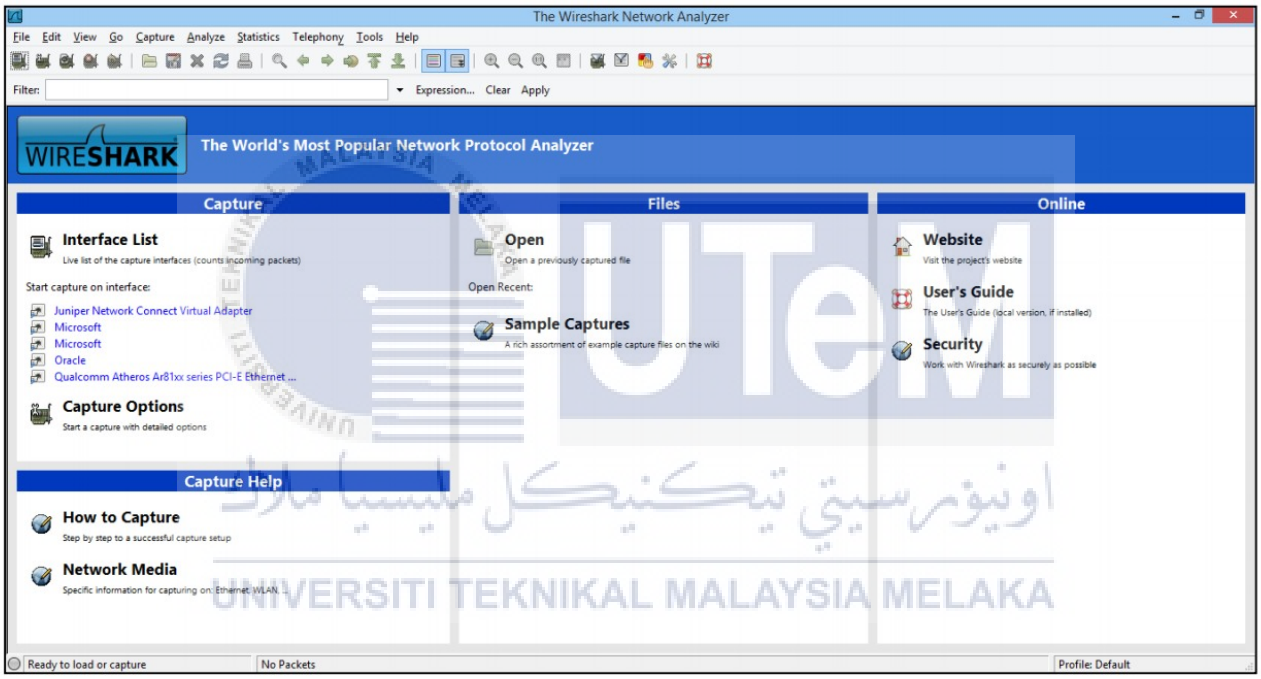


Figure 3.7: The Wireshark Network Analyzer Software

Wireshark is a network packet analyzer that introduces as accurate as possible the captured packets data. Wireshark is a free open-source software and the best packet analyzer today. There are many features of Wireshark, such as live network interface packet captured data, accessible to UNIX and Windows, and text file importation packets with hex-dumps of packet data. The display very particularized protocol information packet, export multiple packets to some capture filter format, filter packets on many criteria, colorize filter-based packet display, and generate statistics

and so on. For viewing the captured packets, only by click on the packet list pane that will show the selected packet in the tree view and byte view panes. In addition, Wireshark can be used to acquire acknowledge of network protocol internal and help in several situations such to troubleshoot the network issues, identify the network security, verify the network applications, and fix the protocol implementation. Figure 3.8 shows how the Wireshark working to capture the packet data and the user can examine the contents.

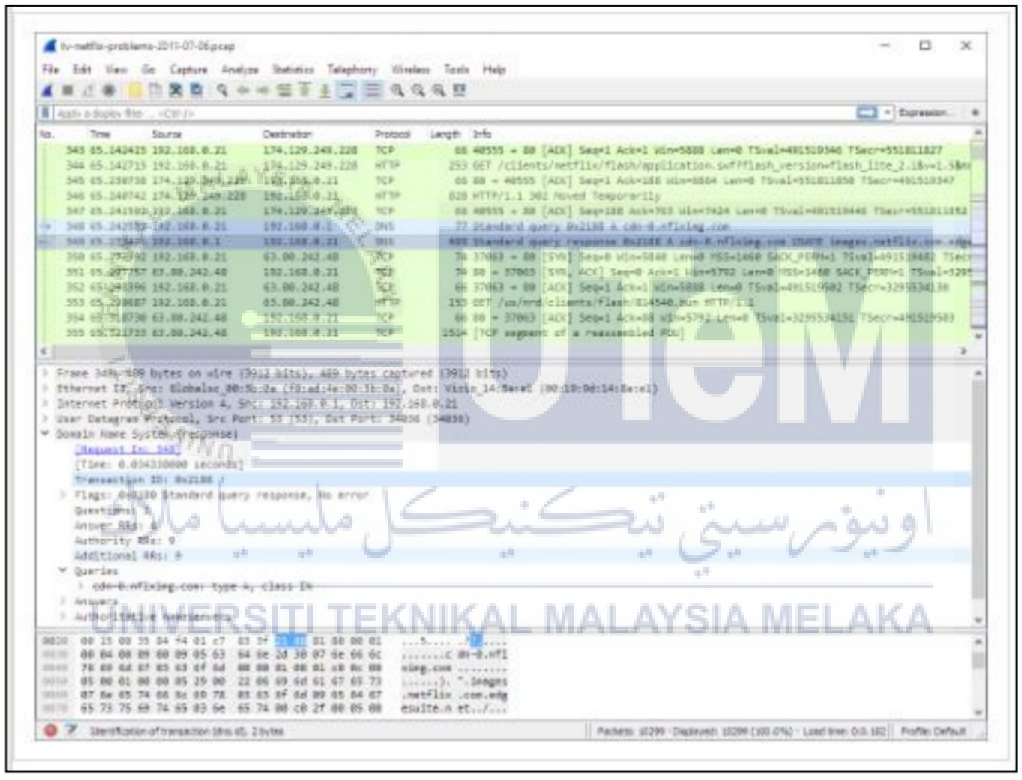


Figure 3.8: Wireshark Packet Data Captured

3.7 The Project Flowchart of PSM

The following flowchart at Figure 3.9 shows the process of this project to be implemented. This project will be accomplished if the clients accept the video streaming from the MCS server. If the clients do not accept the video streaming, we need to reconfigure the routers and switches by recheck the IP multicast group. The first step of this process is by select 4 routers of AR1220, 8 switches of S3700, 16 clients and 1 MCS server. After that, we can start to construct the campus network topology. To configure the MCS server, we need to set the IP unicast. Next, we can configure the routers and switches and enable the multicast routing command. The AR1220 router then uses the command of PIM-SM to configure the routing protocol of PIM-SM. Following to configure the AR1220 router for RP and BSR candidates. Lastly, apply the command of PIM-SM to configure the multi-casting routing protocol of PIM-SM, and use IGMP to enable the group member to handle each switch of S3700 to connect with computer network host.

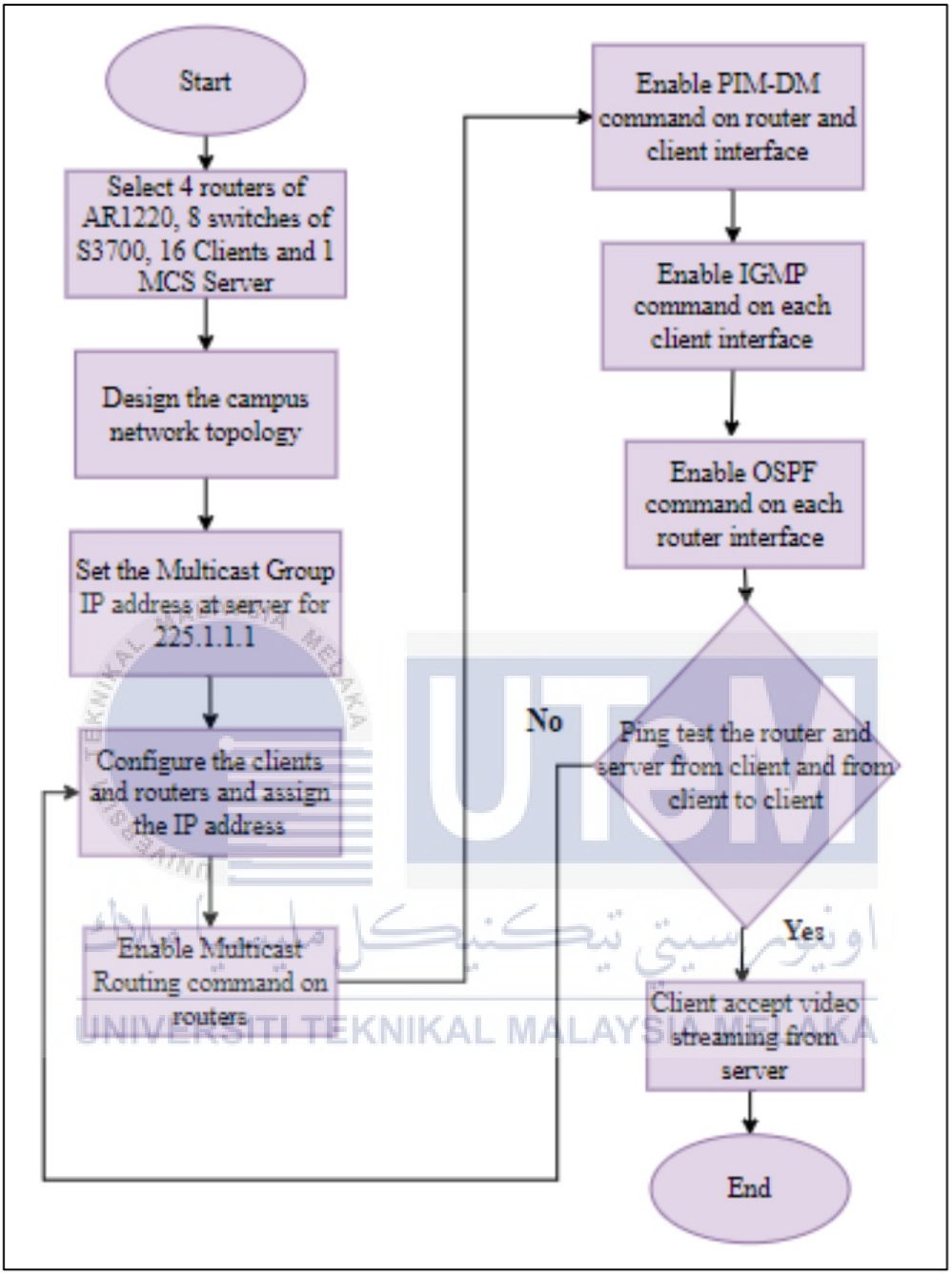


Figure 3.9: The Flowchart of Projek Sarjana Muda (PSM)

3.8 The Design Project of Projek Sarjana Muda (PSM)

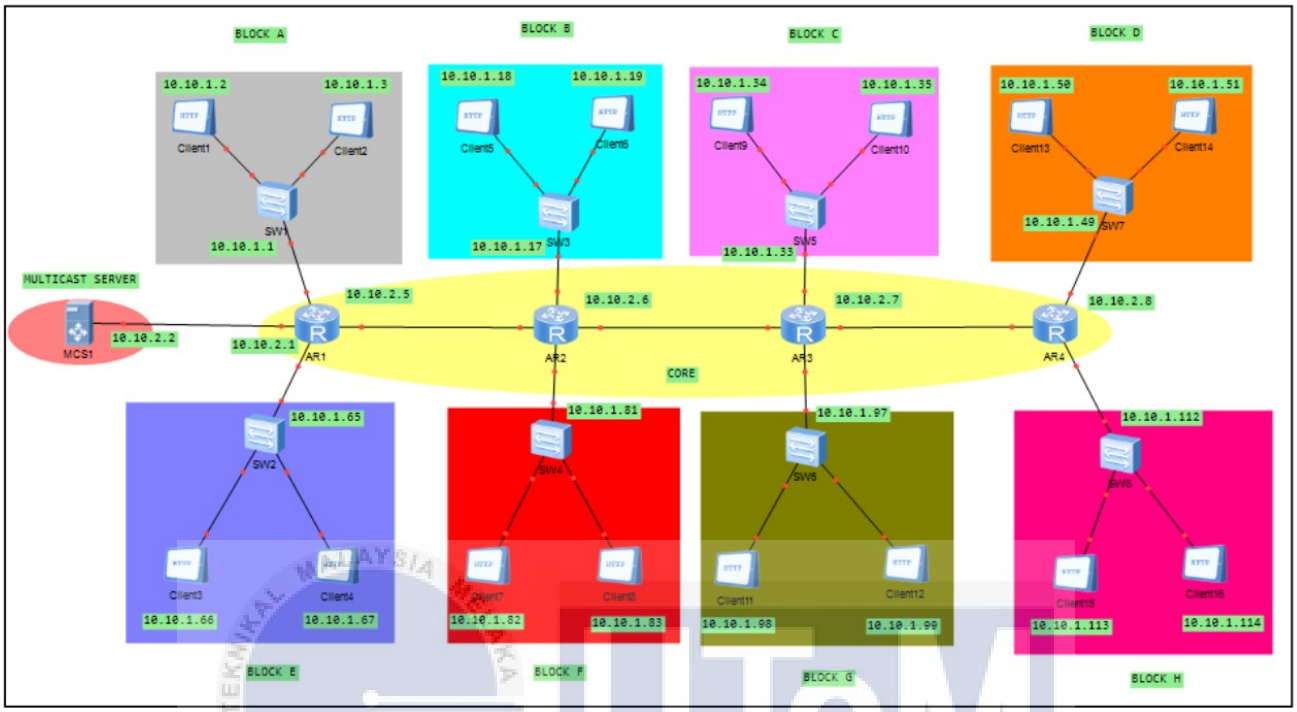


Figure 3.10: The Campus Network Topology Design

Therefore, this is a campus network topology design that we suggested for this project. We will develop this design in Huawei eNSP software and strive to configure all the equipment as shown as in Figure 3.10. After that, we will develop several network elements such as 4 routers, 8 switches, 16 clients and one MCS server in this network topology. The MCS is a multicast server that will interface with the first router. However, the yellow color area will be the network core that consists of four routers AR1220. Next, following with the other colors area consists of eight blocks which is from block A to block H. For every block consist of two clients that connected to one switch S3700. Lastly, for the expected outcome is when all the clients in each block will accepts the video streaming from the MCS server and we can capture packet data in real time from our network and read the data that have been captured from the packet either in tree view pane or byte view pane by using Wireshark software.

CHAPTER 4

RESULT AND DISCUSSION

4.1 Introduction

In this section will demonstrate and represent the improvement of campus network topology design from the suggested design that stated in Chapter 3. This chapter will also give details of the network elements configuration and the results over the simulation of Multicast Protocol Efficiency Campus Network Environment using eNSP software. After that, the implementation of multicast protocols and their efficiencies will be discussed. Then, this section will prove that the Wireshark software can captured packet data traffic from our simulation network by using eNSP software and analysed the data traffic that have been captured from the packet either in tree view pane or byte view pane. Wireshark software can be operate in the simulation too. That is because Wireshark works alongside the eNSP platform. In a sense, we can simulate our required network in the eNSP software. When we run the simulation in the campus network, we can analyse the data packet captured in Wireshark. We can also understand all the data headers while transmission and so on.

4.2 The Campus Network Topology Design

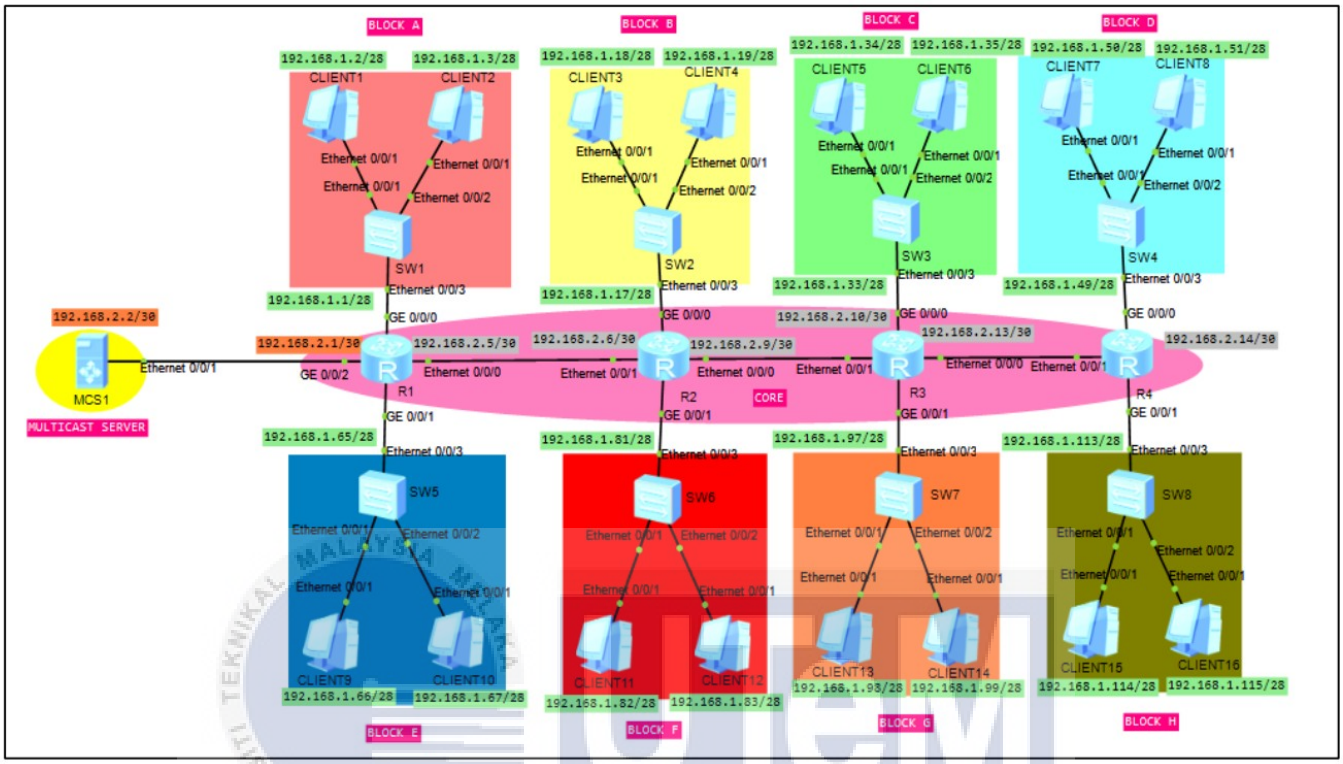


Figure 4.1 Campus Network Topology Design

Based on Figure 4.1 above, this is a campus network topology design by using eNSP software that have been configured. In this design consists of one multicast server (MCS1) in yellow color area that connected with first router (AR1) and next connected with three routers (AR2, AR3, and AR4) of AR1220 in purple color area that known as the core area. After that, eights switches (SW1, SW2, SW3, SW4, SW5, SW6, SW7, and SW8) of S3700 in other colors area which is each switch connected with two PCs or known as clients in one block color area. The total clients in this design was sixteen clients.

4.3 The configuration of Network Elements in Campus Network

4.3.1 IP Address Subnetting

First of all, the configuration of IP address need to be assigned to all the devices in the topology. Before that, only the switches will be not to be configure because of the switches will be functioned as to reduce the usage of routers interface. The calculation of IP address will be used to get the IP address range for each device to keep away from overlapped configuration.

Table 4.1: All the possible subnet mask of /28 networks for 192.168.1.1

Network Address	Usable Host Range	Broadcast Address
192.168.1.0	192.168.1.1 - 192.168.1.14	192.168.1.15
0192.168.1.16	192.168.1.17 - 192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33 - 192.168.1.46	192.168.1.47
192.168.1.48	192.168.1.49 - 192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65 - 192.168.1.78	192.168.1.79
192.168.1.80	192.168.1.81 - 192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.113 - 192.168.1.126	192.168.1.111
192.168.1.112	192.168.1.113 - 192.168.1.126	192.168.1.127

Table 4.2: IP Address Range of /28 Networks on Clients

Network Element / Device	IP Address
Client 1	192.168.1.2
Client 2	192.168.1.3
Client 3	192.168.1.18
Client 4	192.168.1.19

Client 5	192.168.1.34
Client 6	192.168.1.35
Client 7	192.168.1.50
Client 8	192.168.1.51
Client 9	192.168.1.66
Client 10	192.168.1.67
Client 11	192.168.1.82
Client 12	192.168.1.83
Client 13	192.168.1.98
Client 14	192.168.1.99
Client 15	192.168.1.114
Client 16	192.168.1.115

Table 4.3: IP Address Range of /28 Networks on Client Interface from Router

Network Element / Device	**IP Address**
Router 1	192.168.1.1 192.168.1.65
Router 2	192.168.1.17 192.168.1.81
Router 3	192.168.1.33 192.168.1.97
Router 4	192.168.1.49 192.168.1.113

Table 4.1 shows that all the possible subnet mask /28 for 192.168.1.1 IP address. The subnet mask can be expressed in two forms: (i) the dot decimal; (ii) the slash notation. For this configuration, the subnet mask of /28 networks is equivalent to 255.255.255.240 was chosen to be assigned to configure clients interface. Table 4.2 shows that the IP Address range that assigned to

each of client interface. Table 4.3 shows the IP address that assigned on router that interface to each client. The Open Shortest Path First (OSPF) command should be implement too on routers interface in order to reach the full connectivity of the campus network topology. We can summarize the network address such as 192.168.0.0 with subnet mask 255.255.0.0. Before that, the routers should be trucking by assigned IP address of subnet mask /30 that equivalent to 255.255.255.252. This subnet mask of /30 was chosen because of it consists two usable host and the configuration happen only on the two interfaces on the routers. This technique will reduce and keep away from wasted the usable host IP address. Table 4.4 shows the IP address range that used to configure multicast server and the routers. Next, the ICMP ping method will be used to test the all the connectivity of the devices and make sure the devices can receive data from the multicast server. The multicast server was assigned with 192.168.2.2, the first router assigned 192.168.2.1. The first router also will be assigned start from 192.168.2.5 and following with the other routers as shown as in Table 4.4.

Table 4.4: IP Address Range of /30 Networks on Multicast Server and Routers

Network Element / Device	**IP Address**
Multicast Server	192.168.2.2
Router 1	192.168.2.1 192.168.2.5
Router 2	192.168.2.6 192.168.2.9
Router 3	192.168.2.10

	192.168.2.13
Router 4	192.168.2.14

When all the clients and routers configuration completed, the multicast group IP address need to be set on multicast server. The IP address was chosen 225.1.1.1. The multicast group IP address range between 244.0.0.0 - 239.255.255.255 that can be select as shown as in Figure 4.2. After we select the multicast group address the MAC group address will pop up automatically at 01-00-5E-01-01-01.

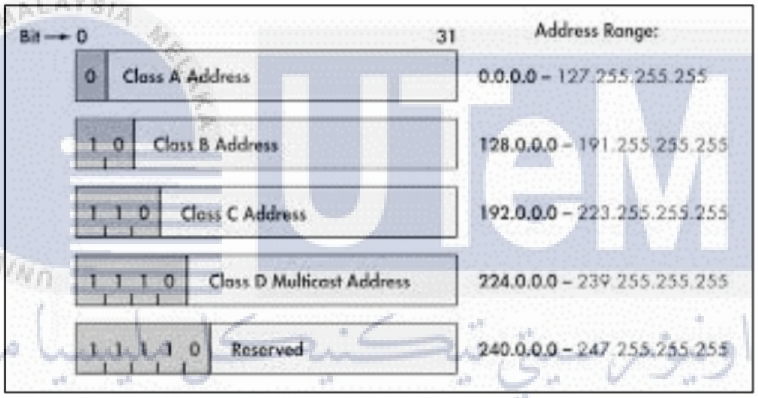


Figure 4.2: IP Address Range by Classes

Based on the study of the theoretical and previous research of Protocol Independent Multicast (PIM), only the Protocol Independent Multicast-Dense Mode (PIM-DM) will be implemented on this campus network topology rather than Protocol Independent Multicast-Sparse Mode (PIM-SM). That is because for crowded users, PIM-DM is ideal, whereas PIM-SM is more suitable for a wide-range network of scattered users. This campus network users are crowded so that the PIM-DM protocol is appropriate for this topology.

The OSPF (Open Shortest Path First) protocol command will be execute on this campus network topology in order to reach the full connectivity on each the router interface. This protocol will be apply on the campus network topology because there is not been used before by anyone for the project purpose in the networking field. There are have possibility to propose this method when no one has ever executed it. The OSPF protocol also supports complex networks with multiple routers, including backup routers to balance traffic loads on multiple links to other subnets. Through the OSPF protocol, neighboring routers in the same broadcast domain or at either end of a point-to-point connection communicate with one another. It is possible to split an OSPF network into areas which are logical classes of hosts and networks. An area involves its connecting router providing network-connected interfaces. Each area maintains a separate link-state database whose data can be summarized by the connecting router for the rest of the network. Thus, outside the field, the topology of an area is unknown. This reduces the traffic flow between components of an autonomous system. In this router configuration will be declare as Area 0 where is known as backbone area and the network address will be use 192.168.0.0 with subnet mask 255.255.0.0 as shown as in Figure 4.3.

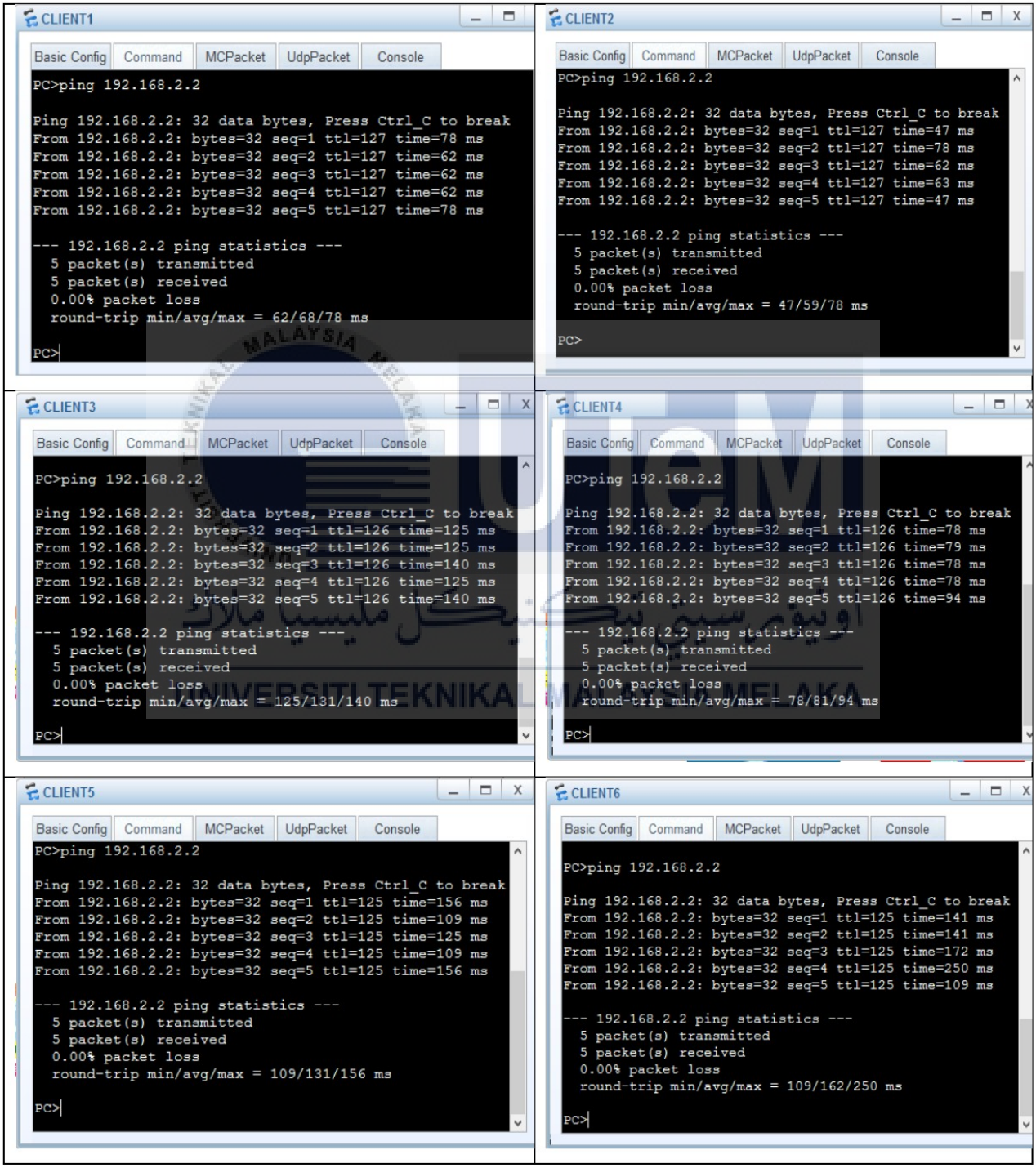

```
ospf
area 0
network 192.168.0.0 255.255.0.0
```

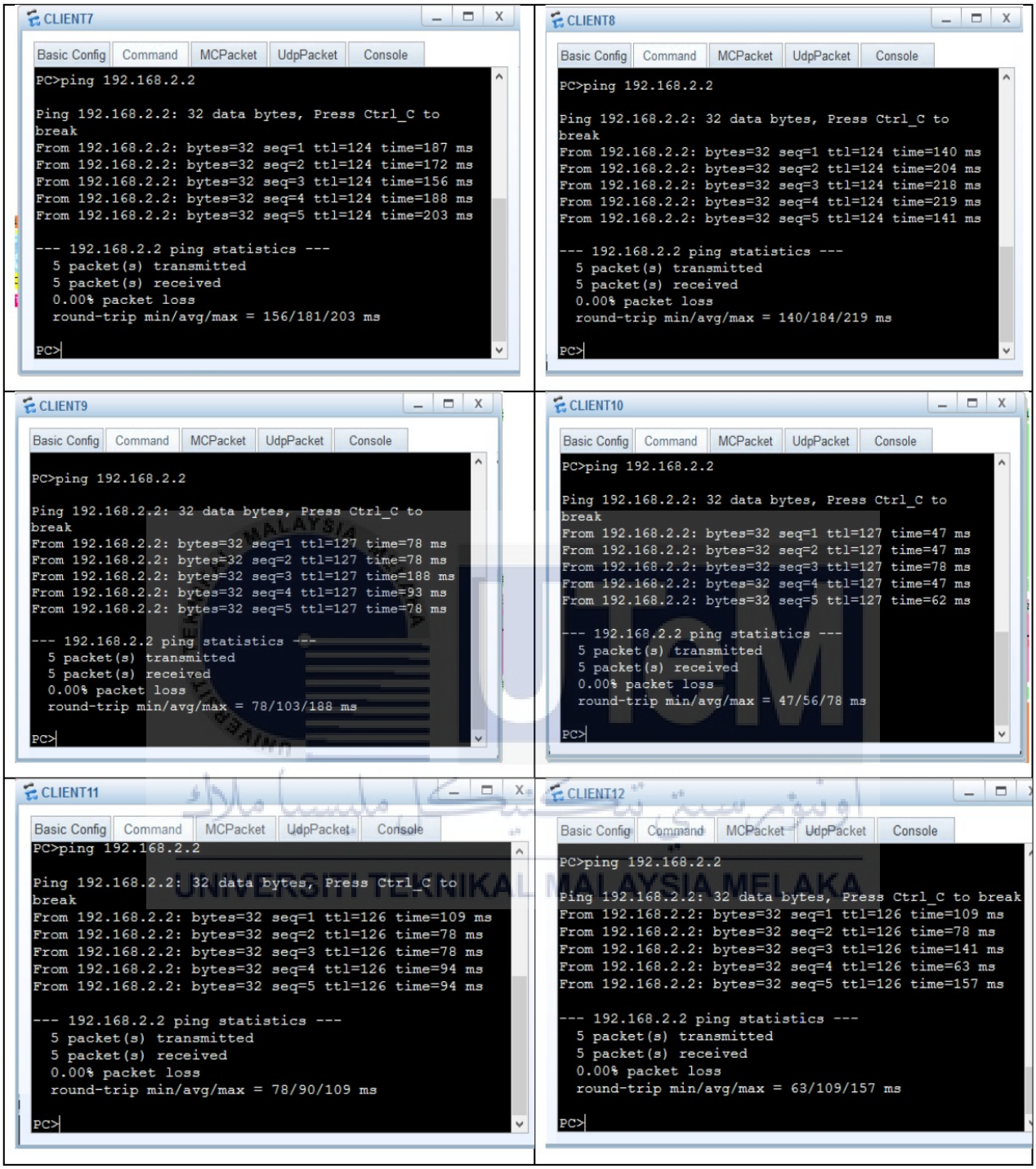
Figure 4.3: OSPF Protocol Command Configuration

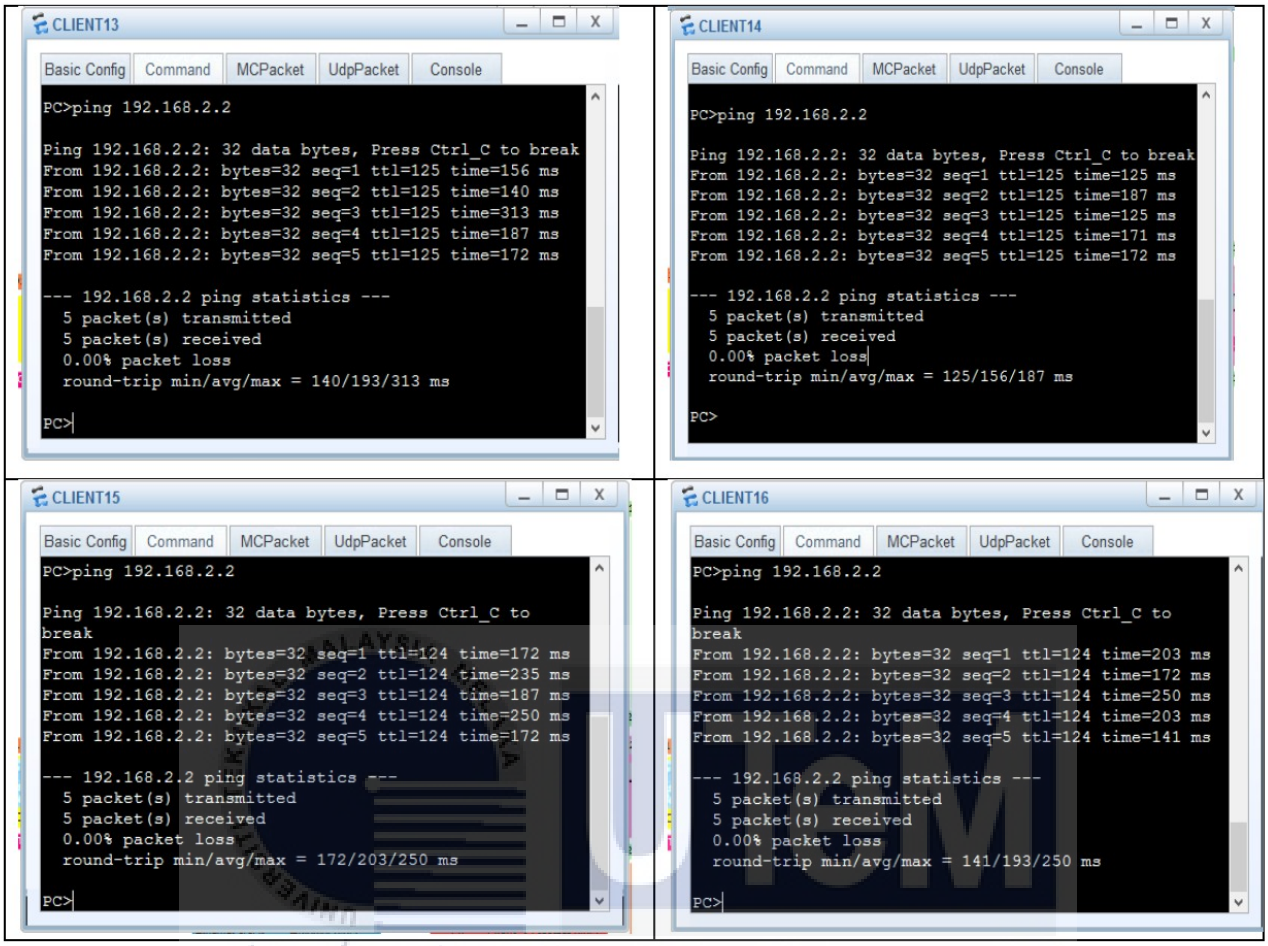
Next part is to configure the routers for the multicast features. The first step is to enable multicast routing command on each routers. After that, enable PIM command at all device interface and enable IGMP command at all client interface. Then, start to ping test from client to client and

from client to server. Table 4.5 shows that the succeed ping test from all clients to multicast server that addressed 192.168.2.2.

Table 4.5: Ping Test from Client 1 until Client 16 to Multicast Server







4.3.2 Protocol Recognition and Network Configuration Testing

The network configuration testing will be a way to check all the device connection. The PIM-DM protocol is maintained by each multicast routing table. That is because the multicast data packet is transmitted to control the connection. All the table below from the Table 4.6 until Table 4.12 shows the interface information that including PIM-DM, IGMP group and multicast routing-table.

Table 4.6: PIM-DM Interface Verbose Details

Router 1	Router 2
<R1>display pim interface verbose VPN-Instance: public net Interface: Ethernet0/0/0, 192.168.2.5 PIM version: 2 PIM mode: Dense PIM state: up PIM DR: 192.168.2.6 PIM DR Priority (configured): 1 PIM neighbor count: 1 PIM hello interval: 30 s PIM LAN delay (negotiated): 500 ms PIM LAN delay (configured): 500 ms PIM hello override interval (negotiated): 2500 ms PIM hello override interval (configured): 2500 ms PIM Silent: disabled PIM neighbor tracking (negotiated): disabled PIM neighbor tracking (configured): disabled PIM join attribute (negotiated): disabled PIM generation ID: 0X6789C7AB PIM require-GenID: disabled PIM hello hold interval: 105 s PIM assert hold interval: 180 s PIM triggered hello delay: 5 s PIM J/P interval: 60 s PIM J/P hold interval: 210 s PIM state-refresh processing: enabled PIM state-refresh interval: 60 s PIM graft retry interval: 3 s PIM state-refresh capability on link: capable PIM BFD: disabled PIM dr-switch-delay timer: not configured Number of routers on link not using DR priority: 0 Number of routers on link not using LAN delay: 0 Number of routers on link not using neighbor tracking: 2 Number of routers on link not using join attribute: 2 ACL of PIM neighbor policy: - ACL of PIM ASM join policy: - ACL of PIM SSM join policy: - ACL of PIM join policy: -	<R2>display pim interface verbose VPN-Instance: public net Interface: Ethernet0/0/0, 192.168.2.9 PIM version: 2 PIM mode: Dense PIM state: up PIM DR: 192.168.2.10 PIM DR Priority (configured): 1 PIM neighbor count: 1 PIM hello interval: 30 s PIM LAN delay (negotiated): 500 ms PIM LAN delay (configured): 500 ms PIM hello override interval (negotiated): 2500 ms PIM hello override interval (configured): 2500 ms PIM Silent: disabled PIM neighbor tracking (negotiated): disabled PIM neighbor tracking (configured): disabled PIM join attribute (negotiated): disabled PIM generation ID: 0XB3E36238 PIM require-GenID: disabled PIM hello hold interval: 105 s PIM assert hold interval: 180 s PIM triggered hello delay: 5 s PIM J/P interval: 60 s PIM J/P hold interval: 210 s PIM state-refresh processing: enabled PIM state-refresh interval: 60 s PIM graft retry interval: 3 s PIM state-refresh capability on link: capable PIM BFD: disabled PIM dr-switch-delay timer: not configured Number of routers on link not using DR priority: 0 Number of routers on link not using LAN delay: 0 Number of routers on link not using neighbor tracking: 2 Number of routers on link not using join attribute: 2 ACL of PIM neighbor policy: - ACL of PIM ASM join policy: - ACL of PIM SSM join policy: - ACL of PIM join policy: -

```
Interface: GigabitEthernet0/0/0, 192.168.1.1
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.1.1 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0XA962DA00
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: Ethernet0/0/1, 192.168.2.6
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.2.6 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 1
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0XDEECE3BD
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 2
    Number of routers on link not using join attribute: 2
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: GigabitEthernet0/0/1, 192.168.1.65
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.1.65 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0X68025A45
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking:
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: GigabitEthernet0/0/0, 192.168.1.17
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.1.17 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0X52086D52
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: GigabitEthernet0/0/2, 192.168.2.1
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.2.1 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0X82ABB124
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: GigabitEthernet0/0/1, 192.168.1.81
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.1.81 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0XBF7EDF6B
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

Router 3

```
<R3>display pim interface verbose
 VPN-Instance: public net
 Interface: Ethernet0/0/0, 192.168.2.13
     PIM version: 2
     PIM mode: Dense
     PIM state: up
     PIM DR: 192.168.2.14
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 25(
     PIM hello override interval (configured): 25(
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM join attribute (negotiated): disabled
     PIM generation ID: 0XF926C06
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM state-refresh processing: enabled
     PIM state-refresh interval: 60 s
     PIM graft retry interval: 3 s
     PIM state-refresh capability on link: capable
     PIM BFD: disabled
     PIM dr-switch-delay timer: not configured
     Number of routers on link not using DR prior:
     Number of routers on link not using LAN delay
     Number of routers on link not using neighbor
     Number of routers on link not using join att:
     ACL of PIM neighbor policy: -
     ACL of PIM ASM join policy: -
     ACL of PIM SSM join policy: -
     ACL of PIM join policy: -
```

Router 4

```
<R4>display pim interface verbose
 VPN-Instance: public net
 Interface: Ethernet0/0/1, 192.168.2.14
     PIM version: 2
     PIM mode: Dense
     PIM state: up
     PIM DR: 192.168.2.14 (local)
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
     PIM hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM join attribute (negotiated): disabled
     PIM generation ID: 0X12C74D2
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM state-refresh processing: enabled
     PIM state-refresh interval: 60 s
     PIM graft retry interval: 3 s
     PIM state-refresh capability on link: capable
     PIM BFD: disabled
     PIM dr-switch-delay timer: not configured
     Number of routers on link not using DR priority: 0
     Number of routers on link not using LAN delay: 0
     Number of routers on link not using neighbor tracking: 2
     Number of routers on link not using join attribute: 2
     ACL of PIM neighbor policy: -
     ACL of PIM ASM join policy: -
     ACL of PIM SSM join policy: -
     ACL of PIM join policy: -
```

```
Interface: Ethernet0/0/1, 192.168.2.10
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.2.10 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 1
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0XF0921B7B
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 2
    Number of routers on link not using join attribute: 2
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: GigabitEthernet0/0/0, 192.168.1.49
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.1.49 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0X25DC0B50
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: GigabitEthernet0/0/0, 192.168.1.33
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.1.33 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0X2CBAF7D9
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: GigabitEthernet0/0/1, 192.168.1.113
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.1.113 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0X82F3ABDA
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

```
Interface: GigabitEthernet0/0/1, 192.168.1.97
    PIM version: 2
    PIM mode: Dense
    PIM state: up
    PIM DR: 192.168.1.97 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM join attribute (negotiated): disabled
    PIM generation ID: 0X697B2083
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM state-refresh processing: enabled
    PIM state-refresh interval: 60 s
    PIM graft retry interval: 3 s
    PIM state-refresh capability on link: capable
    PIM BFD: disabled
    PIM dr-switch-delay timer: not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    Number of routers on link not using join attribute: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

Table 4.7: IGMP Interface Verbose Details

Router 1

```
<R1>display igmp interface verbose
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/0(192.168.1.1):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Value of last member query time: 2 s
   Value of last member query interval: 1 s
   Value of startup query interval: 15 s
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:40
   Querier for IGMP: 192.168.1.1 (this router)
   IGMP activity: 0 joins, 0 leaves
   Robustness (negotiated): -
   Robustness (configured): 2
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Prompt-leave: disabled
   SSM-Mapping: disabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
```

Router 2

```
<R2>display igmp interface verbose
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/0(192.168.1.17):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Value of last member query time: 2 s
   Value of last member query interval: 1 s
   Value of startup query interval: 15 s
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:02
   Querier for IGMP: 192.168.1.17 (this router)
   IGMP activity: 0 joins, 0 leaves
   Robustness (negotiated): -
   Robustness (configured): 2
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Prompt-leave: disabled
   SSM-Mapping: disabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
```

```
GigabitEthernet0/0/1(192.168.1.65):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: none
  IGMP limit: -
  Value of query interval for IGMP (negotiated): -
  Value of query interval for IGMP (configured): 60 s
  Value of other querier timeout for IGMP: 0 s
  Value of maximum query response time for IGMP: 10 s
  Value of last member query time: 2 s
  Value of last member query interval: 1 s
  Value of startup query interval: 15 s
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:40
  Querier for IGMP: 192.168.1.65 (this router)
  IGMP activity: 0 joins, 0 leaves
  Robustness (negotiated): -
  Robustness (configured): 2
  Require-router-alert: disabled
  Send-router-alert: enabled
  Ip-source-policy: disabled
  Prompt-leave: disabled
  SSM-Mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
```

```
GigabitEthernet0/0/1(192.168.1.81):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: none
  IGMP limit: -
  Value of query interval for IGMP (negotiated): -
  Value of query interval for IGMP (configured): 60 s
  Value of other querier timeout for IGMP: 0 s
  Value of maximum query response time for IGMP: 10 s
  Value of last member query time: 2 s
  Value of last member query interval: 1 s
  Value of startup query interval: 15 s
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:02
  Querier for IGMP: 192.168.1.81 (this router)
  IGMP activity: 0 joins, 0 leaves
  Robustness (negotiated): -
  Robustness (configured): 2
  Require-router-alert: disabled
  Send-router-alert: enabled
  Ip-source-policy: disabled
  Prompt-leave: disabled
  SSM-Mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
```

Router 3

```
<R3>display igmp interface verbose
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/0(192.168.1.33):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: none
  IGMP limit: -
  Value of query interval for IGMP (negotiated): -
  Value of query interval for IGMP (configured): 60 s
  Value of other querier timeout for IGMP: 0 s
  Value of maximum query response time for IGMP: 10 s
  Value of last member query time: 2 s
  Value of last member query interval: 1 s
  Value of startup query interval: 15 s
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:23
  Querier for IGMP: 192.168.1.33 (this router)
  IGMP activity: 0 joins, 0 leaves
  Robustness (negotiated): -
  Robustness (configured): 2
  Require-router-alert: disabled
  Send-router-alert: enabled
  Ip-source-policy: disabled
  Prompt-leave: disabled
  SSM-Mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
```

Router 4

```
<R4>display igmp interface verbose
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/0(192.168.1.49):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: none
  IGMP limit: -
  Value of query interval for IGMP (negotiated): -
  Value of query interval for IGMP (configured): 60 s
  Value of other querier timeout for IGMP: 0 s
  Value of maximum query response time for IGMP: 10 s
  Value of last member query time: 2 s
  Value of last member query interval: 1 s
  Value of startup query interval: 15 s
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:03
  Querier for IGMP: 192.168.1.49 (this router)
  IGMP activity: 0 joins, 0 leaves
  Robustness (negotiated): -
  Robustness (configured): 2
  Require-router-alert: disabled
  Send-router-alert: enabled
  Ip-source-policy: disabled
  Prompt-leave: disabled
  SSM-Mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
```

```
GigabitEthernet0/0/1(192.168.1.97):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: none
  IGMP limit: -
  Value of query interval for IGMP (negotiated): -
  Value of query interval for IGMP (configured): 60 s
  Value of other querier timeout for IGMP: 0 s
  Value of maximum query response time for IGMP: 10 s
  Value of last member query time: 2 s
  Value of last member query interval: 1 s
  Value of startup query interval: 15 s
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:55
  Querier for IGMP: 192.168.1.97 (this router)
  IGMP activity: 0 joins, 0 leaves
  Robustness (negotiated): -
  Robustness (configured): 2
  Require-router-alert: disabled
  Send-router-alert: enabled
  Ip-source-policy: disabled
  Prompt-leave: disabled
  SSM-Mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
```

```
GigabitEthernet0/0/1(192.168.1.113):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: none
  IGMP limit: -
  Value of query interval for IGMP (negotiated): -
  Value of query interval for IGMP (configured): 60 s
  Value of other querier timeout for IGMP: 0 s
  Value of maximum query response time for IGMP: 10 s
  Value of last member query time: 2 s
  Value of last member query interval: 1 s
  Value of startup query interval: 15 s
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:03
  Querier for IGMP: 192.168.1.113 (this router)
  IGMP activity: 0 joins, 0 leaves
  Robustness (negotiated): -
  Robustness (configured): 2
  Require-router-alert: disabled
  Send-router-alert: enabled
  Ip-source-policy: disabled
  Prompt-leave: disabled
  SSM-Mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
```


Table 4.8: IGMP Group Details

Router 1

```
<R1>display igmp group
Interface group report information of VPN-Instance: public net
 GigabitEthernet0/0/1(192.168.1.65):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       192.168.1.67    00:03:49    00:00:21
 GigabitEthernet0/0/0(192.168.1.1):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       192.168.1.3     00:01:12    00:01:14
```

Router 2

```
<R2>display igmp group
Interface group report information of VPN-Instance: public net
 GigabitEthernet0/0/1(192.168.1.81):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       192.168.1.83    00:04:47    00:01:39
 GigabitEthernet0/0/0(192.168.1.17):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       192.168.1.19    00:00:43    00:01:41
```

Router 3

Router 4

```
<R3>display igmp group
Interface group report information of VPN-Instance: public net
 GigabitEthernet0/0/1(192.168.1.97):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       192.168.1.98    00:03:41    00:01:31
 GigabitEthernet0/0/0(192.168.1.33):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       192.168.1.35    00:01:43    00:01:45
```

```
<R4>display igmp group
Interface group report information of VPN-Instance: public net
 GigabitEthernet0/0/1(192.168.1.113):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       192.168.1.115   00:00:12    00:01:58
 GigabitEthernet0/0/0(192.168.1.49):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       192.168.1.51    00:00:12    00:01:58
```

Table 4.9: Multicast Routing Details

Router 1

```
<R1>display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry

 00001. (192.168.2.2, 225.1.1.1)
       Uptime: 00:26:26
       Upstream Interface: GigabitEthernet0/0/2
       List of 3 downstream interfaces
           1:  Ethernet0/0/0
           2:  GigabitEthernet0/0/0
           3:  GigabitEthernet0/0/1
```

Router 2

```
<R2>display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry

 00001. (192.168.2.2, 225.1.1.1)
       Uptime: 00:00:48
       Upstream Interface: Ethernet0/0/1
       List of 3 downstream interfaces
           1:  Ethernet0/0/0
           2:  GigabitEthernet0/0/0
           3:  GigabitEthernet0/0/1
```

Router 3

```
<R3>display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry

 00001. (192.168.2.2, 225.1.1.1)
       Uptime: 00:00:28
       Upstream Interface: Ethernet0/0/1
       List of 3 downstream interfaces
           1:  Ethernet0/0/0
           2:  GigabitEthernet0/0/0
           3:  GigabitEthernet0/0/1
```

Router 4

```
<R4>display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry

 00001. (192.168.2.2, 225.1.1.1)
       Uptime: 00:01:44
       Upstream Interface: Ethernet0/0/1
       List of 2 downstream interfaces
           1:  GigabitEthernet0/0/0
           2:  GigabitEthernet0/0/1
```

Based on the Table 4.10 and Table 4.11 below, it shows the PIM-DM and IGMP interface details. These protocols information could be display via CLI command on each router. Through this, the IGMP interface error between server to router and router to router its own can be prevented. The multicast protocols cannot operate well if this happens, and video streaming cannot be shared along with the multicast method.

Table 4.10: PIM Interface Details

Router 1

```
<R1>display pim interface
 VPN-Instance: public net
 Interface           State NbrCnt HelloInt   DR-Pri     DR-Address
 Eth0/0/0            up    1      30         1          192.168.2.6
 GE0/0/0             up    0      30         1          192.168.1.1     (local)
 GE0/0/1             up    0      30         1          192.168.1.65    (local)
 GE0/0/2             up    0      30         1          192.168.2.1     (local)
```

Router 2

```
<R2>display pim interface
 VPN-Instance: public net
 Interface           State NbrCnt HelloInt   DR-Pri     DR-Address
 Eth0/0/0            up    1      30         1          192.168.2.10
 Eth0/0/1            up    1      30         1          192.168.2.6     (local)
 GE0/0/0             up    0      30         1          192.168.1.17    (local)
 GE0/0/1             up    0      30         1          192.168.1.81    (local)
```

Router 3

```
<R3>display pim interface
 VPN-Instance: public net
 Interface           State NbrCnt HelloInt   DR-Pri     DR-Address
 Eth0/0/0            up    1      30         1          192.168.2.14
 Eth0/0/1            up    1      30         1          192.168.2.10    (local)
 GE0/0/0             up    0      30         1          192.168.1.33    (local)
 GE0/0/1             up    0      30         1          192.168.1.97    (local)
```

Router 4

```
<R4>display pim interface
 VPN-Instance: public net
 Interface           State NbrCnt HelloInt   DR-Pri     DR-Address
 Eth0/0/1            up    1      30         1          192.168.2.14    (local)
 GE0/0/0             up    0      30         1          192.168.1.49    (local)
 GE0/0/1             up    0      30         1          192.168.1.113   (local)
```

Table 4.11: IGMP Interface Details

Router 1

```
<R1>display igmp interface
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/0(192.168.1.1):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.1 (this router)

 GigabitEthernet0/0/1(192.168.1.65):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.65 (this router)
```

Router 2

```
<R2>display igmp interface
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/0(192.168.1.17):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.17 (this router)

 GigabitEthernet0/0/1(192.168.1.81):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.81 (this router)
```

Router 3

```
<R3>display igmp interface
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/0(192.168.1.33):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.33 (this router)

 GigabitEthernet0/0/1(192.168.1.97):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.97 (this router)
```

Router 4

```
<R4>display igmp interface
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/0(192.168.1.49):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.49 (this router)

 GigabitEthernet0/0/1(192.168.1.113):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.113 (this router)
```

Table 4.12: RPF (Reverse Path Forwarding) Details on Routers

Router 1

```
<R1>mtrace source 192.168.2.2
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(192.168.2.1), trace reverse path to source (192.168.2.2) acco
rding to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   192.168.2.1
 -1   192.168.2.1     1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute f
inished.
```

Router 2

```
<R2>mtrace source 192.168.2.2
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(192.168.2.6), trace reverse path to source (192.168.2.2) acco
rding to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   192.168.2.6
 -1   192.168.2.6     1      PIM
 -2   192.168.2.1     1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute f
inished.
```

Router 3

```
<R3>mtrace source 192.168.2.2
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(192.168.2.10), trace reverse path to source (192.168.2.2) acc
ording to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   192.168.2.10
 -1   192.168.2.10    1      PIM
 -2   192.168.2.6     1      PIM
 -3   192.168.2.1     1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute f
inished.
<R3>
```

Router 4

```
<R4>mtrace source 192.168.2.2
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(192.168.2.14), trace reverse path to source (192.168.2.2) acc
ording to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   192.168.2.14
 -1   192.168.2.14    1      PIM
 -2   192.168.2.10    1      PIM
 -3   192.168.2.6     1      PIM
 -4   192.168.2.1     1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute f
inished.
<R4>
```

Subsequently, Table 4.12 above shows that the RPF details of multicast source from each routers. Multicast has a Reverse Path Forwarding (RPF) check conception. The RPF method tests when a multicast packet arrives on an interface to verify that this incoming interface is the outgoing

interface used to access the source of the multicast packet through unicast routing. Loops are prevented by this RPF check process.

4.4 The Simulation of Multicast Campus Network

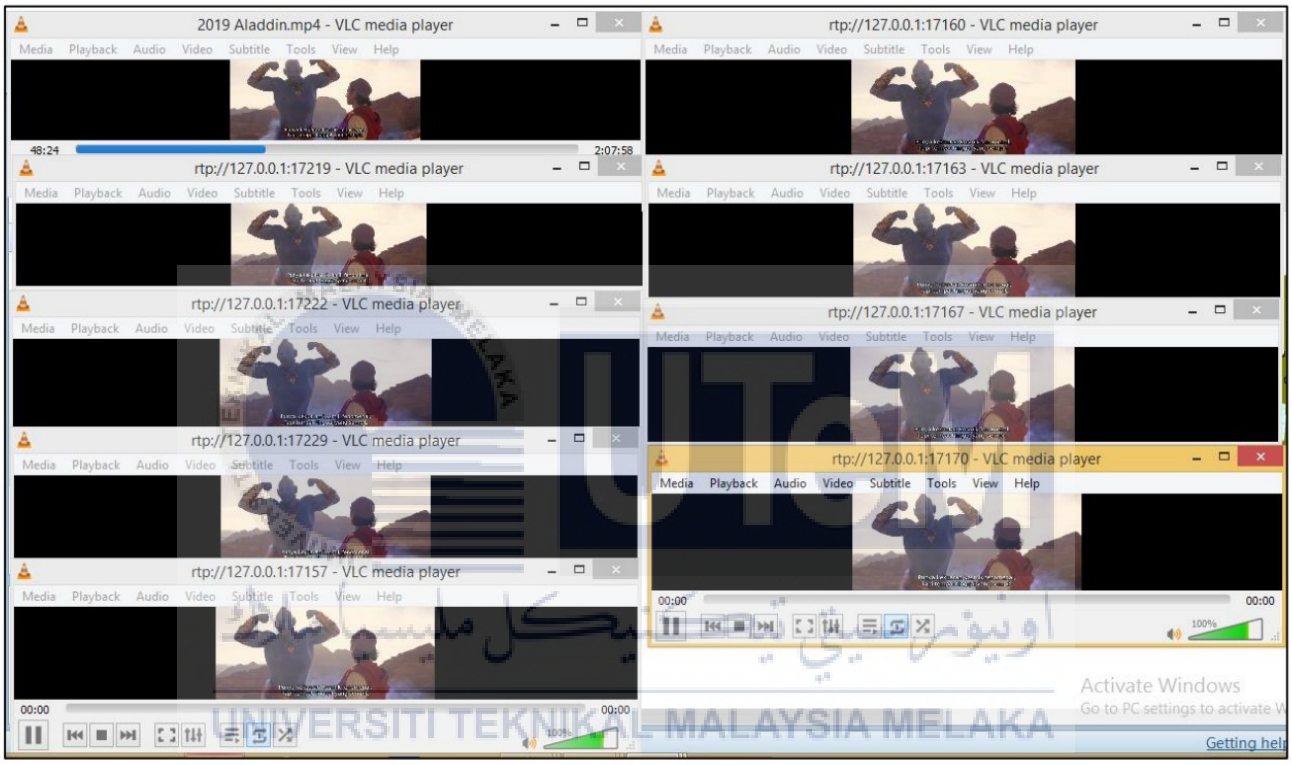


Figure 4.4: Multicast Streaming Video from Multicast Server (at the top and left side) to the Client 1 until Client 8.

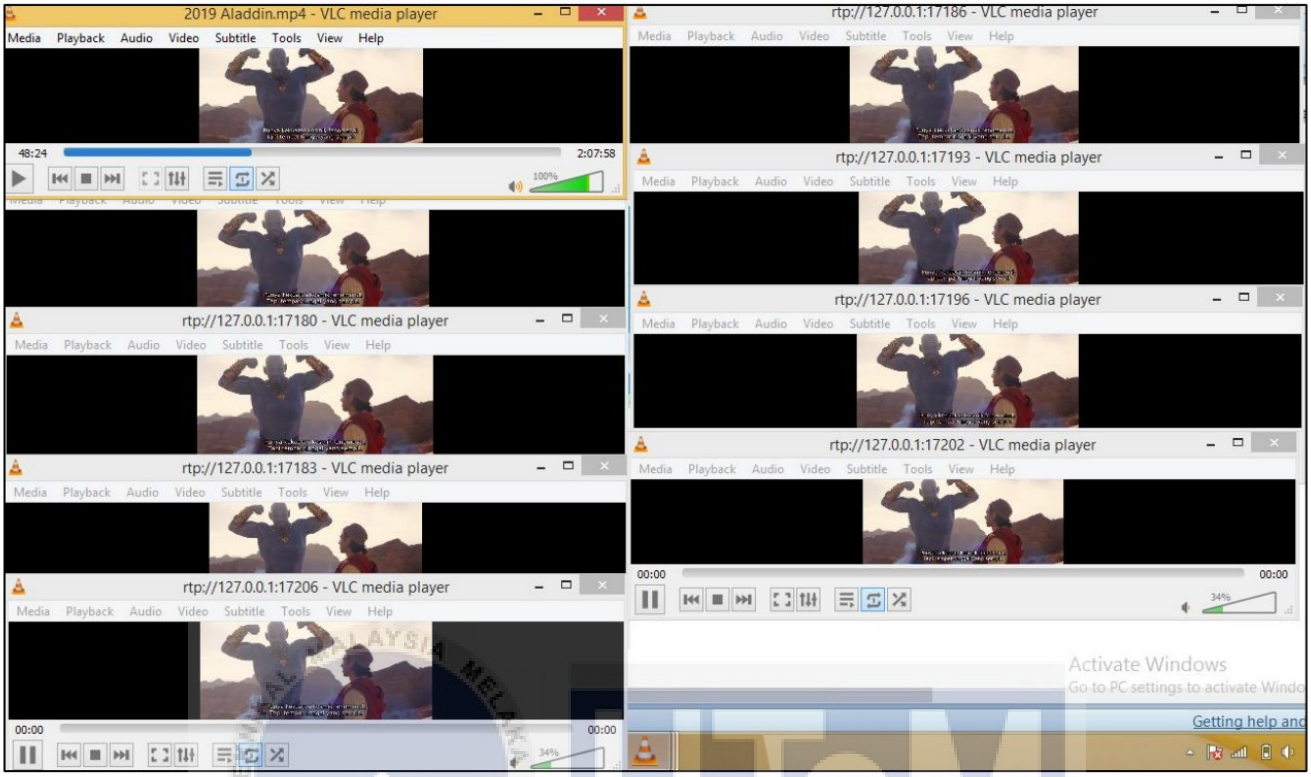


Figure 4.5: Multicast Streaming Video from Multicast Server (at the top and left side) to the Client 9 until Client 16

Figure 4.4 and Figure 4.5 shows the successful multicast streaming video from the multicast server that reached to the all sixteen clients. This happen when all the clients join the multicast group address (225.1.1.1). However, at a certain seconds there will be happen some delay or loading VLC video play at the several client. That is because all the clients has dissimilar IP address and it might causes some interruption.

4.5 Wireshark Analysis Multicast Data Traffic

The Wireshark will be used to analyze and capture the data packets on different links to trace the flow of multicast data in the simulation of campus network. Particularly, Wireshark can identify if the client has join or leave the multicast group.

4.5.1 PIM-DM Data Traffic Analysis

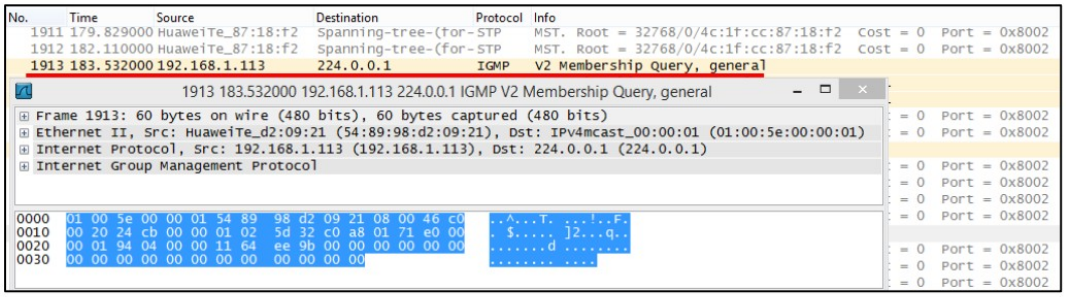


Figure 4.6: A Client from Block H (192.168.1.113) query to join the multicast group (225.1.1.1) using IGMPv2 protocol

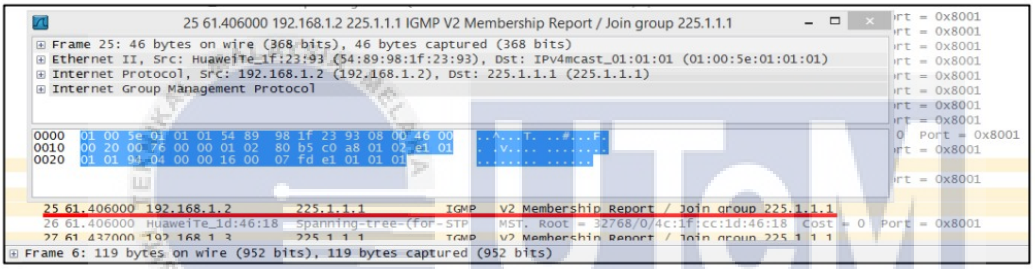


Figure 4.7: Client 1 (192.168.1.2) has join the multicast group (225.1.1.1) using IGMPv2 protocol

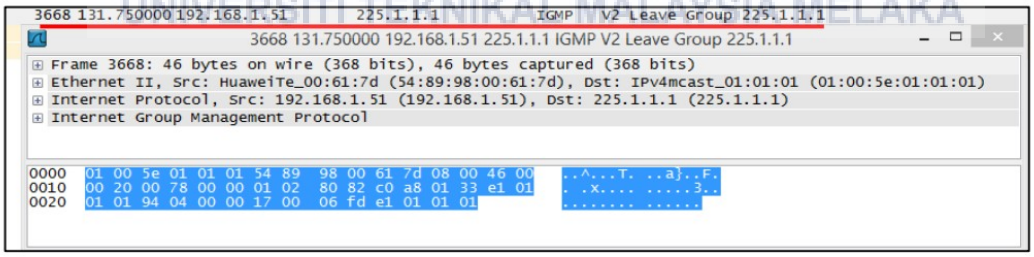
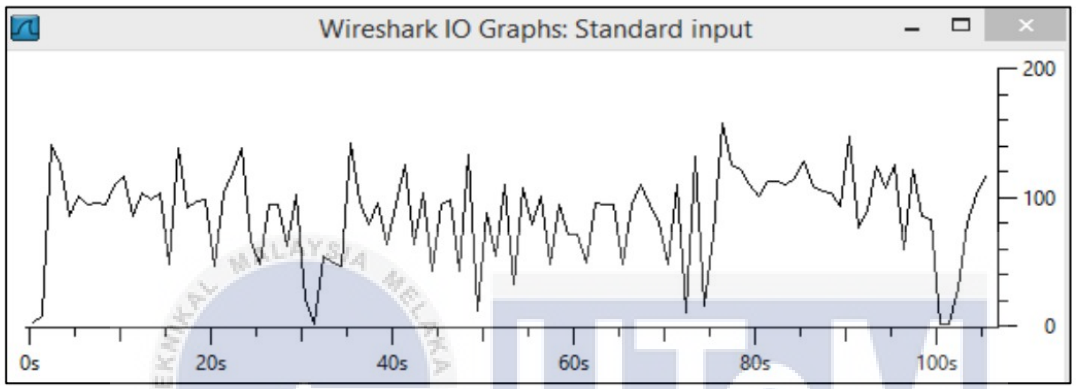


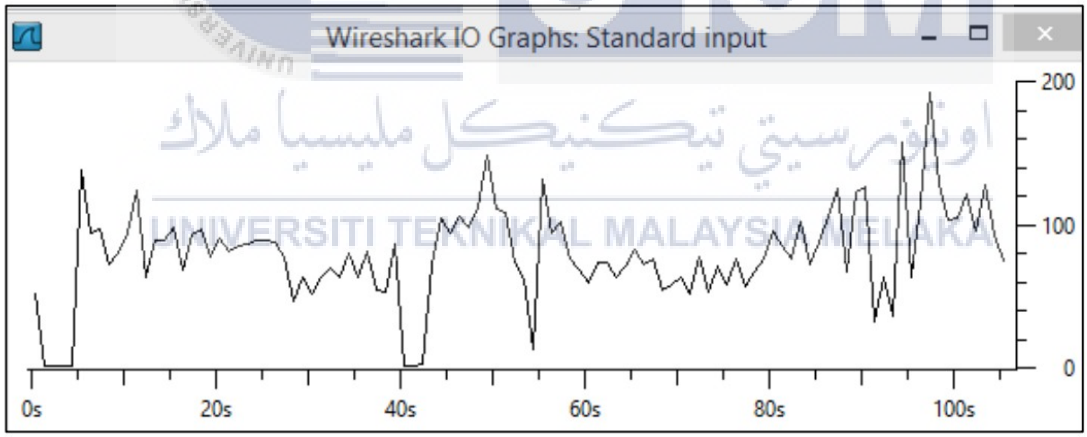
Figure 4.8: Client 8 (192.168.1.51) has leave the multicast group (225.1.1.1) using IGMPv2 protocol

Based on the Figure 4.6 shown the Client from Block H (192.168.1.113) that query to join the multicast group (225.1.1.1) using IGMPv2 protocol. For the Figure 4.7 shown the Client 1 (192.168.1.2)

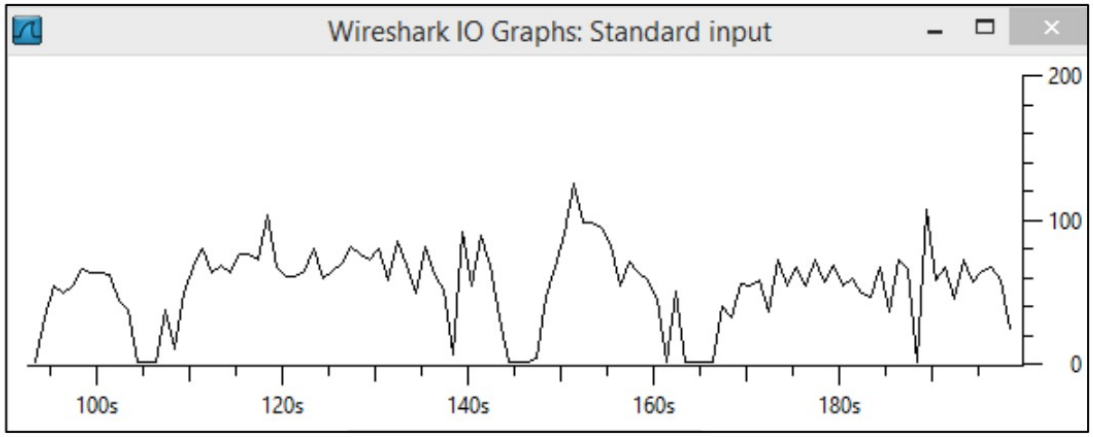
has join the multicast group (225.1.1.1) using IGMPv2 protocol and Figure 4.8 shown the Client 8 (192.168.1.51) has leave the multicast group (225.1.1.1) using IGMPv2 protocol. This Wireshark analyzer can identify the client that query to join or has join or has leave the multicast group with captured data packets and protocol recognition.



a)



b)



c)

Figure 4.9: a) Router 1 to Multicast Server IO Graph, b) Router 2 to Client Interface (GigabitEthernet0/0/1) IO Graph, c) Router 4 to Router 3 IO Graph

Figure 4.9 above shows the IO graph of the User Diagram Protocol (UDP) total data traffic. It's determined the data packets in the rate per second based on the video duration length. The time (second) is measured by the x-axis data and the y-axis data is the number of packets per stick in this graph. This IO graph were took from the three different interfaces. As can see from the IO graph, the low and high of data traffic flow were from the video simulation session.

Wireshark Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	6863	100.00 %	9388094	0.834	0	0	0.000
Ethernet	100.00 %	6863	100.00 %	9388094	0.834	0	0	0.000
Internet Protocol	100.00 %	6863	100.00 %	9388094	0.834	0	0	0.000
User Datagram Protocol	99.84 %	6852	99.99 %	9387240	0.834	0	0	0.000
Data	99.84 %	6852	99.99 %	9387240	0.834	6852	9387240	0.834
Open Shortest Path First	0.13 %	9	0.01 %	702	0.000	9	702	0.000
Protocol Independent Multicast	0.03 %	2	0.00 %	152	0.000	2	152	0.000

Figure 4.10: Protocol Hierarchy from Multicast Server

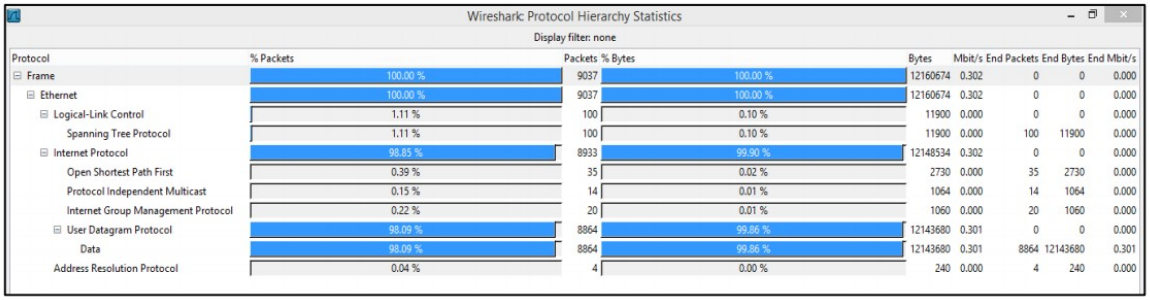


Figure 4.11: Protocol Hierarchy of Clients Interface (GigabitEthernet0/0/0) from Router 1

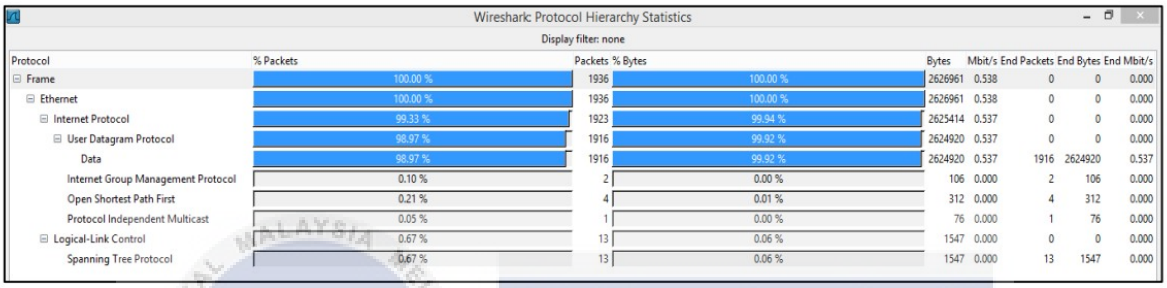


Figure 4.12: Protocol Hierarchy of Clients Interface (GigabitEthernet0/0/1) from Router 1

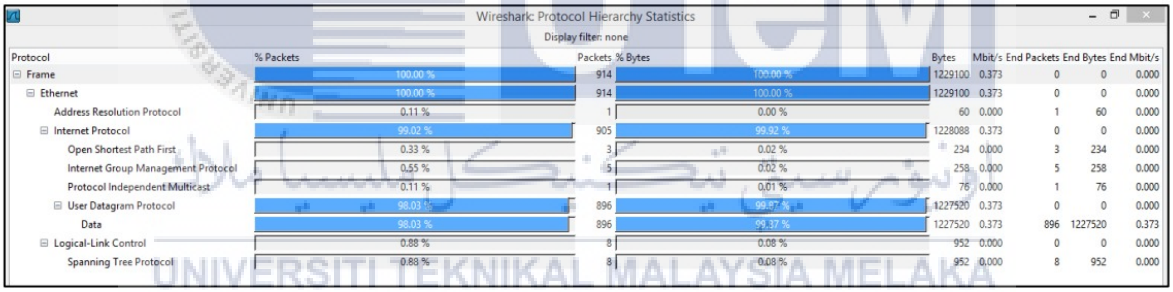


Figure 4.13: Protocol Hierarchy of Clients Interface (GigabitEthernet0/0/0) from Router 2

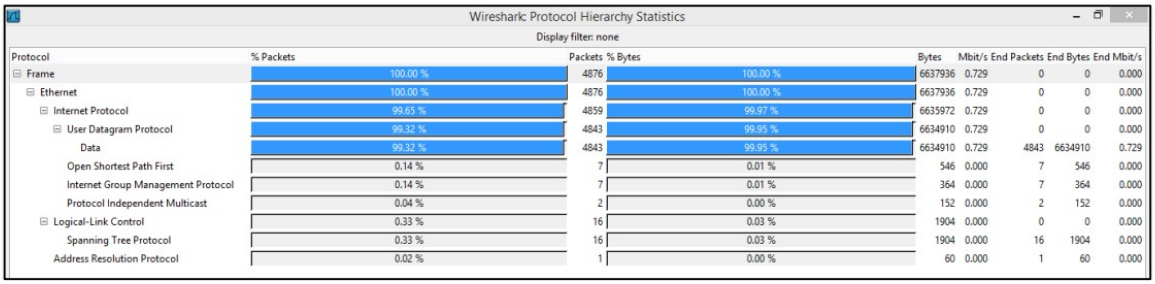
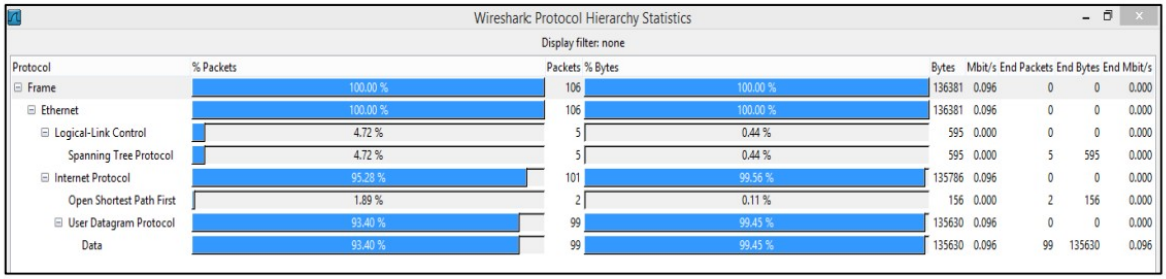
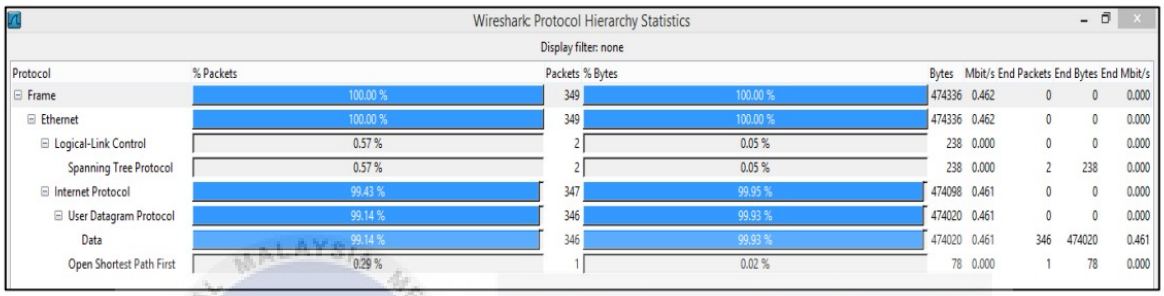


Figure 4.14: Protocol Hierarchy of Clients Interface (GigabitEthernet0/0/1) from Router 2



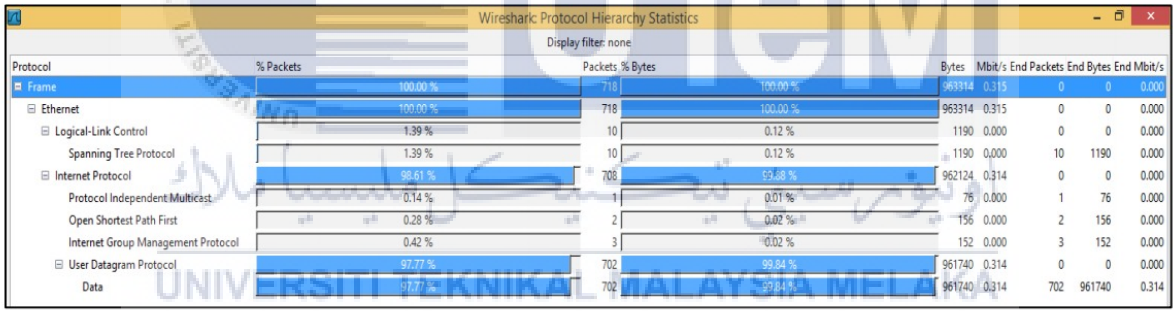
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	106	100.00 %	136381	0.096	0	0	0.000
Ethernet	100.00 %	106	100.00 %	136381	0.096	0	0	0.000
Logical-Link Control	4.72 %	5	0.44 %	595	0.000	0	0	0.000
Spanning Tree Protocol	4.72 %	5	0.44 %	595	0.000	5	595	0.000
Internet Protocol	95.28 %	101	99.56 %	135786	0.096	0	0	0.000
Open Shortest Path First	1.89 %	2	0.11 %	156	0.000	2	156	0.000
User Datagram Protocol	93.40 %	99	99.45 %	135630	0.096	0	0	0.000
Data	93.40 %	99	99.45 %	135630	0.096	99	135630	0.096

Figure 4.15: Protocol Hierarchy of Clients Interface (GigabitEthernet0/0/0) from Router 3



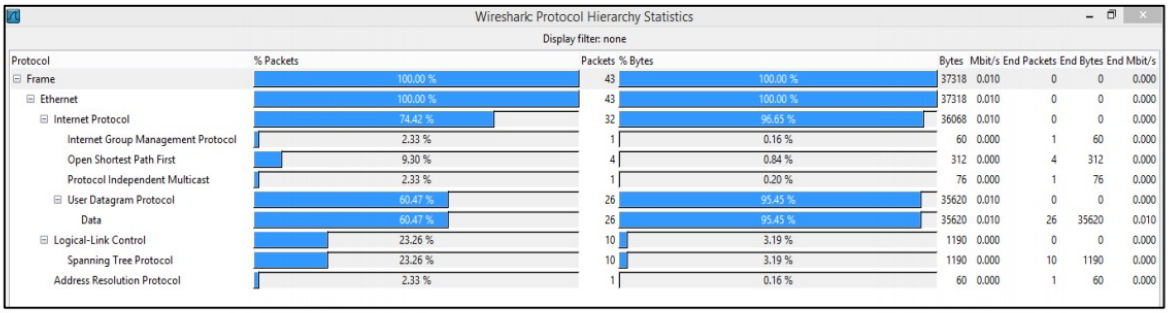
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	349	100.00 %	474336	0.462	0	0	0.000
Ethernet	100.00 %	349	100.00 %	474336	0.462	0	0	0.000
Logical-Link Control	0.57 %	2	0.05 %	238	0.000	0	0	0.000
Spanning Tree Protocol	0.57 %	2	0.05 %	238	0.000	2	238	0.000
Internet Protocol	99.43 %	347	99.95 %	474098	0.461	0	0	0.000
User Datagram Protocol	99.14 %	346	99.93 %	474020	0.461	0	0	0.000
Data	99.14 %	346	99.93 %	474020	0.461	346	474020	0.461
Open Shortest Path First	0.29 %	1	0.02 %	78	0.000	1	78	0.000

Figure 4.16: Protocol Hierarchy of Clients Interface (GigabitEthernet0/0/1) from Router 3



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	718	100.00 %	963314	0.315	0	0	0.000
Ethernet	100.00 %	718	100.00 %	963314	0.315	0	0	0.000
Logical-Link Control	1.39 %	10	0.12 %	1190	0.000	0	0	0.000
Spanning Tree Protocol	1.39 %	10	0.12 %	1190	0.000	10	1190	0.000
Internet Protocol	98.61 %	708	99.88 %	962124	0.314	0	0	0.000
Protocol Independent Multicast	0.14 %	1	0.01 %	76	0.000	1	76	0.000
Open Shortest Path First	0.28 %	2	0.02 %	156	0.000	2	156	0.000
Internet Group Management Protocol	0.42 %	3	0.02 %	152	0.000	3	152	0.000
User Datagram Protocol	97.77 %	702	99.84 %	961740	0.314	0	0	0.000
Data	97.77 %	702	99.84 %	961740	0.314	702	961740	0.314

Figure 4.17: Protocol Hierarchy of Clients Interface (GigabitEthernet0/0/0) from Router 4



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	43	100.00 %	37318	0.010	0	0	0.000
Ethernet	100.00 %	43	100.00 %	37318	0.010	0	0	0.000
Internet Protocol	74.42 %	32	96.65 %	36068	0.010	0	0	0.000
Internet Group Management Protocol	2.33 %	1	0.16 %	60	0.000	1	60	0.000
Open Shortest Path First	9.30 %	4	0.84 %	312	0.000	4	312	0.000
Protocol Independent Multicast	2.33 %	1	0.20 %	76	0.000	1	76	0.000
User Datagram Protocol	60.47 %	26	95.45 %	35620	0.010	0	0	0.000
Data	60.47 %	26	95.45 %	35620	0.010	26	35620	0.010
Logical-Link Control	23.26 %	10	3.19 %	1190	0.000	0	0	0.000
Spanning Tree Protocol	23.26 %	10	3.19 %	1190	0.000	10	1190	0.000
Address Resolution Protocol	2.33 %	1	0.16 %	60	0.000	1	60	0.000

Figure 4.18: Protocol Hierarchy of Clients Interface (GigabitEthernet0/0/1) from Router 4

Based on the Figure 4.10 above, its show the available protocols under the User Datagram Protocol (UDP) are OSPF and PIM on the multicast server. The User Datagram Protocol (UDP) is a substitute communication protocol to the Transmission Control Protocol (TCP), which is primarily used to establish low latency and loss-tolerant connections between internet applications. After that, for the Figure 4.11 until Figure 4.18 shows the hierarchy protocol for all the client interface from router 1 until router 4. Its display the available protocols such as OSPF, PIM and IGMP.

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B
192.168.2.2	225.1.1.1	9 038	12 382 060	9 038	12 382 060	0	0	0.000000000	100.7660	983034.75
192.168.2.1	224.0.0.5	11	858	11	858	0	0	1.219000000	90.5310	75.82
192.168.2.1	224.0.0.13	4	304	4	304	0	0	2.016000000	90.2660	26.94

Figure 4.19: Router 1 to Multicast Server Conversation Data

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B
192.168.2.2	225.1.1.1	19 597	26 847 890	19 597	26 847 890	0	0	0.000000000	264.4060	812323.17
192.168.1.1	224.0.0.5	27	2 106	27	2 106	0	0	5.360000000	254.5620	66.18
192.168.1.1	224.0.0.13	10	760	10	760	0	0	8.750000000	225.3280	26.98
192.168.1.1	224.0.0.1	9	540	9	540	0	0	51.266000000	195.0470	22.15
192.168.1.2	225.1.1.1	9	414	9	414	0	0	51.485000000	194.9680	16.99
192.168.1.3	225.1.1.1	9	414	9	414	0	0	51.500000000	194.9690	16.99

Figure 4.20: Client 1 and Client 2 to Multicast Server Conversation Data

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude
192.168.2.2	17 097	23 422 890	17 097	23 422 890	0	0	-
225.1.1.1	17 097	23 422 890	0	0	17 097	23 422 890	-
192.168.2.1	27	2 092	27	2 092	0	0	-
224.0.0.5	20	1 560	0	0	20	1 560	-
224.0.0.13	7	532	0	0	7	532	-

Figure 4.21: Router 1 to Multicast Server End Point Data

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude
192.168.1.113	8	602	8	602	0	0	-
224.0.0.13	2	152	0	0	2	152	-
224.0.0.5	5	390	0	0	5	390	-
224.0.0.1	1	60	0	0	1	60	-
192.168.1.115	1	46	1	46	0	0	-
225.1.1.1	225	305 602	0	0	225	305 602	-
192.168.1.114	1	46	1	46	0	0	-
192.168.2.2	223	305 510	223	305 510	0	0	-

Figure 4.22: Client 15 and Client 16 to Multicast Server End Point Data

Figure 4.19 until Figure 4.22 shows the conversation and end point captured data from router and client to multicast server. As can see, the Router 1 (192.168.2.1) try to communicate with IP address 224.0.05 where is the OSPF (Open Shortest Path First) default IP address for all routers and IP address 224.0.0.13 which is the PIM default IP address. When it can communicate, it will send Hello packets to all OSPF routers on the network segment and receive data packet from multicast server as shown as in Figure 4.19. However, it same happen to the Client 1 and Client 2 that want to reach the IP address 224.0.0.5 and 224.0.0.13 as shown as in Figure 4.20. Next, for the end point sessions as shown as in Figure 4.21 and Figure 4.22, after it send and receive all data packets to a specific IP address it will end any transmission of data.

4.5.2 Comparison for PIM-DM Protocol Data Traffic on each Interface

Table 4.13: Data Traffic Comparison for PIM-DM protocol on each Interface

Interface	Protocol	Packet Data Captured	Data Captured (Bytes)	Average Data Captured (Bytes/Sec)
Multicast Server to Router 1	PIM-DM	53280	72851421	275302
Multicast Server to Router 2	PIM-DM	53284	72877604	275389
Multicast Server to Router 3	PIM-DM	53290	72906425	275470
Multicast Server to Router 4	PIM-DM	53295	72956810	275682
GigabitEthernet0/0/0 from Router 1	PIM-DM	53288	72972643	169054
	IGMP	52728	72987237	167842
GigabitEthernet0/0/1 from Router 1	PIM-DM	53276	72901644	168912
	IGMP	52859	72976543	278935
GigabitEthernet0/0/0 from Router 2	PIM-DM	53289	72892601	278642
	IGMP	52884	72789161	278851
GigabitEthernet0/0/1 from Router 2	PIM-DM	53293	72459023	278730
	IGMP	52875	72865234	278863
GigabitEthernet0/0/0 from Router 3	PIM-DM	53274	72982450	178923
	IGMP	52967	72563420	279763
GigabitEthernet0/0/1 from Router 3	PIM-DM	53297	72967821	279752
	IGMP	52967	72563420	169875
GigabitEthernet0/0/0 from Router 4	PIM-DM	53282	72992404	278916
	IGMP	52967	72563420	169512
GigabitEthernet0/0/1 from Router 4	PIM-DM	53279	72997652	278963
	IGMP	52967	72563420	279780

Based on the Table 4.13, it's shown the data traffic captured by using Wireshark analyzer software for PIM-DM protocol. The different data traffic are from the Multicast server that has been transferred on each client. From the GigabitEthernet0/0/0 interface from Router 1 until GigabitEthernet0/0/1 interface from Router 4 data captured, it's all around 72000000 Bytes. This is a proven where the PIM-DM protocol implementation is more efficient and bandwidth reduction. As can see, all the data transferred by Multicast Server to the all client interface is nearly similar value which is over 72000000. Moreover, the PIM-DM protocol can be stable when the network become complex.

4.6 Discussion

As discussion from this multicast campus network project, all the network elements were successful configured and functioned well in the simulation. The first step is to settle up the basic configuration. To avoid IP address overlapping, the calculation of IP address to get the range were needed. In this project, the IP address for client interface start from 192.168.1.1 with chosen subnet mask 255.255.255.240 that equivalent to /28. Although in this topology have switches, the switches will remain unconfigured since it functioned can reduce the usage of router interface. Following with the routers configuration, the routers need to be trucking by assigned IP address of 192.168.2.1 with subnet mask /30 that equivalent to 255.255.255.252. This subnet mask of /30 was chosen because of it consists two usable host and the configuration only on the two interfaces of the routers. This technique will reduce and keep away from wasted the usable host IP address. Next, the configuration for the multicast server that need to be assigned with multicast group IP address. The multicast group IP address have a

range where it start from 244.0.0.0 until 239.255.255.255 and the address of 225.1.1.1 has been chosen as the multicast address.

After all the configuration were completed, the multicast protocol at the CLI command prompt on the router interface need to be implemented. Firstly, enable the multicast routing on each router interface. Secondly, enable the PIM-DM protocol at every interface where have connection with all client and router. Same goes to IGMP protocol, enabled the command on every client interface only. Then, enable OSPF protocol to reach the full connectivity of the campus network topology. The summarization of network address such as 192.168.0.0 with subnet mask 255.255.0.0 and declare all the area network elements on this topology as Area 0 where it known as the backbone area. After that, ping test the client to client and client to server, and also from router to server and client were successfully. This ping test is to check whether the connections are reachable or not.

The next part is to run the simulation by browsing any video play that have VLC player media path. Before continue to run the simulation, check all the client configuration that must be configure with multicast group IP address 225.1.1.1 at the destination IP address and the destination MAC address 01-00-5E-01-01-01 on the MCPacket section. Finally, the video with 2 hours duration length and before that all the client need to select 'Join' button then select the 'Show VLC' to display the same video play on the MCPacket section can be run. All the packets data captured that has been obtained over 72000000 Bytes and has been prove the PIM-DM protocol implementation is more efficient and reduce the bandwidth. However, to get the successful video streaming to all client, from the multicast server should run the video simultaneously with all the client. Besides that, at a few seconds sometimes will happen buffering video play. Typically it happen because of different IP address range and might causes some interruption.

Other than that, the captured data packets and observed the data flow during the simulation occurs by using Wireshark software had been done. It can obtained the IO graph that show the total data traffic based on the video duration length. The protocol hierarchy and the conversation and endpoint data of several devices in the topology were observed. Although the simulation were successful, there are some issues that had faced during the simulation process. The main problem is to configure the routers. The understanding on how to ensure all the client and router interface have suitable multicast protocol to enable is very important. The next issue is incorrectly assigned for multicast group IP address at the client configuration. The mistaken IP address that used is 255.1.1.1 and the correct IP address has been change to 225.1.1.1. Lastly, this multicast campus network were successful accomplished with the proven results of streaming video and Wireshark software can captured packet data traffic from the simulation network by using eNSP software and analysed the data traffic that have been captured from the data packet.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Overview

The Multicast Protocols Efficiency in A Campus Network Environment using eNSP project has been done study and accomplished. The suitable PIM protocol to be applied is PIM-DM protocol. That is because PIM-DM does not use Rendezvous Point or RP and it is only uses source-based trees, which makes it easier to execute and implement than PIM-SM. For this finale chapter, there will have some recommendation and suggestion that beneficial to enhance this multicast campus network project in the future.

5.2 Conclusion

At the end of this chapter, from a source information can transfer a single copy of the information to a single multicast address that can distributed to the whole group of recipients by using multicast technique. Other than that, multicast can reduces the overload burden of client computers who are not involved in the handling of unnecessary data packets with the multicast traffic. The multicast method of network communication saves a great deal of bandwidth. For instance, the data size of many traffic types for video streaming is very high. By transmitting a single stream to multiple recipients, the multicast form of network communication enables significant savings in bandwidth requirements. It can also minimize the unnecessary number of streaming servers. If the unicast form of network communication is used for heavy video streaming, more server hardware and other resources are required.

However, the design of the network topology of campus network and able to deliver video streaming to the clients using eNSP software in this project were successfully. In this project topology consist of one multicast server, four routers, eight switches and sixteen clients which is a quite large

scale network. With the precisely IP address configuration and multicast protocol enabled on all the network element, the main objective is to deliver video streaming to all the clients were achieved.

Based on the study, the PIM-DM protocol is more stable for a large campus network compared to PIM-SM protocol. In this project, there is only PIM-DM protocol to be implemented. From the data traffic captured by using Wireshark analyzer software, it has been prove that the PIM-DM protocol is more efficient and bandwidth reduction since the data captured that transferred to all client has similar values around 72000000 Bytes from the Multicast Server. Last but not least, the PIM-DM protocols are the most suitable to be implemented in the campus network because of it is easy to be flooded with data packet when the network become complex.

5.3 Future Work Recommendation

There are have some ideas and recommendation for this part. The first is, the multicast campus network could be design in larger scale network than before in order to study the precisely efficiency of multicast protocol implementation. After that, the multicast campus network could be design in different network simulator such as Cisco Packet Tracer or GNS3 (Graphical Network Simulator 3) and OPNET Network Simulator since the eNSP software is no longer supported by Huawei. Besides, provide the specification of the device such as PC or laptop that good in performance of processor and large RAM in order to smoothly run the large scale network simulation.

REFERENCES

CUI, X. and SHEN, Q. (2018) 'Development of Network Protocol Resolver Based on Wireshark', *DEStech Transactions on Computer Science and Engineering*, (cnai), pp. 208–212. doi: 10.12783/dtcse/cnai2018/24158.

Chen, J. *et al.* (2019) 'WLAN Simulation Experiment Based on ENSP WLAN Simulation Experiment Based on ENSP'. doi: 10.1088/1742-6596/1325/1/012046.

Choi, J., Reaz, A. S. and Mukherjee, B. (2012) 'A survey of user behavior in VoD service and bandwidth-saving multicast streaming schemes', *IEEE Communications Surveys and Tutorials*, 14(1), pp. 156–169. doi: 10.1109/SURV.2011.030811.00051.

Fan, Y. and Li-zhen, Z. (2017) 'Research on Dynamic Visualization Teaching Method of Computer Network', 81(Iccse), pp. 129–135.

Huang, H. *et al.* (2017) 'EMGR: Energy-efficient multicast geographic routing in wireless sensor networks', *Computer Networks*. Elsevier B.V., 129, pp. 51–63. doi: 10.1016/j.comnet.2017.08.011.

Ko, J., Park, S. and Lee, E. (2010) 'An extended PIM-SM for efficient data transmission in IPTV services', *Proceedings - 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC 2010*. IEEE, pp. 115–119. doi: 10.1109/ICNIDC.2010.5657907.

Kim, H., Lee, H. and Lim, H. (2020) 'Performance of Packet Analysis between Observer and WireShark', *International Conference on Advanced Communication Technology, ICACT*, 2020, pp.

268–271. doi: 10.23919/ICACT48636.2020.9061452.

Ma, H., Lv, G. and Wu, C. (2018) 'Campus Network Planning and Design', *Journal of Computer Hardware Engineering*, 1(1), pp. 35–41. doi: 10.24294/JCHE.V1I1.273.

Musa, A. *et al.* (2019) 'An Investigation into Peer-to-Peer Network Security Using Wireshark', *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*. IEEE, (December 2019), pp. 1–6. doi: 10.1109/icecco48375.2019.9043236.

Oliveira, P., Silva, A. and Valadas, R. (2016) 'The HPIM-DM Multicast Routing Protocol'. Available at: http://arxiv.org/abs/2002.06635.

Pavithirakini, S. *et al.* (2016) 'Improve the Capabilities of Wireshark as a tool for Intrusion Detection in DOS Attacks', *International Journal of Scientific and Research Publications*, 6(4), p. 378. Available at: www.ijsrp.org.

Papan, J. *et al.* (2016) 'The new PIM-SM IPFRR mechanism', *ICETA 2015 - 13th IEEE International Conference on Emerging eLearning Technologies and Applications, Proceedings*. doi: 10.1109/ICETA.2015.7558504.

Suntu, S. L. (2017) 'Design and Security Simulation of Wi-Fi Networks', pp. 1–10. doi: 10.22247/ijcna/2017/49249.

Shihab, S. S. and Mohammed, I. J. (2017) 'PIM-SM based Multicast Comparison for IPv4 verses

IPv6 using GNS3 and JPERF', *Iraqi Journal of Science*, 58(1), pp. 140–151.

Vodnala, D., Phani, S. and Aluvala, S. (2014) 'An Analysis Study of Various Multicast Routing Protocols in MANETs', 4(8).

Yen, L. *et al.* (2018) 'PIM-Compliant SDN-Enabled IP Multicast Service', pp. 2–5.

Yu, Z., Xu, X. and Wu, X. (2010) 'Application of wireless mesh network in campus network', *2010 2nd International Conference on Communication Systems, Networks and Applications, ICCSNA 2010*, 1, pp. 245–247. doi: 10.1109/ICCSNA.2010.5588704.

Zhao, Q. and Ding, G. Z. (2017) 'The design and analysis of campus network under the background of triple play', *Proceedings - 2016 International Conference on Information System and Artificial Intelligence, ISAI 2016*. IEEE, pp. 100–103. doi: 10.1109/ISAI.2016.0030.

Zhou, D. (2017) 'A Survey on Campus Network Log Derong Zhou', 114(Ammee), pp. 859–863.

Zhang, Y. and Wang, Q. (2017) 'Development of Simulation Experiments for the Curriculum of Data Communication and Computer Network', 118(Amcce), pp. 1087–1090.

APPENDIX

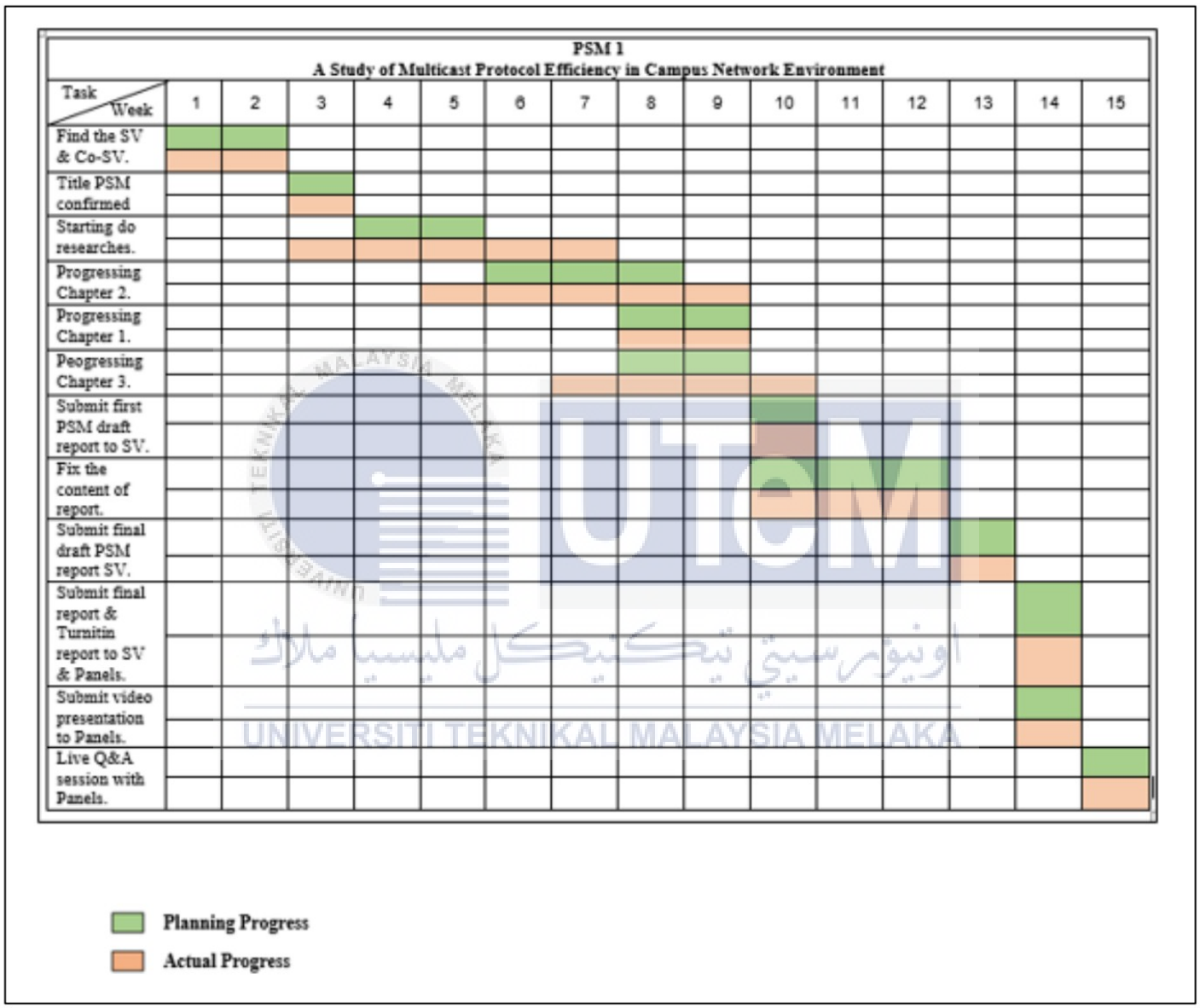


Figure 5.1: Projek Sarjana Muda 1 (PSM 1) Gantt Chart