



HARAMAYA UNIVERSITY
HARAMAYA INSTITUTE OF TECHNOLOGY
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

HOSTING COMPANY: INFORMATION NETWORK SECURITY
ADMINSTRATION (INSA)

DOCUMENT TITLE: INTERNSHIP REPORT

DURATION: Oct 27,2024-Jan 17,2024

**SUBMITTED TO: - SCHOOL OF ELECTRICAL AND COMPUTER
ENGINEERING**

NO.	NAME	ID
1.	ABABIYA TUJUMA	0297/12
2.	ABDI GEREMU	0281/12
3.	MAHLET WORKENEH	2294/12
4.	SEID JEMAL	2734/12
5.	YARED DEBEBE	2997/12

ADVISOR: - Mr. ASEFA SEHALU

FEB, 5 2024 ETHIOPIA

DECLARATION

We now state that the content of this report is our own original creation, and that we have properly cited all sources and materials utilized in its creation. With our signature, we would like to reassure you.

NAME	SIGNATURE
ABABIYA TUJUMA
ABDI GEREMU
MAHLET WORKENEH
SEID JEMAL
YARED DEBEBE

APPROVAL PAGE

The undersigned attests that the aforementioned applicants have fully complied with the requirements of the project Paper in for the internship report in the department of electrical and computer engineering.

Signed by the Examining Committee:

Name	Signature	Date
------	-----------	------

Advisor: _____

Examiner: _____

Examiner: _____

Signed by the Head of the Department:

Name	Signature	Date
------	-----------	------

ACKNOWLEDGMENT

First of all, we would like to thank Almighty God for his blessing. In addition we are grateful to thank our family to their unreserved support and inspiration and we want to thank the Electrical and Computer Engineering department for giving us the opportunity to enhance our knowledge through a practical attachment.

Second, we want to express our gratitude to INSA for allowing us to collaborate with them. Specially, We are thankful to System and Secure Network Department for their lesson, support and appreciation during our internship program and lastly but not least we would like to thank MR. ASEFA (the university advisor) for sparing his valuable time by outlining specific instructions for creating the appropriate documentation formats.

ACRONYMS AND ABBREVIATIONS

INSA.....	Information Network Security Administration
AD.....	Active Directory
ADDS.....	Active Directory Domain Service
ADCS.....	Active Directory Certificate Service
DNS.....	Domain Name System
IIS.....	Internet Information Service
UCM.....	Unified Communications Managed API
OWA.....	Outlook Web Access
ECP.....	Exchange Control Panel
EAC.....	Exchange Admin Centre
EPRDF	Ethiopian People’s Revolutionary Democratic Front
MAC	Media Access Control address
LAN.....	Local Area Network
WAN.....	Wide Area Network
MAN.....	Metropolitan Area Network
VLAN.....	Virtual Local Area Network
OSI.....	Open System Interconnection
UTP.....	Unshielded Twisted Pair-Cable
STP.....	Shielded Twisted Pair-cable
LACP.....	Link Aggregation Control Protocol
VRRP.....	Virtual Router Redundancy Protocol
HSRP.....	Hot Standby Routing Protocol
IP	Internet Protocol
OSPF.....	Open Shortest Path First
VTP.....	VLAN Trunk Protocol
VHF.....	Very High Frequency
NAT.....	Network Address Translation

CLI.....	Command Line Interface
IGP.....	Interior Gateway Protocol
SPF.....	Shortest Path First
DLL.....	Data Link Layer
HTTP.....	Hyper Text Transfer Protocol
FTP.....	File Transfer Protocol
STP.....	Spanning Tree Protocol
RSTP.....	Rapid Spanning Tree Protocol
PVST.....	Per VLAN Spanning Tree
MST.....	Multiple Spanning Tree Protocol
VPC.....	Virtual Private Cloud
LSA.....	Link State Advertisement
LAG	Link Aggregation Group
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
FTS	File Transfer Server
POP3	Post Office Protocol version 3
SSH	Secure Shell/Secure Socket Shell
DMZ.....	De-Militarized Zone
SMTP.....	Simple Mail Transfer Protocol
IMAP.....	Internet Message Access Protocol

LIST OF FIGURES

Figure 1: INSA Building.....	1
Figure 2: Logo of INSA.....	2
Figure 3: overall organization structures.....	4
Figure 4: Flow chart of method.....	13
Figure 5: Network Simulation	29
Figure 6: Ping img 1.....	34
Figure 7: ping img 2.....	34
Figure 8: ping img 3.....	35
Figure 9: PowerShell command line	43
Figure 10: PowerShell command line 2	44
Figure 11: UCM	44
Figure 12: Visual C++.....	45
Figure 13: 2010 Filter pack.....	45
Figure 14: Schema extend.....	46
Figure 15: Installation	46
Figure 17: DNS Manager	47
Figure 18: Ecp server wizard	47
Figure 19: New user mailbox	48
Figure 20: Account information	49
Figure 21: SSL	49
Figure 22: certificate request.....	50
Figure 24: File source	52
Figure 25: Client Inbox	53
Figure 26: OWA.....	53
Figure 27: EAC.....	54
Figure 28: OWA Mobile access	54

List of Tables

Table 1: IP address	18
Table 2: IP address 2	19
Table 3: IP and vlan plan for head office	22
Table 4: IP plan for branch office 1.....	22
Table 5: IP and Vlan plan for branch office 1.....	23
Table 6: network between devices	25
Table 7: public network ip plan.....	25
Table 8. List of recommended device	57

Contents

DECLARATION.....	i
APPROVAL PAGE	ii
ACKNOWLEDGMENT	iii
List of Tables	vii
CHAPTER ONE.....	1
INTRODUCTION.....	1
1.1 Background of Information Network Security Administration (INSA).....	1
1.2 Mission, Vision Values and Principles of INSA	2
1.2.1 Mission	2
1.2.2 Vision.....	2
1.2.3 Values and Principles of INSA	3
1.3 Main Services and Product of INSA	3
1.4 Goal of the Company	3
1.5 Overall Organization Structure and Workflow of INSA	4
1.6 Major tasks.....	4
1.7 Overall objectives going on.....	5
1.8 Main customers of INSA	5
1.9 Overall objective of the task	6
CHAPTER 2.....	7
OVERALL INTERNSHIP EXPERIENCE.....	7
2.1 Objective of the Internship	7
2.2 Our Internship Working Section	7
2.3 How good I have been in performing my tasks	7
Chapter-3	8
The Overall benefits we gained from the internship	8
3.1 Theoretical and Practical Experience in Internship	8
3.1.1 Theoretical Experience	8
3.1.2 Practical Experience	8
3.1.3 Work ethics	9
3.2 Interpersonal Communication Skills	10
CHAPTER 4.....	11



PROJECT 1	11
4.1 Abstract	11
4.2 Introduction	11
4.3 Problem Statement	11
4.4 Objective	12
4.4.1 General Objective	12
4.4.2 Specific Objective	12
4.5 Scope	12
4.6 Methodology	13
4.7 Basic Infrastructure ABC Company	13
4.7.1 Requirements of ABC Company Network Infrastructure	13
4.8 Network Basic	14
Ether channel	15
4.9 General IP Plan for ABC Head Office and the branches.....	20
4.9.1 IP and VLAN Plan for HEAD-OFFICE	21
4.9.2 IP and VLAN Plan for Branch-Office	22
4.9.3 IP and VLAN Plan for Branch-Office 2	23
4.9.4 Connection between Network Devices	23
4.9.5 OUT-SIDE NETWORK	25
4.10 Network Simulation Software.....	26
4.10.1 Cisco Packet Tracer	26
4.10.2 Configurations.....	26
4.11 Simulation Design.....	29
4.12 Implementation	30
4.13 Results and Drawback.....	33
4.13.1 Result	33
4.13.2 Drawback	35
4.14 Conclusion	36
Chapter 5	37
Project 2.....	37
5.1 Abstract	37
5.2 Introduction	37
5.3 Problem Statement	38
5.4 Objective	38
5.4.1 General Objective	38
5.4.2 Specific Objective	38

5.5 Scope.....	38
5.6 Methodology.....	39
5.7 Requirements.....	40
5.7.1 Software requirements.....	40
5.7.2 Hardware requirements	42
5.8 Microsoft exchange server installation process	43
5.9 INTERNAL AND EXTERNAL URL CREATION	47
5.10 Client Access	48
5.10.1Mailbox user Account creation.....	48
5.11 SSL Certificate	49
5.12 Customization	51
5.13 Result and drawback.....	53
5.13.1 Result	53
5.13.2 Drawback	54
5.14 Conclusion	55
CHAPTER 6.....	56
CONCLUSION AND RECOMMENDATIONS	56
6.1 Conclusion.....	56
6.2 Recommendation.....	57
6.2.1 Recombination for the company	57
Reference.....	58
Appendix	59

EXECUTIVE SUMMARY

This report outlines the entire internship experience, beginning with the background of the internship hosting company, INSA's Department Division. It then attempts to discuss the three-month experience, benefits obtained from the internship, conclusions, and recommendations for the hosting company. It also goes into great detail about Network design and Microsoft Exchange Server. The report also covers the skills we developed as a result of fusing the theoretical knowledge we learned in class with the real-world experience we obtained throughout the internship term, such as work ethics, intercommunication skills, team-playing abilities, and entrepreneurship skills.

CHAPTER ONE

INTRODUCTION

1.1 Background of Information Network Security Administration (INSA)

Information Network Security Administration (INSA) was first established in 2006(GC) by Council of Ministers Regulation No. 130/2006, with the goal of defending our nation's information and information infrastructure from attack and safeguarding our national interest. Initially, INSA stood for Information Network Security Agency. However, after Ethiopian People's Revolutionary Democratic Front became the ruling party, the name was changed to Information Network Security Administration (INSA). However, the agency's establishment regulation was modified by Council of Ministers Regulation No. 250/2011 and most recently updated by Proclamation No. 808/2013 because it was necessary to change the agency's authority and duties in order to stop cybercrimes that become progressively more complex and to safeguard our national interest.

When the Ethiopian People's Revolutionary Democratic Front (EPRDF) was in power, Abiy Ahmed formed INSA (Information Network Security Administration), which now serves as Ethiopia's national signals intelligence and cyber-security agency and is in charge of the PM office.



External building structure



Internal building structure

Figure 1: INSA Building



Figure 2: Logo of INSA

1.2 Mission, Vision Values and Principles of INSA

1.2.1 Mission

- To build national cyber power capable of protecting the national interest.
- To provide technical intelligence pertaining to national interest so as to support decisions and actions of the government.
- To build data and computing capacity so as to ensure the transformation of the national high-tech and security industry.
- To ensure that information and computer based key infrastructures are secured so as to be enable of national peace, democratization and development program.

1.2.2 Vision

- To see a globally competent National Cyber Security Institution that plays a key role in the renaissance of the country.
- To realize a globally competent National Cyber capacity which plays a key role in protecting the national interests of Ethiopia

1.2.3 Values and Principles of INSA

- Our customers are pillars of our existence.
- your employees are key to our success
- Making difference in the field of information security
- Continuous learning and development
- Making difference/adding value
- Transparency /Accountability
- Resilience
- Making difference Integrity
- Respect for the people
- Respect for the law

1.3 Main Services and Product of INSA

- Security auditing
- Information technology security
- Export and import of product and security technology
- Cyber operation
- Digital forensics
- Intelligence
- Computer emergency responding centre

1.4 Goal of the Company

- To protect the national interest through building a capacity that enables safeguard the country information and information infrastructure.
- To enable the country to effectively use information, information network and communication, systems in implementing peace and democracy and implementing development strategies without any risk to national security

1.5 Overall Organization Structure and Workflow of INSA

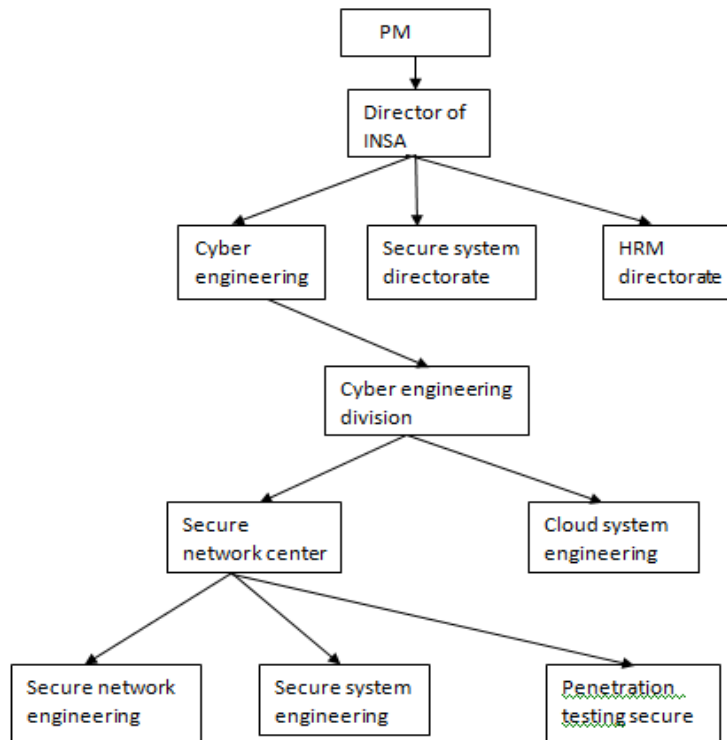


Figure 3: overall organization structures

1.6 Major tasks

- Virtual Machine Installation
- Active Directory preparation
- Window server Installation
- Microsoft Exchange server 2013
- Simple network design
- Company network design
- Datacentre tour

1.7 Overall objectives going on

- ✓ To provide research-based information security services and products
- ✓ Set national infrastructure that enables information security research and development programs.
- ✓ Formulate national information security related policies, legislation, and regulatory frameworks
- ✓ To create an eco-system that enables public-private interconnectivity and co addition
- ✓ Make sure that information security service the defence and national security-related decision-making process,
- ✓ Ensure that information security support socio-economic programs such as health, education, agriculture, and utilities.
- ✓ Facilitate national database development and utilization

1.8 Main customers of INSA

Financial services

Banks and other businesses in the financial industry work with INSA for safe transactions.

Government

Government agencies such as public safety and utilities have a particular need for information security since they have multiple sources of data that can be mined for insights.

Health care

Protection of Sensitive Data: Healthcare data is often highly sensitive, containing personal and medical information about patients¹. This data needs to be protected to maintain patient confidentiality and trust.

Media companies

Media companies can protect against data breaches by implementing strong data security protocols, such as encryption and access controls. It is also important for companies to regularly review and update their security measures to ensure they are keeping up with the latest threats.

Telecommunication

The telecom industry has long been a target of any cyber risk, as telephone companies are the critical tool that guarantees successful operations of communications infrastructures. Cybersecurity is necessary because security measures protect all forms of data from loss, cyber risk, and identity theft.

Generally almost all companies work with INSA since information and network security is vital for every company in this era of growing cyber-attack.

1.9 Overall objective of the task

During our internship program, we were working on the area of System engineering. The specific task is Active directory and Microsoft Exchange server. Microsoft Exchange Server is a server used for managing mail and calendars, essential for business communication. It runs exclusively on Windows Server operating systems and works with web-based mail clients like Microsoft Outlook. Exchange Server offers seamless integration with collaboration tools, providing robust email solutions, calendar integration, and compatibility with various protocols.

We were also working on Company network design using cisco packet tracer network simulation software. Company network design, also known as network topology, is the process of planning and designing the physical, virtual, and logical arrangement of infrastructure in an IT network¹. It's a crucial aspect of a company's IT strategy because it directly impacts the performance, security, and scalability of the company's operations.

CHAPTER 2

OVERALL INTERNSHIP EXPERIENCE

2.1 Objective of the Internship

- Let the students enhance their interpersonal, theoretical, and practical communications.
- To apply and generalize the academic theory and knowledge learned in the classroom lessons to real-world engineering fields to give us the opportunity to gain practical, hands-on experience.
- Give us more opportunities to manage a job and advance our careers.
- Establish a setting that is favourable for evaluating professional qualifications.
- To improve our ability to communicate with others and our professional abilities.

2.2 Our Internship Working Section

While working for the company, we were given two sectors to work on .Networking and System Engineering Department. For two months we worked in System department and for one moth we worked with both secure network and System department. Now this departments work together and they are called cloud computing and Datacentre.

2.3 How good I have been in performing my tasks

During our internship program, we work our tasks with enthusiasm, as well as our supervisor is such a sincere man when we ask a question he answered courteously. All in all, we did our task effectively and efficiently, and we were punctual when we performed our tasks.

Chapter-3

The Overall benefits we gained from the internship

3.1 Theoretical and Practical Experience in Internship

3.1.1 Theoretical Experience

Active Directory (AD): AD is a directory service developed by Microsoft for Windows domain networks. It provides centralized authentication and authorization to network resources.

Active Directory Domain Services (AD DS)

AD DS is the main component of Active Directory. It stores and manages directory data and objects on the network. AD DS provides security, schema, global catalog, query, replication, and search features for network users and administrators.

Microsoft Exchange Server: Microsoft Exchange Server is a mail server and calendaring server developed by Microsoft¹. It runs exclusively on Windows Server operating systems¹. The first version was called Exchange Server 4.01

Networking

Networking is the practice of transporting and exchanging data between nodes over a shared medium in an information system. Networking comprises not only the design, construction, and use of a network but also the management, maintenance, and operation of the network infrastructures.

Routing and Switching

Routing refers to establishing the routes that data packets take on their way to a particular destination. In general, routing involves the network topology, or the setup of hardware that can effectively relay data.

Switching is the practice of directing a signal or data element toward a particular hardware destination. Switching may be applied in various formats and can function in diverse ways within a greater network infrastructure. It uses a media access control (MAC) address to route data to a specific workstation.

3.1.2 Practical Experience

- Gained a deep understanding of Microsoft Exchange, a messaging platform that helps organizations manage email, calendar, and contact information.

- Active Directory: we learned about Active Directory, a directory service that provides a central location for storing and managing information about users, computers, and other resources on a network.
- PowerShell: we gained some skills on PowerShell, a powerful scripting language that can be used to automate many tasks in Exchange Server.
- Windows Server: we got hands-on experience with Windows Server, the platform upon which Exchange is installed and runs.
- Virtualization: we learn about virtualization technologies, which can be used to run multiple instances of Exchange Server on a single physical machine¹.
- Troubleshooting: we developed problem-solving skills as you learn to identify and resolve issues that may impact the performance of the Exchange system.
- Security: we understood how to manage security settings and enforce security policies in Exchange Server.
- Network Design: we gained a deep understanding of how to plan and execute network architectures.
- We learned about the configuration and activation of switch, routers, and other devices which are crucial components of any network.
- Network Infrastructure: we understood how to manage and configure network settings, which is crucial for the smooth operation of any network.
- Communication Skills: You'll likely need to explain your designs and decisions to other members of your team, stakeholders, or clients, helping you to develop your communication skills.

3.1.3 Work ethics

Integrity and Ethics: INSA places a high emphasis on integrity and ethics. The organization is committed to conducting its operations in an ethical manner.

Moral Compass: INSA expects its officers to have a strong moral compass. This means they should be able to distinguish right from wrong and make decisions that align with the agency's ethical standards.

Punctuality: Being on time is likely highly valued in INSA, as it is in many professional settings. This includes being punctual for meetings, deadlines, and other time-sensitive tasks. For this purpose INSA allocates transportation services to all workers.

Time Management: Efficient use of time is crucial in intelligence work. This could involve prioritizing tasks, setting realistic goals, and making effective decisions under time pressure.

3.2 Interpersonal Communication Skills

During our internship period the Interpersonal skills, which are the life skills I we used every day to communicate and interact with other people, individually and in groups are good for us. Not only how we communicate with others, but also, we got confidence and my ability to listen and understand. Problem-solving, decision making, and personal stress management are also considered interpersonal skills.

CHAPTER 4

PROJECT 1

4.1 Abstract

In this project we designed and configured a company ABC WAN network infrastructure for distribution. The project comprises of designing and configuring network infrastructure for fifteen departments, those fifteen departments have fifteen different VLAN. To design this WAN network infrastructure, we used Cisco Packet Tracer software (a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer) and components inside this software library such as router (a network-layer device that forwards data packets on the internet), switch (a data link layer which is closest to end users and is used to connect terminals to the company network), nodes and cables.

4.2 Introduction

There is a head office and two branch offices for AB Company. 500 users and five departments make up the head office (HR, Finance, Engineering, Administration, and ICT). Also, each of the two branch offices has five departments and 20 users, just like the head office. Also ABC Company has Web applications that should be accessed from the head office. The application is accessible to public.

4.3 Problem Statement

Most company are using two tier collapsed core multilayer switch, but it lacks of redundancy, Lack of load balancing and VLAN distribution is not configured properly, so they are vulnerable for different attack like Mac flood, Arp spoofing and spanning tree attack.

4.4 Objective

4.4.1 General Objective

- ✓ Design and configure a company AB WAN network infrastructure for distribution.
- ✓ Maintain the availability of network by using redundancy protocol and adding additional security features.

4.4.2 Specific Objective

- ✓ To control Broadcast flood problem
- ✓ To control unwanted loop
- ✓ uninterrupted data flow

4.5 Scope

Our project is limited to design and configure the company WAN network infrastructure for distribution and this project to design and simulation of a standard based Redundancy network infrastructure, improving VLAN. This all are designed on Cisco packet tracer

4.6 Methodology

On this project different methods were used:

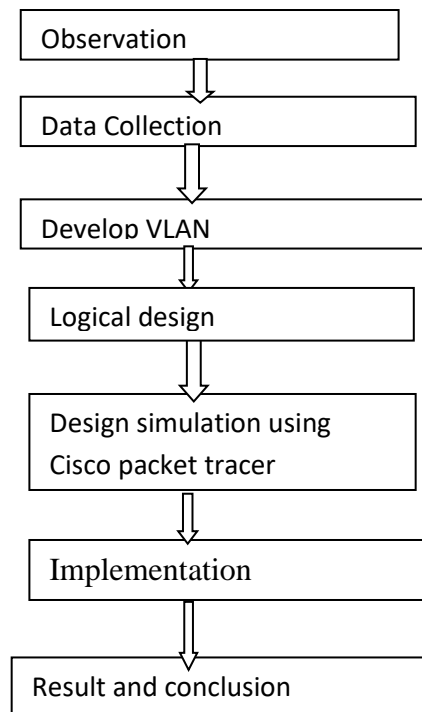


Figure 4: Flow chart of method

4.7 Basic Infrastructure ABC Company

4.7.1 Requirements of ABC Company Network Infrastructure

❖ The Company AB need to design network infrastructure with the following requirement: -

1. The company is located in 2 different branch offices.
 - i. Each site has at list 40 users (Ground Floors)
 - ii. Head office has 500 users. (G+4)
 - iii. The company have 5 departments (HR, Finance, Administration, Engineering and ICT)
2. ABC Company has Web applications that should be accessed from the head office. The application is accessible to public.
3. Have a design to access the branch offices.

4. Access list must be applied
5. The all site must have perimeter firewall
6. The branch and Head office should be connected through VPN
7. Have a hierarchical design (core, distribution, access) for head office LAN.
8. Have a collapsed core/distribution design for branch offices.
9. Make sure all devices and connections are redundant.
10. Have a device naming conventions and design for all offices.
11. Have a VLAN plan and an IP plan(explain why you chose it)

4.8 Network Basic

TRUNKING

Trunking is a technique used in data communications transmission systems to provide many users with access to a network by sharing multiple lines or frequencies. As the name implies, the system is like a tree with one trunk and many branches. Trunking is commonly used in very-high-frequency (VHF) radio and telecommunication systems. Trunking can also be defined as a network that handles multiple signals simultaneously. The data transmitted through trunking can be audio, video, controlling signals or images.

Dynamic Host Configuration Protocol (DHCP)

In manual network configuration random IP address configuration may cause IP address conflict. Network administrators centrally configure network parameters, with heavy workloads and repetitive tasks creating heavy work load. To overcome this, disadvantage we use Dynamic Host Configuration Protocol (DHCP). Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to hosts. It allows for easier administration and works well in small to very large network environments. Many types of hardware can be used as a DHCP server, including a Cisco router. Automatically allocates IP address to the devices connected to the local area network with the help of DHCP server. When the devices star up it broadcasts message around the local

area network to find DHCP server, then DHCP server gives IP address to the devices. To configure a DHCP server for your hosts, you need the following information at minimum: Network and mask for each LAN Network ID also called a scope. All addresses in a subnet can be leased to hosts by default. Reserved/excluded addresses: Reserved addresses for printers, servers, routers, etc. These addresses will not be handed out to hosts.

We usually reserve the first address of each subnet for the router, but you don't have to do this.

Default router: This is the router's address for each LAN.

DNS address: A list of DNS server addresses provided to hosts so they can resolve name.

Ether channel

Ether Channel is a technology that allows many physical Ethernet cables to be combined into a single logical channel, resulting in enhanced bandwidth and redundancy. Ether Channel's goal is to improve network stability and bandwidth while decreasing network complexity.

Ether Channel increases bandwidth by combining numerous physical links into a single logical channel, allowing more data to be transferred over the network. This aids in the alleviation of network bottlenecks and the overall functioning of the network.

In addition to higher capacity, Ether Channel provides redundancy, allowing network activity to continue even if one of the physical links fails. This contributes to network availability and avoids interruption.

Ether Channel supports a variety of protocols, including Link Aggregation Control Protocol (LACP) and Port Aggregation Protocol (PAGP), allowing Ether Channels to be established across various types of network devices.

Overall, Ether Channel is a beneficial technology for enterprises seeking to improve network speed and reliability while enhancing efficiency and disruption.

- In our project we used LACP because it is open standard and supported by most of vendors, while PAGP is Cisco proprietary only used between Cisco devices.

Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) is a networking protocol used in switches to prevent loops in the network.

STP's primary goal is to prevent loops from occurring, which can cause a large volume of data to be transmitted in an endless cycle, slowing down the network.

STP uses algorithms to discover the best path for data to take from one network device to the next. STP will choose the most efficient path and temporarily block other paths to prevent loops if many options are available. This ensures that data is sent effectively and reliably throughout the network, avoiding network slowdowns and data loss. STP is widely used in both large and small networks, and it is an essential component of current networking technology.

HSRP Configuration

HSRP is an IP routing redundancy protocol designed allows for transparent failover at the first-hop IP route. It provides high network availability, because it routes IP traffic from hosts on network without relying on the availability of any single router.

HSRP is useful for hosts that do not support a router discovery protocol such as ICMP AND can't switch to a new router when their selected router reloads or loses power.

It is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP sub network.

The protocol achieves this by the creation of virtual routers, which are an abstract representation of multiple routers, i.e. primary/active and secondary/Standby routers, acting as a group. The virtual router is assigned to act as a default gateway of participating hosts, instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the primary/active router.

Routing

Routing is a critical aspect of network communication that enables data to travel from one device to another over a network. It involves the selection of the best path for data to follow based on various factors, such as network congestion, distance, and security. The goal of routing is to ensure that data is delivered efficiently and effectively from a source to a destination.

Dynamic route

Dynamic routing is a method of routing data packets in a network that uses protocols to dynamically determine the best path for data to travel from source to destination. Unlike static routing, where the network administrator manually sets up specific routes for data packets to follow, dynamic routing allows for automatic adjustments to be made in real-time based on changing network conditions, such as link failures or congestion. This allows for more efficient use of network resources and can help prevent network outages or slowdowns.

Link state Protocols

Link-State Protocols (LSPs) are a type of routing protocol that is used to communicate information about a network's topology to other routers in the network. LSPs build a complete map of the network and then each router uses that information to calculate the best path to each destination. Examples of link-state protocols include Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS).

Internetwork Security

Internetwork security refers to the measures taken to protect networks and their components, including devices, data, and users, from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing security protocols and technologies, such as firewalls, encryption, access controls, and intrusion detection systems, to ensure that the network is secure and protected against security threats.

One of the most significant aspects of internetwork security is the implementation of firewalls, which serve as the first line of defence against security threats. Firewalls are devices that monitor incoming and outgoing network traffic and block unauthorized access to the network. They can be hardware-based or software-based and are essential for preventing unauthorized access to the network, especially from the internet.

IP Address (Logical Address)

An IP address identifies a node (or an interface on a network device) on a network. It is used to forward IP packets on the network. On an IP network, if a user wants to connect a computer to the Internet, the user needs to apply for an IP address for the computer. The interface that needs to use an IP address is usually the interface of a router or computer. Logical addressing is a function of the Network layer of the OSI Model (Layer-3), and provides a hierarchical structure to separate networks. Logical addresses are never hardcoded on physical network interfaces, and can be dynamically assigned and changed freely. A logical address contains two components:

Network ID: identifies which network a host belongs to. Network devices with the same network ID are located on the same network, regardless of their physical locations.

Host ID: uniquely identifies the host on that network. IP provides two fundamental Network layer services:

1. Logical Addressing: provides a unique address that identifies both the host, and the network that host exists on.

IP Version 4 (IPv4) was the first version to experience widespread deployment. IPv4 employs a 32-bit address and the possible number of users can be determined by the formula 2^n , where n is the number of host bits. An IP address is most often represented in decimal, in the following format: 192.168.0.0

An IP address is comprised of four octets, separated by periods.

1st octet	2nd octet	3rd octet	4th octet
192	168	0	0

Table 1: IP address

Each octet is an 8-bit number, resulting in a 32-bit IP address

IP Address Classes

The IPv4 address space has been structured into several classes. The value of the first octet of an address determines the class of the network.

Class	First Octet Range	Default Subnet Mask	Description
Class A	1-127L	255.0.0.0	1st octet define network, last 3 octet host
Class B	128-191	255.255.0.0	1 st2octet define network, last 2 octet host
Class C	192-223	255.255.255.0	1 st3 octet define network last 1 octet host
Class D	224-239	–	–
Class E	240-255	–	–

Table 2: IP address 2

Class A, B, and C addresses are unicast IP addresses (except some special addresses). Only these addresses can be assigned to host interfaces. Class D addresses are multicast IP addresses. Class E addresses are used for special experiment purposes. From these IP address classes, we used C type address for our project with proper subnet mask.

Subnet mask

It determines what part of an address identifies the network, and what part identifies the host. A network mask (subnet mask) is 32 bits long, which is also represented in dotted decimal notation, like bits in an IP address. The network mask is not an IP address. The network mask consists of consecutive 1s followed by consecutive 0s in binary notation. The subnet mask follows two rules: If a binary bit is set to a 1 (or on) in a subnet mask, the corresponding bit in the address identifies

the network. If a binary bit is set to a 0 (or of) in a subnet mask, the corresponding bit in the address identifies the host.

4.9 General IP Plan for ABC Head Office and the branches

The first step in creating an IP plan is to determine the number of IP addresses required for each location, including the head office and branches. Let's say that the head office has 500 devices and each branch has 500 devices (by applying if the possibility of scaling occurs), a total of 1500 devices.

Once the number of IP addresses has been determined, the next step is to decide on the IP addressing scheme that will be used. Depending up on the number of users class B ip address is decided for usage.

- ✓ We have minimum of 500 users in head office and company networks are known practically for having many logical groups of an IP address, indicating that class B IP should be chosen.
- ✓ $2^h - 2 = \text{No. hosts}$, $2^h - 2 = 500$ where h: host bit
- ✓ Even if only one department were there in a branch, there would be a minimum of 40 users. This indicates that we have a minimum of 540 total users and above.
- ✓ 40 user in each sites means there must be a minimum of 40 host IPs in a subnet.
- ✓ Based on the above requirements we will do subnetting.
- ✓ We would have chosen class A but since our company is medium sized enterprise class B has chosen.
- ✓ Since we are designing for a company we should choose a private IP range.
- ✓ 5 departments selected to be in head office and Branch office.

Base Network: **172.16.1.0**

VLAN IDs are assigned to each department accordingly.

A Dynamic Host Configuration Protocol (DHCP) server should be set up to manage the assignment of IP addresses. This will ensure that IP addresses are dynamically assigned to devices as they connect to the network, and will also simplify the management of IP addresses in the network. So, we set DHCP server at the head office and configured to assign IP addresses to devices at both the head office and branches.

Configure network routers and switches: Network routers and switches will need to be configured to route traffic between the head office and branches. This may involve setting up Virtual Private Network (VPN) connections, or using other routing protocols to ensure that data is transmitted securely between locations. So, we set a Firewall at the head office and configured to route traffic between the head office and branches using a VPN connection.

Monitor and manage IP addresses: Regular monitoring and management of IP addresses will be required to ensure that the network continues to operate efficiently. This may involve monitoring the usage of IP addresses and releasing IP addresses that are no longer in use, or adjusting the sub netting scheme as the network grows.

4.9.1 IP and VLAN Plan for HEAD-OFFICE

Department	VLAN ID	Network ID	Subnet	Host IP Range	Broadcast ID
Administration	10	172.16.1.0	255.255.255.128/25	172.16.1.1- 172.16.1.126	172.16.1.127
HR	20	172.16.1.128	255.255.255.128/25	172.16.1.129- 172.16.1.254	172.16.1.255
Finance	30	172.16.2.0	255.255.255.128/25	172.16.2.1- 172.16.2.126	172.16.2.127
Engineering	40	172.16.2.128	255.255.255.128/25	172.16.2.129- 172.16.2.255	172.16.2.255

				172.16.2.254	
ICT	50	172.16.3.0	255.255.255.128/25	172.16.3.1- 172.16.3.126	172.16.3.127
SERVER POOL	-	172.16.6.24	255.255.255.248/29	172.16.6.25- 172.16.6.30	172.16.6.31

Table 3: IP and vlan plan for head office

4.9.2 IP and VLAN Plan for Branch-Office

Department	VLAN ID	Network ID	Subnet	Host IP Range	Broadcast ID
Administration	60	172.16.3.128	255.255.255.128/25	172.16.3.129- 172.16.3.254	172.16.3.255
HR	70	172.16.4.0	255.255.255.128/25	172.16.4.1- 172.16.1.126	172.16.4.127
Finance	80	172.16.4.128	255.255.255.128/25	172.16.4.129- 172.16.2.254	172.16.4.255
Engineering	90	172.16.5.0	255.255.255.128/25	172.16.5.1- 172.16.5.126	172.16.5.127
ICT	100	172.16.5.128	255.255.255.128/25	172.16.5.129- 172.16.5.254	172.16.5.255

Table 4: IP plan for branch office 1

4.9.3 IP and VLAN Plan for Branch-Office 2

Department	VLAN ID	Network ID	Subnet	Host IP Range	Broadcast ID
Administration	200	172.16.11.0	255.255.255.128/25	172.16.6.49- 172.16.6.174	172.16.11.127
HR	300	172.16.11.128	255.255.255.128/25	172.16.6.177- 172.16.7.46	172.16.11.255
Finance	400	172.16.12.0	255.255.255.128/25	172.16.7.49- 172.16.7.174	172.16.12.127
Engineering	500	172.16.12.128	255.255.255.128/25	172.16.7.177- 172.16.8.46	172.16.12.255
ICT	600	172.16.13.0	255.255.255.128/25	172.16.8.49- 172.16.8.174	172.16.13.127

Table 5: IP and Vlan plan for branch office 1

4.9.4 Connection between Network Devices

<u>Device</u>	<u>Network ID</u>	<u>Subnet</u>	<u>Host IP Range</u>	<u>Broadcast ID</u>
(Head-OFF-MLSW-1)-(Head-OFF-R1)	172.16.6.0	255.255.255.252/30	172.16.6.1 172.16.6.2	172.16.6.3
(Head-OFF-MLSW-1)-(Head-OFF-R2)	172.16.6.4	255.255.255.252/30	172.16.6.5 172.16.6.6	172.16.6.7

(Head-OFF-MLSW-2)-(Head-OFF-R1)	172.16.6.8	255.255.255.252/30	172.16.6.9 172.16.6.10	172.16.6.11
(Head-OFF-MLSW-2)-(Head-OFF-R2)	172.16.6.12	255.255.255.252/30	172.16.6.13 172.16.6.14	172.16.6.15
(Head-OFF-R1)- (Head-OFF-Firewall)	172.16.6.16	255.255.255.252/30	172.16.6.17 172.16.6.18	172.16.6.19
(Head-OFF-R2)- (Head-OFF-Firewall)	172.16.6.20	255.255.255.252/30	172.16.6.21 172.16.6.22	172.16.6.23
(Head-OFF-Firewall)- (Head-OFF-R3)	172.16.6.32	255.255.255.252/30	172.16.6.33 172.16.6.34	172.16.6.35
(ISP)- (Branch-OFF-Firewall)	172.16.6.36	255.255.255.252/30	172.16.6.37 172.16.6.38	172.16.6.39
(Branch-MLSW-1)- (Branch-OFF-Firewall)	172.16.6.40	255.255.255.252/30	172.16.6.41 172.16.6.42	172.16.6.43
(Branch-MLSW-2)- (Branch-OFF-Firewall)	172.16.6.44	255.255.255.252/30	172.16.6.45 172.16.6.46	172.16.6.47
(Head-OFF-Firewall)- (ISP2)	10.10.10.160	255.255.255.252/30	10.10.10.161- 10.10.10.162	10.10.10.163
(BRANCH-OFF-R1)- (ISP)	10.10.10.164	255.255.255.252/30	10.10.10.165- 10.10.10.166	10.10.10.167
(OUTSIDE-R)- (ISP1)	10.10.10.168	255.255.255.252/30	10.10.10.169- 10.10.10.170	10.10.10.171
(OUTSIDE-R)- (ISP2)	10.10.10.172			

(Branch-OFF-2-Firewall)- (ISP2)	10.10.10.180			
(ISP2)- (Branch-OFF-Firewall)	10.10.10.164			
(Branch-OFF-2-Firewall)- (ISP)	10.10.10.176			
(Branch-2-MLSW-1)- (Branch-OFF-2-Firewall)	172.16.8.176			
(Branch-2-MLSW-2)- (Branch-OFF-2-Firewall)	172.16.8.180			

Table 6: network between devices

4.9.5 OUT-SIDE NETWORK

OUTSIDE NET	192.168.1.0	255.255.255.0/24
--------------------	--------------------	-------------------------

Table 7: public network ip plan

Virtual Local Area Network (VLAN)

A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. Virtual LANs, or VLANs, which are used when you logically break up broadcast domains in a layer 2, switched network. It's really important to understand that even in a switched network environment; you still need a router to provide communication between VLANs. Each port on the switch is a separate collision domain, and each VLAN would be a separate broadcast domain. Virtual Local Area Network (VLAN) allows you to logically segment a Local Area Network

(LAN) into different broadcast domains. By deploying VLANs on switches, you can logically divide a large broadcast domain into several small broadcast domains. This effectively improves network security, lowers junk traffic, and reduces the number of required network resources.

VLAN Planning

Our project for VLAN depends on departments. We assigned one VLAN Access layer switch of each department will have a trunk port for carrying traffic from all VLAN and it is connected to distribution layer switch and has access mode switch port which connects to end device. VLAN name of all VLAN is the name of the department and the VLAN ID is the number of the department where the switch resides.

4.10 Network Simulation Software

4.10.1 Cisco Packet Tracer

As networking systems continue to evolve in complexity, new curricula and educational tools are emerging to facilitate teaching and learning about networking technology. The Cisco Networking Academy program is designed to keep pace with the evolution of networking systems by providing innovative curricula and educational tools that help students understand the complexities of information and communication technologies (ICTs).

Within this framework, the Cisco Packet Tracer e-learning software was developed to help Networking Academy students gain practical networking technology skills in a rapidly changing environment. Packet Tracer is a cross-platform visual simulation program designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

4.10.2 Configurations

The Cisco IOS (Internetwork Operating System) is a command-line interface used by nearly all current Cisco routers and Catalyst switches. The IOS provides the mechanism to configure all Layer 2 and Layer 3 functions on Cisco devices

4.10.2.1 Configuration on Router

We configure on router: - Inter VLAN configuration. Inter VLAN configuration: -in order to communicate one VLAN to another VLAN.

N. B: The commands (codes) we wrote for our project is located on the appendix1.

4.10.2.2 Multilayer Switches Configuration

The switch may be set using the graphical user interface (GUI) or command line interface (CLI) after the fundamental network design has been determined (GUI). This might involve undertakings like:

Creating and assigning VLAN IDs to network segments is known as configuring VLANs.

Assigning IP addresses and other network settings to interfaces is known as configuring an interface.

Setting up static or dynamic routing protocols to manage network traffic flow is known as configuration of routing.

Setting up firewalls, ACLs, and other security features to regulate network access is known as security feature configuration.

Remember that multilayer switch configurations might differ significantly based on the manufacturer, model, and network needs. In order to guarantee appropriate configuration and optimum network performance, network administrators should refer to the vendor's documentation and best practices.

N.B: The commands (codes) we wrote for our project is located on the appendix 1

4.10.2.3 DMZ Switch Configuration

The arrangement of switches in a DMZ environment is referred to as a DMZ (Demilitarized Zone) switch configuration. A network segment called a "DMZ" is used to keep private internet traffic away from vulnerable internal network resources. The switch configuration in a DMZ is intended to give users of the internal network and the general public secure and restricted access to the DMZ resources.

The protection of the DMZ resources is the main objective of the DMZ Switch Configuration. This involves guarding against network-based assaults and blocking illegal access from the general internet. To prevent unwanted access, the switch configuration should contain security features including access control lists (ACLs), port security, and network segmentation. In order to increase

security, the switch configuration should also enable technologies like firewalls and intrusion detection systems (IDS).

Performance and availability are key factors in the DMZ switch configuration. The switch configuration needs to be set up such that authorized users can always access and use the DMZ resources. As part of this, make sure the switch configuration supports link aggregation and virtual LANs and has highly available, redundant components (VLANs). The switch configuration also has to support network performance and reduce congestion and delay. This can be accomplished by strategically placing switches, setting up Quality of Service (QoS) policies, and utilizing cutting-edge switching technologies like virtual switching.

4.10.2.4 Configuration on Access layer Switch

We configure on access switch: -To assign VLAN on the access layer switch port

4.11 Simulation Design

The project final simulation of AB company network on packet Tracer is shown as follows:

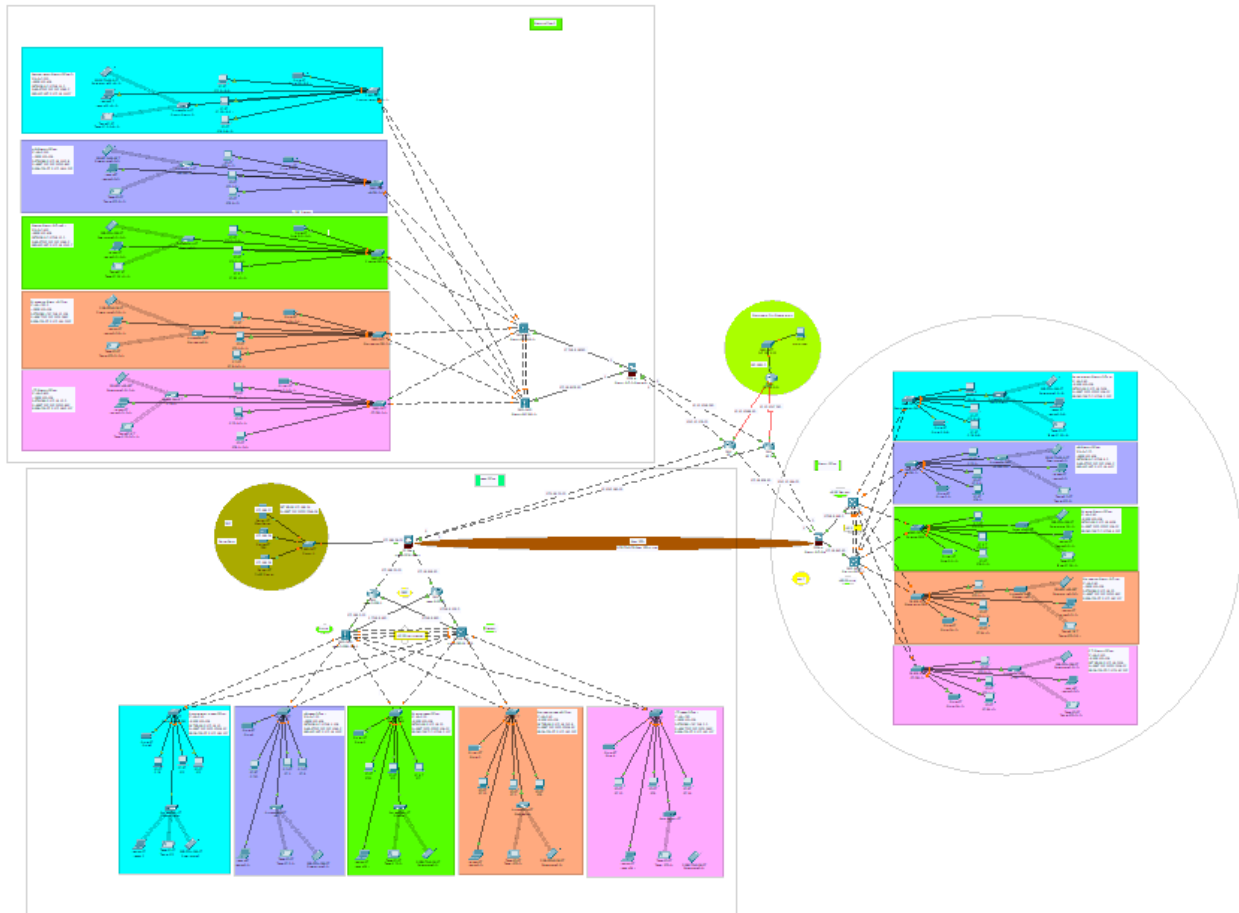


Figure 5: Network Simulation

4.12 Implementation

Administrative configurations

Firewall configuration:

```
Ciscoasa(config)# int gig 1/1
```

```
Ciscoaa(config-if)# no shut
```

```
Ciscoasa(config-if)# name if INSIDEE } 1
```

```
Ciscoasa(config-if)# security-level 100
```

```
Ciscoasa(config-if)# ip add 172.16.6.4 255.255.255.252
```

```
#ex
```

```
#wr mem
```

NAT configuration:

```
Ciscoasa(config)# route OUTSIDE 0.0.0.0 0.0.0.0 172.16.6.33
```

```
Ciscoasa(config)# object network INSIDE1-OUTSIDE
```

```
Ciscoasa(config-network-object)#subnet 172.16.1.0 255.255.255.128
```

```
Ciscoasa(config-network-object)# nat(INSIDE1,OUTSIDE) dynamic interface
```

```
#ex
```

```
Ciscoasa(config)# object network INSIDE2-OUTSIDE
```

```
Ciscoasa(config-network-object)#subnet 172.16.1.0 255.255.255.128
```

```
Ciscoasa(config-network-object)# nat(INSIDE2,OUTSIDE) dynamic interface
```

```
#ex
```

Inspection Policy:

```
Casa(config)# access-list RES-ACCESS Extended permit icmp any any
Casa(config)# access-list RES-ACCESS Extended permit udp any any eq 67
Casa(config)# access-list RES-ACCESS Extended permit udp any any eq 68
Casa(config)# access-list RES-ACCESS Extended permit udp any any eq 53
Casa(config)# access-list RES-ACCESS Extended permit tcp any any eq 53
Casa(config)# access-group RES-ACCESS Extended in interface DMZ
Casa(config)# access-group RES-ACCESS Extended in interface outside
```

IPSEC VPN:

!

```
Crypto ikev1 policy 10
```

```
Hash sha
```

```
Authentication pre-share
```

```
Group 2
```

```
Life time 86400
```

```
Encryption 3des
```

```
Exit
```

!

```
Tunnel-group 172.16.6.38 type ipsec-121
```

```
Tunnel-group 173.16.6.38 ipsec-attributes
```

```
Ikev1 pre-shared-key cisco
```

!

```
Crypto isec ikev1 transform-set TSET esp-3des esp-sha-hmac
```

!

Access-list PN_ACL permit ip 172.16.1.0 255.255.255.128 172.16.3.128 255.255.255.128

!

Crypto map CMAP 10 set peer 172.16.6.38

Crypto map CMAP 10 set ike1 transform-set TSET

Crypto map CMAP 10 match address VPN_ACL

!

Crypto map CMAP 10 match address VPN_ACL

!

Crypto map CMAP interface OUTSIDE

Crypto ikev1 enable OUTSIDE

vlan configuration:

SW(config)# inter range fa 0/1-2

SW(config-if-range)# switchport-mode trunk

Sw(config) vlan 10

SW(config-vlan)# name “ “

SW(config)# int range fa0/1-24

SW(config-if-range)#switchport mode access

SW(config-if-range)# switchport access vlan 10

Trunk port configuration:

MLSW(config)# int range gig1/0/2-6

MLSW(config-if-range) switchport mode trunk

Ether channel:

```
MLSW(config)#int range gig 1/0/1-3
```

```
MLSW(config-if-range)#channel-group 1 mode active
```

```
MLSW(config-if-range)interface port-channel 1
```

```
MLSW(config-if)#switch port mode trunk
```

OSPF configuration:

```
MLSW(config)#router ospf 1
```

```
MLSW(config-router)#router-id 2.1.2.1
```

```
MLSW(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

4.13 Results and Drawback

4.13.1 Result

Verifying connectivity of device

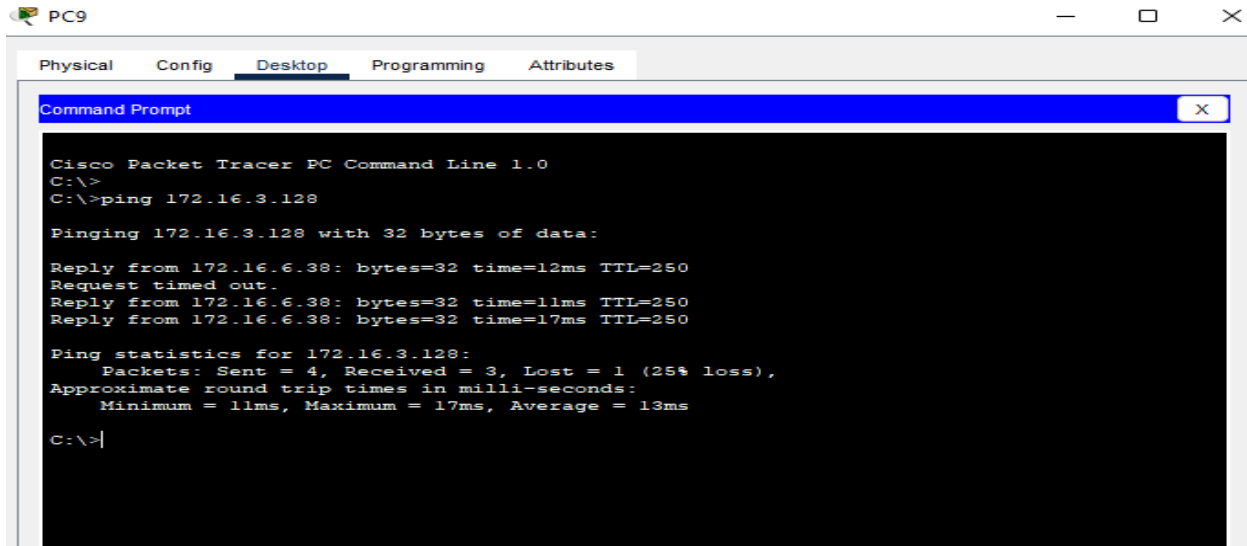
Ping command

Now we are going to use the Windows Command Prompt in our project to test the devices connectivity by ping. Among the Command Prompt commands, we use the ping command. A ping is used to verify connectivity at an IP-level to a second TCP/IP device. To use the ping command to test the connectivity

1. On the client, open a command prompt.
2. Type the ping command, “ping IP address of the device you want to verify”

Ping from HEAD OFFICE on VLAN 10 to BRANCH1 ON VLAN 60

Ping from HEAD OFFICE on VLAN 10 to BRANCH1 ON VLAN 60



```

PC9
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>
C:\>ping 172.16.3.128

Pinging 172.16.3.128 with 32 bytes of data:

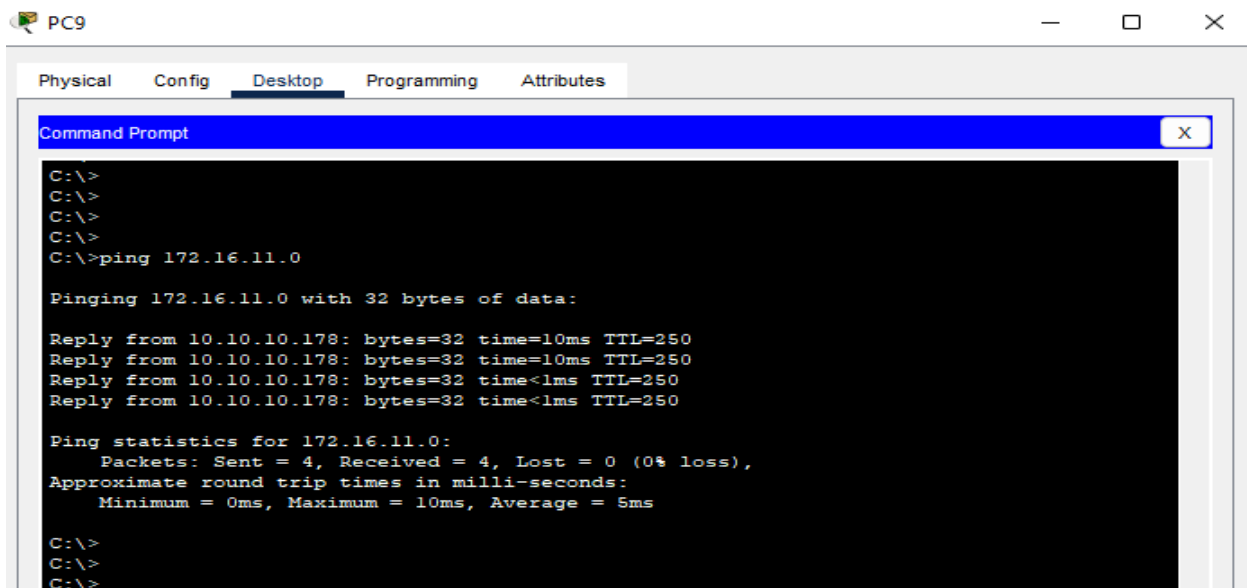
Reply from 172.16.6.38: bytes=32 time=12ms TTL=250
Request timed out.
Reply from 172.16.6.38: bytes=32 time=11ms TTL=250
Reply from 172.16.6.38: bytes=32 time=17ms TTL=250

Ping statistics for 172.16.3.128:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 17ms, Average = 13ms

C:\>
  
```

Figure 6: Ping img 1

Ping from HEAD OFFICE on VLAN 10 to BRANCH2 ON VLAN 200



```

PC9
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>ping 172.16.11.0

Pinging 172.16.11.0 with 32 bytes of data:

Reply from 10.10.10.178: bytes=32 time=10ms TTL=250
Reply from 10.10.10.178: bytes=32 time=10ms TTL=250
Reply from 10.10.10.178: bytes=32 time<1ms TTL=250
Reply from 10.10.10.178: bytes=32 time<1ms TTL=250

Ping statistics for 172.16.11.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>
C:\>
C:\>
  
```

Figure 7: ping img 2

Ping from BRANCH Office 2 on VLAN 200 to BRANCH1 ON VLAN 60

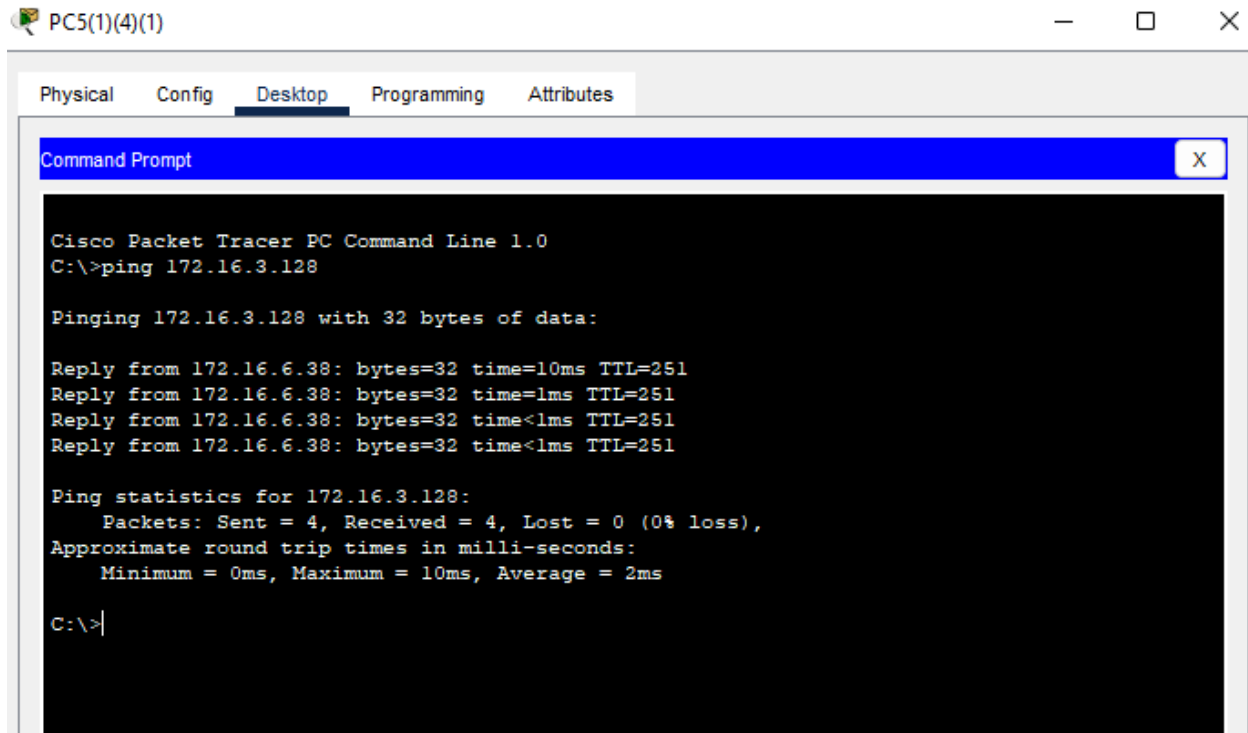


Figure 8: ping img 3

4.13.2 Drawback

- ✓ We have only designed and implemented this project with simulation.
- ✓ Sometimes the DHCP server fails with no reasons ,this shows the simulation software's drawback
- ✓ The Firewall is not friendly to work with.

4.14 Conclusion

In the time we have been working in this project we have gone through a lot off methodologies and process until the end of the project, we conclude that the network is fully operational on working on both cores with redundancy. we managed to create VLAN Trucking protocols, VLANS, we managed to create Ether-Channel between core switches, we managed to create a fast secure gigabit internet connection for the devices. And also, from this project we have got at least the know-how to design and implement network, identified network devices and their operation system like routers, switches, etc.

Since a network is a system of interconnected devices for the purpose of file or information sharing so a network should be secure and easily manageable by the network administrator ; to do this we have used some devices configuration and concept of VLAN.We have understood how we can assign dynamic IP address for hosts or users which are tedious for manual IP address configuration especially for large networks, and identified some special host or devices that need static IP address allocation like printers, servers. We also understood the features of Cisco Packet Tracer software application to design and simulate network infrastructure. In general, we get more about the basic understanding and knowledge about networking to allocate network for the intended purpose.

Chapter 5

Project 2

5.1 Abstract

This research paper focuses on the deployment of an Exchange Server at Haramaya University. The Exchange Server is a critical component for efficient communication and collaboration within the university community. By implementing this server, Haramaya University aims to enhance email services, calendar management, and other collaborative features for students, faculty, and staff. In this project we installed, configured, and deployed Microsoft exchange server as a secure communication means for an organization.

5.2 Introduction

Now days, data becomes the back bone of every institute, company, even government organizations. Securing one's data and information against any unauthorized person is becoming more and more important since the number of attackers and hackers rapidly increasing day by bay . In order to control these treats we need a trusted and secure communication to exchange the information. Therefore Microsoft Exchange Server plays a critical role in enabling efficient and secure mail communication with in company or organization.

This report mainly focus on the deployment of Microsoft Exchange Server 2013 installation, client access, certificate and customization on ABC Company

5.3 Problem Statement

Most organizations still use Internet mailing method whose their database are not found in their own Datacentre (i.e. E-mail, Telegram) , but these communication method lack security, so the information transmitted may be easily found by third party.

5.4 Objective

5.4.1 General Objective

- ✓ Install and configure Exchange server for ABC company
- ✓ Solving security problems during communication.

5.4.2 Specific Objective

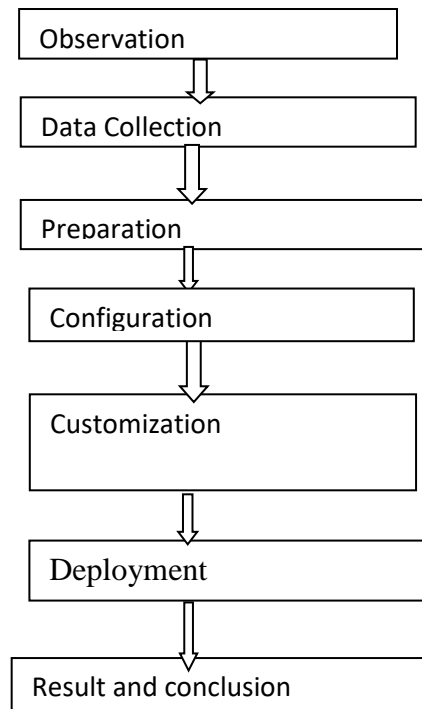
- ✓ Client Access
- ✓ Customization
- ✓ Creating user mailbox(new as well as existing user from Active directory)

5.5 Scope

Our project is limited to configuring SSL certificate, client Access, Internal and External URL creation and Customization .This all is done on Microsoft exchange server 2013. Also for this purpose we used VMware Workstation hypervisor.

5.6 Methodology

On this project different methods were used:



5.7 Requirements

5.7.1 Software requirements

1. VMWare work station

VMware Workstation is a software program that allows you to run multiple operating systems simultaneously on a single physical computer. It does this by creating virtual machines (VMs), which are essentially software-based computers that act independently of the host machine. Each VM has its own operating system, applications, and files, just like a regular computer.

2. Window server 2012 R2

Windows Server 2012 R2, codenamed "Windows Server Blue", was a server operating system released by Microsoft in October 2013. It served as the successor to Windows Server 2012 and was itself succeeded by Windows Server 2016. However, it's important to note that Microsoft ended mainstream support for Windows Server 2012 R2 in January 2020 and extended support in October 2023. This means Microsoft no longer provides new features or non-security fixes for the software. While paid extended security updates are available until October 2026 for volume licensed editions, using an unsupported operating system exposes your system to potential security vulnerabilities.

3. Unified communication management API

Unified communication management (UCM) refers to the tools and processes used to manage and optimize an organization's communication systems. These systems typically integrate various communication channels like voice, video, instant messaging, email, and collaboration tools into a single platform. UCM helps organizations.

4. Microsoft filter pack 2010

Microsoft Filter Pack 2010 is a collection of software components called **IFilters** specifically designed for the 2010 version of Microsoft Office applications. These IFilters enable search services like Windows Search, SharePoint, SQL Server, and Exchange Server to index the content of various file types. Essentially, they allow these services to understand and extract information from different file formats, making them searchable within your system

5. Microsoft filterpack 2010 service pack 2

Microsoft Filter Pack 2010 Service Pack 2 (SP2) was an update package released in 2013 for the Microsoft Filter Pack 2010. Remember, Microsoft Filter Pack 2010 itself is no longer supported as of October 2023. However, let's go over what SP2 offered:

- Updated IFilters: SP2 provided updated versions of the IFilters included in the base Filter Pack 2010. These improved IFilters enhanced the ability of search services like Windows Search, SharePoint, SQL Server, and Exchange Server to index and understand the content of various file formats.
- Bug fixes and stability improvements: SP2 addressed various bugs and stability issues reported in the initial release of Filter Pack 2010.
- Security patches: It included security patches to address vulnerabilities discovered in the IFilters.

6. Exchange server 2013

Microsoft Exchange Server 2013 was an on-premises email server application and collaboration platform released in 2013. It offered a variety of features for businesses, including:

- Email: Secure and reliable email for businesses of all sizes.
- Calendar: Shared calendars for scheduling meetings and events.
- Contacts: Centralized storage for contact information.
- Tasks: Task management tools for individuals and teams.
- Unified Messaging: Voicemail, email, and faxes in a single inbox.
- Archiving: Long-term storage of email, calendar, and other data.
- eDiscovery: Tools for searching and retrieving electronic data for legal or compliance purposes.

5.7.2 Hardware requirements

Computer

Computer with the following specifications:

Processor

» x64 architecture-based computer with Intel processor that supports Intel 64 architecture (formerly known as Intel EM64T)

Memory: Memory Varies depending on Exchange roles that are installed:

» Mailbox: 8GB minimum

» Client Access: 4GB minimum

» Mailbox and Client Access combined: 8GB minimum

Disk space:

» At least 30 GB on the drive on which you install Exchange

» An additional 500 MB of available disk space for each Unified Messaging (UM) language pack that you plan to install

» 200 MB of available disk space on the system drive

» A hard disk that stores the message queue database on with at least 500 MB of free space.

5.8 Microsoft exchange server installation process

❑ Prerequisite:

➤ Active Directory Preparation

- Window Server 2012 operating system.
- Installing and Configuring the ADDS
- Installing and Configuring another ADDS and replicate to install exchange server.

➤ Exchange Server

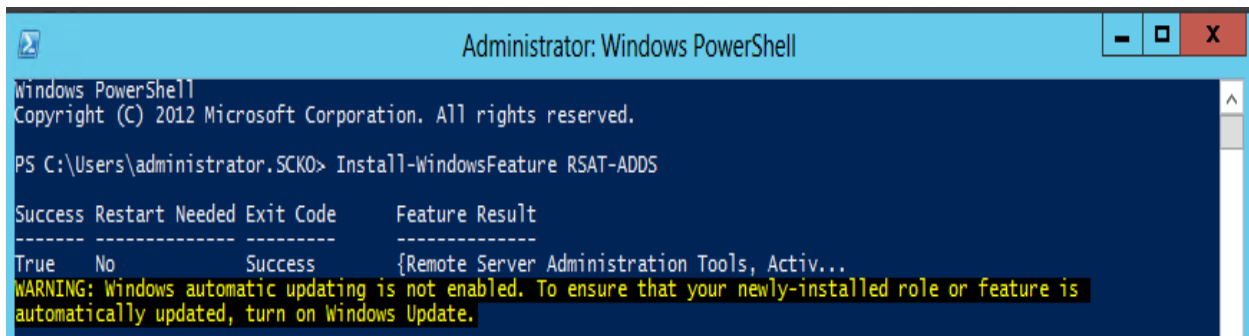
- Operating System - Window Server 2012
- Associated Server Roles:

1. Mailbox Server Role.

2. Client Access Server Roles.

We follow the next steps:

A. Run : *Install-WindowsFeature RSAT-ADDS* PowerShell command line .



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.SCKO> Install-WindowsFeature RSAT-ADDS

Success Restart Needed Exit Code      Feature Result
-----
True     No             Success      {Remote Server Administration Tools, Activ...
WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is
automatically updated, turn on Windows Update.
    
```

Figure 9: PowerShell command line

- B. Windows Server 2012 prerequisites for Mailbox Server Role
- C. Windows Server 2012 prerequisites for standalone Mailbox Server Role or Mailbox and Client Access Server role.

```

Administrator: Windows PowerShell

PS C:\Users\administrator.SCKO> Install-WindowsFeature RSAT-ADDS

Success Restart Needed Exit Code      Feature Result
-----
True      No      Success      {Remote Server Administration Tools, Activ...}
WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is
automatically updated, turn on Windows Update.

PS C:\Users\administrator.SCKO> Add-WindowsFeature RSAT-ADDS

Success Restart Needed Exit Code      Feature Result
-----
True      No      NoChangeNeeded {}

PS C:\Users\administrator.SCKO> Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features
, RPC-over-HTTP-proxy, RSAT-Clustering, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-A
uth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-H
ttp-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, W
eb-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Wind
ows-Identity-Foundation

Success Restart Needed Exit Code      Feature Result
-----
True      Yes      SuccessRest... {Application Server, HTTP Activation, .NET...}
WARNING: You must restart this server to finish the installation process.
WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is
automatically updated, turn on Windows Update.

PS C:\Users\administrator.SCKO>
  
```

Figure 10: PowerShell command line 2

- D. Download and Install the Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit software

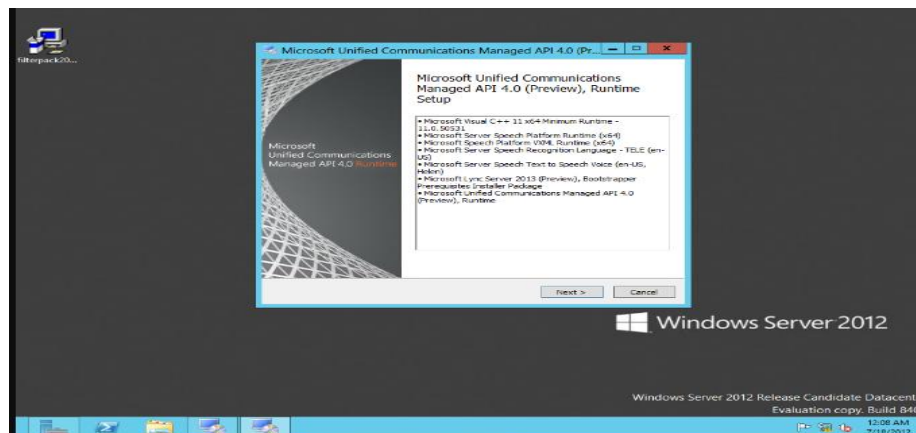


Figure 11: UCM

- E. For Exchange Server 2013 preview, Microsoft Visual C++ 11 beta redistributable (x64) component should be removed from the system.

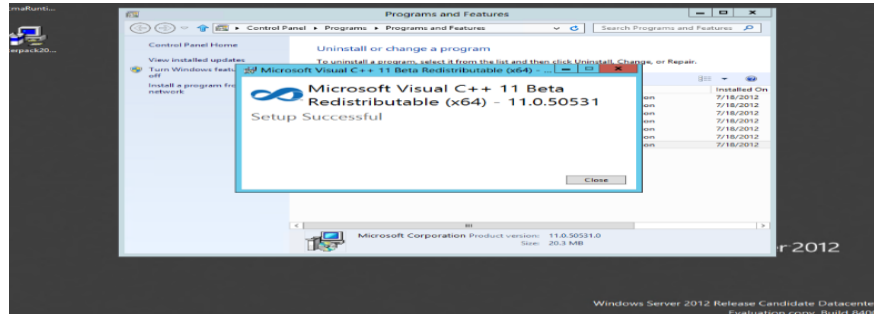


Figure 12: Visual C++

- F. Uninstall Visual C++ 11 Beta Redistributable (x64) – 11.0.50531
- G. Uninstall the Microsoft Visual C++ 11 Beta setup,
- H. Download and Install the Microsoft Office 2010 Filter Pack 64 bit software.
- I. Download and Install the Microsoft Office 2010 Filter Pack SP1 64 bit.

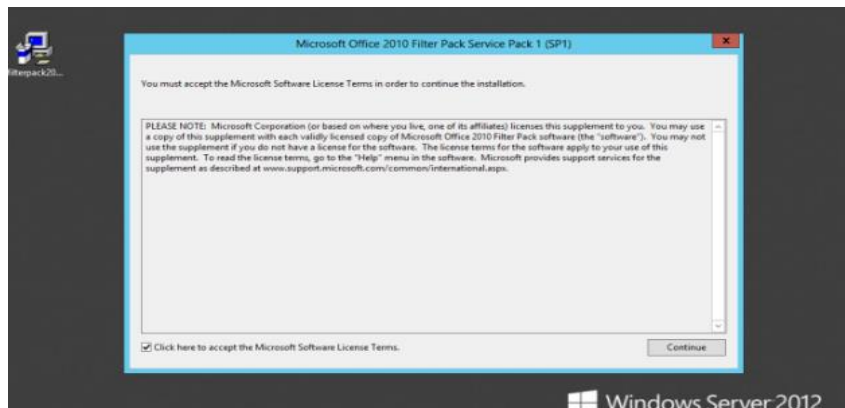


Figure 13: 2010 Filter pack

J. Prepare Active Directory and domains.

- To execute the commands, the commands should be run using the Schema Admins group and the Enterprise Admins group membership
- `setup /PrepareSchema /IAcceptExchangeServerLicenseTerms`
- `setup /PrepareAD /OrganizationName: /IAcceptExchangeServerLicenseTerms`

```
C:\Users\administrator.SCK0\Desktop\Exch>setup /PrepareSchema /IAcceptExchangeServerLicenseTerms

Welcome to Microsoft Exchange Server 2013 Preview Unattended Setup
Copying Files...

Performing Microsoft Exchange Server Prerequisite Check
    Prerequisite Analysis                                COMPLETED
Configuring Microsoft Exchange Server
    Extending Active Directory schema                    COMPLETED

The Exchange Server setup operation completed successfully.
C:\Users\administrator.SCK0\Desktop\Exch>
```

Figure 14: Schema extend

K. Install Exchange Server 2013

Installation wizard of Microsoft exchange server will appear and Installation progress must be followed step by step.



Figure 15: Installation

5.9 INTERNAL AND EXTERNAL URL CREATION

- ✓ First we go to Forward DNS lookup zone and we create domain name for our external and internal URL.
- ✓ We created domain name called “mail” and we concatenated to our main domain controller.

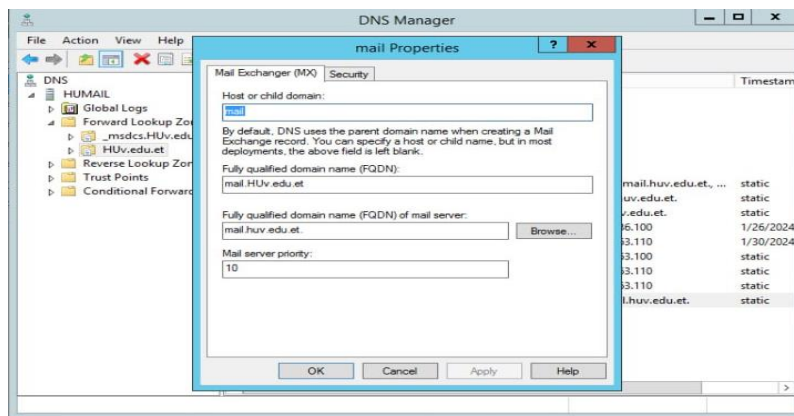


Figure 17: DNS Manager

- ✓ Now go to exchange server’s web ecp outlook and login as Administrator And then change the External and Internal URL to the domain we created accordingly for both ecp and owa.

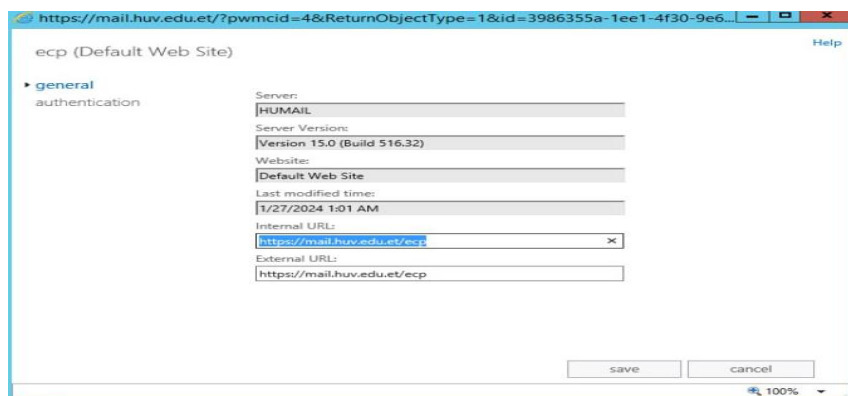


Figure 18: Ecp server wizard

- Internal URL: is used to access the Exchange services from within the internal network.
- External URL :is used to access the services from outside the network
- I.e, Internal URL: <https://mail.huv.edu.et/ecp>
<https://mail.huv.edu.et/owa>
- External URL:<https://mail.huv.edu.et/ecp>
<https://mail.huv.edu.et/owa>
- Note: Internal URL and External URL may not be always the same.

5.10 Client Access

5.10.1Mailbox user Account creation

- ✓ Login as administrator to the ecp and then we created new user mailbox accordingly.

Figure 19: New user mailbox

- ✓ Then we logged in to the OWA with the account we created.
- ✓ You can send and receive mails.

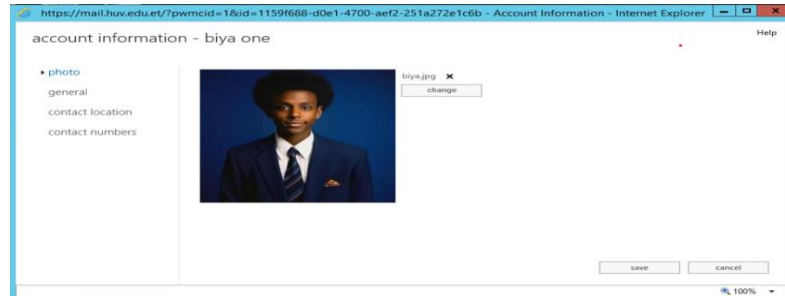


Figure 20: Account information

- ✓ Also so many things can be done in Microsoft exchange server such as Calendaring, resource creation and so many.

5.11 SSL Certificate

- ✓ An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection.
- ✓ SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol.
- ✓ It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications.
- ✓ SSL is the predecessor to the modern TLS encryption used today.

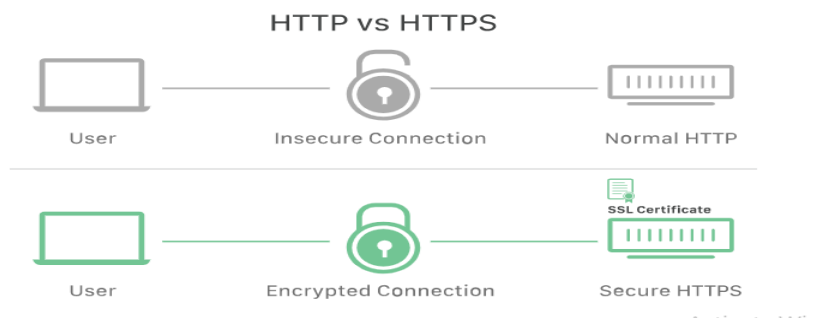


Figure 21: SSL

- ✓ In Exchange 2013 self-signed certificate are created when we install Exchange server.

But these self-signed certificate are not trusted by other system.

- ✓ We requested new certificate from Certificate authority.
- ✓ Then gave the name for the certificate
- ✓ Then we specified the domain that we wanted to include
- ✓ we specified information about our organization
- ✓ We sent certificate request encryption script to certificate authority to get the certificate based on our requirement.
- ✓ To access enterprise root-certification authority web page we used the following url
<http://humail.huv.edu.et/certsrv>

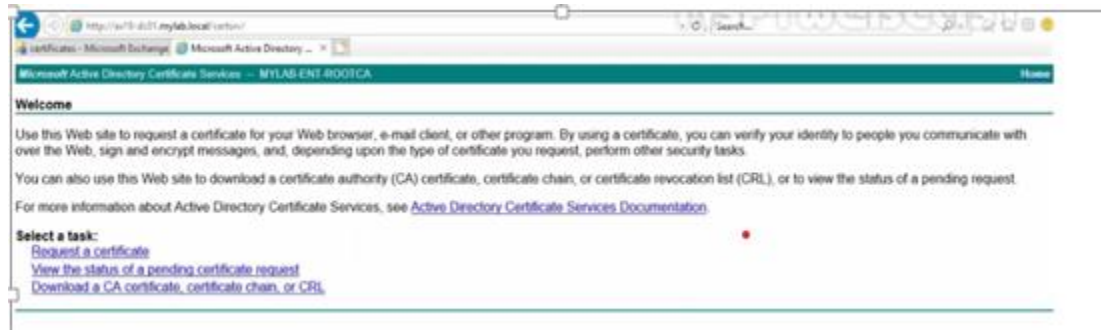


Figure 22: certificate request

- ✓ Based on our request our certificate has issued

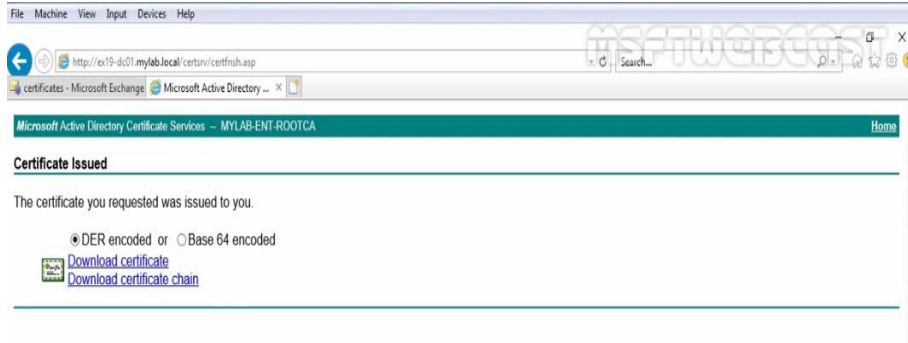


Figure 23: certificate service

- ✓ We downloaded our certificate and bound it to our mail server.
- ✓ Finally we configured the following protocols:

POP3: Is used to receive emails from a remote server and send to a local client

IMAP :(Internet Message Access Protocol version) Protocol for receiving email that allows users to access their email from different devices.

IIS: plays a crucial role in the functioning of Exchange's web-based services

SMTP: is a protocol used to send emails on the internet. In the context of Microsoft Exchange Server, SMTP plays a crucial role in the delivery of email messages.

5.12 Customization

- ❑ We can customize the Outlook on the web (formerly known as Outlook Web App) sign-in, language selection, and error pages in Exchange Server.
- ❑ Backup the default Outlook on the web files before you make any changes. Create a back-up copy of your customized files so you can reapply them after a reinstallation or upgrade of the Exchange server.
- ❑ Customize the color of the Outlook on the web sign-in page: Use Notepad to open the file %ExchangeInstallPath%FrontEnd\HttpProxy\owa\auththemes\resources\log themes\resources\logon.css

Customize the title and Icon on Browser of the Outlook on the web sign-in page:

Use Notepad to open the file

%ExchangeInstallPath%FrontEnd\HttpProxy\owa\auth\<ExchangeVersion>\themes\resources\logon.apax

- ❑ Customize the logo file by replacing image in resource files.

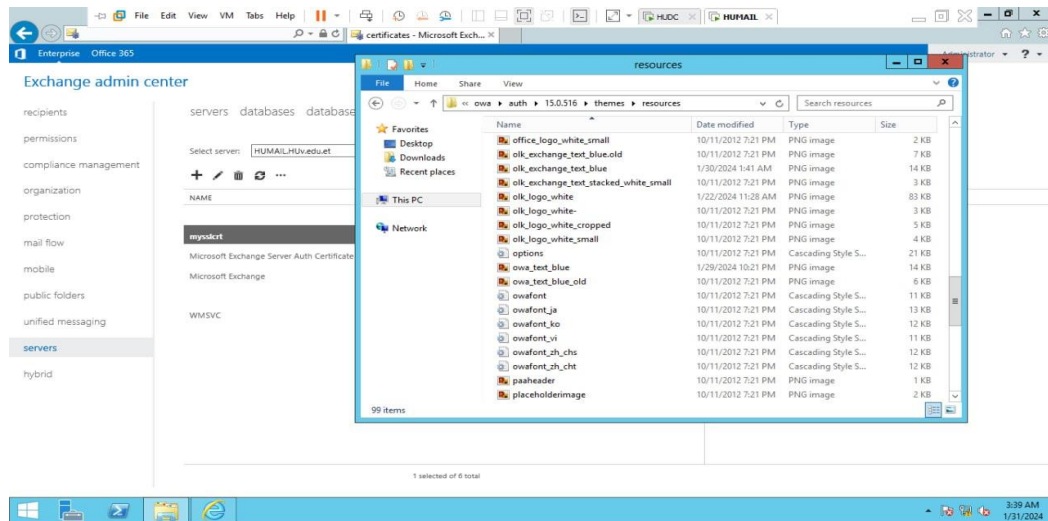


Figure 24: File source

5.13 Result and drawback

5.13.1 Result

- ✓ The client successfully accessed the exchange Admin center and outlook web access page.
- ✓ The client successfully booked for resources and the feedback automatically given by the server.
- ✓ Client successfully sent and received a mail.

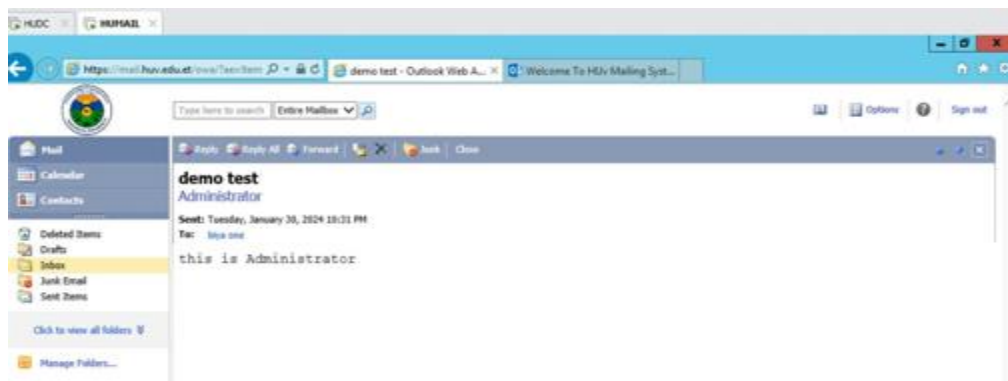


Figure 25: Client Inbox

- ✓ Outlook page successfully customized

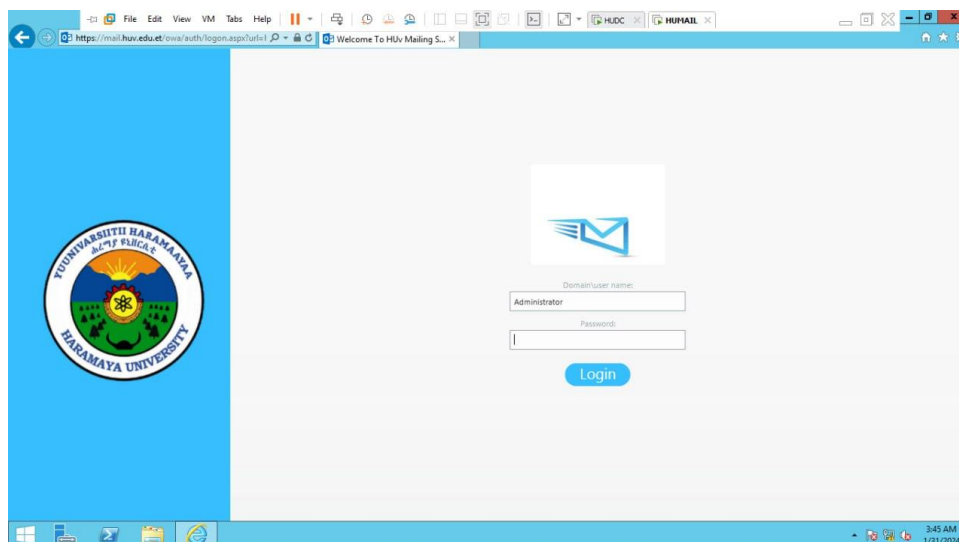


Figure 26: OWA

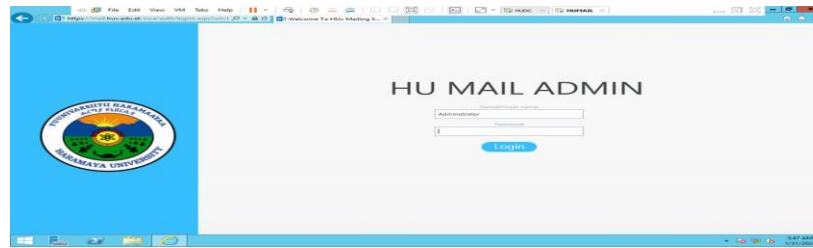


Figure 27: EAC

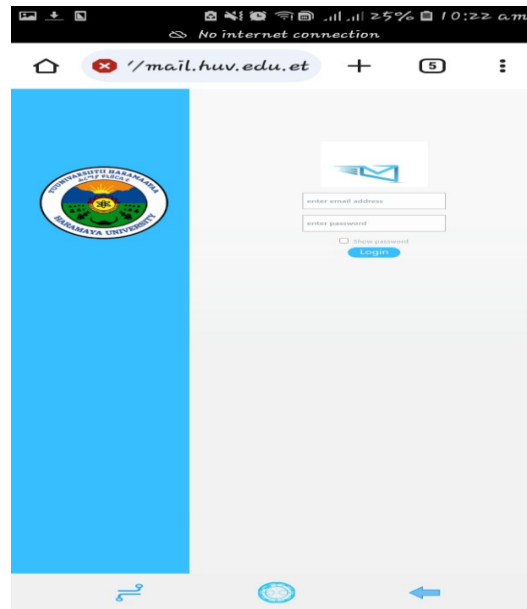


Figure 28: OWA Mobile access

5.13.2 Drawback

Hardware drawback we were unable to create more user account database (lack of storage).

The client were accessing only in local network due to lack of public IP address.

5.14 Conclusion

The implications of this work is about the successful implementation of exchange server for Haramaya University. Through the implementation process we were able to done different tasks like client access which plays a crucial role in facilitating user interaction with their mailboxes. It acts as a central hub for various functions, essentially serving as the "front door" for accessing email services. And create user mail box. Also we issued certificate that ensure secure and trustworthy communication using Secure Sockets Layer (SSL). This encryption protects sensitive information like usernames, passwords, and email content from being intercepted during communication. In addition to this we were able to customize to fit the specific needs of our organization. We had successfully modified the user interface like Outlook Web Access (OWA) , the OWA logo, colour schemes, and login page appearance. Also we had modified the interface of Exchange Admin Centre (EAC) which offers a comprehensive and user-friendly interface for administrators to manage various aspects of the server.

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

The internship program has paramount importance for us to get both theoretical and practical skills, starting from finding the hosting company, working inside, and observing the ways in which the work flows and how the job is done. It helped us know what the working environment looks like since we will be graduates after our internship. We know that the way we communicate with others ultimately determines the quality of our lives, and an internship is crucial to developing this skill. Therefore, this internship program gave us a chance not only to work with INSA but also to work with the outside world.

We have developed important work ethics like punctuality, honesty, working with others in harmony, respecting the working environment, responsibility, and transparency. We also grasped some leadership skills from INSA workers, and now we have at least the know-how to handle it in the future of our life. In this internship program, we have had the chance to put what we have learned in theory into practice. Finally, from this internship period, in addition to formal academic knowledge, we were able to get general experience in every other aspect of life; this experience was unforgettable, and we believe it shaped our personality and behaviour by helping us to be optimistic in our future tasks, to be stronger to overcome challenges and be successful, and to develop critical thinking ability and problem-solving skills.

6.2 Recommendation

- We recommend to use Microsoft Exchange server 2019 for our Mail exchange project since it has some additional roles and futures like Performance and Accuracy, Storage Replica, Software-defined Networking.
- We recommend to the company of our network project to use lists of the device with this model and amount write below .it is better for designing network infrastructure for AB Company.

Device	Model	Amount	Why we used
Router	4331	12	<ul style="list-style-type: none"> • Delivers highly secure data, voice, video and application service. • Fully integrated power distribution.
Layer two switch	2960	16	<ul style="list-style-type: none"> • Scalable and secure ease of use functionality • Software updates at no additional cost
Layer three switch	3650	8	the foundation for full convergence between wired and wireless on a single platform
Server	—	1	
Cable	—	—	

Table 8. List of recommended device

6.2.1 Recombination for the company

The company should help apparent students with pocket money since most students are far from their family during the internship program.

The company should provide some hardware components for intern students (i.e. RAM, SSD) since most tasks require good computing capabilities and huge hardware requirements.

Reference

Websites:

<https://www.cybersecurityintelligence.com/information-network-security-agency-insa-3379.htm>

<https://cybilportal.org/stage64/actors/ethiopia-information-network-security-agency->

[insahttps://www.arcgis.com/home/group.html?id=47f768d17a6642068c139593b6da2f16#ove](https://www.arcgis.com/home/group.html?id=47f768d17a6642068c139593b6da2f16#ove)

P Boger, CCNA Exploration Course Booklet, Basic Configuration, Cisco networking Academy,

February 2018, accessed on June 2019: online. Available

<https://www.cisco.com>training center>

<https://www.cisco.com>training center, switching, router>

<http://searchnetworkingtechtargt.com,utp categories>

<http://searchnetworkingtechtargt.com, cabling, wiring cable>

www.arubanetwork.com, dhcp pool, ip address, network ID, host ID

<http://avinetworks.com, Subnet mask, classes>

<https://www.cisco.com>training center>

<http://www.cabrillo.edu/~rgraziani>

<https://techdifferences.com>

<http://www.learnabhi.com>

<http://www.sciencedirect.com>

<https://judeperera.wordpress.com/2012/07/19/step-bystep-guide-for-installing-exchange-server-2013-preview/>

Appendix

A. vlan configuration

```
SW(config)# inter range fa 0/1-2
SW(config-if-range)# switchport-mode trunk
Sw(config) vlan 10
SW(config-vlan)# name " "
SW(config)# int range fa0/1-24
SW(config-if-range)#switchport mode access
SW(config-if-range)# switchport access vlan 10
```

B. Trunk port configuration

```
MLSW(config)# int range gig1/0/2-6
MLSW(config-if-range) switchport mode trunk
```

C. Ether channel

```
MLSW(config)#int range gig 1/0/1-3
MLSW(config-if-range)#channel-group 1 mode active
MLSW(config-if-range)interface port-channel 1
MLSW(config-if)#switch port mode trunk
```

D. OSPF configuration

```
MLSW(config)#router ospf 1
MLSW(config-router)#router-id 2.1.2.1
MLSW(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

Active Directory Domain Controller

	Operating System	Windows Server 2012
	Forest Functional Level	Windows Server 2012
	Domain Functional Level	Windows Server 2012

Exchange Server 2013

	Operating System	Windows Server 2012
		Mailbox Server Role
	Associated Server Roles	Client Access Server Role