Faculty of Electrical and Electronic Engineering Technology

DESIGN AND IMPLEMENTATION OF SECURED MULTICAST SERVICE IN CAMPUS NETWORK

KHAIRUNNAJWA BINTI M KAMAL

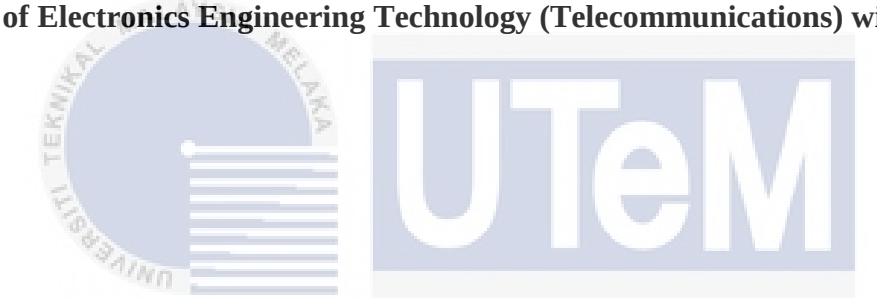
Bachelor of Electronics Engineering Technology (Telecommunications) with Honours

2021

DESIGN AND IMPLEMENTATION OF SECURED MULTICAST SERVICE IN CAMPUS NETWORK

KHAIRUNNAJWA BINTI M KAMAL

A project report submitted
in partial fulfillment of the requirements for the degree of
Bachelor of Electronics Engineering Technology (Telecommunications) with Honours



Faculty of Electrical and Electronic Engineering Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

DECLARATION

I declare that this project report entitled “Design and Implementation of Secured Multicast Services in Campus Network “ results from my research except as cited in the references. Therefore, the project report has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

Signature : 

Student Name : KHAIRUNNAJWA BINTI M KAMAL

Date : 10 JANUARY 2022

APPROVAL

I, at this moment, declare that I have checked this project report. In my opinion, this project report is adequate in terms of scope and quality for the award of the degree of Bachelor of Electronics Engineering Technology (Telecommunications) with Honours.

Signature :

Supervisor Name : TS. FAKHRULLAH BIN IDRIS

Date : 11 JANUARY 2022

DEDICATION

I strongly want to dedicate this project to my loving and supportive parents, M Kamal Bin Abdul Kadir and Umi Khalsum Binti Saberi, who has always been a source of inspiration and strength throughout my journey on completing this project. Also, not forget about my friends, who are continuously motivating me to improve as a person in the future. I have nothing but love and the deepest appreciation for Ts. Fakhrullah bin Idris, my gentle and kind-hearted supervisor, for his encouragement and advice. Finally, I want to express my gratitude to Allah S.W.T. for blessing my life much more than I deserve.

ABSTRACT

Network security is an important component of a campus network design. The Campus network addresses network infrastructure security challenges. The protected network protects the key information and data of the industry against network safety threats. A network of institutions offers a wide variety of applications, including teaching, learning, research, management, e-library and publication of results. The network of universities must be constructed to safeguard against various threats and attacks. The Hierarchical Network Model was used to bring together the numerous services that make up the network system as a whole in this article. The physical and logical network topology for the Faculty of Engineering infrastructures was designed, and the simulation results revealed that any user who attempted to connect to the network and initiated http traffic was redirected to the authentication server for credential verification before being allowed on the network. The Cisco Adaptive Security Appliance, Core Router, Distribution Switches, and Integrated Service Routers were also appropriately configured, according to the results. This architecture also improved communication, with the addition of new devices having no impact on packet transit. Finally, the specifications and commands utilised in this research are a model that might be updated and used by other Faculties or Universities.

ABSTRAK

Keselamatan rangkaian adalah komponen penting dalam reka bentuk rangkaian kampus. Rangkaian Kampus menangani cabaran keselamatan infrastruktur rangkaian. Rangkaian yang dilindungi melindungi maklumat dan data utama industri daripada ancaman keselamatan rangkaian. Rangkaian institusi menawarkan pelbagai aplikasi termasuk pengajaran, pembelajaran, penyelidikan, pengurusan, e-perpustakaan dan penerbitan hasil. Jaringan Universiti mesti dibina untuk melindungi dari pelbagai ancaman dan serangan. Model Rangkaian Hierarki telah digunakan untuk mengumpulkan pelbagai perkhidmatan yang membentuk sistem rangkaian secara keseluruhan dalam artikel ini. Topologi rangkaian fizikal dan logik untuk infrastruktur Fakulti Kejuruteraan telah direka, dan hasil simulasi mendedahkan bahawa mana-mana pengguna yang cuba menyambung ke rangkaian dan memulakan trafik http telah diubah hala ke pelayan pengesahan untuk pengesahan kelayakan sebelum dibenarkan pada rangkaian. Perkakas Keselamatan Adaptif Cisco, Penghala Teras, Suis Pengedaran dan Penghala Perkhidmatan Bersepadu juga dikonfigurasikan dengan sewajarnya, mengikut keputusan. Seni bina ini juga meningkatkan komunikasi, dengan penambahan peranti baharu tidak memberi kesan kepada transit paket. Akhir sekali, spesifikasi dan arahan yang digunakan dalam penyelidikan ini adalah model yang mungkin dikemas kini dan digunakan oleh Fakulti atau Universiti lain.

ACKNOWLEDGEMENTS

First and foremost, I want to express my gratitude to Ts. Fakhrullah Bin Idris, my supervisor, for their excellent guidance, unwavering support, and patience during my bachelor's degree programme. Their vast knowledge and wealth of experience have aided me throughout my academic career and daily life.

I owe a debt of gratitude to Universiti Teknikal Malaysia Melaka (UTeM) and my sibling for their financial assistance in helping me to complete the project during a challenging time.

My highest appreciation goes to my parents and family members for their love and prayer during the period of my study. An honourable mention also goes to Mohamad Syafiq Bin Mohd Zukeri for all the motivation and understanding.

Finally, I would like to thank all my friends, fellow colleagues and classmates, the Faculty members, as well as other individuals who are not listed here for being co-operative and helpful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

LAN	-	Local Area Network
CNPS	-	Campus Network Primarily Scenario
DHCP	-	Dynamic Host Configuration Protocol
FTP	-	File Transfer Protocol
SMTP	-	Simple Mail Transfer Protocol
OSI	-	Open System Interconnection
WAN	-	Wide Area Network
UANS	-	University Area Network Scenario
UDN	-	University Data Network
VLANs	-	Virtual Local Area Network
ACL	-	Access Control List
CPT	-	Cisco Packet Tracer
SSM	-	Source-Specific Multicast
HTTP	-	Hypertext Trasfer Protocol
eNSP	-	Enterprise Network Simulation Platform
OPNET	-	Optimize Network Engineering Tool)
GUI	-	Graphical User Interface
NS2	-	Network Simulation 2
NAM	-	Network Animator
OTcl	-	Object-oriented Tool Command Language
TCL	-	Telephone Communication Limited
DSR	-	Dynamic Source Routing
UDP	-	University Data Protocol
NS3	-	Network Simulation 3
VPN	-	Virtual Private Network
SAN	-	Secure Area Network
EIGRP	-	Enhanced Interior Gateway Routing Protocol
CAN	-	Campus Area Network
QoS	-	Quality of Service
STP	-	Spanning Tree Protocol
WAPS	-	Wireless Access Point
MACL	-	MAC Access Control List
VACLs	-	VLAN Access Control List
PSM	-	Projek Sarjana Muda
MAC	-	Media Access Control Address
VTP	-	VLAN Trunking Protocol
DMVPN	-	Dynamic Multipoint Virtual Private Network

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background

Information and communication have become essential factors in our everyday lives. It helps to cross borders between communities. People obviously use technology in all aspects of their lives, including education, healthcare, politics, the economy and the military. Many network applications now do not contain security, namely data leakage, modification of information, illegal use of network resources, illegal data penetration, false information, and so on [1]. Because multi-computer network security concerns are uncommon, "hackers," corporate and government websites are increasingly "attacked," resulting in increased economic losses. Security and prevention of the network information system and its secrecy therefore appear increasingly crucial.

As network connectivity on the campus has expanded rapidly, network applications have grown speedily and information security on the campus network has now received greater attention. Recent network monitoring, systems, and hosts have discovered that there are attempts to attack others, that there are many security vulnerabilities in the system, and that many security vulnerabilities are difficult to prevent and eliminate, and that a network virus has severely harmed the normal operation of the campus network. The concepts, principles, models, secure networks and network design architectures are all covered in this project. It also discusses network safety and the benefits that may be realized by a consistent design approach, since it ensures that all the information provided by networked computers is protected.

1.2 Problem Statement

In college or university network development, the biggest problem is the limited funds invested in network equipment. Systemic inputs for building and network security management are not taken seriously. A potential problem with non-hierarchical networks, besides broadcast packets, is the server workload required for routers to communicate with many other routers and process numerous route advertisements.

In general, the college or university has a computer room, and specific PCs in this area have direct access to the campus computer network. Students and staff are normally available to use the computers for online and online learning. However, the lack of security for logging system does not make these computer rooms unsecure for administration. Most rooms have serious registration and administration flaws, which means that the identity of the internet user cannot be recognized [2].

It makes it very convenient for us to use campus network functions, but it's also a rapid way to distribute the malware. Outbreaks of network viruses can immediately lead to privacy for the user and important data leaks. Due to the data leaks that use a large of network resources, it will lead to a significant decrease in network performance.

1.3 Project Objective

This project aims for Secured Multicast Services in the Campus Network with packet tracer design and implementation. The design is based on the hierarchical architecture of a university model campus as a case study. Specifically, the objectives are as follows:

a) To design campus network architecture by using a hierarchy network design

b) To simulate the security for all system in campus network using Cisco Packet Tracer software.

c) To analyze the performance of two scenario network design by identify security cisco firewalling solutions scanning processes and measurable parameters such as latency and throughput.

1.4 Scope of Project

The proposed project is to design the architecture with two scenarios of a network utilizing Cisco Packet Tracer (CPT) to analyze the performance which enables a virtual design of an advanced computing network to work on test scenarios without requiring any real components. The size of classes, laboratories, office complexes, and the number of students and employees for each Department in the Faculty were all gathered, as well as the Faculty's future demands. The Faculty of Engineering has eight Departments, Agriculture & Environmental Engineering, Chemical Engineering, Civil Engineering, Computer Engineering, Electrical Engineering, Marine Engineering, Mechanical Engineering and Petroleum Engineering. To assist in the design of the Institution's Enterprise Network's logical and physical topology.

Total number of users in the case study = number of employees + number of students = 7,674. The network is designed for 32,736 users, although it may be grown up to roughly 65,000. This topology delivers data relatively quickly from one location to another. The performance security tasks with Wireshark include intrusion detection, the identification and definition of harmful signatures and passive discovery of hosts, operating systems and services.

1.5 Thesis outline

There is a total of five chapters in this thesis, including introduction, literature review, methodology, outcome and discussion, and conclusion and recommendation. The outline of the project and the progress of the work are discussed and written in detail corresponding to each chapter.

The main objective of Chapter One is to introduce the project to the target panel by Identifying the reasons and the kick-starter for starting this project. This chapter is detailed Explains the background of the project with its related real-life problems.

Chapter Two reviewed the past research journal and the related case study. This chapter mainly discusses and analyses the literature on design network campus and their secure network information from different research papers related to the network before this project is critically analyzed and summarized. Summary information is integrated into an automated design.

Chapter three focuses on the methodology of the project and the process taken to complete the project. The application of the software program to development is discussed in this chapter. This chapter also highlights the equipment involved in this project, together with the specification for each part of the elements used.

Chapter four highlights information developments for all variables involved in this project. The detailed methods used for data capture are outlined in this chapter, together with the proper figures, tables and charts. The information captured was analyzed and discussed to gain an even more overview of this project.

Finally, Chapter Five observes the findings and the outcome of the work. True results have been highlighted once again to show that the result is drawn based on the facts and the correct data. The recommendation was put into place to provide specific recommendations for a future case study on this project.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

A campus network is an important aspect of college life, and network security is especially important. A secure network protects a company from network-based security threats. A university network includes teaching, learning, research, administration, e-library, and outcome publication [3]. The application systems of digital information systems can only run normally if a high-speed, stable, safe, and reliable campus network is established [1]. The campus network is a big branch of many types of networks that can be used for a variety of purposes. University Net provides powerful computers and Internet applications for staff and students in fields such as education, scientific research, administration, and other sectors. On-campus, the internet was successfully tested for the first time. The success of a campus network depends on its investment capital, network technology, and management. The campus network is a big branch of many types of networks that can be used for a variety of purposes. University Net provides powerful computers and Internet applications for staff and students in fields such as education, scientific research, administration, and other sectors. On-campus, the internet was successfully tested for the first time. The success of a campus network depends on its investment capital, network technology, and management [4].

2.2 A network architecture in the campus area

The separation of identification and location, access or core separation and the architecture of the network control or transmission can improve mobility, safety and dependability [5]. Developing a campus network may not appear to be as interesting or exciting as designing an associate IP telephone, an associate telephone network, an IP video network, or perhaps creating a wireless network. It establishes a common topology of building blocks that allows the network to easily evolve. Figure 2.1 shows the basic Design and Implementation of the Secure University Network. Regardless of network size or requirements, adhering to the well-structured engineering principles outlined below is crucial to the effective execution of any network design [6].

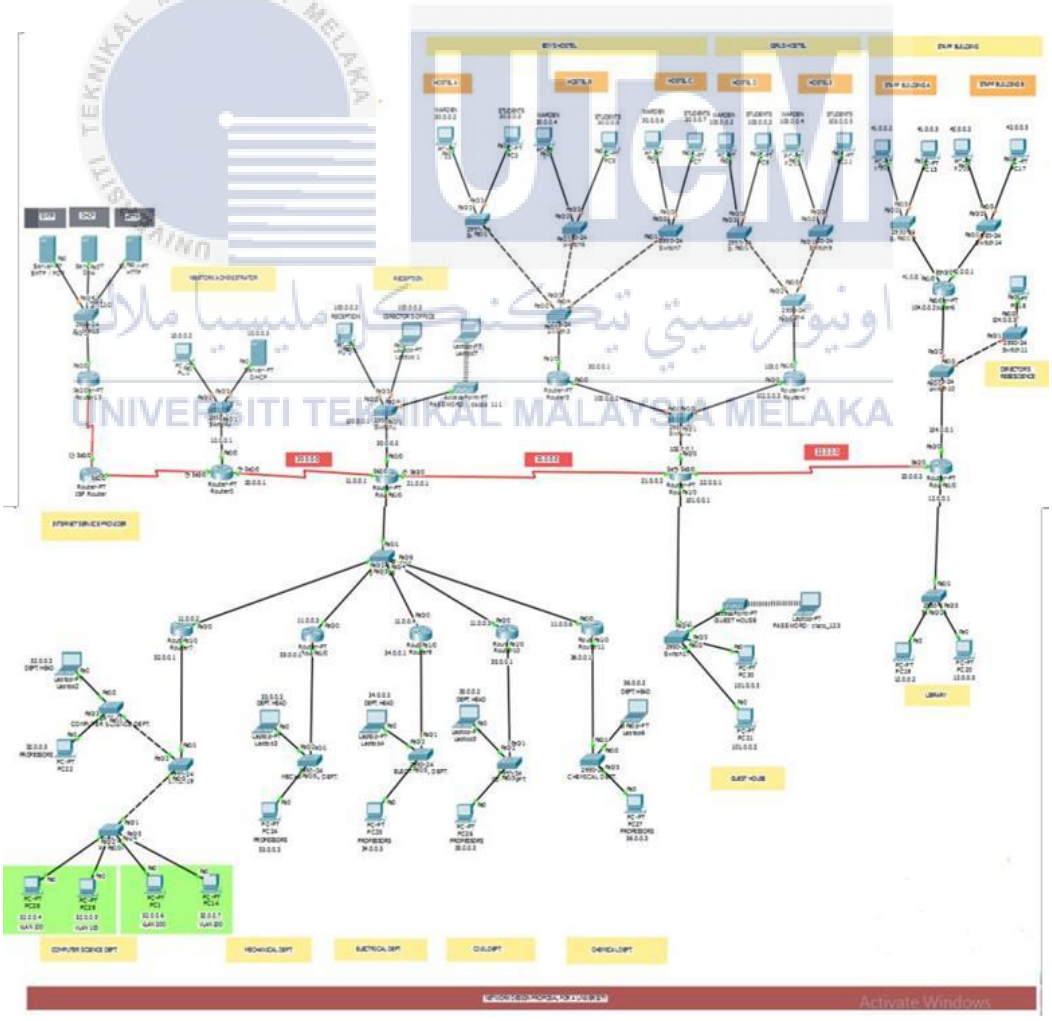


Figure 2.1 Basic complete architecture campus area [6]

2.2.1 Hierarchical design

The hierarchical design paradigm of the network divides up the complex flat network into several smaller and more manageable networks. It offers a great level of flexibility to network designers to optimize and choose the proper network hardware, software and features [7]. First, the campus is usually characterized as a three-tier hierarchy model with core, distribution and access layers such as figure 2.2 show below. The fundamental principle of the hierarchical design is that each part of the hierarchy has a different set of tasks and services and a different role for the overall design [4]. This hierarchical network design has the advantage of being scalable. When we grow on the campus and obtain additional users, buildings and floors, we can add more tiers of distribution. We will add another layer when this happens:

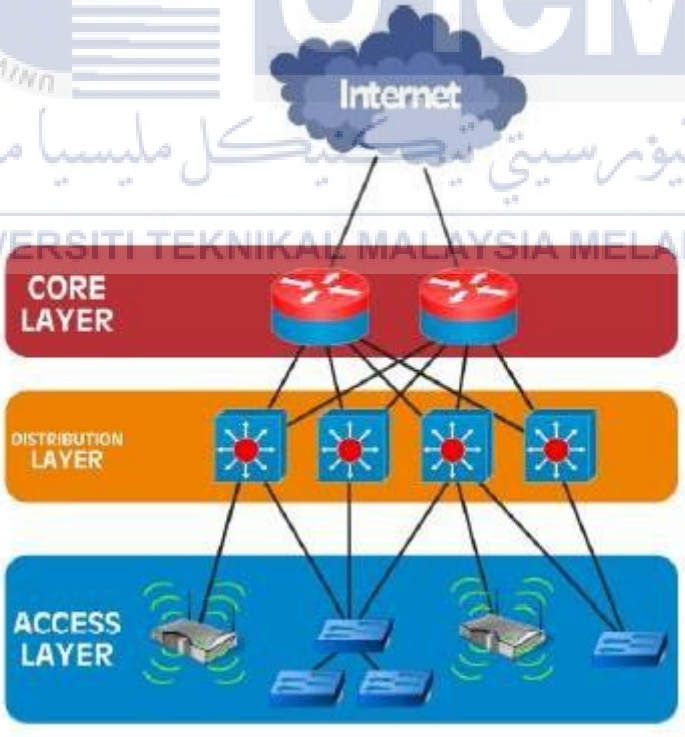


Figure 2.2 Flow network hierarchical design [8]

2.2.1.1 Core Layer

The core layer function is to offer rapid and efficient transportation of data. The high-speed switching backbone of the network is the core layer. Core layer devices should achieve high availability and reliability because the core is critical for connectivity. The core layer adds all the various distribution layer switches. This design also helps to predict and analyze our traffic routes [9].

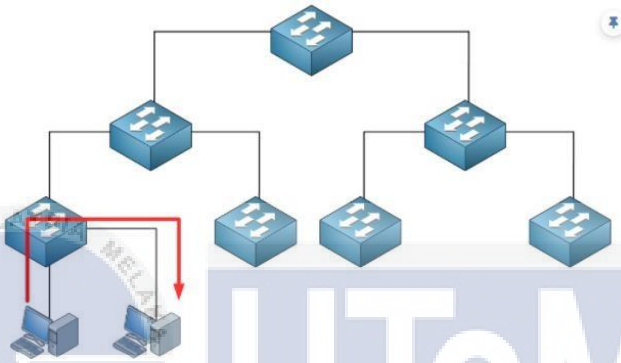


Figure 2.3 Basically three different transportation flows

All traffic begins at the access layer and moves the distribution and core layer as necessary. In this scenario, traffic is local the access layer switch does not depart. Traffic between two hosts in the same VLAN could occur such as figure 2.3 show above.

2.2.1.2 Distribution layer

The distribution layer serves as a bridge between the different access points and the core layer and a separation between the access and core levels. The distribution layer manages access and provides policy-based connectivity to departments and workgroups. A multilayer router or switch is used to split workgroups and isolate network problems. The distribution can also enable LAN or WAN connection aggregation, redundancy and load balance [4]. The distribution layer additionally adds capacity in a campus environment by integrating many low-speed access connectivity links to a high-speed core link and

segmenting network defects to prevent them from damaging the core layer. This layer ensures the redundant connections of access devices. Load balance between devices with redundant connections is also conceivable. This layer also has the aim of defining boundaries by implementing access lists and other filters. The distribution layer thereby defines the network policy. The distribution layer includes 3 switches in the high-end layer. The Distribution Layer guarantees that packets are appropriately routed between your industry's subnet and VLAN.

2.2.1.3 Access layer

The access layer is the focus point where customers access the network. Access layer devices traffic control by localizing access media service requests. The edge of the wired network is the access layer. The access layer often contains switched LAN devices with ports that offer connectivity for workstations and servers in the campus setting. It is where terminal devices are connected to the rest of the campus [4]. Some devices attached at the access layer create a micro-extension beyond an access switch's physical port. It provides security, QoS, device discovery and even physical infrastructure services.

2.3 Security issues in a campus network

Security has been an essential issue within the style in readying of an enterprise proprietary network. A secured network protects a business from network-related security threats. Teaching, learning, research, management, e-library, and result publication are all part of a university network. This study's theoretical contribution could be used as a model for university campus planning [9]. Many universities today have a wide range of network attacks and security risks, as well as network attack tactics and categorizations. The problem of college network security is becoming increasingly prominent. The development of college

campus networks should be boosted. Schools must improve the design and implementation of security defense systems. The article examines the most frequent security issues on college campuses.

2.3.1 Identify the threat

2.3.1.1 Computer virus

The largest threat to the security of the campus network is a computer virus. Computer viruses do a lot of damage. Viruses are software developers designed to spread from machine to machine. They are often sent by email or downloaded from specialist websites as attachments. Viruses are known to spam, disable security policies, damage your laptop and steal data [10].

2.3.1.2 Rogue security software

Malicious software might trick people into thinking that they have a computer virus installed on their machine. You can install or change security settings for users. Both situations lead to genuine malware on your machine is installed [11].

2.3.1.3 Trojan horse

A Trojan horse is a piece of malicious code or software that misleads users. They are often spread via email. It could look like a friend's correspondence. Trojans can also be spread by clicking on a fake ad. A Trojan horse can record your passwords while it has access to your machine by picking up keystrokes [10].

2.3.1.4 Adware and spyware

Some malicious attacks can make use of the "fool-like" spy attack software flooded on the network. Illegal users can carry out unscrupulous attacks on the campus.

2.3.2 Types of network attacks

Classes of attacks could add passive monitoring of communications, active network attacks and service provider attacks. Data systems and data networks offer attractive objectives and are resistant to attacks by many threatening entities, from hackers to national states [12]. Here are some attacks types:

a) Passive Attack
b) Active Attack
c) Distributed Attack
d) Insider Attack
e) Close-in Attack
f) Phishing Attack
g) Hijack attack
h) Spoof attack
i) Password attack

2.4 Multicast Service (MS)

Multicast is a point-to-multipoint communication technique in which data packets are sent from a single source to numerous destinations at the same time. Multicast, on the other hand, is the delivery of content to a specific set of subscribers to those services. The multicast content is broadcast over a geographical area known as a zone, which is made up of one or more base stations all broadcasting the same material. Multicast Service (MS) was

designed to make efficient use of radio and network resources while broadcasting audio and video information to many end-users. This is also accomplished via MS, which sends out as many unicast signals as the number of original receivers. This technique necessitates at least as many transmissions as the multicast group's total number of stations. Multicast allows a sender to deliver a single feed of data to numerous receivers, duplicating data only when it needs to follow a diverging path for the various receivers [13]. This results in substantially less bandwidth being consumed across downlinks, even when hundreds of hosts are involved. Internally and to and from the worldwide internet, the University Data Network (UDN) backbone enables multicast. The institutional network administrator determines support institutions connected to the UDN, if users within an institution have any questions, they should first contact their local network administrator.

2.5 Classified network device

2.5.1 LAN

LAN is a network that uses physical connections to connect multiple computers in a small geographical area. It allows for high-bandwidth communication and is also a relatively inexpensive media. The performance of a LAN is also influenced by external factors such as hardware, topology, traffic load, and the network's purpose. There are a number of professional tools on the market that can forecast a LAN's performance [14].

2.5.2 Switch

The campus network mostly consists of Gigabit Ethernet switches. Install a primary switch and seven subsidiary switches. Each switch features fibre extension ports and extension modules slots. The backbone of the Gigabit network is the campus network. Fast exchange on the desktop, in order to keep all users on calling service resources, allow the

role of the teacher in the multimedia classroom to playfully while ensuring the smoothest working of the campus network for all users at the same time. A switch that also transfers data in packet form. By looking at the physical device address, it delivers data from one user to another user. A switch also has an advantage as a router [8].

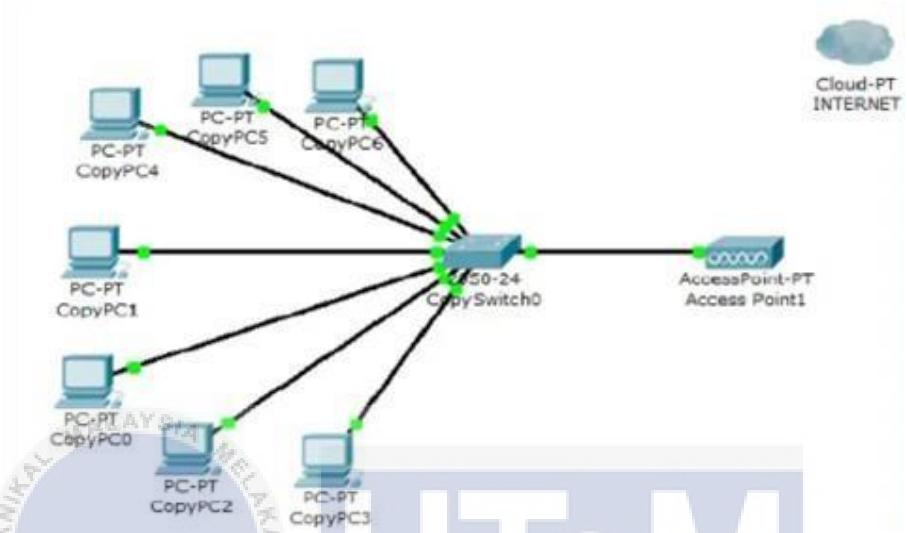


Figure 2.4 Switch of ethernet

2.5.3 Hub

A hub is the simplest networking device that links different network devices to each other through ethernet. Multiple connection devices in a Local Area Network (LAN), but network switches have replaced hubs and are connected to the hub because they consist of different input and output ports [15]. In current days, finding a network hub in a genuine LAN is becoming increasingly challenging. Hubs are the main connectivity point for a LAN. If a hub gets an Ethernet frame from a network device at one of its ports from a data packet, the hub distributes the packet repeats to all ports on all other network devices. A collision happens when two network devices on the same network attempt to send packets simultaneously as Figure 2.5 shows.

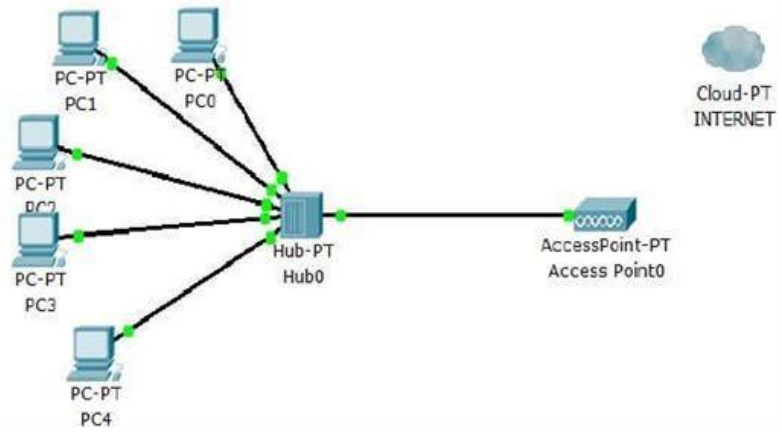


Figure 2.5 Hub of ethernet

2.5.4 Virtual Local Area Network (VLANs)

Virtual Local Area Network (VLAN) is a virtual local area network consisting of one or more LANs. It allows for the integration of several network devices into a single logical network. A virtual LAN that can be managed in the same way as a physical LAN was thus built. A computer network can be established by dividing a single network-layer into several different broadcasting domains. Packets can only be isolated from each other via routers [16].

2.5.5 Access Control List (ACL)

ACL (Access Control List) is a traffic access control protocol that is configured on network devices and works as a supervisor while routing different types of traffic. Gateway devices that perform lane traffic filtering might contain hundreds of rules in their access control lists, which are typically used to categorize traffic at the network level. A set of access control rules has been designed to filter data traffic connected to each protocol, destination IP, source IP, and port number in a network environment to limit the forwarding of sophisticated traffic.

ACL optimization can significantly increase the performance of packet forwarding devices. The two types of network problems that typically occur on campus networks are physical and logical defects. Physical faults include line faults, port faults, network equipment faults, host physical faults, and other physical issues. The network will be disrupted either permanently or sporadically when this type of breakdown occurs. Logical failure is defined as an error in network equipment configuration or host network information configuration, such as network equipment configuration, network protocol fault, security fault, and so on. A router is programmed to check each packet against the conditions stated in the ACL before filtering them out. When the router secure, these requirements are frequently applied to the router's interfaces [17].

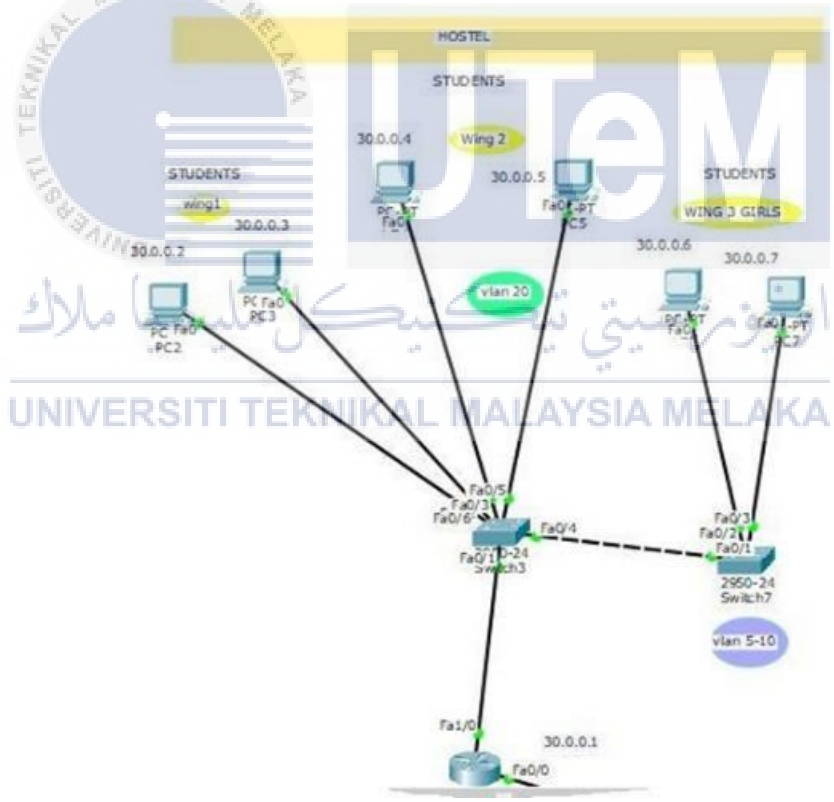


Figure 2.6 Basic access control of University network [17]

2.6 Type of LAN topologies

2.6.1 Star topology

The source computer delivers data to the cable ring, which looks for its destination by contacting each computer on the ring until it reaches its destination node. It's simple to set up, but it's difficult to keep up with, and it's slow to send and receive data. This type of topology isn't appropriate for institutions in underdeveloped nations, where network failure is common [18]. The hardware that connects each device is expensive, and data transferred over it may take a long time to reach its intended destination. The ring topologist is ineffective in underdeveloped nations since many universities lack the financial resources to purchase such machines [18].

2.6.2 Mesh topology

The nodes in a mesh topology do not have a single point of connection. Each device or PC in the network has its own cable that connects it to every other device or PC in the network. The fault tolerance of this network topology is the highest of all network topologies. Traffic is only shared between two nodes in a mesh topology. With this structure, identifying and isolating errors is simple. The star, ring, and ring topologies are currently in use on the Covenant University LAN [19].

2.7 Software simulation

2.7.1 Cisco Packet Tracer (CPT)

CPT is a multi-task network simulation coder. CPT simulator that provides a unique set of functions for teaching and learning such as topology design, setting of IP addresses and how data can be transported in packets over a single network [20]. CPT has recently

been updated to add new features such as additional devices, sensors, and programming languages. Resilient Ethernet Protocol (REP), Precision Time Protocol (PTP), better PoE support, and Link Layer Discovery Protocol are all new features in Cisco Packet Tracer 7.0. (LLDP). One of CPT's key features is a registration server for IoT devices [21]. In order to segregate the traffic produced by separate departments, virtual local area networks (VLANs) as figure 2.7 shows.

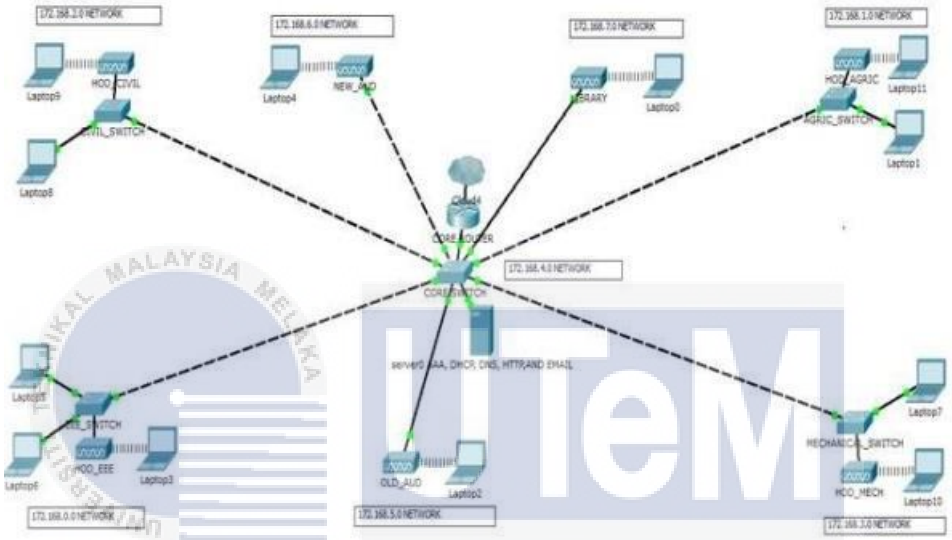


Figure 2.7 Basic diagram of the college of local area network [18]

2.7.2 Enterprise Network Simulation Platform (eNSP)

eNSP primarily replicates corporate network routers, switches, firewalls, wireless local area networks, and other devices. It has a user-friendly interface and can perfectly exhibit the equipment in real-time operation. Students, professors, and technical engineers can use eNSP to learn about network fundamentals, simulate a network, and learn about data communication products [22]. System security can use ACL filtering, multicast route management, multicast route load balancing, and source-specific multicast (SSM) mapping, among other features. The key features of eNSP are the loopback interface, tunnel interface, and Ethernet sub-interface.

2.7.3 Optimized Network Engineering Tool (OPNET)

OPNET Network Simulation is a new technology used for the modelling, simulation, and analysis. Users can construct a variety of protocol models. The network utilization rate is improved, and the investment risk is reduced by the design and construction of the scientific network [23]. OPNET provides a stronger visual or graphical user experience for consumers. For user convenience, the simulation result and data can be examined and shown using graphs, charts, statistics, and even animations. The results of the simulation can also be used to generate a web report [24]. OPNET's key features include preconfigured node models and integrated GUI-based debugging and analysis. Libraries provide several preconfigured node models that can be utilized by simply importing and enabling the relevant functionality. The principal distinction between OPNET Network Simulator and others in comparison to other simulators is its power and diversity [24].

2.7.4 Network Simulation 2 (NS2)

Simulations of computer networks the implementation and simulation of real-world computer network protocols are addressed when using NS2. NS2 is a programmer that simulates networks and events in a packet-by-packet manner. Network Animator (NAM) is a visual depiction included with NS2. With varying data, the performance analysis replicates a virtual network and examines transport layer protocols at the same time [25]. Features can be linked, including a discrete event scheduler and the usage of TCL as a scripting language. It has a lot of features for simulating protocols, including TCP, FTP, UDP, HTTPS, and DSR. Implement a design that can be graphically visualized and represented.

2.7.5 Network Simulation 3 (NS3)

NS3 provides us with unique functionalities that can be applied in real integrations. NS3 is writing scripts in C++ or Python [26]. Some of these features include gnu plot, which is used to create graphs from data obtained from a trace file. NS3 allows us to follow the paths of the nodes, allowing us to determine how much data is sent and received [27]. Network Animator is an animated representation of how a network will seem in real life and NS3 assists in the generation of a pcap file that can be used to obtain all packet information. A software tool can be used to view these pcaps [27].

2.8 Comparison advantage and limitations in CPT, eSNP, OPNET, Ns2 And Ns3

Network simulation software it is possible to model routing and switching and the network in its whole. It is also feasible to model and simulate network protocols as well as the processes on the servers. Students of all skill levels can benefit from free or low-cost simulator software that includes a wide range of open laboratories. The finest simulation software should be able to design network topologies and conduct simulations successfully. The table 2.1 shows compare the advantages and disadvantages of several types of software for network design that do not require hardware.

Network simulation	Advantage	Limitations
Cisco Packet Tracer (CPT)	It allows its users to emulate the Cisco router settings.	CPT only has a small number of the actual functions found in routers and switches.
Enterprise Network Simulation Platform (eNSP)	accessing the content an unlimited number of times	only a few devices are given especially high end to make the topology
Optimize Network Engineering Tool (OPNET)	The fast-discrete event simulation engine	It does not allow many nodes in a single connected device
Network Simulation 2 (NS2)	Complex scenarios can be easily tested	The compilation and interpretation combination made it difficult to analyze the code.
Network Simulation 3 (NS3)	NS3 support for ported code should make model	NS3 needs a lot of specialized maintainers to avail the merits

Table 2.1 Advantage and laminations of software

2.9 Comparison of previous research

Table 2.2 shows the comparison of previous related project. The project that can be compared is the few articles which is, it used the same flow or software, which is the Cisco Packet Tracer (CPT).

No	Author	Year	Software	Type of network security protection	Techniques or technology
1.	[1]	2017	Cisco packet tracer	Network segmentation Firewall	Cisco anti-virus software (web version), Cisco anti-virus wall and Cisco network security early warning system
2.	[2]	2019	IPCop	Remote-access VPNs	Host-to-net VPN was used for remote users, and subsequently a Net-to-Net VPN was developed for secure communication between the main office and the ministry of education.
3.	[3]	2018	Arcai.com's Netcut	Firewall	Standard building pieces allow the network to evolve more quickly. Network nodes do not have to be connected to each other if the architecture is hierarchical.
4.	[4]	2019	Cisco packet tracer	Application security	Using EIGRP and OSPF, such as stub routing, route summarization, and route filtering, as well as LSA and SPF throttle tuning and stubby areas for OSPF to ensure optimal convergence for the routed access design.
5.	[5]	2021	Analysis	Network segmentation	The platform uses principally B/S architecture and SSM framework, and MySQL database technology for database management.

No	Author	Year	Software	Type of network security protection	Techniques or technology
6.	[6]	2018	Cisco packet tracer	Network access control	Open Wi-Fi and a library and guesthouse network access are also included in the network, which includes an ISP, network administration functions and interconnections between various departments.
7.	[7]	2019	Cisco packet tracer	Virtual Private Network (VPN)	Expanding on the dual relationship of DHCP-F, DHCP-HF works with three or more failover servers and allows network managers to work with networks that are not tied to virtual machine (VM) servers combined with monitoring.
8.	[8]	2018	Cisco packet tracer (analysis)	Network segmentation	The architecture of a network can provide a service that is available 24 hours a day, can accommodate an increasing number of users in the future, can priorities packets, and can enhance security.
9.	[9]	2013	Cisco packet tracer	Network penetration testing	Optic fiber is used extensively in each distribution and access layer switch, which requires two different switches
10.	[10]	2019	Analysis	-	A network intrusion detection system (IDS) is used in the campus network security to detect the behavior of unauthorized users and intrusive systems, as well as to detect the illegal operation of system resources.

No	Author	Year	Software	Type of network security protection	Techniques or technology
11.	[11]	2015	Cisco packet tracer	Virtual Private Network (VPN)	Modular topologies allow the network to grow and change quickly.
12.	[12]	2017	Cisco Packet Tracer	Virtual Private Network (VPN) Firewall	Network evolution is made easier by providing a standard topology for building blocks. A fully-meshed network, in which every node is connected to every other node, is not necessary with a hierarchical design.
13.	[13]	2019	Cisco Packet Tracer	Network penetration testing	- The bigger IP address is divide into little portions by utilising VLSM (Various Length Subnet Mask) (Various Length Subnet Mask). - To ensure seamless IP communication between nodes in a network, next-generation network architectures should make use of VLANs.
14.	[14]	2018	Cisco Packet Tracer	Network segmentation	VLAN technology, access lists, and AAA servers are used to protect the network's security.
15.	[15]	2019	Analysis	-	Scopus was searched using terms such as open innovation, systems fractal, knowledge networks and hub, social entrepreneurship, the university, regional development, innovation ecosystems, and models to find relevant research.

No	Author	Year	Software	Type of network security protection	Techniques or technology
16.	[16]	2018	Cisco Packet Tracer	Network segmentation	-VTP reduces configuration and integrates VLAN management for any changes on the VTP server, it will be distributed to other switches in the same VTP domain. -Time required to configure the same VLAN is reduced, VLANs provide security, broadcast control, and physical layer transparency.
17.	[17]	2019	Cisco Packet Tracer	Access Control	The operating system's built-in diagnostic instructions and protocol analysis software are examples of software testing tools.
18.	[18]	2017	Cisco Packet Tracer	Network penetration testing Network segmentation	A router and switch set up with VLANs allowed data packets to be routed from one network device to another while maintaining a logical grouping of users.
19.	[19]	2019	Cisco Packet Tracer	VoIP Access Control	Using Voice over IP (VoIP) method of transmitting voice signals over the Internet Protocol (IP) network. This enables the user to use IP Telephone instead of dedicated voice transmission telephone lines.

No	Author	Year	Software	Type of network security protection	Techniques or technology
20.	[20]	2021	Cisco Packet Tracer	Virtual Private Network (VPN)	-Interconnect and control several IOE devices through coding -Devices that are connected to the Internet of Things (IoT) and operated by an authorized user
21.	[21]	2017	Cisco Packet Tracer	Access Control	-Wireless IOE RFID -A microcontroller unit (MCU) that connects and controls various IOE devices via coding.
22.	[22]	2020	eNSP	FAT AP (FAT Access Point) FIT AP (FIT Access Point)	Verify the CAPWAP session establishment process (AP once powered on obtains IP address from AC using DHCP), terminal connection to AP, and terminal getting IP address from AP and so on.
23.	[23]	2017	OPNET	Firewall	Used STP to connect each computer to the central switch, which should be a 64-port switch, so that the network can expand in the future.

No	Author	Year	Software	Type of network security protection	Techniques or technology
24.	[24]	2018	OPNET (analysis)	-	The campus network applications can satisfy the expectations of users, the application response time, network latency, network throughput, network usage and other performance indicators need to be applied
25.	[25]	2018	NS-2 (analysis)	-	-Wire mesh models were used in this study to examine and monitor the performance of the networks they were based on. -Network performance and apply two of the most essential network protocols (TCP and UDP) to the suggested network in terms of delay time, throughput, and data jitter.
26.	[26]	2020	NS-3 (analysis)	-	Payload and header information are contained in packets, which are used to represent data that is transmitted across the network
27.	[27]	2020	NS-3 (analysis)	-	According to data, the scientific community sees it as a useful tool in a variety of subjects, and third-party resources are being used to extend it and build new add-ons for new neighboring application fields.

Table 2.2 Comparison of previous research

2.10 Summary

The literary review in Chapter 2 focused mostly on the application of the fundamental premise. More emphasis was paid to the methodologies used to plan and implement the third part of the project. External attacks are quite widespread in the collegiate network environment, and network destroyers have constantly developed resources and equipment. The network security system we have created for the college network cannot be changed. In view of the current situation, on the one hand, we must make rational and acceptable adjustments, while on the other, we must adapt to changes in the external environment. Only by modifying our campus network security design can we ensure the safety and reliability of the campus network.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter describes the major stream structure in the project lifting. The proposed project is titled Secured Campus Network Multicast Services Design and Implementation. This study was conducted based on various phases of the enterprise that are carried out and achieved based on the objectives.

3.2 Methodology

The figure 3.1 represents the way this project works. First, two network security design scenarios are performed. The next step is to set up the devices with the basic configuration and security policy. If this configuration is successful, the result will come out and from there the analysis will be made. The configuration need to redo if devices is not connected.

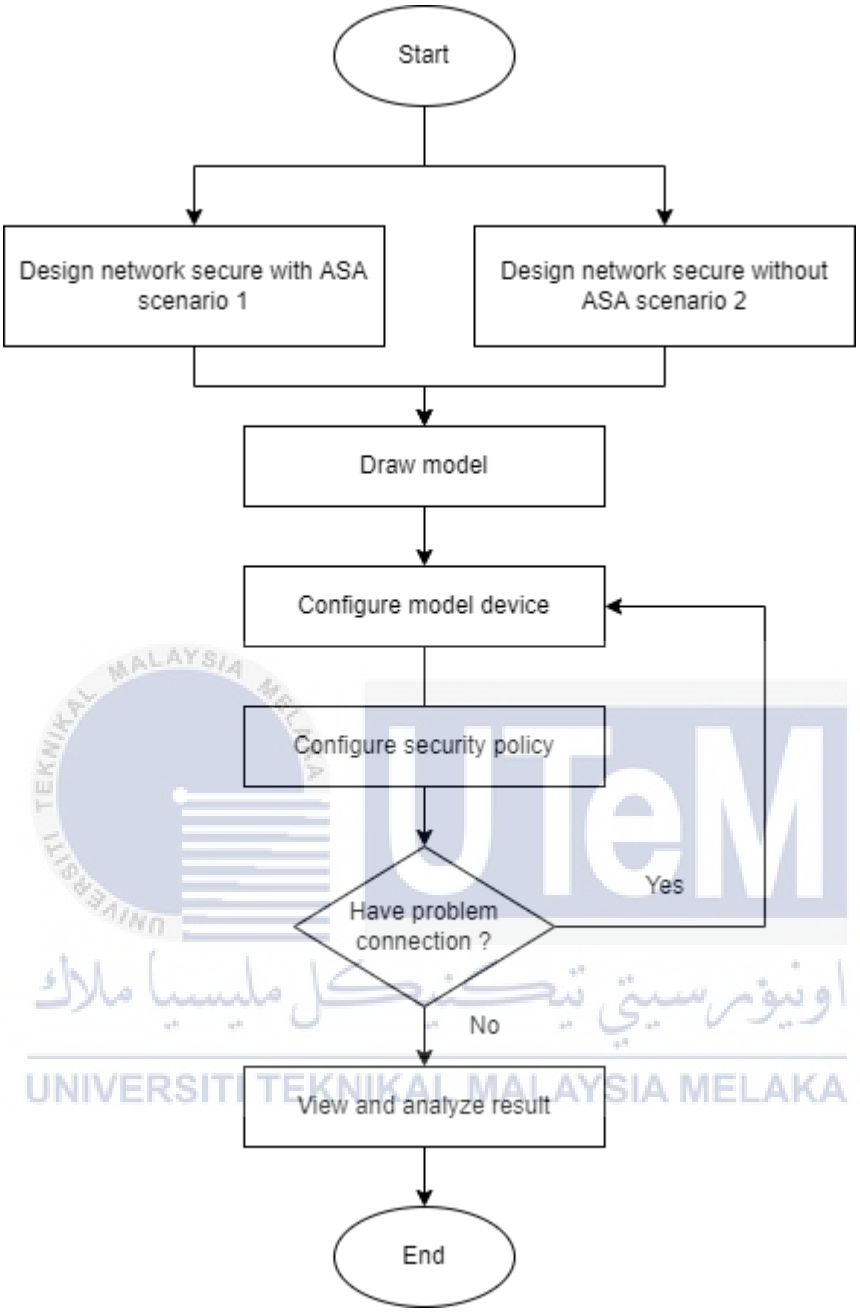


Figure 3.1 Flowchart of project progress

3.2.1 Methodology PSM progress

Planning was made to ensure the project can be completed within the given time frame successfully. Without proper planning, this project cannot be completed successfully. The PSM1 processes are shown in Figure 3.2. This project will last exactly two semesters, but PSM1 typically begins with student registration at the start of the semester, followed by a discussion with the supervisor (s) to propose appropriate project issues. After a departmental committee has accepted the title, students need to meet and discuss it regularly with the supervisor. The detailed processes involved in PSM1 are covered in the following sub-sections.

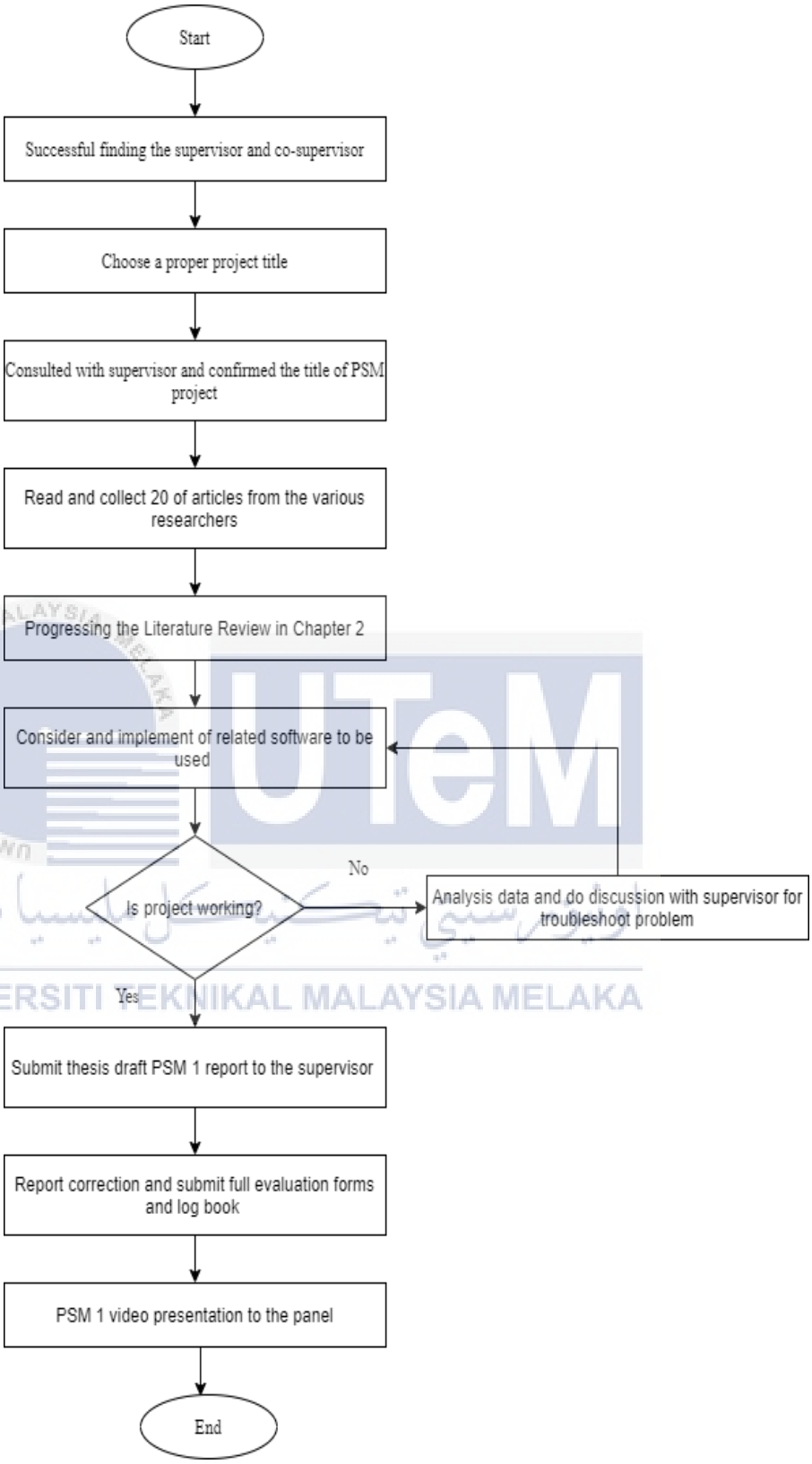


Figure 3.2 Flowchart of PSM 1 progress

3.2.2 Experimental setup

3.2.2.1 Scenario 1

In figure 3.3 shows the ASA packet flow. The ingress interface will receive a packet, which will be stored in the internal buffer, and the interface counter will be incremented. A new session or one that is already active will be detected by ASA. if a packet does not belong to an existing TCP session, it will be searched for TCP state information (if packet is a SYN packet or not) packets will be dropped if a state check fails, or the connection counter will be incremented and the packet will be forwarded for ACL check if the connection succeeds. ACL and xlate checks are bypassed if the packets are part of an already-running one. When an ingress ACL allows traffic, a counter on the ACL is incremented and the packet is forwarded to its destination. Event logs are created when the ACL does not allow a packet. The NAT rule will be verified. When a matching NAT rule is identified, a connection entry is formed and the packet proceeds. Packets are lost, and an event is logged if a matching NAT rule cannot be located. Inspection of the packet is carried out. The ASA checks to see if this packet conforms to protocol. Otherwise, it will be dropped and an event will be recorded if the packet doesn't conform. NAT rules dictate that the IP header information be altered. The egress interface is chosen, and packets are forwarded to it. If the NAT rule or a global route query determines the egress interface, it is used. On the egress interface, a layer 3 route lookup will be conducted. Layer 2 lookup is going to happen. Packets are sent out of the egress interface and the interface counter is incremented.

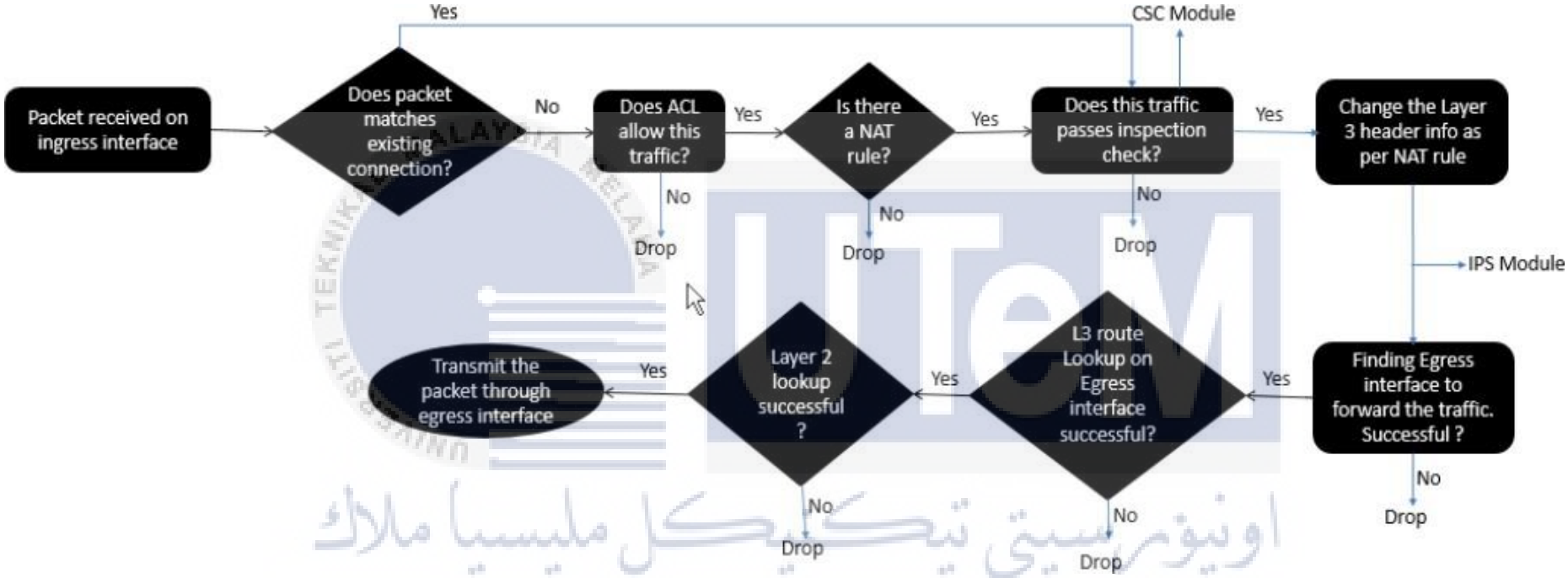


Figure 3.3 Flow chart ASA packet flow

3.2.2.2 Scenario 2

The ASA device should not be used as a firewall in scenario 2. The HQ router (router 1941) should be configured with a Context-Based Access Control as firewall and ACLs to implement security policies. Device configurations are made in order to guard against STP attacks and enable broadcast storm control. Configure port security and turn off switch ports that are no longer in use. An IPS on the IOS system configure a ZPF in order to put in place security policies. Create an IPsec VPN between two different locations.

3.2.3 Parameters

3.2.3.1 Parameters Scenario 1 and Scenario 2

Table 3.1 shows a list of Scenario 1 and Scenario 2 parameters for the ISAKMP phase 1 policy and the phase 2 IPsec policy. The HQ router is configured with an ACL (ACL 110) to identify interesting traffic. The HQ router is configured with ISAKMP Phase 1 properties. The Isakmp policy is 10 in crypto. In Table 3.1 the policy parameters of ISAKMP phase 1 provide the specific information required. Configure the IPsec parameters on the branch router in the same way as the headquarters router. The HQ and branch routers will be reloaded with the previously saved operating configuration and the new saved configuration. Using an FTP session on the Web Server uses a cisco login and password, which can verify the VPN configuration on the Branch Administrator PC. The Web Server in Secure Area Network (SAN) can be accessed via an FTP session from the Branch Administrator PC using a cisco login and password.

ISAKMP Phase 1 policy parameters			**ISAKMP Phase 2 policy parameters**		
Key distribution method	**ISAKMP**		**Parameters**	**HQ Router**	**Branch Router**
Encryption algorithm	AES		Transform set name	VPN-SET	VPN-SET
Number of bits	256		Transform set	esp-aes 256 esp-sha-hmac	esp-aes 256 esp-sha-hmac
Hash algorithm	SHA-1		Peer host name	Branch	HQ
Authentication method	Pre-Share		Peer IP address	172.16.20.2	10.1.1.1
Key exchange	corpkey		Encrypted network	209.165.200.240/28	172.16.40.1/24
IKE SA lifetime	86400		Crypto map name	VPN-MAP	VPN-MAP
ISAKMP key	Cisco		SA Establishment	Ipsec-isakmp	Ipsec-isakmp

Table 3.1 List the parameters for the ISAKMP phase 1 policy and IPsec phase 2 policy

3.2.4 Equipment Implementation

This section will explore and explain the equipment and the features that are used in the Multicast Protocol Efficiency in a Campus Network Environment using Cisco Packet Tracer (CPT) for simulation of network topology. The software required to develop routers, switches, servers and clients in this project was designed by using CPT. Nevertheless, this project does not use any hardware implementation, and it includes only the simulation.

3.2.4.1 Router-PT

A router is physical network equipment that allows a local internet network to be connected. The router creates a private network by receiving modem data that is connected from an Internet service provider by cable, DSL, or other wired connections. Routers establish system-level network connections and hence work on the OSI model's third layer. The private or local addresses of the home or office routers are derived from a few reserved IP addresses. A private IP address can only identify a router device and does not influence other networked devices in the same home, Department or campus.

Figure 3.4 Router-PT

3.2.4.2 Cisco Switch

Switches function both on the physical layer and on the OSI model data link layer. A network switch is a computer networking device connecting devices in a computer network together. Switches are used to accept, process and forward data to the destination device

through packet switching. In contrast to the less complex network hubs that offer an additional intelligence layer to basic physical hubs, a network transmits data to only one or more devices that require it, rather than the identical data from each of its ports.

Figure 3.5 Cisco Switch

3.2.4.3 Server-PT

Server-PT can use a device or computer programme supporting additional devices or applications called clients. A server can support multiple customers and deliver various features to different customers. Many servers have very high purchase costs, and universities in impoverished nations cannot afford such high-priced systems. Few servers will be employed for the network design of this project, such FTP, Web, Email and application servers.

Figure 3.6 Server-PT

3.2.4.4 Cisco Adaptive Security Appliance (ASA)

The Cisco ASA fundamental operating system is Cisco Adaptive Security Appliance (ASA) Software. For any dispersed network environment, it provides enterprise-class firewall features for ASA devices in a variety of form factors, including standalone appliances, blades, and virtual appliances. ASA Software also interfaces with other essential

security technologies to provide comprehensive solutions that address ever-changing security requirements. Among its benefits, Cisco ASA:

a) Offers integrated IPS, VPN, and Unified Communications capabilities
b) Helps organizations increase capacity and improve performance through high-performance, multi-site, multi-node clustering
c) Delivers high availability for high resiliency applications
d) Provides collaboration between physical and virtual devices
e) Meets the unique needs of both the network and the data center
f) Provides context awareness with Cisco TrustSec security group tags and identity-based firewall technology
g) Facilitates dynamic routing and site-to-site VPN on a per-context basis

Figure 3.7 Cisco Adaptive Security Appliance (ASA)

3.2.4.5 Cisco access point or wireless router

An access point functions as an independent root unit in an all-wireless network. It's not connected to a wired LAN. The access point instead works as a hub that connects all stations. It serves as the Centre point for communications, expanding wireless users' communication range. WAPs are a more convenient, safe, and affordable way to connect every computer or device in your network with wires and cables. And implementing WAPs to build a wireless network can provide your small business with many advantages and benefits. For one thing, a wireless network is easier to access. It is also far less complicated to add new users. And you can quickly provide guest users with Internet access by giving

them a password to safely access your wireless network. You may also easily segment users and guests to secure your network assets and resources.

Figure 3.8 Access point

Figure 3.9 Wireless router

3.2.4.6 End device

A client is an end device that has installed software that allows it to request and display the information obtained from a server. Server and client use the network as a method to be connected and communicate with each other. When the clients want to express to them sever, the client will use the network to deliver and accept the communication or request over their order.

3.3 Overview of LAN services

LAN services enable connectivity to end devices within the office's corporate network. Devices such as laptops, telephones, monitoring cameras, cash registers, kiosks and inventory scanners require network connections via the LAN. Branch offices also need guest network access, and in some circumstances, secured area should be supported (SANs). Branch security is a fundamental component of LAN branch services. The LAN must be secured from malicious assaults, and network users must be authorized/authenticated. This

chapter contains some of the most prevalent services in the LAN network on campus. Some of the aspects that should be examined here include Layer 2 LAN, Layer 3 LAN, Security LAN and Management LAN.

3.3.1 Layer 2 LAN service

3.3.1.1 VLANs

Virtual LANs (VLANs) define broadcast domains in a Layer 2 network. This is an administrative subnet of switch ports in the same field of broadcasting, via which a broadcast frame propagates in a network. The inter VLAN routing function is available on IP or SMI or IP or EMI Layer 3 switches. You need a Layer 3 routing device with any of the previous pictures for Layer 2-only switches. The IP Base Feature Set provides advanced service quality (QoS), rate restriction, access control list (ACLs), and basic RIP operations. Only on the IP services image, dynamic IP routing protocol (Open Shortest Path First (OSPF), BGPv4, EIGRP) is available. The IP Services image offers a wide range of corporate services that include powerful IP unicast and IP Multicast routing based on hardware. The IPv6 Layer 3 hardware switching support is also available, adding either the IP Base or the IP Services images to the Advanced IP Services license. Both the IP Image Base and the IP Services Image provide QoS and security lookups for layer three and layer 4.

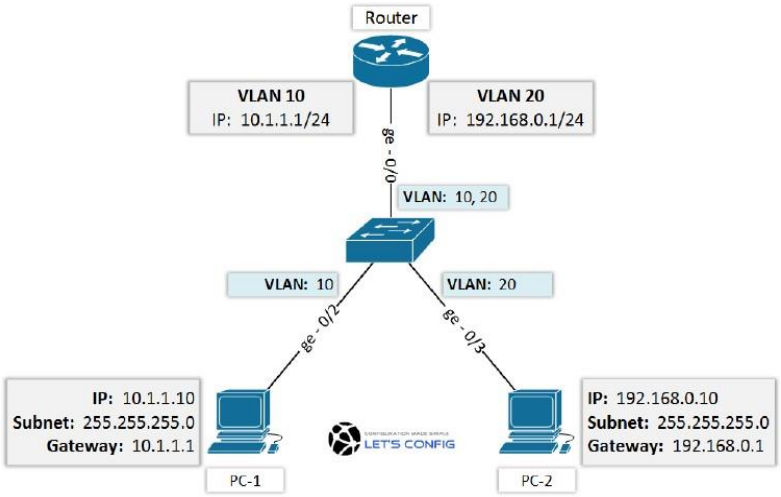


Figure 3.10 Example VLANs config

3.3.2 Layer 3 LAN service

3.3.2.1 Multicast Service (MS)

Multicast services save bandwidth by obliging the network to duplicate packets only if required. They also allow hosts to automatically join and quit groups. Multicast traffic will only be transmitted to ports with associated hosts requiring multicast traffic.

i) Cisco Group Management Protocol (CGMP)—Multicast Traffic Management Server for CGMP. Multicast traffic is only transmitted to ports with associated hosts requesting multicast traffic.

ii) Snooping Internet Group Management Protocol (IGMP) — Multicast management of IGMP snooping.

3.3.3 Security LAN service

3.3.3.1 Firewall

A firewall is a hardware or programme meant to prevent external threats to the network and its resources. A firewall is frequently installed where the network is connected to a Wide Area (WAN) network. These walls function as a filter or filter for verification of any connectivity attempts to the local network. It allows only useful and safe communication while banning any other dangerous information, such as viruses.

3.3.3.2 Encrypted password

By configuring network resources for all users permissions and passwords, the network administrator can save the user name and password, send and offer a comprehensive user record with an encrypted analysis mechanism to ensure system security. Network administrators also need to set up and maintain a complete database for network users, and strict system log management is also required. In order to monitor and examine the safety situation on the campus network system on a regular basis, pay greater attention to dynamic network security concerns and adapt the appropriate intrusion safety conditions, urgent repair system.

Figure 3.11 Service password-encryption command

passwords configured on an IOS device, with the exception of the passwords configured with enable secret password, are stored in clear-text in the device configuration file. This means that all that attacker needs to do to find out the passwords is to run the show running-config command in figure 3.11 shows.

3.3.3.3 Network security with ACLs

The Access Control List (ACL), which filters network traffic, controls if routed packets are sent or stop from router interfaces. The LAN switch analyses each packet based on the criteria you have established in the access lists to determine whether or not it should be forwarded. It is possible to employ MAC Access Control Lists (MACL) and VLAN Access Control Lists (VACLs). VACLs are also known as VLAN maps in Cisco IOS. The following security measures are supported by MAC address filtering, which allows you to block unicast traffic for MAC address in a VLAN interface. Security features also enable port ACLs, which allow you to apply ACLs to layer two interfaces on the inbound traffic switch. Here you may find ACLs, MACLs, VLAN mapping, MAC address filtering and port ACLs.

3.4 Implementation secure multicast service network design Scenario 1 and Scenario 2

Figure 3.12 depicts a simulation screen capture of a secured network prototype. Cisco Adaptive Security Appliance, the Core Router, the two distribution switches, and the integrated service routers were set correctly to cover the full Campus Infrastructure. Because of the integrated service routers or access points, the Faculty now has wireless connectivity and communication among PCs, laptops, and other WiFi-enabled devices and direct internet

at every building. The green circle in figure 3.12 shows Cisco Adaptive Security Appliance linked to Secure Area Network (SAN). FTP, Web, Email, and application servers were all hosted on the SAN switch. Next VLANs were established for laboratories, lecture halls, the library, departmental offices, IT Lab, administrative units and others in external network (purple) and admin branch (blue). Same as figure 3.12 but for Scenario 2 in figure 3.13 shows don't have ASA through it. Connection router HQ directly on SAN without ASA such as figure 3.13 show below. For Scenario 1 is created firewall rules security policies on ASA device. While for Scenario 2 the firewall is different which is at the router internal.

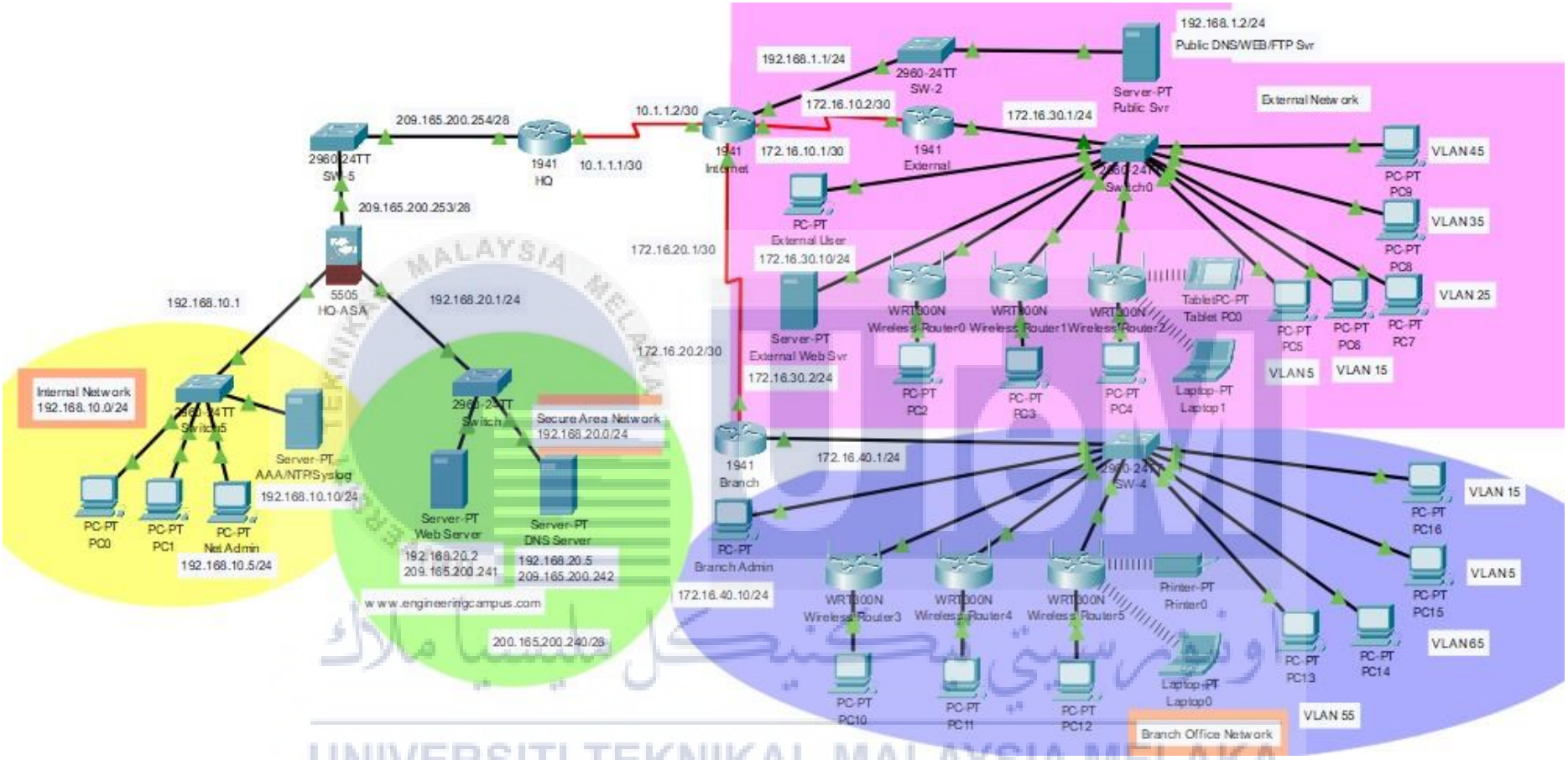


Figure 3.12 Scenario 1 design secure network

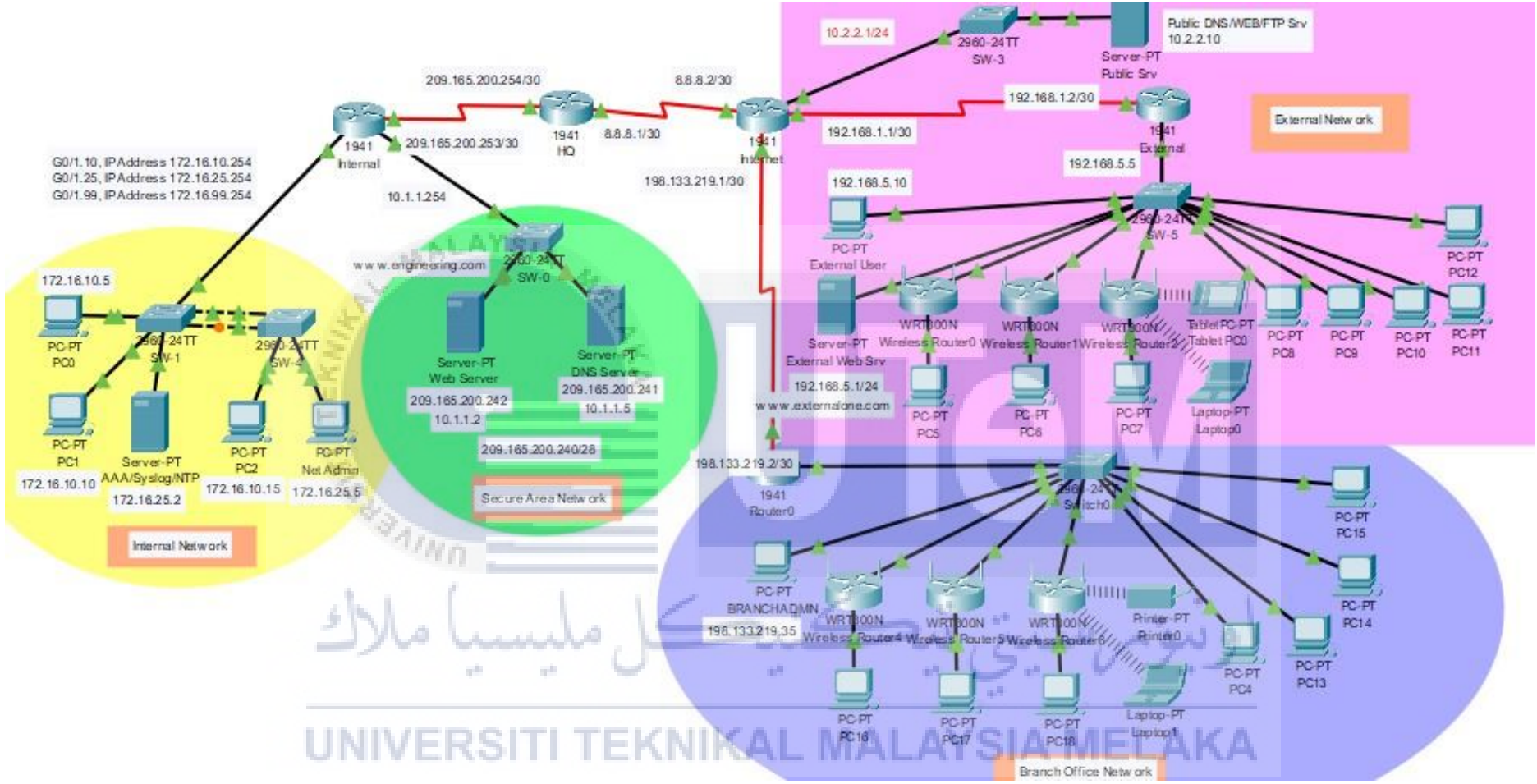


Figure 3.13 Scenario 2 design secure network

3.4.1 Addressing plan

Table 3.2 shows the range of network host addresses that will be used to allocate IP addresses on the LAN for each building within the Campus of Engineering. Table 3.2 show the addressing table there was also a list of the network and broadcast addresses that each LAN device or user will be operating on at any of the Campus of Engineering buildings. This addressing is being used in both scenario.

Device	Interface	IP Address	Subnet Mask	Gateway	DNS Server
Internet	S0/0/0	10.1.1.2	255.255.255.252	n/a	
	S0/0/1	172.16.10.1	255.255.255.252	n/a	
	S0/1/0	172.16.20.1	255.255.255.252	n/a	
	G0/0	192.168.1.1	255.255.255.0	n/a	
HQ	S0/0/0	10.1.1.1	255.255.255.252	n/a	
	G0/0	209.165.200.254	255.255.255.240	n/a	
HQ-ASA	E0/0	209.165.200.253	255.255.255.240	n/a	
	E0/1	192.168.10.1	255.255.255.0	n/a	

Device	Interface	IP Address	Subnet Mask	Gateway	DNS Server
	E0/2	192.168.20.1	255.255.255.0	n/a	
Branch	S0/0/0	172.16.20.2	255.255.255.252	n/a	
	G0/1	172.16.40.1	255.255.255.0	n/a	
External Web Server	NIC	172.16.30.2	255.255.255.0	172.16.30.1	192.168.1.2
External PC	NIC	172.16.30.10	255.255.255.0	172.16.30.1	192.168.1.2
AAA/NTP/ Syslog Server	NIC	192.168.10.10	255.255.255.0	192.168.10.1	192.168.20.5
SAN DNS Server	NIC	192.168.20.5	255.255.255.0	192.168.20.1	192.168.20.5
SAN Web Server	NIC	192.168.20.2	255.255.255.0	192.168.20.1	192.168.20.5
PC0 and PC1	NIC	DHCP client	255.255.255.0	192.168.10.1	
Branch Admin	NIC	172.16.40.10	255.255.255.0	172.16.40.1	192.168.1.2
Net Admin PC	NIC	192.168.10.5	255.255.255.0	192.168.10.1	192.168.20.5

Table 3.2 The addressing table

3.5 Summary

This paper proposed to performance campus architecture design Scenario 1 and Scenario 2 by secure multicast service network. Both design also includes Hierarchical Network Design as a hierarchical design is used to group devices into multiple layers. In the new system's logical architecture, it was found that information security is unavoidable in order to guarantee that networks run smoothly and maximise their functions. Environmental hardware guarantees a good informative education environment that provides a strong support to models of instruction and popularises information technology education and campus networks. An major issue is how the campus networks perform with high efficiency. The paper introduces and analyses many variables and possible elements that affect the security of campus networks and provides guidance on how to build on management and technical systems of campus networks.

.

CHAPTER 4

RESULT AND DISCUSSIONS

4.1 Introduction

This chapter will discuss the full project, including the analysis and discussion the performance of two scenario network design by identify security cisco firewalling solutions scanning processes and measurable parameters such as latency and throughput. In this paper, a secure multicast service network was designed to carry out campus architecture two design scenarios that is Scenario 1 uses Cisco ASA, while Scenario 2 makes use of Cisco IOS router traditional firewall. A hierarchical architecture is used in both the design and functionality of zones and zone pairings, as well as their interaction in hierarchical policies.

4.2 Result

4.2.1 Connectivity Scenario 1

Figure 4.1 shows how PC1 internal network connects to the External User's outside network at a rate of one second intervals in the OSI model. The green colour part which is Internet Control Message Protocol (ICMP) and the pink that refering to the Spanning Tree Protocol (STP). Connecting with switch 5 in ethernet0/1 receives frame in 0.04 seconds, so focus on that action. It was identified in the table of ASA's MAC addresses. The MAC address of the active VLAN interface is the destination of the transmission. Receiver ports, broadcast addresses, or multicast addresses are all possible destinations for the frame's destination MAC address. To make it possible to use it, the device removes the PDU from the Ethernet frame. Look for the IP address of the destination in CEF table. The destination

IP address is listed in the CEF table for out layers. The TTL of the packet is decremented by the device, and the packet is moving from an internal network to an external network. Translations are found in the NAT table. In this case, the packet matches an internal source list and adds a new item for the source local address, which is then used to translate the packet from local to global addresses by the device directly. The adjacency table contains the IP address of the following hop. The destination MAC address of the frame is set to the one shown in the table by the device. The PDU is encased in an Ethernet frame by the device. The ASA uses the active VLAN interface as the outgoing VLAN number, and this is a unicast frame. To find the destination MAC address, the ASA searches its MAC table for it. An access port is one that connects to a computer from the outside. That port is used by ASA to send the frame out. Transmission of the frame takes place on Ethernet port 0/0.

The HQ-ASA path to SW-5 is also shown at 0.005. The frame is received by GigabitEthernet0/1. In the Switch's MAC table, the source MAC address of this unicast frame was discovered. The destination MAC address is sought after in the switch's MAC table. As a result, the outbound port is a gateway. In this case, FastEthernet0/1 receives the frame and sends it out.

nulation Panel

nt List

s.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.003	PC1	Switch5	ICMP
	0.004	Switch5	HQ-ASA	ICMP
	0.005	HQ-ASA	SW-5	ICMP
	0.006	SW-5	HQ	ICMP
	0.007	HQ	Internet	ICMP
	0.008	Internet	External	ICMP
	0.009	External	Switch0	ICMP
	0.010	Switch0	External User	ICMP
	0.011	External User	Switch0	ICMP
	0.012	Switch0	External	ICMP
	0.013	External	Internet	ICMP
	0.014	Internet	HQ	ICMP
	0.015	HQ	SW-5	ICMP
	0.016	SW-5	HQ-ASA	ICMP
	0.017	HQ-ASA	Switch5	ICMP
	0.018	Switch5	PC1	ICMP
	0.491	--	SW-5	STP
	0.492	SW-5	HQ	STP
	0.492	SW-5	HQ-ASA	STP
	0.508	--	Wireless Router4	STP
	0.509	Wireless Router4	PC11	STP
	0.607	--	Switch0	STP
	0.608	Switch0	External User	STP
	0.608	Switch0	External Web Svr	STP
	0.608	Switch0	Wireless Router0	STP
	0.608	Switch0	PC9	STP
	0.608	Switch0	External	STP
	0.617	--	SW-4	STP
	0.618	SW-4	PC15	STP
	0.618	SW-4	Branch	STP
	0.789	--	Wireless Router2	STP
	0.790	Wireless Router2	PC4	STP
	0.801	--	Wireless Router0	STP
	0.802	Wireless Router0	PC2	STP
	0.868	--	Switch	STP
	0.869	Switch	DMZ DNS Svr	STP
	0.869	Switch	DMZ Web Svr	STP
	0.869	Switch	HQ-ASA	STP
	0.938	--	Switch0	STP
	0.939	Switch0	External User	STP
	0.939	Switch0	External Web Svr	STP
	0.939	Switch0	Wireless Router0	STP
	0.939	Switch0	PC5	STP
	0.939	Switch0	External	STP
	1.000	--	PC1	ICMP

Figure 4.1 Connectivity PC1 to External User using traffic generator for Scenario 1

4.2.2 Connectivity Scenario 2

Figure 4.2 shows how PC1 internal network connects to the External User's outside network at a rate of one second intervals in the OSI model. As seen in figure 4.2 at 0.002 seconds, the SW-1 to Internal router link is active. At port GigabitEthernet0/1, the frame is received. GigabitEthernet0/1.25 allows frames from this VLAN on the sub-interface. Receiver ports, broadcast addresses, or multicast addresses are all possible destinations for the frame's destination MAC address. IEEE 802.1Q frames are de-encapsulated by the device, allowing access to the PDU. To find the destination IP address, the device consults the routing table. Next, the routing table locates an entry for the destination IP address in the out-layer routing table. It is possible to access the destination network by using the IP address 209,165,200,254. In addition, serial0/0/1 transmits the HDLC frame in which the packet is encapsulated.

Shown at 0.003 second intervals, the frame is received by the internal router and forwarded to the HQ in layers serial0/0/1. The payload is de-encapsulated from the HDLC frame and sent to the higher layer by the device. A lookup of the destination IP address in the routing database is also performed. This is done by using the routing database to locate a static route to the target IP address and connecting it there. TTL is also reduced by the device, which sets the next-hop destination. Firewalls based on zone pairs can be found. Serial0/0/0 transmits the HDLC frame that has been created from the packet by the device.

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	SW-1	ICMP
	0.002	SW-1	Internal	ICMP
	0.003	Internal	HQ	ICMP
	0.004	HQ	Internet	ICMP
	0.005	Internet	External	ICMP
	0.006	External	SW-5	ICMP
	0.007	SW-5	External User	ICMP
	0.008	External User	SW-5	ICMP
	0.009	SW-5	External	ICMP
	0.010	External	Internet	ICMP
	0.011	Internet	HQ	ICMP
	0.012	HQ	Internal	ICMP
	0.013	Internal	SW-1	ICMP
	0.014	SW-1	PC1	ICMP
	0.521	--	HQ	EIGRP
	0.522	HQ	Internal	EIGRP
	0.696	--	Internal	EIGRP
	0.697	Internal	HQ	EIGRP
	1.000	--	PC1	ICMP

Figure 4.2 Connectivity PC1 to External User using traffic generator for Scenario 2

4.2.3 FTP Scenario 1

Figure 4.3 show the flow of FTP at Branch Admin user to Public Server. Start at Public Server to SW-2 in layers FastEthernet0/1 will receives the frame. The frame source MAC address was found in the MAC table of switch and switch looks in its MAC table for the destination MAC address. For out layers the outgoing port is an access port, switch sends the frame out that port and GigabitEthernet0/1 will sends out the frame.

Next, each device is connected to the others by a specific technique, as displayed in figure 4.3. The last FTP session in SW-4 was connected to Branch Admin in OSI model layers and received frames are sent to FastEthernet0 when their destination MAC address matches the receiving port's MAC address, or the broadcast or multicast addresses. It is the device's job to decapsulate PDUs from Ethernet frames so that they can be sent to their proper

destinations. The device receives a TCP PUSH+ACK segment from 192.168.1.2 on port 21 after de-encapsulating the packet. Data length 52 and sequence number 1 were received as part of the segment. The intended peer sequence number can be found in the TCP segment. Fin wait 2 is set as the connection state by the device.

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.014	Branch	Internet	TCP
	0.014	Internet	SW-2	TCP
	0.015	Branch	Internet	TCP
	0.015	Internet	SW-2	TCP
	0.015	SW-2	Public Svr	TCP
	0.015	--	Public Svr	FTP
	0.016	Internet	SW-2	TCP
	0.016	SW-2	Public Svr	TCP
	0.016	Public Svr	SW-2	FTP
	0.017	SW-2	Public Svr	TCP
	0.017	SW-2	Internet	FTP
	0.018	Public Svr	SW-2	TCP
	0.018	Internet	Branch	FTP
	0.019	SW-2	Internet	TCP
	0.019	Branch	SW-4	FTP
	0.020	Internet	Branch	TCP
	0.020	SW-4	Branch Admin	FTP
	0.021	Branch	SW-4	TCP
	0.022	SW-4	Branch Admin	TCP
	0.128	--	Switch0	STP

Figure 4.3 Traffic generator FTP Branch Admin to Public Server for Scenario 1

4.2.4 FTP Scenario 2

Figure 4.4 depicts the transit of FTP from the Branch Admin user to the Public Server in Scenario 2. There are no significant differences between Scenario 1 and Scenario 2 in terms of how long it takes to send a file via FTP.

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.015	--	Public Srv	FTP
	0.016	Internet	SW-3	TCP
	0.016	SW-3	Public Srv	TCP
	0.016	Public Srv	SW-3	FTP
	0.017	SW-3	Public Srv	TCP
	0.017	SW-3	Internet	FTP
	0.018	Public Srv	SW-3	TCP
	0.018	Internet	Router0	FTP
	0.019	SW-3	Internet	TCP
	0.019	Router0	Switch0	FTP
	0.020	Internet	Router0	TCP
	0.020	Switch0	BRANCH ADMIN	FTP
	0.021	Router0	Switch0	TCP
	0.022	Switch0	BRANCH ADMIN	TCP
	0.071	--	Internal	EIGRP
	0.072	Internal	SW-0	EIGRP
	0.073	SW-0	DMZ Web Srv	EIGRP
	0.073	SW-0	DMZ DNS Srv	EIGRP
	0.676	--	HQ	EIGRP
	0.677	HQ	Internal	EIGRP
	0.940	--	Internal	EIGRP
	0.941	Internal	HQ	EIGRP

Figure 4.4 Traffic generator FTP Branch Admin to Public Server for Scenario 2

4.2.5 Traceroute Scenario 1

Traceroute is a network troubleshooting tool that follows the path of packet travel from source to destination on an IP network in real-time, revealing the IP addresses of all the routers it pings along the way. Traceroute also keeps track of the time it takes for each hop a packet takes on its way to its destination. On Cisco equipment, the traceroute command may be used to determine the path taken by a packet to reach its destination. It can be beneficial for diagnosing network problems since it identifies all the routers in the path from the source host to the destination host. The figure 4.5 are trace SAN network from external user and branch admin will stop or not successful at route 10.1.1.1 because the route HQ have the ASA security that will protect the user from outside server enter the inside server.

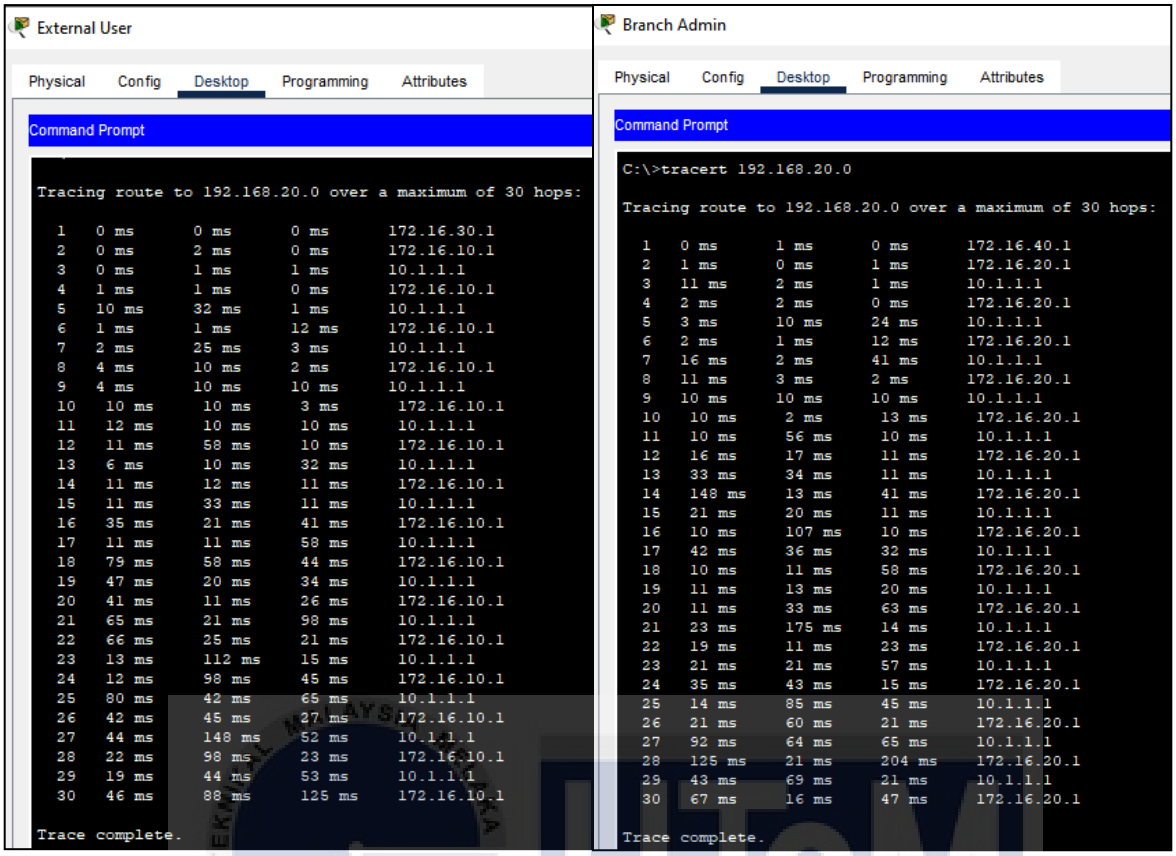


Figure 4.5 Traceroute SAN network from PC External User and PC Branch Admin

The figure 4.6 that are trace PC external user and PC branch admin from PC internal network are successful to destination that have trace. Because the server can enter from inside server to outside server.

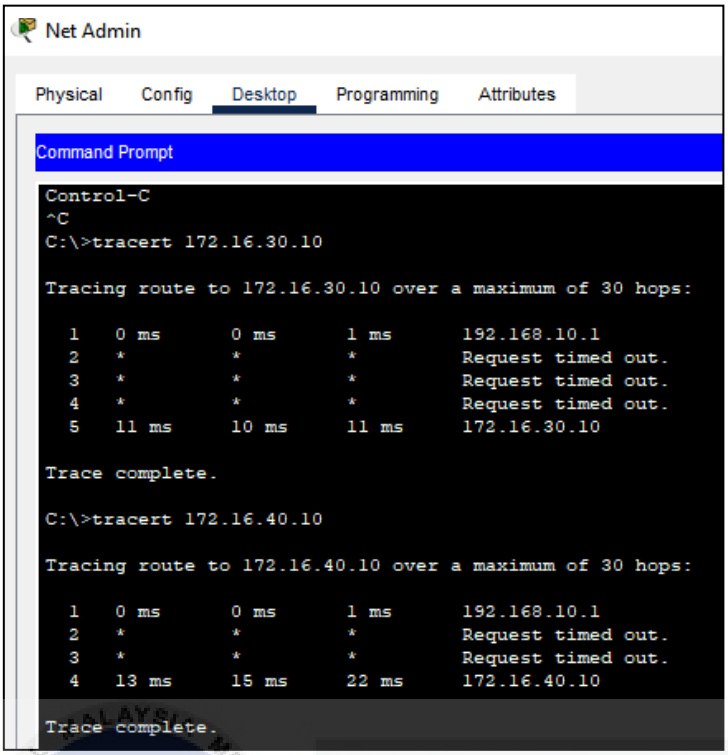


Figure 4.6 Traceroute PC External User and PC Branch Admin from PC Internal Network

4.2.6 Traceroute Scenario 2

The figure 4.7 are trace SAN network from external user and branch admin will stop or not successful at route 8.1.1.1 because the route HQ have the CCNA security that will protect the user from outside server enter the inside server.

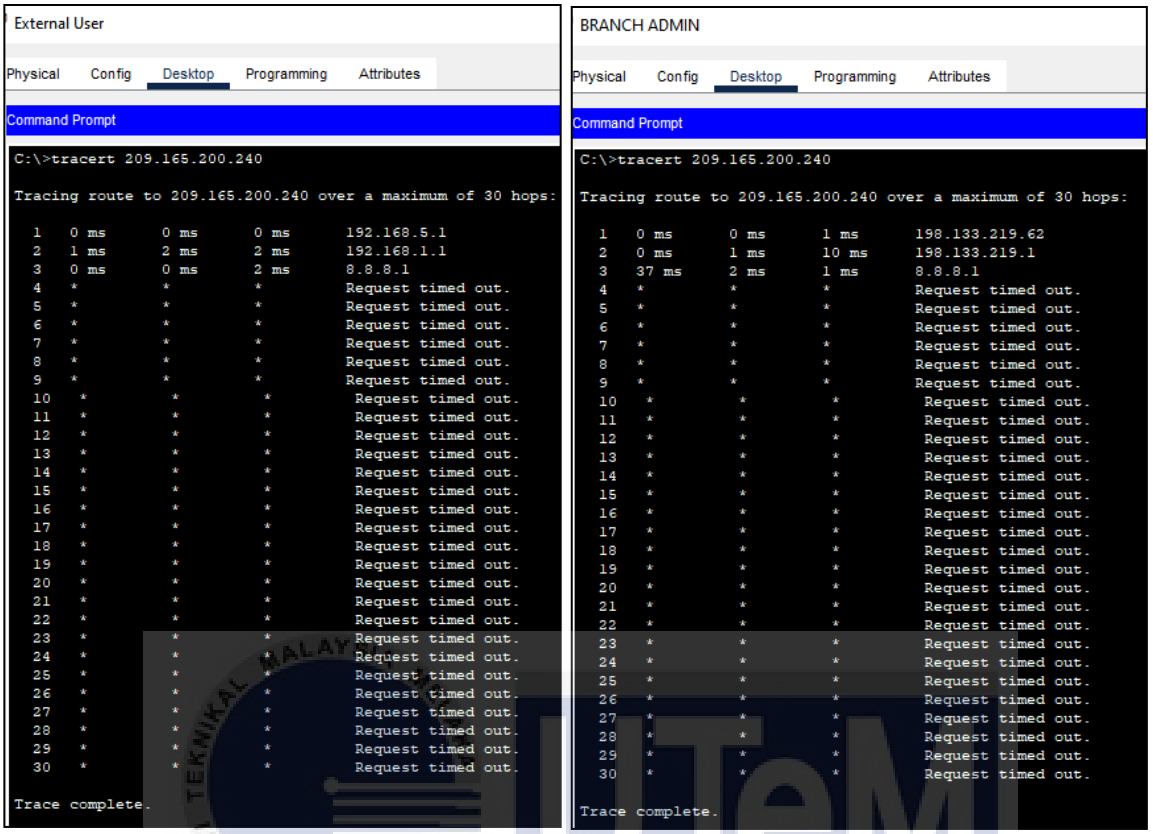


Figure 4.7 Traceroute SAN network from PC External User and PC Branch Admin

The figure 4.8 that are trace PC external user and PC branch admin from PC internal network are successful to destination that have trace. Because the server can enter from inside server to outside server.

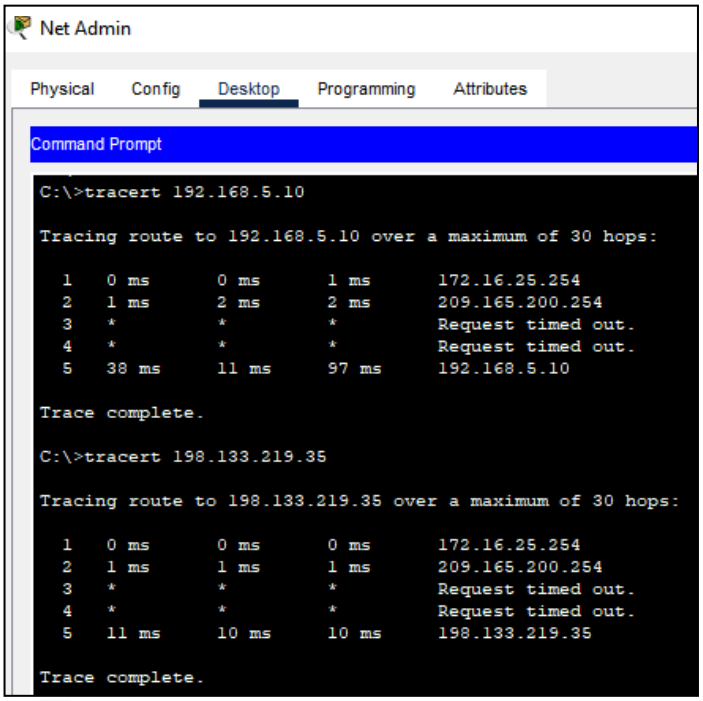


Figure 4.8 Traceroute PC External User and PC Branch Admin from PC Internal Network

4.2.7 Adaptive Security Appliance (ASA) Scenario 1

As seen in the figure, the ASA drops packets sent by the External router and sends them back to the external router. The ASA packet is identified by its blue ICMP. While ICMP packets in the pink colour indicate that they have been sent to the ASA. On the HQ router, a packet's status will be checked to see if it has been included in the access list before to being sent. Otherwise, the ASA will reject the packet. The red box in figures 4.9 and 4.10 indicates that the package is an unauthorised one. Because the Cisco ASA does not do dynamic routing, it provides quicker performance (particularly on VPN tunnels). As an additional benefit of the ASA, the firewall is capable of operating in transparent mode the firewall works as a Layer 2 bridge and is not seen in the network path.

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	HQ-ASA	ICMP
	0.000	--	External	ICMP
	0.001	HQ-ASA	SW-5	ICMP
	0.001	External	Internet	ICMP
	0.002	SW-5	HQ	ICMP
	0.002	Internet	HQ	ICMP
	0.003	HQ	Internet	ICMP
	0.003	--	HQ	ICMP
	0.004	HQ	Internet	ICMP
	0.004	Internet	External	ICMP
	0.005	Internet	HQ	ICMP
	0.005	External	Internet	ICMP
	0.006	HQ	Internet	ICMP
	0.006	Internet	HQ	ICMP
	0.007	Internet	HQ	ICMP
	0.007	HQ	SW-5	ICMP
	0.008	HQ	Internet	ICMP
	0.008	SW-5	HQ-ASA	ICMP
	0.009	Internet	HQ	ICMP
	0.010	HQ	Internet	ICMP
	0.011	Internet	HQ	ICMP

Figure 4.9 Traffic External router to ASA and ASA to External router

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.004	Internet	Branch	ICMP
	0.005	HQ	Internet	ICMP
	0.005	Branch	SW-4	ICMP
	0.006	Internet	HQ	ICMP
	0.006	SW-4	Branch Admin	ICMP
	0.007	HQ	Internet	ICMP
	0.007	Branch Admin	SW-4	ICMP
	0.008	Internet	HQ	ICMP
	0.008	SW-4	Branch	ICMP
	0.009	HQ	Internet	ICMP
	0.009	Branch	Internet	ICMP
	0.010	--	Wireless Router4	STP
	0.010	Internet	HQ	ICMP
	0.010	--	Internet	ICMP
	0.011	Wireless Router4	PC11	STP
	0.011	Internet	HQ	ICMP
	0.011	HQ	Internet	ICMP
	0.012	HQ	SW-5	ICMP
	0.012	Internet	HQ	ICMP
	0.013	SW-5	HQ-ASA	ICMP
	0.013	HQ	Internet	ICMP
	0.014	Internet	HQ	ICMP
	0.015	HQ	Internet	ICMP

Figure 4.10 Traffic Branch Admin to ASA and ASA to Branch Admin

4.2.8 Internal router Scenario 2

Figure 4.11 shows, the Internal router drops a packet sent by the External router and sends it back to the external router. The Internal router packet is identified by its brown ICMP. While the ICMP packet in light blue color indicates that it has been sent to the Internal router. On the HQ router, the status of the packet will be checked to see if it has been included in the access list before being sent. for scenario 2 this is quite different from scenario 1 where packets sent from the external router to the internal will continue to be deleted by the router HQ if there is no access list permit. while packets from the internal router to the External router will return to the internal router and packets will be allowed to enter. this case occurs because internal routers Using an iOS router with a Zone -Based Firewall can facilitate the use of DMVPN in highly decentralized internal networks where branch offices routinely talk to each other.

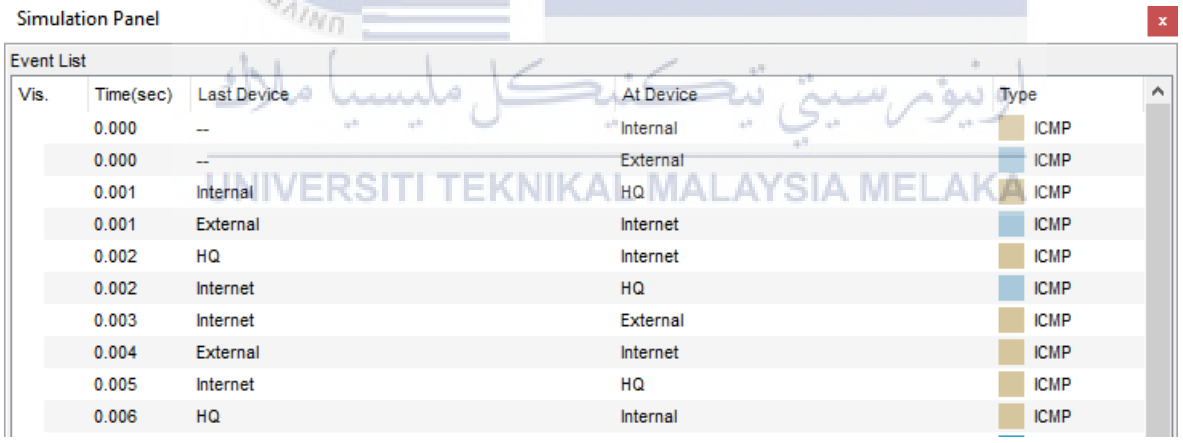


Figure 4.11 Traffic External router to Internal router and Internal router to External router

4.3 Analysis

In this part analysis is done to determine traffic network and perform firewall solutions basic security operations on a network for Scenario 1 and Scenario 2. Based on table 4.1 shows flow traffic Zone based related security policy firewall network.

	Source to destination	**Zone pair exists?**	**Policy exists?**	**Result**
Scenario 1	PC1 to External user	Yes	Yes	Policy action
	PCI to Branch Admin	Yes	Yes	Policy action
	External user to Net Admin	Yes	N/A	Drop
	Branch Admin to Net Admin	Yes	N/A	Drop
	PC1 to Net Admin	N/A	N/A	No policy lookup (pass)
	Branch Admin to External user	Yes	N/A	No policy lookup (pass)
Scenario 2	PC1 to External user	Yes	Yes	Policy action
	PCI to Branch Admin	Yes	Yes	Policy action
	External user to Net Admin	Yes	N/A	Drop
	Branch Admin to Net Admin	Yes	N/A	Drop

	Source to destination	Zone pair exists?	Policy exists?	Result
	PC1 to Net Admin	N/A	N/A	No policy lookup (pass)
	Branch Admin to External user	Yes	N/A	No policy lookup (pass)

Table 4.1 Traffic flow Zone based security policy firewall network

	Scenario 1 (with ASA)	Scenario 2 (without ASA)
Type of protocol (Internal to External network)	1. Internet Control Message Protocol (ICMP) 2. Spanning Tree Protocol (STP)	1. Internet Control Message Protocol (ICMP) 2. Enhanced Interior Gateway Routing Protocol (EIGRP)
Firewall	ASA device: Internal- security level 100 SAN- security level 2 Outside-Security level 70 Service policy global	Router 1941 (Internal): Service policy type inspect
Traffic time packet send	Same	
FTP	Access with SAN server and public server (permit)	Only access to public server

Table 4.2 Analysis for both Scenario

4.4 Summary

This paper shows the result and analysis for two scenarios. Scenario 1 is created firewall rules security policies on ASA device. While for Scenario 2 the firewall is different which is at the router internal. All traffic from the internal network to the external network is allowed by default, as it passes across interfaces with higher levels of trust. Internal users on the inside interface of a real network can easily access SAN resources in this way. With no additional policy or instruction, they can likewise connect to the Internet without any restrictions or limitations. In the same way, traffic that originates on the outside network and enters either the SAN or the inside network is automatically blocked. It is permitted, however, to return traffic that originates on the inside network and returns through the outside interface.

These traffic flows are designed to meet the needs of real networks. As a reminder, firewalls aren't the only way to protect the network against cyberattacks. As part of a comprehensive security strategy, countermeasures should be implemented. By way of example, an outward traffic policy restricting access should be put in place to override any pre-existing permissive behavior based on security levels, so that hostile attackers cannot take advantage of these policies to launch assaults from the inside of the network.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

In conclusion, a secure multicast service network for two scenarios has been achieved at Campus as a result of this project. In Scenario 1, firewall rules and security policies are set up on the ASA appliance. When it comes to Scenario 2, the firewall is located inside the router. Internal network communication to the external network is permitted by default since it travels via interfaces with greater confidence. SAN resources are easily accessible from the inside interface of a genuine network. There is no additional policy or instruction needed for them to connect to the Internet. Similarly, traffic that starts on the outside network and then enters the SAN or the internal network is automatically blocked from forwarding. However, traffic that originates on the internal network and returns via the external interface is allowed to pass backward in time. In order to suit the needs of actual networks, these traffic flows have been built.

A reminder that firewalls are not the main defence against cyberattacks. Countermeasures should be applied as part of an overall security strategy. To illustrate, a policy prohibiting outbound traffic should be implemented to override any previously permissive behaviour based on security levels, so that hostile attackers cannot exploit these policies to launch attacks from within the network. Since the ASA only has one active default gateway, it does not offer Policy-Based Routing, as routers do, and it cannot classify packets based on source service.

Because the Cisco ASA does not do dynamic routing, it provides quicker performance (particularly on VPN tunnels). As an additional benefit of the ASA, the firewall

is capable of operating in transparent mode the firewall works as a Layer 2 bridge and is not seen in the network path. There are no complicated NAT configurations or routing patterns to set up, which makes deployment a lot easier.

The ASA is a good choice if need an appliance to inspect traffic, such as in a web SAN or publicly accessible network. Using an IOS router with a Zone-Based Firewall can greatly simplify the deployment of DMVPN in a highly decentralised internal network where branch offices routinely talk to each other.

5.2 Recommendations for Future Work

Future work on this project should include the use of Biometric and CCTV technologies for advanced access control and security in order to provide solid end-to-end security. Using another device for create security and IPv6 addresses is strongly advised. As a result, everyone on the network will have their own personal IP address, making it easier for them to be identified and authenticated. Acquire extra large storage devices and a cloud storage solution for network users to boost the institution's backup storage target capacity.

REFERENCES

[1] S. Zheng, Z. Li, and B. Li, 'Campus Network Security Defense Strategy', vol. 61, no. Mecae, pp. 356–359, 2017, doi: 10.2991/mecae-17.2017.67.

[2] T. Naing and A. N. Oo, 'DESIGN AND IMPLEMENTATION OF A SECURE NETWORK CONNECTION OF', no. 3, pp. 582–587, 2019.

[3] K. Sita, P. S. Akram, and K. H. Javvaji, 'Design and implementation of Smart Campus Network', *Science (80-.).*, vol. 337, no. 6090, pp. 10.2-10, 2012, [Online]. Available: https://www.sciencemag.org/lookup/doi/10.1126/science.337.6090.10-b.

[4] Y. M. Ajiji, 'Design and Implementation of Optimized Features in a Local Area Network for Improved Enterprise Network', no. July 2019, 2020.

[5] Z. Yang, 'Strategy of Building Perfect Campus Security Management Mode under the Internet Age', *J. Phys. Conf. Ser.*, vol. 1881, no. 2, 2021, doi: 10.1088/1742-6596/1881/2/022098.

[6] Z. Sarkar, 'Final Paper-'.

[7] L. Trombeta and N. M. Torrisi, 'DHCP hierarchical failover (DHCP-HF) servers over a VPN interconnected campus', *Big Data Cogn. Comput.*, vol. 3, no. 1, pp. 1–16, 2019, doi: 10.3390/bdcc3010018.

[8] M. F. Kadhim, N. S. Ali, and S. Al-Khammasi, 'Multi-phase methodology for proposing a high performance switched campus network: University of Kufa Case Study', *J. Eng. Appl. Sci.*, vol. 13, no. 16, pp. 6700–6707, 2018, doi: 10.3923/jeasci.2018.6700.6707.

[9] M. N. Bin Ali, M. L. Rahman, and S. A. Hossain, 'Network architecture and security issues in campus networks', *2013 4th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2013*, no. July, 2013, doi: 10.1109/ICCCNT.2013.6726595.

[10] M. Huang, W. Luo, and X. Wan, 'Research on Network Security of Campus Network', *J. Phys. Conf. Ser.*, vol. 1187, no. 4, 2019, doi: 10.1088/1742-6596/1187/4/042113.

[11] T. S. S. Krishna, N. S. Priya, and Dr.C.rajabhushanam, 'Design And Implementation Of A Secure Campus Network', *Int. J. Grid Distrib. Comput.*, vol. 13, no. 2, pp. 1026–1031, 2020.

[12] G. Michael, 'Design and Implement Secure Campus Network', vol. 116, no. 8, pp. 303–307, 2017.

[13] M. A. Hossain and M. Zannat, 'Simulation and Design of University Area Network Scenario(UANS) using Cisco Packet Tracer', *Glob. J. Comput. Sci. Technol.*, vol. 19, no. August, pp. 7–11, 2019, doi: 10.34257/gjcstgvol19is3pg7.

[14] P. Khani, M. Sharbaf, M. Beheshti, and S. Faraji, 'Campus network security : TThreats, analysis and strategies', *Proc. - 2018 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2018*, pp. 781–787, 2018, doi: 10.1109/CSCI46756.2018.00157.

[15] S. P. Mejia, J. M. M. Hincapie, and J. A. T. Giraldo, 'A hub-based university innovation model', *J. Technol. Manag. Innov.*, vol. 14, no. 1, pp. 11–17, 2019, doi: 10.4067/S0718-27242019000100011.

[16] M. K. and S. K., 'Project Scenario of Communication Network using Cisco Packet Tracer', *Int. J. Comput. Appl.*, vol. 181, no. 29, pp. 37–41, 2018, doi: 10.5120/ijca2018918150.

[17] Q. Wang *et al.*, 'Exploration and Practice of Complex Teaching Cases Based on Campus Network', 2021, doi: 10.38007/proceedings.0001812.

[18] N. S. Tarkaa, P. I. Iannah, and I. T. Iber, 'Design and Simulation of Local Area Network Using Cisco Packet Tracer', *Int. J. Eng. Sci.*, pp. 2319–1813, 2017, doi: 10.9790/1813-0610026377.

[19] Mon Mon Aye | Naing Kyaw Soe | Zar Chi Soe, 'Design and Simulation of VoIP System for Campus usage A Case Study at PTU', *Int. J. Trend Sci. Res. Dev. Int. J. Trend Sci. Res. Dev.*, vol. 3, no. 5, pp. 1350–1354, 2019, doi: https://doi.org/10.31142/ijtsrd26657.

[20] A. Ziradkar, N. Mahendrakar, A. Palande, P. R. Sonawale, C. Engineering, and M. G. M. C. Engineering, 'CAMPUS NETWORK ARCHITECTURE USING CISCO PACKET TRACER', pp. 3614–3620, 2021.

[21] I. Shemsi, 'Boosting Campus Network Design Using Cisco Packet Tracer Boosting Campus Network Design Using Cisco Packet Tracer'.

[22] D. Djomadji, E. Michel, M. Petmegni, D. Steve, and E. Sone, 'WLAN simulations using Huawei eNSP for e-laboratory in engineering schools WLAN simulations using Huawei eNSP for e-laboratory in engineering schools .', no. April, 2020, doi: 10.9790/2834-1502014770.

[23] T. A. Rashid and A. O. Barznji, 'A virtualized computer network for salahaddin university new campus of HTTP services using OPNET simulator', *Lect. Notes Networks Syst.*, vol. 22, no. March, pp. 731–740, 2018, doi: 10.1007/978-3-319-64352-6_69.

[24] L. Nie and S. Hu, 'Simulation and analysis of campus network based on OPNET', *J. Comput. Methods Sci. Eng.*, vol. 19, no. 1, pp. 3–12, 2019, doi: 10.3233/JCM-180847.

[25] S. Ns-, 'Network Performance Analysis Based on Network Directorate of Education of Nineveh', vol. 31, no. 2, pp. 222–229, 2018.

[26] J. P. G. Sterbenz, 'Network Simulation with ns-3', *Simulation*, no. March, pp. 1–15, 2010, doi: 10.2313/NET-2020-11-1.

[27] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, 'Computer network simulation with ns-3: A systematic literature review', *Electron.*, vol. 9.

APPENDICES

Appendix A Gantt Chart

PERANCANGAN PROJEK *PROJECT PLANNING*
(GANTT CHART)

	SEM I																			SEM BREAK					SEM II															
Aktiviti Projek *Project Activities*	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Literature Review	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			
Finding the related journal, article,book for references	x	x	x	x																																				
Discussion with a supervisor about the project objectives, problem statement, scope of project and etc.		x	x	x	x	x																																		
Finding journal on design secure network campus			x	x	x	x	x	x																																
Preparing Literature Review summary				x	x	x	x	x																																
Determine what design should be used for the architecture network campus						x	x	x	x																															

SEMINAR PSM I **SEMINAR PSM II**

Decide equipment that needs to be used in the network campus.									x	x	x																											
Study on how to use the software that will be used for the project									x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x												
Design, construct and test the design using software CPT.																					x	x	x	X														
Constructing the design and its connection																								x	x	x	X											
Project testing																										x	x	x	X									
Troubleshooting any problems that occur.																												x	x	x	x	x	x	x				
Final checking for the project																																		X	x	x		
Presentation of the project																																					x	X

Appendix B Turnitin Originality Report

turnitin **Turnitin Originality Report**

DESIGN AND IMPLEMENTATION OF SECURED MULTICAST SERVICE IN CAMPUS NETWORK by Khairunnajwa Binti M Kamal

From PSM2 (PSM K8)

Similarity Index	Similarity by Source	
25%	Internet Sources:	16%
	Publications:	6%
	Student Papers:	17%

Processed on 10-Jan-2022 16:28 +08
ID: 1739473525
Word Count: 14564

sources:

1 2% match (Internet from 21-Nov-2020)
https://www.invialgo.com/2015/ccna-security-packet-tracer-practice-sba-v1-2/

2 1% match (student papers from 08-Jan-2022)
Submitted to Universiti Teknikal Malaysia Melaka on 2022-01-08

3 1% match (student papers from 17-Jun-2021)
Submitted to Universiti Teknikal Malaysia Melaka on 2021-06-17

4 1% match (student papers from 09-Jan-2022)
Submitted to Universiti Teknikal Malaysia Melaka on 2022-01-09

5 1% match (Internet from 05-Dec-2021)
https://www.researchgate.net/publication/340438170_DESIGN_AND_IMPLEMENTATION_OF_OPTIMIZED_FEATURES_IN_A_LOCAL_A

6 1% match (Internet from 06-Apr-2019)
http://www.bluedata.net/Cisco/Security/Adaptive-Security-Appliances-(ASA)

7 1% match (publications)
Min Huang, Wanbo Luo, Xing Wan, "Research on Network Security of Campus Network", Journal of Physics: Conference Series, 2019