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

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
FAKULTI TEKNOLOGIKEJUTERAAN ELEKTRIK DAN ELEKTRONIK

BORANG PENGESAHAN STATUS LAPORAN
PROJEK SARJANA MUDA II

Tajuk Projek : DESIGN AND IMPLEMENTATION OF SECURED MULTICAST SERVICE IN CAMPUS NETWORK

Sesi Pengajian : 2021

Saya KHAIRUNNAJWA BINTI M KAMAL mengaku membenarkan laporan Projek Sarjana Muda ini disimpan di Perpustakaan dengan syarat-syarat kegunaan seperti berikut:

1. Laporan adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan laporan ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. Sila tandakan (✓):

□ **SULIT*** (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

□ **TERHAD*** (Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

☑ **TIDAK TERHAD**

Disahkan oleh:

(TANDATANGAN PENULIS)

(COP DAN TANDATANGAN PENYELIA)

Alamat Tetap:
NO. 10, JALAN 4/5B KG TASEK TAMBAHAN, 68000 AMPANG SELANGOR.

FAKHRULLAH BIN IDRIS
Jurutera Pengajar
Jabatan Teknologi Kejuruteraan Elektrik dan Komputer
Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik
Universiti Teknikal Malaysia Melaka

Tarikh: 10 JANUARY 2022

Tarikh: 11 JANUARY 2022

*CATATAN: Jika laporan ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali tempoh laporan ini perlu dikelaskan sebagai SULIT atau TERHAD.

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].

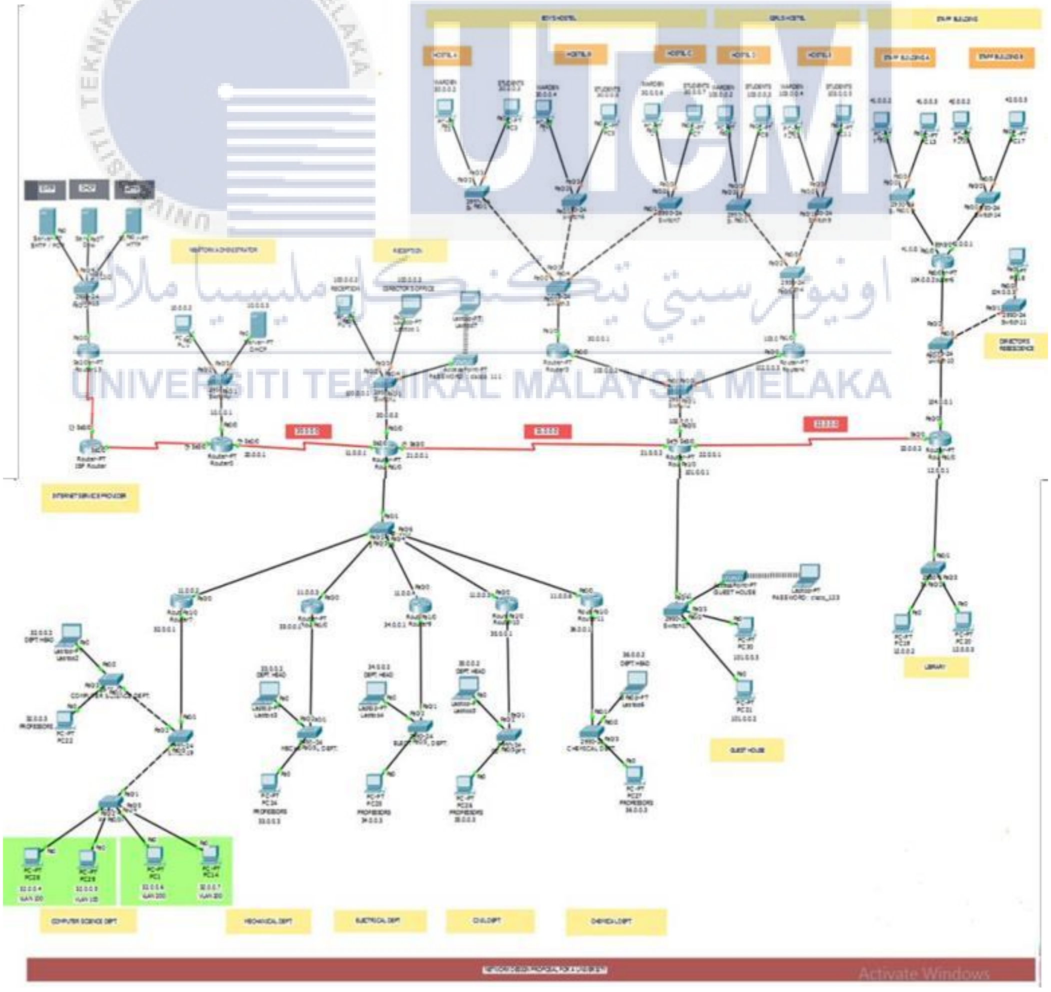

Figure 2.1 Basic complete architecture campus area [6]

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:

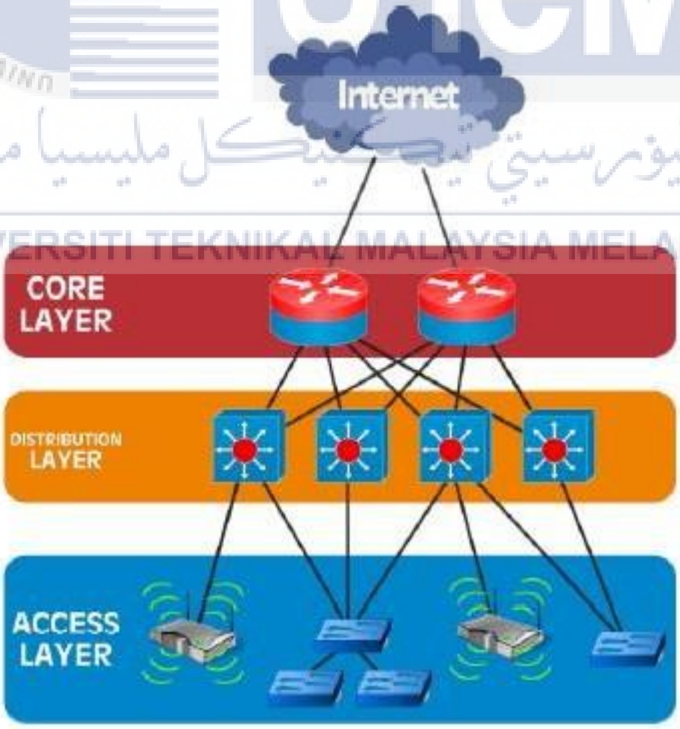

Figure 2.2 Flow network hierarchical design [8]