INTERNAL VERIFICATION – ASSIGNMENT BRIEF		
Programme Title:	HND in Computing	
Assessor Name:	Mr. Anjula Kalum	
Internal Verifier Name:		
Unit or Component Number and Title:	Unit 02 - Networking	
Assignment title:	LAN Design & Implementation for Alliance Health	
Assessment criteria targeted by this assignment brief:	LO1, LO2, LO3, LO4	
Is this an Authorised Assignment Brief published by Pearson? If so, has it been amended by the Assessor in any way? Please give details. *(If using the Authorised Assignment Brief 'off the shelf' with no amendments, please answer the question marked * in the checklist only)*	N/A	
Has this assignment been submitted to the Assignment Checking Service? *(If Yes, please keep a copy of the ACS feedback with this form)*	**Yes**	**No**
		√

INTERNAL VERIFIER CHECKLIST	Y/N
Are the programme and unit details accurate?	**Y**
*Are clear deadlines for assessment given?	**TBC**
Is the time frame of an appropriate duration?	**Y**
Is there a suitable vocational scenario or context?	**Y**

Are the assessment criteria to be addressed stated accurately?			**Y**	
Does each task show which criteria are being addressed?			**Y**	
Do the tasks meet the assessment requirements of the unit/s?			**Y**	
Is it clear what evidence the learner needs to generate?			**Y**	
Is it likely to generate evidence that is valid and sufficient?			**Y**	
Overall, is the Assignment fit for purpose?	**Yes**	√	**No**	
**If 'No' is recorded the Internal Verifier must recommend actions detailing the issues to be addressed. The Assessor and the Internal Verifier must then confirm that the action has been undertaken and that the Assignment Brief is authorised for use before being issued to learners.*				

Action required: *(If none then please state n/a)*	Target Date for Completion	Date Action Completed

General Comments (if appropriate)

Assignment Brief Authorised for Use:			
Internal Verifier signature		**Date**	
Assessor signature		**Date**	
Lead Internal Verifier signature (if appropriate)	oshada@esoft.lk	**Date**	2022/06/13

Higher Nationals

Internal verification of assessment decisions – BTEC (RQF)

INTERNAL VERIFICATION – ASSESSMENT DECISIONS				
Programme title	BTEC Higher National Diploma in Computing			
Assessor	Mr. Anjula Kalum	**Internal Verifier**		
Unit(s)	**Unit 02: Networking**			
Assignment title	LAN Design & Implementation for Alliance Health			
Student's name	Liyanagamage Hasara Sesadi			
List which assessment criteria the Assessor has awarded.	**Pass**	**Merit**	**Distinction**	
INTERNAL VERIFIER CHECKLIST				
Do the assessment criteria awarded match those shown in the assignment brief?	Y/N			
Is the Pass/Merit/Distinction grade awarded justified by the assessor's comments on the student work?	Y/N			
Has the work been assessed accurately?	Y/N			
Is the feedback to the student: Give details: • Constructive? • Linked to relevant assessment criteria? • Identifying opportunities for improved performance? • Agreeing actions?	 Y/N Y/N Y/N Y/N			
Does the assessment decision need amending?	Y/N			
Assessor signature		**Date**		
Internal Verifier signature		**Date**		
Programme Leader signature (if required)		**Date**		

Confirm action completed			
Remedial action taken Give details:			
Assessor signature		**Date**	

Internal Verifier signature		**Date**	
Programme Leader signature (if required)		**Date**	

Higher Nationals - Summative Assignment Feedback Form

Student Name/ID	Liyanagamage Hasara Sesadi/ E211307		
Unit Title	**Unit 02: Networking**		
Assignment Number	**1**	**Assessor**	Mr. Anjula Kalum
Submission Date	08/12/2024	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	

Assessor Feedback:

LO1 Examine networking principles and their protocols.

Pass, Merit & Distinction **P1** ☐ **P2** ☐ M1 ☐ **D1** ☐

Descripts

LO2 Explain networking devices and operations.

Pass, Merit & Distinction **P3** ☐ **P4** ☐ **M2** ☐

Descripts

LO3 Design efficient networked systems.

Pass, Merit & Distinction **P5** ☐ **P6** ☐ **M3** ☐ **D2** ☐

Descripts

LO4 Implement and diagnose networked systems.

Pass, Merit & Distinction **P7** ☐ **P8** ☐ **M4** ☐

Descripts

Grade:	**Assessor Signature:**	**Date:**
Resubmission Feedback:		
Grade:	**Assessor Signature:**	**Date:**

Internal Verifier's Comments:
Signature & Date:

* Please note that grade decisions are provisional. They are only confirmed once internal and external moderation has taken place and grades decisions have been agreed at the assessment board.

Assignment Feedback

Formative Feedback: Assessor to Student
Action Plan
Summative feedback

Feedback: Student to Assessor			
Assessor signature		**Date**	
Student signature	E211307@esoft.academy	**Date**	08/12/2024

Pearson Higher Nationals in

Computing

Unit 02: Networking

Assignment 01

General Guidelines

1. A Cover page or title page – You should always attach a title page to your assignment. Use previous page as your cover sheet and make sure all the details are accurately filled.
2. Attach this brief as the first section of your assignment.
3. All the assignments should be prepared using a word processing software.
4. All the assignments should be printed on A4 sized papers. Use single side printing.
5. Allow 1" for top, bottom , right margins and 1.25" for the left margin of each page.

Word Processing Rules

1. The font size should be **12** point, and should be in the style of **Time New Roman**.
2. **Use 1.5 line spacing**. Left justify all paragraphs.
3. Ensure that all the headings are consistent in terms of the font size and font style.
4. Use **footer function in the word processor to insert Your Name, Subject, Assignment No, and Page Number on each pag**e. This is useful if individual sheets become detached for any reason.
5. Use word processing application spell check and grammar check function to help editing your assignment.

Important Points:

1. It is strictly prohibited to use textboxes to add texts in the assignments, except for the compulsory information. eg: Figures, tables of comparison etc. Adding text boxes in the body except for the before mentioned compulsory information will result in rejection of your work.
2. Avoid using page borders in your assignment body.
3. Carefully check the hand in date and the instructions given in the assignment. Late submissions will not be accepted.
4. Ensure that you give yourself enough time to complete the assignment by the due date.
5. Excuses of any nature will not be accepted for failure to hand in the work on time.
6. You must take responsibility for managing your own time effectively.
7. If you are unable to hand in your assignment on time and have valid reasons such as illness, you may apply (in writing) for an extension.
8. Failure to achieve at least PASS criteria will result in a REFERRAL grade .
9. Non-submission of work without valid reasons will lead to an automatic RE FERRAL. You will then be asked to complete an alternative assignment.
10. If you use other people's work or ideas in your assignment, reference them properly using HARVARD referencing system to avoid plagiarism. You have to provide both in-text citation and a reference list.
11. If you are proven to be guilty of plagiarism or any academic misconduct, your grade could be reduced to A REFERRAL or at worst you could be expelled from the course

Student Declaration

I hereby, declare that I know what plagiarism entails, namely to use another's work and to present it as my own without attributing the sources in the correct form. I further understand what it means to copy another's work.

1. I know that plagiarism is a punishable offence because it constitutes theft.
2. I understand the plagiarism and copying policy of Pearson UK.
3. I know what the consequences will be if I plagiarise or copy another's work in any of the assignments for this program.
4. I declare therefore that all work presented by me for every aspect of my program, will be my own, and where I have made use of another's work, I will attribute the source in the correct way.
5. I acknowledge that the attachment of this document signed or not, constitutes a binding agreement between myself and Pearson, UK.
6. I understand that my assignment will not be considered as submitted if this document is not attached to the assignment.

E211307@esoft.academy

Student's Signature:
(*Provide E-mail ID*)

Date: 08/12/2024
(*Provide Submission Date*)

Higher National Diploma in Computing

Assignment Brief

Student Name /ID Number	Liyanagamage Hasara Sesadi/E201307
Unit Number and Title	**Unit 2: Networking**
Academic Year	2022/23
Unit Tutor	Mr. Anjula Kalum
Assignment Title	**LAN Design & Implementation for Alliance Health**
Issue Date	27/02/2024
Submission Date	08/12/2024
IV Name & Date	

Submission format
The submission should be in the form of an individual report written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using Harvard referencing system. Please also provide an end list of references using the Harvard referencing system. **The recommended word count is 3,000–3,500 words for the report excluding annexures, although you will not be penalised for exceeding the total word limit.**

	Unit Learning Outcomes:
	LO1 Examine networking principles and their protocols. **LO2** Explain networking devices and operations. **LO3** Design efficient networked systems.

	LO4 Implement and diagnose networked systems.
	Assignment Brief and Guidance:

Scenario

Alliance Health is a technology-enabled solutions company that optimizes the revenue cycle of the US healthcare industry where its global delivery center is located in Colombo. The company is planning to expand their business operations with their latest branch at Matara and wants it to be one of the state-of-the-art companies in Matara with the latest facilities.

Assume you have been appointed as the new network analyst of Alliance Health to plan, design and restructure the existing network. Prepare a network architectural design and implement it with your suggestions and recommendations to meet the company requirements.

The floor plan of the head office in Colombo is as follows:

Floor 1:

- Reception area
- Sales & Marketing Department (10 employees)
- Customer Services Area – with Wi-Fi facilities

Floor 2:

- Administration Department (30 Employees)
- HR Department (20 employees)
- Accounting & Finance Department (15 employees)
- Audit Department (5 employees)
- Business Development Department (5 employees)

Floor 3

- Video conferencing room
- IT Department (60 employees)
- The Server Room

The floor plan of the branch in Matara is as follows:

Floor 1:

- Reception area
- Customer Services Area– with Wi-Fi facilities

Floor 2:

- Administration Department (10 Employees)
- HR Department (7 employees)
- Accounting & Finance Department (8 employees)
- IT Department (50 employees)

Following requirements are given by the Management.

- All the departments **must be separated** with **unique subnet**.
- **The conferencing room of the head office and Customer Services Areas** of each branch are to be **equipped with Wi-Fi connections**.
- **Connectivity between two branches** (Head Office and Matara) would allow the intra branch connectivity between departments. (Use of VPN is not compulsory)
- **The necessary IP address classes and ranges** must be decided by the network designer and should be used for all the departments **except the server room**.
- **Number of servers required for the Server room** need to be decided by the Network designer and should be assigned with **10.254.10.0/24** subnet. (Uses **static IPs**)

- **Sales and Marketing** Team also needs to access Network resources **using WIFI** connectivity.

(Note: Clearly state your assumptions. You are allowed to design the network according to your assumptions, but main requirements should not be violated)

Activity 01

- Discuss the benefits and constraints of different network system types that can be implemented in the Matara branch and the main IEEE Ethernet standards that can be used in above LAN and WLAN design.

- Discuss the importance and impact of network topologies and assess the main network protocol suites that are used in network design using examples. Recommend suitable network topology and network protocols for above scenario and evaluate with valid points how the recommended topology demonstrates the efficient utilization of the networking system of Matara branch.

Activity 02

- Discuss the operating principles of network devices (Ex: Router, Switch, Etc.) and server types that can be used for above scenario while exploring different servers that are available in today's market with their specifications. Recommend server/servers for the above scenario and justify your selection with valid points.

- Discuss the inter-dependence of workstation hardware and networking software and provide examples for networking software that can be used in above network design.

Activity 03

- Prepare a written network design plan to meet the above-mentioned user requirements including a blueprint drawn using a modeling tool (Ex: Microsoft Visio, EdrawMax) .Test and evaluate the proposed design by analyzing user feedback with the aim of optimizing your design and improving efficiency.

(Support your answer by providing the VLAN and IP subnetting scheme for the above scenario and the list of devices, network components and software used to design the network for above scenario and while justifying your selections.)

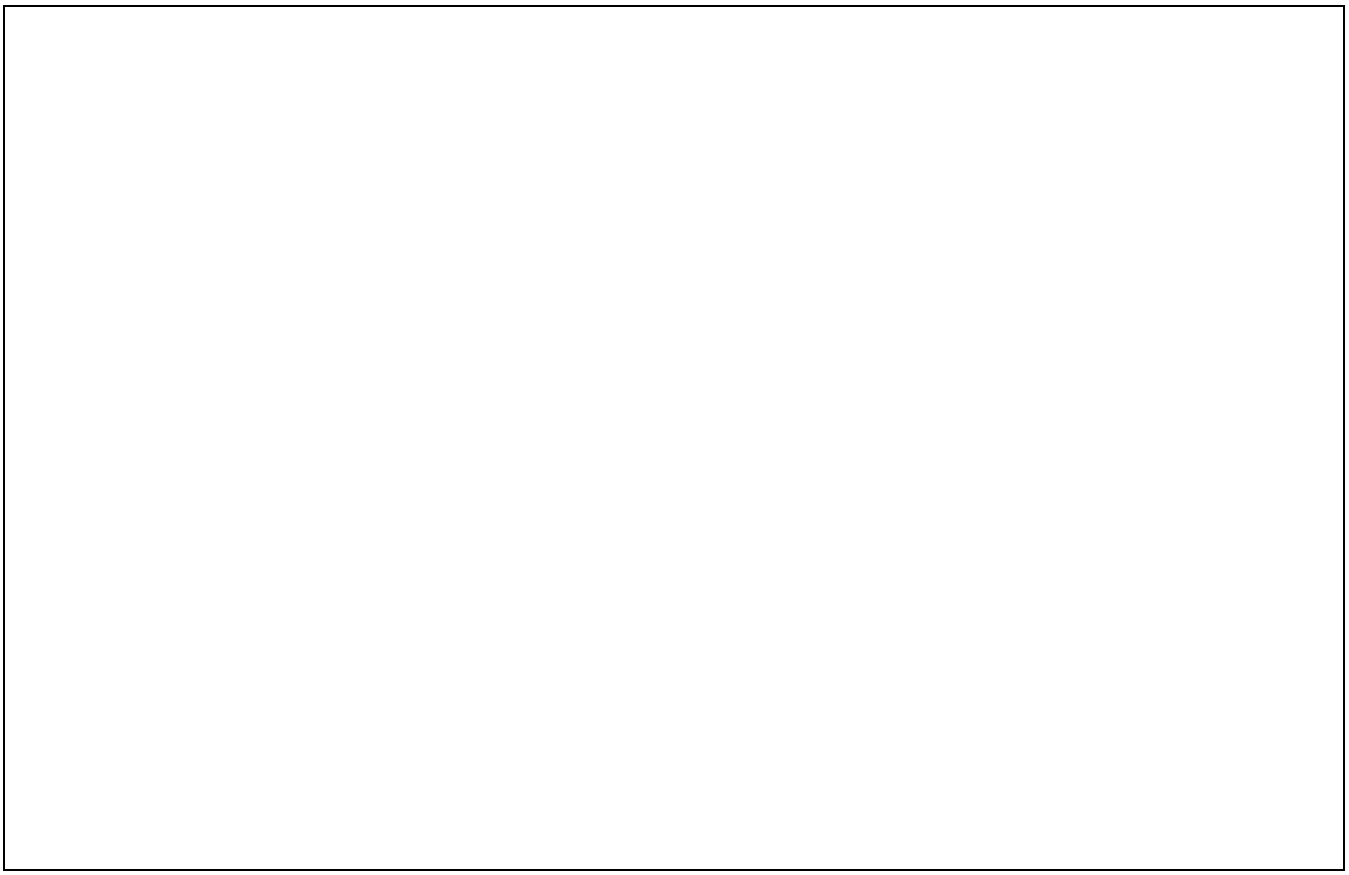
- Install and configure Network services, devices and applications (Ex: VLAN,WiFi, DNS,Proxy, Web, Etc.) according to the proposed design to accomplish the user requirements and design a detailed Maintenance schedule for above Network.

***Note: - Screen shots of Configuration scripts should be presented.**

Activity 04

- Implement a networked system based on your prepared design with valid evidences.

- Develop test cases and conduct verification (Ex: Ping, extended ping, trace route, telnet, SSH, etc.) to test the above Network and analyse the test results against the expected results. Recommend potential future enhancements for the networked system with valid justifications and critically reflect on the implemented network, including the plan, design, configurations, tests and the decisions made to enhance the system.



Grading Rubric

Grading Criteria	Achieved	Feedback
LO1 : Examine networking principles and their protocols.		
P1 Discuss the benefits and constraints of different network types and standards.		
P2 Explain the impact of network topology, communication and bandwidth requirements.		
M1 Assess common networking principles and how protocols enable the effectiveness of networked systems.		
LO2 : Explain networking devices and operations		
P3		

Discuss the operating principles of networking devices and server types.		
P4 Discuss the interdependence of workstation hardware and relevant networking software		
M2 Explore a range of server types and justify the selection of a server for a given scenario, regarding cost and performance optimisation		
LO 1 & LO2		
D1 Evaluate the topology protocol selected for a given scenario and how it demonstrates the efficient utilisation of a networking system.		
LO3 : Design efficient networked systems		
P5 Design a networked system to meet a given specification.		
P6 Design a maintenance schedule to support the networked system.		

M3 Analyse user feedback on your designs with the aim of optimising your design and improving efficiency.		
D2 Critically reflect on the implemented network, including the design and decisions made to enhance the system.		
LO4 : Implement and diagnose networked systems		
P7 Implement a networked system based on a prepared design.		
P8 Document and analyze test results against expected results.		
M4 Recommend potential enhancements for the networked systems.		

D2 Critically reflect on the implemented network, including the design and decisions made to enhance the system.		

LAN Design & Implementation for Alliance Health

Figure 1 Cover page

Acknowledgment

First of all, I would like to express my thanks to our preacher Mr. Anjula Kalum who advised me to succeed in this assignment. He gave us a lot of support and encouragement to succeed in this assignment. I really got a lot of support from him to make this project successful and my networking knowledge also increased because of him.

Finally, I would like to thank ESOFT Metro Campus for providing the resources.

And due to the support, patience and encouragement of my parents, I was able to complete this assignment successfully.

Also, I would like to thank all my friends who have given me a lot of support.

Thank you all for your contributions.

Thank you!

Hasara Sesadi

Table of Contents

List Of Figurer

List of Tables

Introduction

This assignment shows the network diagrams and configurations of the Matara branch of the alien's health company.

LO1: Examine networking principles and their protocols.

P1 Discuss the benefits and constraints of different network types and standards.

What is Networking?

- A computer network is a collection of autonomous computer devices interconnected in various ways to exchange information through common conventions called protocols over a shared communication medium. Computers use common communication protocols to communicate with each other over digital interconnects, where information flows seamlessly from one location to another.

Uses of Computer Networks

1. Communicating using email, video.
2. Sharing files.
3. Sharing devices such as printers, scanners.

Network Types

1. LAN
2. WAN
3. MAN (Kapoor, 2022)

LAN (Local Area Network)

A LAN, or local area network, is a busy neighborhood where computers, printers, servers and more - are connected to each other within a relatively small geographical area. Your house, workplace, school, or any other small facility can serve as this region. Like neighbors in a community, devices on a LAN communicate directly with each other at high speeds without having to go through the Internet. This makes it possible to collaborate on projects and share data and resources like printers and Internet connections quickly and effectively.

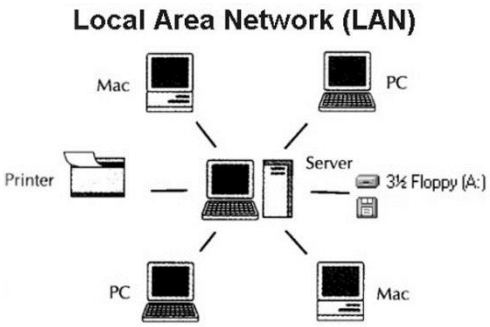


Figure 2 LAN

WAN (Wide Area Network)

WAN or Wide Area Networks is are span large geographic areas like highways connecting distant cities rather than neighboring areas, connecting LANs across cities, countries, or continents. It acts as a global network infrastructure that enables communication between widely dispersed locations. WAN uses various technologies including fiber optics, satellites to transmit data over long distances. They facilitate communication between different offices of an organization, enable Internet access for users around the world, and support services such as video conferencing and cloud computing.

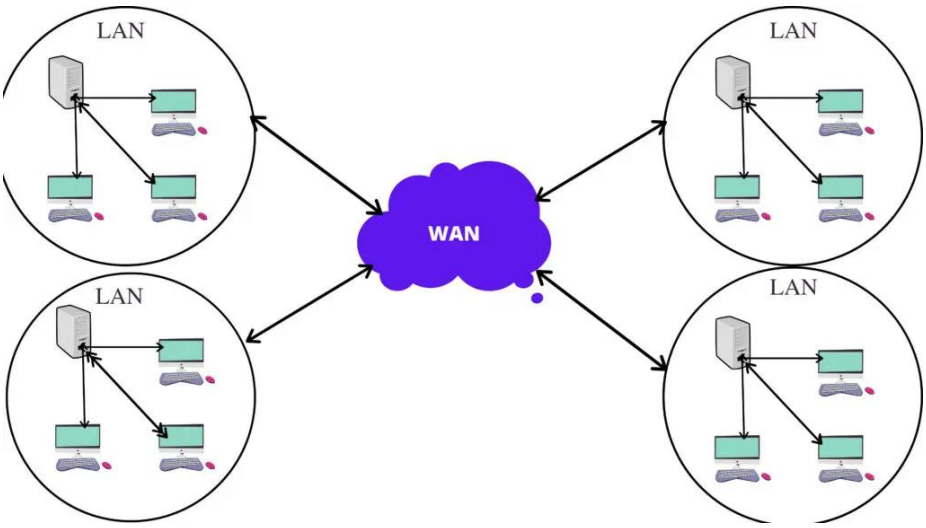


Figure 3 WAN

MAN (Metropolitan Area Network)

MAN, or Metropolitan Area Network are providing internet for a city or urban area. Connects multiple LANs across a relatively large geographic area. It acts as an interconnected network infrastructure that facilitates communication and data exchange within a city or urban region. MANs typically use high-speed fiber optic cables and other networking technologies to connect various local networks, businesses, institutions, and

government offices within the metropolitan area. They enable efficient data transmission, resource sharing and collaboration between institutions spread across the city, supporting services such as internet access, telecommunications and municipal utilities. MANs bridge the gap between LANs and WANs, providing wider coverage than LANs while allowing faster communication over shorter distances than WANs.

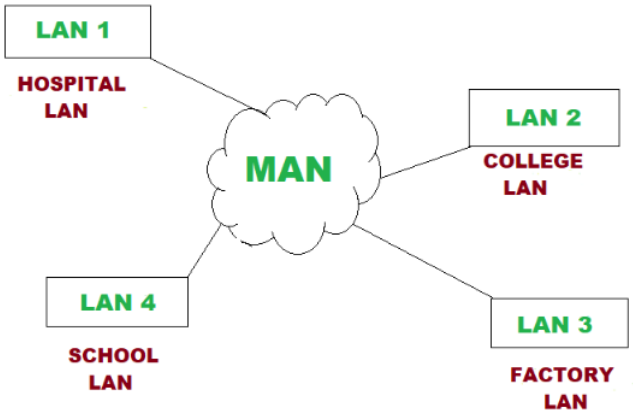


Figure 4 MAN

Peer to Peer System (P2P)

Peer-to-peer systems are computer networks that enable peers to share resources without depending on a central authority, such as processing power and data storage. Imagine a circle of friends where any person may speak with any other friend directly, without the need for a leader or middleman. Similar to this, devices like computers, mobile phones, and Internet of Things gadgets can function as clients and servers in a peer-to-peer network, exchanging data, resources, or processing capacity with one another. Benefits of this model include fault tolerance, scalability and the capacity for the network to continue operating even in the event that certain peers are unavailable. New peers may join the network with ease. P2P networks are commonly employed in decentralized applications, such video streaming, and cryptocurrencies.

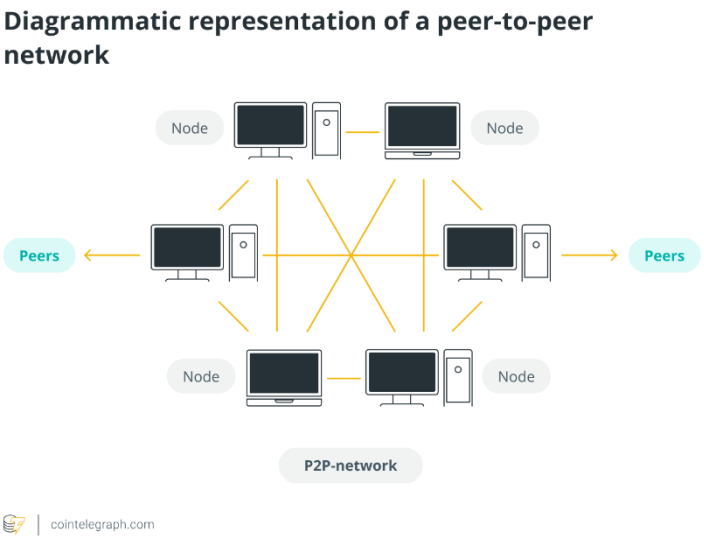


Figure 5 Peer to Peer network

Advantages & Disadvantages of P2P network

Advantages	**Disadvantages**
P2P networks distribute labour and resources across all linked devices in instead of a central server.	P2P networks lack centralized management and monitoring, they are more vulnerable to security concerns including malware infections, illegal access, and data breaches.
P2P networks are readily scalable, meaning they don't need to make major adjustments to the network architecture in order to handle more users or devices.	Depending on the resources and capabilities of individual devices, a P2P network's performance might vary, resulting in inconsistent speed and dependability.
There is redundancy in data storage and services since any device in a peer-to-peer (P2P) network may function as both a client and a server. This lowers the danger of single points of failure.	Since there is no centralized authority to impose rules or monitor network activities, managing and keeping an eye on a P2P network might be trickier than on client-server networks.

Since P2P networks do not require costly central servers or specialized networking equipment, they usually demand a lower initial infrastructure investment.	P2P networks might experience disruptions if important devices are offline or unavailable because they depend on participating devices to offer resources or services.
P2P networks allow devices to join and exit the network with ease without affecting the network's general operation, giving them more connection flexibility.	P2P networks are frequently linked to illicit file sharing and copyright violations, which might present problems legally and for network operators and users.

Table 1 Peer to Peer advantages & disadvantages

Client Server

Devices in client-server network architecture fall into two major groups. Specifically, as servers and clients. Imagine a restaurant where customers (customers) order with a waiter (server), who then delivers food from the kitchen (server) to the customers' tables. Similar to this, in a client-server network, client's computers, mobile phones, or Internet of Things (IoT) devices request resources or services from certain servers, which are strong computers built to carry out particular functions. Accessing files, getting information from databases, and using server-hosted apps are a few examples of these services. After processing these requests, the server gives the clients access to the resources or services they have requested. Client-server networks are appropriate for situations where centralized control and administration are crucial because of the advantages of this centralized approach, which include enhanced security, centralized management, and greater resource usage.

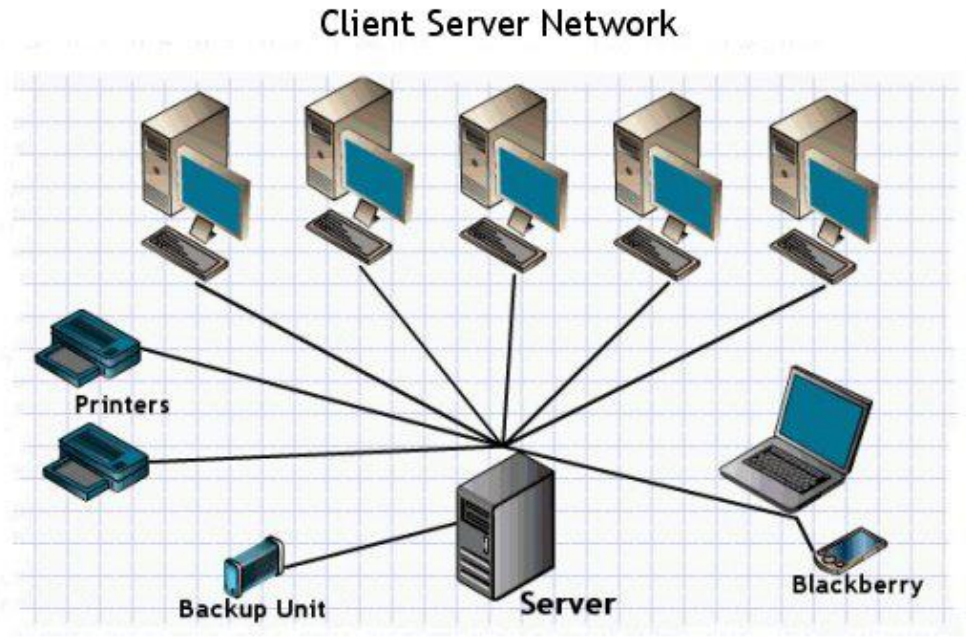


Figure 6 Client sever

Advantages & Disadvantages of Client server network

Advantages	Disadvantages
Client-server networks offer concentrated administration, permitting overseers to handily screen and control network assets, security arrangements, and client access.	Client-server networks are powerless against weak links, as the disappointment of a focal server can disturb admittance to basic assets for every single associated client.
Client-server networks give better security contrasted with shared networks, as delicate information and assets are put away on devoted servers with powerful safety efforts set up. Client-server networks can easily scale up to accommodate growing numbers of users or devices by adding additional servers or upgrading existing infrastructure.	Executing and keeping up with client-server organizations can be exorbitant, as it requires interest in particular server equipment, organizing gear, and gifted IT work force. Client-server networks are more mind boggling to set up and oversee contrasted with shared networks, requiring skill in server organization, network arrangement, and security.

With committed servers taking care of explicit assignments and administrations, client-server networks normally offer better execution and unwavering quality contrasted with shared networks.	Client-server organizations might encounter network bottlenecks, particularly during top utilization periods, as all client demands should be handled by the focal server, prompting potential execution issues.
Client-server networks work with incorporated reinforcement and recuperation systems, guaranteeing information security and debacle recuperation capacities across the organization	Client-server networks rely intensely upon the accessibility and unwavering quality of the focal server, and any issues or personal time with the server can influence the whole organization, making disturbances client efficiency and tasks.

Table 2 Client server network advantages & disadvantages

How network types matter to the scenario.

Each network type has its own advantages and disadvantages, and the choice of network architecture depends on factors such as the organization's size, geographic spread, budget, security requirements, and scalability needs. By understanding the characteristics of each network type, network designers can choose the most suitable architecture to meet the specific requirements of Alliance Health's Matara branch and ensure efficient communication and resource sharing among departments.

Extranet

An extranet is a controlled private network that allows organizations to securely share information, resources, and services with external parties such as customers, suppliers, partners, or vendors. Its capabilities as an expansion of an association's intranet, giving restricted admittance to explicit approved clients beyond the association's inward organization. Extranets ordinarily use encryption and verification instruments to guarantee secure correspondence and access control. They empower associations to team up more actually with outside partners, smooth out business processes, and further develop correspondence and data sharing while at the same time keeping up with secrecy and security. Instances of extranet utilization incorporate imparting item data to providers, giving client assistance entrances, or working with coordinated effort on joint activities with accomplices.

Intranet

An intranet is a private network within an organization that uses internet technologies to securely share information, resources, and services among its employees, departments, or branches. Consider it a confidential variant of the web that is open just to approved clients inside the association. Intranets typically include web-based applications, file sharing systems, communication tools, and other collaborative platforms that facilitate internal communication, document sharing, and workflow automation. They furnish representatives with incorporated admittance to organization approaches, methods, reports, and other important data, assisting with smoothing out business tasks, further develop efficiency, and encourage joint effort among colleagues. Intranets are frequently safeguarded by safety efforts like firewalls, encryption, and access controls to guarantee the privacy, trustworthiness, and accessibility of delicate corporate information.

VPN

What is the VPN?

- The term VPN represents Virtual Private Network. With the use of this technology, users may access private networks remotely just like they would if they were physically there. The connection is created securely and encrypted across the internet.

- To put it another way, a VPN protects all data that goes through it and acts as a secure tunnel between your device and the internet. Your online activities, including sending emails, accessing sensitive information, and web browsing the internet, will be safe and secret from hackers and other unauthorized parties to its encryption. VPN is used in three ways. That is,

1. Site to Site VPN
2. Remote Access VPN
3. Mobile VPN

Site to Site

Site-to-Site VPN is a type of VPN connection that can be created a secure and encrypted connection between two or more geographically networks over the Internet. Each site in a site-to-site VPN configuration usually contains a local area network (LAN) with several devices, including computers, servers, and other network resources. These distinct LANs may safely communicate with one another as though they were a single physical network to the VPN connection.

Remote Access VPN

Remote Access VPN, otherwise called a Virtual Confidential Organization, is an innovation that empowers individual clients connect to from a distant area over the web safely. It permits clients to get to assets, applications, and administrations that are ordinarily accessible just inside the bounds of the association's inward organization, from anyplace with a web association.

Mobile VPN

With the usage of a mobile virtual private network, or mobile VPN, users may safely access a private network from their smartphones or tablets whether they are online via public Wi-Fi hotspots or cellular networks.

How VPN matter to the scenario.

In the context of the Alliance Health scenario, VPNs can be used to establish secure connections between the head office in Colombo and the branch in Matara, allowing employees at both locations to access shared resources and collaborate securely over the internet. VPN technology can help ensure the confidentiality and integrity of sensitive healthcare data transmitted between the two locations, while also providing flexibility and convenience for remote workers accessing the network from outside the office premises.

Network Standard

What is a network standard?

- A network standard is a set of rules, protocols that define how devices communicate and exchange data within a network These principles guarantee interoperability and similarity between various organization gadgets and frameworks. One of the fundamental systems administration norms is the IEEE (Institute of Electrical and Electronics Engineers) Ethernet standard, which oversees the physical and information interface layers of the OSI (Open Systems Interconnection) model.

Ethernet

Ethernet is a widely used networking technology that enables devices to connect and communicate within a local area network (LAN). The main IEEE Ethernet standards that can be used in the LAN and WLAN (Wireless LAN) design for Alliance Health's Matara branch include: (Gaurav., 2022)

- IEEE 802.3 Ethernet (CSMA/CD): This is the first Ethernet standard that characterizes the physical and data link layers of the OSI model. It determines the qualities of the Ethernet links, connectors, and flagging techniques utilized for wired correspondence inside the LAN. This Ethernet is divided into three parts. That is,
    1. Ethernet - The original standard, supports data rates up to 10 Mbps.
    2. Fast Ethernet - Ethernet upgrade, supports data rates up to 100 Mbps.
    3. Gigabyte Ethernet - An improvement over Fast Ethernet, supporting data rates up to 1 Gbps.

- IEEE 802.11 WLAN: This standard characterizes the details for remote correspondence inside a WLAN. It incorporates different variants, Ex:, 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax, each offering various information rates, recurrence groups, and tweak strategies for remote systems administration.

By adhering to these IEEE Ethernet standards, Alliance Health can ensure compatibility and interoperability between their network devices and infrastructure components. This facilitates seamless communication and data exchange between different departments and locations within the organization, enabling efficient collaboration and productivity. Following these standards ensures that the network design meets industry best practices for reliability, performance, and security.

P2 Explain the impact of network topology, communication and bandwidth requirements.

Network Topologies

What is network topology?

- Computer networking, topology is the arrangement of nodes, devices, and connections in a network. It defines how data is transmitted between devices and how they connect to each other. There are two main types of network topologies. That is, (GfG., 2020)
    1. Physical Topology
    2. Logical Topology

Physical Topology

- This refers to the actual layout of the network, including the physical arrangement of cables, devices, and other hardware components. Physical locations can include: (Gillis, 2024)
    1. Bus Topology
    2. Star Topology
    3. Ring Topology
    4. Tree Topology
    5. Mesh Topology
    6. Hybrid Topology configurations.

Bus Topology

- Bus topology, all devices are connected to a single cable to form a linear structure. As data is transmitted over the cable, each device receives the data, but only the intended recipient processes it.

Advantages & Disadvantages of Bus topology

Advantages	Disadvantages
The length of the wires is less than that of star Topology.	Difficult to troubleshoot.
As the computers are connected in a linear method The construction is easy.	If the main wire becomes deactivated the whole Network becomes deactivated.

Table 3 Advantages & Disadvantages of Bus topology

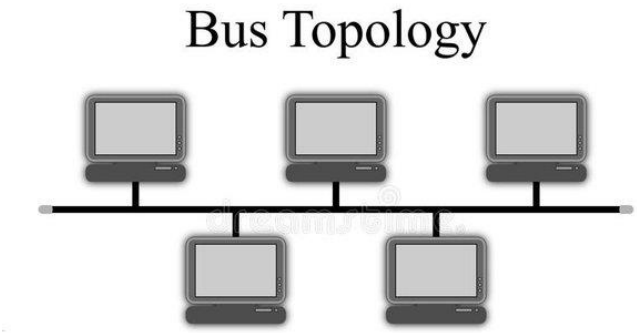


Figure 7 Bus topology

Star Topology

- Star topology, each device is connected to a central hub or switch, forming a star-like structure. All communication between devices goes through a central hub, which helps in easy management and troubleshooting.

Advantages & Disadvantages of Star topology

Advantages	Disadvantages
Easy to build.	Wires are required than linear structure.
Easy to troubleshoot.	As the central unit is expensive, the cost is high.

Table 4 Advantages & Disadvantages of Star topology

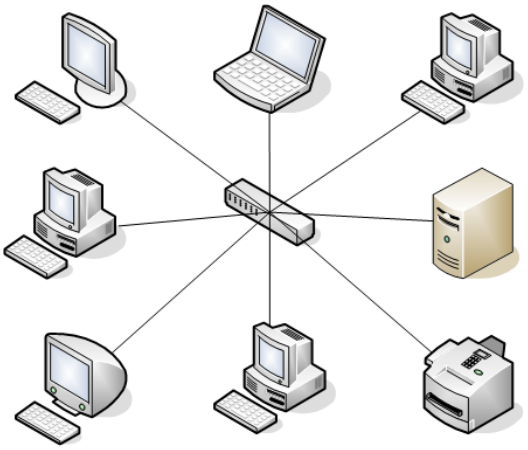


Figure 8 star topology

Ring Topology

- Ring topology, each device is connected to two other devices forming a closed loop. The data circulates around the ring until it reaches the intended receiver, and the devices act as repeaters to regenerate the signal.

Advantages & Disadvantages of Ring topology

Advantages	Disadvantages

As the data is flown to a single direction, data Transmission is fast.	If an error occurs in the main cable it causes for the Network to be collapsed.
No hubs or switches are required.	Expansion is difficult.

Table 5 Advantages & Disadvantages of ring topology

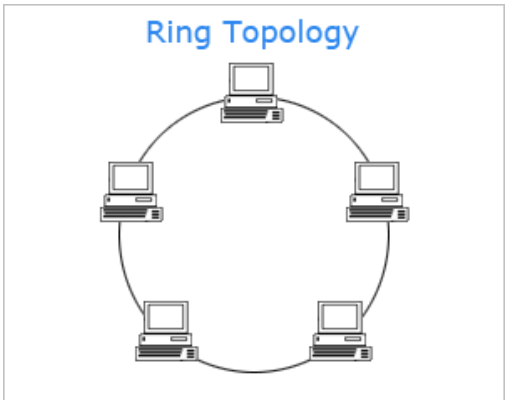


Figure 9 ring topology

Tree Topology

Tree topology, otherwise called hierarchical topology, is a tree-like organization structure with a focal root hub and spreading hubs at numerous degrees of interconnection. In a tree Topology, hubs are coordinated in a progressive way, with each level hub associated with a parent hub above it. This plan empowers effective correspondence and information stream, as data can undoubtedly go through the pecking order from the root hub to the leaf hubs as well as the other way around. Tree topology is normally utilized in wide Area Network (WANs) and local Area Network (LANs).

Advantages & Disadvantages of Tree Topology

Advantages	Disadvantages
Easy to troubleshoot as the main parts of the Network is wired separately.	If the main cable deactivated the entire network Becomes deactivated. Cabling is difficult than other Methodology.

Table 6 Advantages & Disadvantages of tree topology

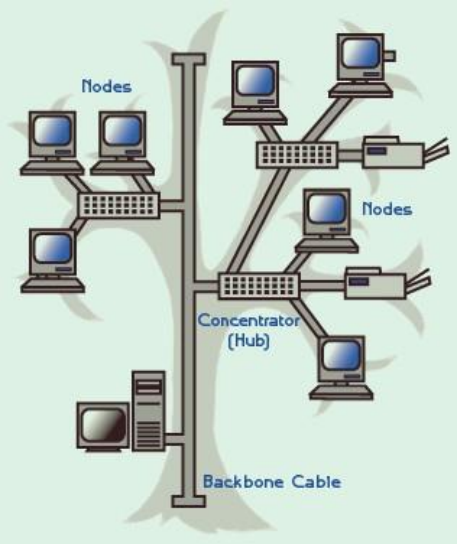


Figure 10 tree topology

Mesh Topology

Mesh topology, instead of relying on a central hub or switch, each device is directly connected to several other devices, forming a mesh-like structure. This means that every node has a direct point-to-point connection with every other node in the network. Mesh typologies can be implemented using physical connections such as cables or wireless connections. This topology provides robustness and fault tolerance because if one connection fails, there are alternate paths for data transmission.

Advantages & Disadvantages of Mesh topology

Advantages	Disadvantages
Ability to connect and remove computers without Disturbing the operation of the network.	Complexity of the maintenance of the network.
Has the ability to transmit data to all the computers Of the network at the same time as each computer Is connected with a separate cable.	When compared with other network structures, the cost is high as separate cables have to be used from one computer to all the other computers.

Table 7 Advantages & Disadvantages of Mesh topology

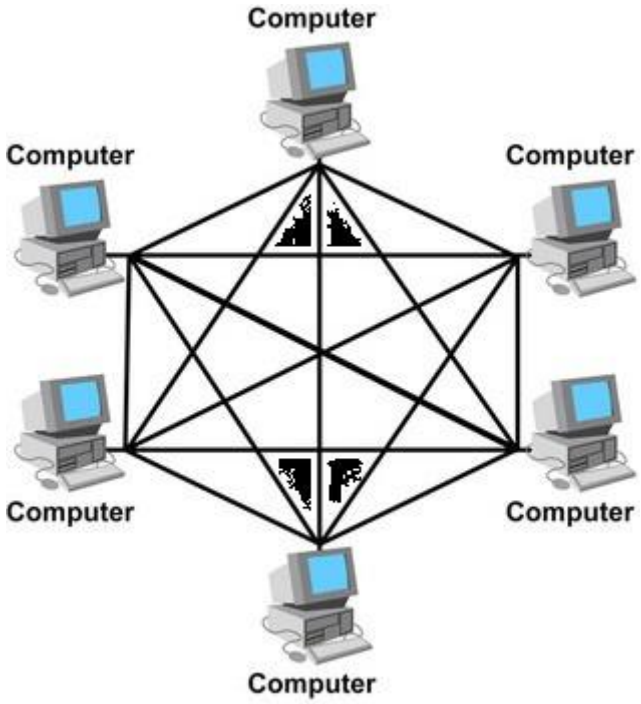


Figure 11 Mesh topology

Hybrid Topology

A hybrid topology is a type of network topology in which two or more different topologies are combined to form a network. It is a combination of two or more basic network points such as star, bus, ring or mesh. It combines the advantages of different topologies to create a more robust and flexible network infrastructure.

Advantages & Disadvantages of Hybrid topology

Advantages	Disadvantages
Redundancy and reliability	Cost
Scalability	Complexity
Customization	Security concerns
Fault isolation	Interoperability challenges

Table 8 Advantages & Disadvantages of Hybrid topology

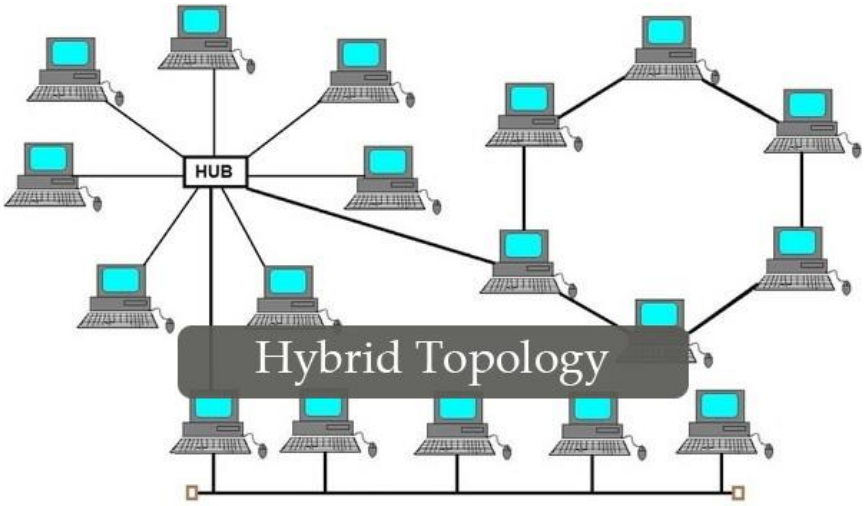


Figure 12 Hybrid topology

Logical Topology

This refers to how data is transmitted within the network independent of its physical layout. Logical topology defines the path that data travels from its source to its destination. Common logical topologies include:

1. Ethernet
2. Token Ring
3. ATM

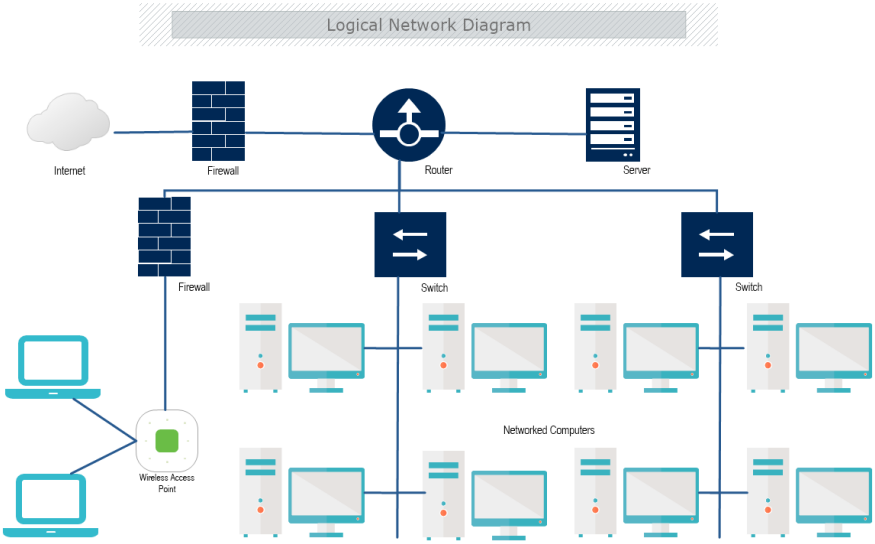


Figure 13 Logical topology

Ethernet

- Ethernet is a widely used logical topology that transmits data in packets over a shared medium. It uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to manage access to the network.

Token ring

- Token ring topology, devices are connected in a logical ring, and a token passes sequentially around the ring. Only the device holding the token can transmit data, ensuring collision-free communication.

ATM (Asynchronous Transfer Mode)

- ATM is a high-speed logical topology that uses fixed-size cells for data transmission. It provides fast and efficient communication over both LAN and WAN.

Difference between physical and logical topology

Physical Topology	Logical Topology
Represents the physical layout of the network.	Represents network logistics related to data transmission.
The layout can be changed based on the requirements.	There is no interference and manipulation here.
This has a major impact on the cost, scalability and bandwidth capacity of the network based on device selection and availability.	This has a huge impact on the speed and delivery of data packets. It also performs flow control and ordered data packet delivery.
It is a real way of transmission.	It is a high-level representation of data flow.

Table 9 Difference between physical and logical topology

What is cisco enterprise architecture and Cisco collapsed core architecture?

- Cisco enterprise architecture, network topologies are designed based on the specific needs of the organization. One common architecture is the collapsed core architecture, in which the core and distribution layers are collapsed into a single layer, simplifying network design and management. This

architecture is often used in small networks or branch offices where scalability and simplicity are important factors.

M1 Assess common networking principles and how protocols enable the effectiveness of networked systems.

Networking protocol

What is networking protocol?

A networking protocol is a set of rules and conventions that govern how data is transmitted and received over a network. It defines the format, timing, sequence and error handling of data transfer between devices in a network. Protocols enable communication between different devices and systems by ensuring compatibility and standardization. In addition, there are several network protocols that are used. That is, (Kinza Yasar, 2023)

1. HTTP (Hypertext Transfer Protocol): HTTP is the basis of data communication on the World Wide Web. It is used to transmit hypertext documents such as HTML files between a web server and a web browser. HTTP runs over TCP/IP and typically uses port 80.

2. FTP (File Transfer Protocol): FTP is a standard network protocol used to transfer files between a client and a server on a computer network. It allows users to upload, download and manage files on a remote server. FTP runs over TCP/IP and typically uses ports 20 and 21.

3. DNS (Domain Name System): DNS is a decentralized naming system for computers, services or other resources connected to the Internet or a private network. It translates domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1), allowing users to access websites using human-readable names. DNS operates over UDP or TCP and typically uses port 53.

4. DHCP (Dynamic Host Configuration Protocol): DHCP is a network management protocol used to dynamically assign IP addresses and other network configuration parameters to devices on a network. It automates the IP address allocation process, allowing devices to connect and communicate on the network without manual configuration. DHCP operates over UDP and typically uses port 67 for server communication and port 68 for server communication.

5. POP3 (Post Office Protocol Version 3): POP3 is an email protocol used by email clients to receive email from a remote mail server. It allows users to download emails from the server to their local device for offline access. POP3 works over TCP/IP and usually uses port 110.

6. TELNET: TELNET is a network protocol used to provide bi-directional interactive communication between two remote computers. It allows users to log into and control a remote computer over a network connection, usually using a command-line interface. TELNET works over TCP/IP and usually uses port 23. However, it is considered insecure due to its lack of encryption and is often replaced by more secure protocols such as SSH (Secure Shell).

7. TCP (Transmission Control Protocol): TCP is a connection-oriented protocol used for reliable and ordered data transmission between devices on a network. It operates at the transport layer (layer 4) of the OSI model and provides features such as error detection, flow control, and congestion control. TCP ensures that data packets are delivered in the correct order and that lost or corrupted packets are retransmitted. It is widely used for applications that require reliable data delivery, such as web browsing, e-mail, and file transfer.

8. UDP (User Datagram Protocol): UDP is a connectionless protocol used for fast and lightweight data transmission between devices on a network. It operates at the transport layer (layer 4) of the OSI model but does not provide reliable mechanisms like TCP. UDP does not establish a connection before transmitting data and does not perform error correction or packet retransmission. Instead, it sends data packets from source to destination without guaranteeing delivery or order. UDP is typically used for real-time applications such as voice and video streaming, online gaming, and DNS (Domain Name System) lookups.

9. IP (Internet Protocol): IP is the basic protocol used for addressing and routing data packets over networks. It operates at the network layer (Layer 3) of the OSI model and provides the addressing and routing functions necessary for data communication on the Internet. IP assigns unique IP addresses to devices on a network and determines the best path for data packets to travel from source to destination. It is responsible for breaking data packets into smaller pieces, adding source and destination IP addresses and encapsulating them for transmission. IP works in conjunction with other protocols such as TCP and UDP to enable end-to-end communication between devices on different networks. There are two IP address types.

- IPv4 (Internet Draft Version 4): IPv4 addresses are 32-bit numeric addresses, usually expressed in decimal form (e.g., 192.168.1.1). Due to the limited number of IPv4 addresses available (4.3 billion), the exhaustion of IPv4 addresses has become a significant problem, leading to the development and adoption of IPv6.

- IPv6 (Internet Draft Version 6): IPv6 addresses are 128-bit numeric addresses, allowing for a significantly larger address space compared to IPv4. IPv6 addresses were introduced to solve the problem of exhaustion of IPv4 addresses and to provide enough addresses for the increasing number of devices and networks connecting to the Internet. (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)

The DOD (Department of Defence) model and the OSI (Open Systems Interconnection) model are two commonly referenced networking models that describe the protocol layers used in network communications. (admin., 2023)

DOD Format (TCP/IP)

The DOD model, also known as the TCP/IP model, is a conceptual framework used to understand and implement network protocols. It consists of four layers:

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Data-Link Layer

Application Layer

- This layer contains protocols that facilitate communication between applications running on different devices.

Transport Layer

- This layer manages end-to-end communication between devices and ensures data reliability and integrity.

Internet Layer

- This layer handles data transmission across various networks and is responsible for addressing, routing and packet forwarding.

Data- Link Layer

- Also known as Network Interface Layer, this layer deals with the physical transmission of data over network media. It includes protocols such as Ethernet and Wi-Fi.

OSI Model

The OSI model is a conceptual framework developed by the International Organization for Standardization (ISO) to standardize network communications. It consists of seven layers:

1. Application layer
2. Presentation layer
3. Session layer
4. Transport layer
5. Network layer
6. Data link layer
7. physical layer

Application layer

- Application Layer This article acts as an interface to the user and facilitates the connection of users to the network. Applications support access to networked devices. This user sees and connects to the network system. Software such as web browsers and email clients initiate network connections depending on the application layer. Application status function can be specified as follows:
    1. Authentication of users (user authentication)
    2. file transfer, sending by e-mail and providing software necessary to access the Internet.
    3. World Wide Web Browsing

Protocols used in Application Layer

1. FTP-File Transfer Protocol
2. DNS-Domain Name System
3. HTTP-Hypertext Transfer Protocol
4. SMTP - Simple Mail Exchange
5. POP3-Post Office Protocol version 3
6. DHCP-Dynamic Host Configuration Protocol

Devices used

- Gateway

Protocol data unit of this layer - PDU

- Data

Presentation layer

- This layer is primarily used to process data so that it can be used by the application layer, and layer 6 can present data to applications. The presentation layer is responsible for data transformation, encryption and compression.

The presentation function can be stated as follows.

1. Convert to data structure (ASCII, BCD, MPEG)
2. Sender end data encryption (encrypt)
3. Decrypt the subscriber's data
4. Data distribution (compression)

Protocol data unit of this layer - PDU

- Data

Session layer

- Recommendations for starting and stopping communication between the two devices. The session layer ensures that the session stays open long enough to open, close, timeout, and transfer all the data being exchanged, and then closes the session promptly to avoid resource wastage.

Session functionality can be specified as follows.

1. Connecting devices used for data transmission purposes.
2. Identify data transfer methods. Determining whether the data transmission method is Simplex, Half Duplex or Full Data Duplex.
3. Continue and stop data transmission.

Protocols used in Session Layer

- NetBIOS
- AppleTalk
- Winsock

Protocol Data Unit of this layer - PDU

- Data

Transport layer

The transport layer is responsible for end-to-end communication between two devices. This involves taking data from the session layer and breaking it into chunks before sending it to the network layer. The transport layer on the receiving device is responsible for reassembling the fragments into data that can be consumed by the session layer. The transport layer is also responsible for flow control and error control.

Transport layer functionality can be mentioned as follows.

1. In the transmission of data in a network, the transfer of data to the transmission medium between the data sender and the receiver
2. Multiplexing
3. Controlling the flow of data.
4. Correction of data errors, if any, during transmission.

Protocols used in transport Layer

- UDP-User Data Protocol
- TCP-Transport Control Protocol

Network layer

This performs the task of carrying data from the website to the receiver. To facilitate data exchange between two different networks, the network must be connected. If the two communicating devices are on the same network, the network layer is unnecessary. The network layer separates the transport layer from the transport layer into smaller items, called packets, and reassembles the packet for the recipient. The network layer also finds the best path for data to reach its destination. This is called routing.

Network Layer functionality can be mentioned as follows.

1. Carrying data from one transmission point to another transmission point.
2. Identifying the suitable paths to transmit data.
3. Identifying the IP addresses connected to the transmission.

Protocols used in the Network Layer

- ICMP - Internet Control Message Protocol
- ARP-Address Resolution Protocol (ARP)

Devices used

- Router and the 3-layer switch

Protocol data unit of this layer

- Data packets

Data- Link layer

- Checking for errors of data received by the network. Adding Media Access Addresses (MAC) of data generating and destination devices to Frames. Keeping a connection between hardware and software. This is the 02nd layer of the Open System Interconnections Structure. Tasks of this layer that is located between physical layer and transport layer are as follows. Conversion of data into packets at the sender's end and converting data into bits at the receiver's end is done by this.

Protocol used in the presentation layer

- Ethernet
- ARP- Address Resolution Protocol
- ATM - Asynchronous Transfer Mode
- Token Ring

Devices used

- Network Interface Card (NIC)
- Bridge
- Switch

Protocol Data Unit of the Data Link Layer

- Frame

Physical layer

This is the 01st layer of Open System Interconnections Structure. In a network, flowing data truly is occurred within this layer. Other tasks of this layer are as follows.

1. Decides the speed of the transmission.
2. Determines voltage required for transmission.
3. Forwards signals of several transmission channels to a single channel and this is called Multiplexing.

Protocols used in Physical Layer

- Ethernet
- Bluetooth
- ATM

Devices Used

- Connectors
- Modems
- Repeaters
- Hubs

Protocol Data Unit of this layer

- Bits

Each layer of the OSI model has specific functions and protocols associated with it. While the OSI model provides a more detailed and comprehensive understanding of networking protocols, the TCP/IP model is more widely used in practice, especially in the context of the Internet.

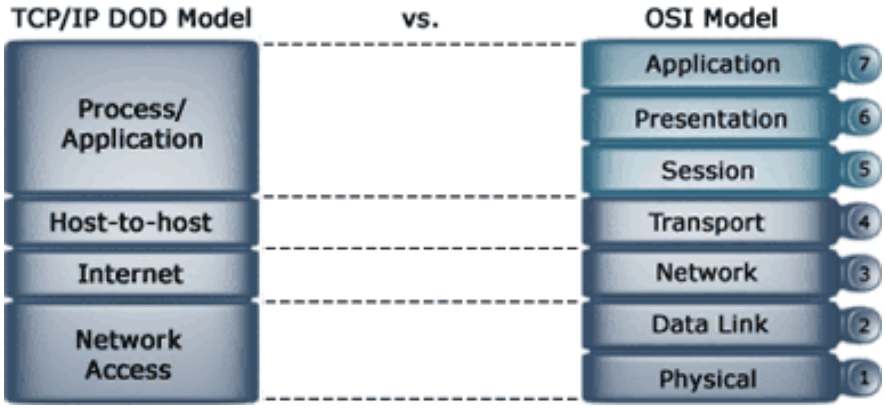


Figure 14 DOD model & OSI model

The differences between the OSI and DOD models

1. The OSI model has seven layers, while the DOD model has only four layers.
2. The OSI model is a conceptual model while the DOD model is a practical implementation.
3. The OSI model is more complex than the DOD model making it harder to implement.

Protocols play a critical role in enabling effective communication in networked systems and understanding common networking models such as the DOD (TCP/IP) model and the OSI model helps in understanding the protocol layers involved in network design and implementation.

LO2 Explain networking devices and operations.

P3 Discuss the operating principles of networking devices and server types.

The context of Alliance Health scenario, understanding the operating principles of network devices and server types is crucial for designing an efficient network infrastructure.

Network devices

Network devices play a crucial role in facilitating communication and data transfer in computer networks. Below is a brief explanation of some common network devices.

Network Interface Card (NIC)

- NICs facilitate communication between a computer and a network. They enable data transmission through cables or wirelessly.

Figure 15 NIC

Wireless Access Point (WAP)

- WAP allows wireless devices to connect to a wired network. They transmit and receive data between wireless devices and the wired network.

Figure 16 Wireless Access Point

Hub

- A hub operates at the physical layer (Layer 1) of the OSI model. It receives data packets from one device and broadcasts them to all other devices connected to the network.

Figure 17 Hub

Bridge

- The bridge operates at the data link layer (Layer 2) of the OSI model. It connects two or more network segments based on MAC addresses and forwards data between them. Isolating partitions helps reduce network congestion and conflicts.

Figure 18 Bridge

Switch

- The switch also operates at the data link layer (Layer 2) of the OSI model. It connects multiple devices within a LAN and forwards data packets based on MAC addresses. Provides high-speed, full-duplex communication between devices.

Figure 19 Switch

Router

- Routers connect multiple networks and determine the best path for data packets to travel from one network to another. They use routing tables and protocols to make these decisions.

Figure 20 Router

Gateway

A gateway is a network device that acts as an entry and exit point for data packets between different networks. It performs protocol translation, address mapping, packet filtering, and other functions to facilitate communication between networks with different protocols or addressing schemes.

Figure 21 Gateway

Repeater

A repeater is a network device used to regenerate and amplify signals to extend the distance of a network segment. Repeaters receive incoming signals, amplify them, and then retransmit them to the next part of the network, effectively increasing the overall reach of the network.

Figure 22 Repeater

Modem

A modem (short for modulator-demodulator) is a network device that enables communication between a computer or network and an Internet Service Provider (ISP) over a telephone line, cable line, fiber optic cable, or other communication channels. Modems convert digital data from computers into analog signals suitable for transmission over the communication channel. In turn, they convert outgoing digital signals into analog signals for transmission and convert incoming analog signals into digital signals for processing by the computer or network. Modems are commonly used to set up broadband Internet connections, such as DSL (digital subscriber line) and cable Internet connections.

Figure 23 Modem

Hardware Firewall / IPS / IDS

- These devices protect the network from unauthorized access, malware and other security threats. Firewalls filter network traffic, while intrusion prevention systems (IPS) and intrusion detection systems (IDS) monitor network traffic for suspicious activity.

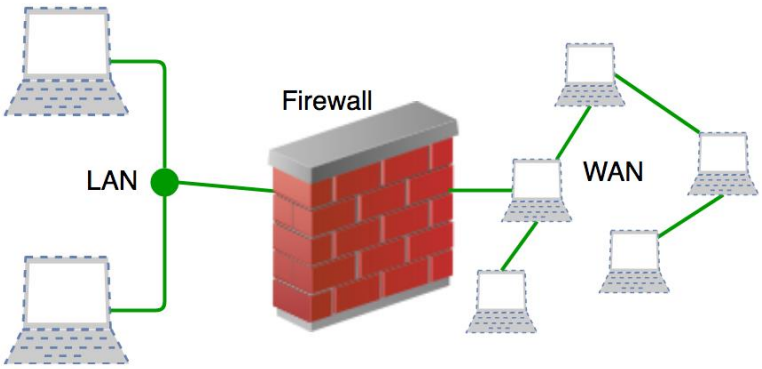


Figure 24 Firewall

Types of Servers

Servers are powerful computers or software applications that provide various services, resources and functionality to server devices or users in a network. Below is a brief explanation of the different types of servers and their functions.

DHCP Server

- Dynamic Host Configuration Protocol (DHCP) servers dynamically assign IP addresses to devices on the network, simplifying network configuration and management.

DNS Server

- Domain Name System (DNS) servers translate domain names into IP addresses, allowing users to access websites using human-readable domain names.

Web Servers

- Web servers host websites and deliver web content to clients over the Internet or the Internet.

AAA servers

- Authentication, authorization, and accounting (AAA) servers authenticate users, grant access to network resources, and log user activity.

File Servers

- File servers store and manage files, allowing users to access and share data over the network.

When choosing servers for Alliance Health, factors such as scalability, reliability, security and compatibility with existing infrastructure should be considered.
Ex: a robust DHCP server is essential for efficiently managing IP addresses across multiple departments, while a secure web server is required for hosting internal applications and securely accessing medical data.

Exploring server hardware specifications includes evaluating factors such as processing power, memory, storage capacity, and network connectivity.
Ex: servers with multi-core processors, sufficient RAM, redundant storage options and Gigabit Ethernet ports will ensure optimal performance and reliability for Alliance Health's network infrastructure. Choosing servers from vendors known for quality products and reliable support services is critical to meeting company needs and ensuring uninterrupted network operations.

P4 Discuss the interdependence of workstation hardware and relevant networking software.

Network design for Alliance Health, the interdependence of workstation hardware and networking software plays a critical role in ensuring seamless communication and efficient data management. Below is an explanation of client-side software and network software and their interconnection breakdowns.

Server-Side Software

FTP Servers

- File Transfer Protocol (FTP) servers facilitate the transfer of files between client computers and the server. They are essential for sharing documents, images and other data within the organization.

Centralized database server

- A centralized database server stores and manages critical healthcare data, including patient records, billing information and medical history. It ensures data integrity, security and accessibility across departments.

- Email Server

An email server enables internal communication between employees and external communication with clients and partners. It ensures reliable email delivery, supports attachments and provides security features such as spam filtering and encryption.

Client-Side Software

FTP client (e.g., FileZilla)

- FTP clients allow users to connect to FTP servers to upload, download, and manage files. They provide a user-friendly interface to securely transfer data over the network.

Microsoft Server Management Studio

- This software suite enables administrators to manage and monitor Microsoft SQL Server databases. It allows for database administration, query writing and performance tuning.

Email client (e.g., Outlook)

- Email clients such as Microsoft Outlook provide a platform to send, receive and organize emails. They support features like calendar integration, contact management, and email encryption.

Network Software

Cisco IOS (Internetwork Operating System)

- Cisco IOS is the operating system used in Cisco networking devices such as routers and switches. It provides functionality for routing, switching, security and network traffic management.

NetFlow collectors (e.g., Wireshark)

- NetFlow collectors, including Wireshark, capture and analyse network traffic data. They help diagnose network problems, monitor bandwidth usage, and troubleshoot performance issues.

The interdependence between workstation hardware and networking software is evident in their collaborative role in facilitating data communication, access, and management within the network infrastructure. Ex:, server-side software such as Microsoft Server Management Studio relies on server-side database servers to access and manipulate healthcare data, while network software such as Cisco IOS controls the transfer of data packets between various departments and branches of Alliance Health. This symbiotic relationship ensures smooth functioning and functionality of the network environment. Ultimately supporting the organization's goals of optimizing the healthcare industry's revenue cycle.

M2 Explore a range of server types and justify the selection of a server for a given scenario, regarding cost and performance optimization.

For the network design of Alliance Health's head office and Matara branch, several types of servers can be considered based on the organization's requirements for performance, reliability and cost-effectiveness. Below are some physical server hardware suggestions with their justifications.

File Server

- A file server is essential for storing and sharing files, reports, and documents between different departments at Alliance Health. This server will provide a centralized location for file management, making it very easy for employees to access. Key features include access control, which improves data security by allowing only authorized users to access sensitive files. To handle large volumes of data, it is recommended that a file server have sufficient storage capacity and redundancy features such as RAID (Redundant Array of Independent Disks). RAID protects data by copying it across multiple disks so that even if a hard drive fails, the data is available. This type of server is well suited for HR, Finance, and Sales departments that store large amounts of data and access it frequently.
    - Cost Optimization- Using RAID (Redundant Array of Independent Disks) for redundancy provides data protection without the need for expensive cloud storage solutions.
    - Performance Benefits- High-capacity hard drives (HDDs) with backup capabilities ensure quick access to frequently used files. The server enables multiple employees to access documents simultaneously without delay, improving productivity.

Application Server

- An application server hosts business-critical applications such as HRMS, CRM tools, and accounting software. This ensures reliable and consistent access to applications across the organization.

  Ex: would be a shared HRMS application accessed by HR departments in both Colombo and Matara. The server requires high processing power, sufficient RAM, and sufficient storage to allow multiple users to use it simultaneously. In this case, accessing and running applications that are critical to maintaining productivity ensures smooth operation without delays.

  - Cost Optimization- Hosting multiple applications on a single, robust server reduces the need for separate servers, minimizing hardware and maintenance costs.
  - Performance Benefits- A server with multi-core processors and sufficient RAM supports concurrent users without performance degradation, ensuring that employees experience smooth and uninterrupted access to applications.

Database Server

- Alliance Health handles a lot of sensitive data, such as billing details and operational reports. A dedicated database server is required to handle this much data securely and effectively. The server must have high-performance storage subsystems, such as SSDs - Solid State Drives, which ensure data retrieval at high speeds compared to traditional hard drives. Sufficient RAM ensures that database queries and transactions run at a fast speed, even when the database is used at maximum capacity. The IT department relies on the database server for data-driven operations, such as analytics and reporting.
  - Cost Optimization- Investing in SSD (Solid-State Drives) for storage ensures faster read/write speeds, reducing latency in data retrieval. This is cost-effective compared to the repeated productivity losses caused by slower storage solutions.
  - Performance Benefits- With sufficient memory and processing power, the server can handle complex queries and transactions quickly, ensuring that departments such as accounting and human resources can process data without delay.

Web Server

- The web server hosts the company's websites, internal portals, and web-based applications. It processes requests from users' browsers to ensure that users can access online content in the fastest and most secure way.

  Ex: Employees who open internal portals to access schedules or customers who use online appointment booking services rely on this server. It should have features such as load balancing to distribute traffic

evenly and support SSL to encrypt data so that there is no breach of user privacy. A scalable web server can handle increased traffic as the company grows, ensuring service without downtime.

- Cost Optimization- A scalable web server with load balancing capabilities ensures that it can handle high traffic without the need for multiple servers.
- Performance Benefits- Features like caching and SSL (Secure Sockets Layer) encryption ensure fast content delivery and secure data transmission, which is critical for maintaining client trust and meeting compliance standards.

Backup Server

- Data loss from hardware failure, human error, or even cybersecurity threats can dent operations seriously. A backup server safeguards against such risks and stores critical data in multiple copies. The features of backup schedules and versioning capabilities ensure backups are regular and that even previous versions of files are kept. It should also include redundant storage systems for added reliability. The backup server ensures that data can be recovered quickly in case of data loss, hence minimizing downtime and safeguarding critical business operations.
  - Cost Optimization- Automating backups reduces administrative overhead and ensures consistent data protection without relying on expensive manual processes.
  - Performance Benefits- Features such as redundant storage systems and versioning allow for quick data recovery, minimize downtime, and maintain operational efficiency.

Server Virtualization

- Server virtualization is an advanced technology that allows a single physical server to host multiple virtual machines (VMs). This reduces hardware costs, optimizes server resources, and improves scalability. For Alliance Health, a virtualization server is ideal for multiple applications and services while minimizing physical server requirements.

  Ex: A single virtualization server can run multiple VMs dedicated to file sharing, applications, and test environments. High-performance hardware with multi-core processors, sufficient RAM, and fast storage are essential to effectively support virtualization.
  - Cost Optimization- By consolidating workloads onto fewer physical servers, Alliance Health can reduce hardware, energy, and maintenance costs.
  - Performance Benefits- With advanced virtualization software, the server can dynamically allocate resources to VMs based on demand, ensuring optimal performance for critical applications.

Network Attached Storage (NAS) Server

- A NAS server provides centralized storage for backups, archives, and shared files. This type of server is especially useful for storing infrequently accessed data, such as old records and large media files. A NAS server supports protocols such as NFS (Network File System) and SMB (Server Message Block), enabling easy file sharing over the network. For Alliance Health, a scalable NAS server ensures efficient storage management and easy access to historical data, improving operational efficiency.

Unified Threat Management (UTM) Server

- Given the sensitive nature of healthcare data, a UTM server is essential to protect the network from cyber threats, malware, and unauthorized access. A UTM appliance combines multiple security features into a single device, including firewall, intrusion detection/prevention, antivirus, VPN, and content filtering. The all-in-one solution provides comprehensive security for Alliance Health's network, ensuring that patient data and internal communications remain secure. A UTM server is especially important for meeting the compliance requirements of the healthcare industry.
    - Cost Optimization- A UTM appliance integrates multiple security functions such as firewall, intrusion detection, antivirus, and VPN - reducing the need for separate security systems.
    - Performance Benefits- Comprehensive threat protection ensures data integrity and compliance with healthcare regulations, protecting the organization from costly breaches or fines.

When choosing server hardware for Alliance Health, considerations should include scalability to accommodate future growth, redundancy for fault tolerance, performance to meet current workload demands, and budget constraints to optimize cost-effectiveness. Adherence to industry best practices for data security, compliance requirements, and disaster recovery planning should guide the selection and deployment of server infrastructure.

D1 Evaluate the topology protocol selected for a given scenario and how it demonstrates the efficient utilization of a networking system.

For the Alliance Health situation, considering factors such as cost, performance, and maintainability, the appropriate network topology would be a hierarchical topology. Specifically, a modified form of extended star topology. The reasons for these are given below.

Hierarchical topology

This topology organizes devices into multiple layers. Each layer performs specific functions. In the case of Alliance Health, hierarchical topology can efficiently manage the network by separating different departments into distinct layers, providing scalability and ease of management. Following are the reasons for using hierarchical topology.

- Cost

  One of the main reasons for choosing a hierarchical topology is its cost-effectiveness. Unlike full mesh or ring topologies, which require extensive cabling and additional hardware, a hierarchical topology uses fewer connections to achieve efficient communication.

  Ex: switches are placed at departmental levels, and each device is connected to a core switch rather than directly connecting every other device. This reduces both installation costs and ongoing maintenance costs while maintaining high performance.

  For an organization like Alliance Health, which spans multiple floors and branches, this cost-effective approach ensures that the network infrastructure stays within budget without compromising performance or reliability.

- Performance

  Performance is a critical factor in the design of any network. In a hierarchical topology, traffic management is significantly improved by dividing departments into separate subnets. Each department has its own VLAN (Virtual Local Area Network), which reduces the size of broadcast domains. This means that unnecessary traffic within a department is contained, reducing congestion and improving overall network speed.

  The hierarchical design ensures that data is efficiently routed through designated paths.

  Ex: Communication within a department is handled at the local switch level, while interdepartmental or interbranch communication is managed by core routers. This structured approach ensures that critical data reaches its destination quickly, without competing for bandwidth with unrelated traffic.

- Maintainability

  Its clear structure makes it easier to maintain the network in a hierarchical topology. When problems arise, IT personnel can isolate and troubleshoot problems in specific layers or departments without affecting the entire network.

  Ex: If a switch in the HR department fails, it only affects that department’s connectivity, while the rest of the network remains operational.

This segmentation also simplifies network upgrades or modifications. If Alliance Health decides to expand its Matara branch, new departments or floors can be added to the existing topology without major reorganization. This module reduces downtime and ensures that business operations continue uninterrupted.

Recommended network protocols

- Ethernet (IEEE 802.3)

  Ethernet is a widely used networking technology for local area networks (LANs). It is popular because of its high reliability, ease of use, and cost-effectiveness. Ethernet enables devices on the same network, such as computers, printers, and servers, to communicate with each other via wired connections. In the context of Alliance Health, Ethernet will be the backbone of internal communications within each department and across devices on the same floor or branch.

  Ex: At the Colombo head office, Ethernet will connect devices in the Human Resources Department, the Accounting Department, and the Information Technology Department via switches and cables. These connections ensure that data is transmitted quickly and securely. Ethernet provides high speeds in modern networks, often ranging from 1 Gbps to 10 Gbps, which is ideal for handling the large volumes of data exchanged between devices in a busy organization like Alliance Health.

  Ethernet is also known for its stability and low latency. This means that employees experience fewer delays when accessing shared files, printing documents, or communicating within the office. By using Ethernet for wired connections, Alliance Health ensures a strong and stable foundation for its local networks.

- TCP/IP

  TCP/IP or Transmission Control Protocol/Internet Protocol is the standard protocol suite for Internet and network communication. It is essential for ensuring reliable data transfer between different networks or locations, such as the Colombo head office and the Matara branch. TCP/IP consists of two main parts. There are,

  - TCP (Transmission Control Protocol)- This ensures that data is delivered correctly and in the correct order.

    Ex: If an employee in the Matara branch accesses a database stored in the Colombo office, TCP divides the data into packets, ensures their delivery, and reassembles them at the receiving end without any loss.

- IP (Internet Protocol)- This handles the addressing and routing of data packets, ensuring that they reach the correct destination. It assigns unique IP addresses to devices, enabling them to identify where the data is going. Within Alliance Health's network, TCP/IP will be crucial for enabling inter-branch communication.
  Ex: When the HR team in Matara needs to access payroll data stored in the server room in Colombo, TCP/IP ensures that the data is transmitted securely and reliably over the network.

TCP/IP supports a variety of applications such as email, video conferencing, and cloud-based systems. This makes it a versatile protocol that fits well with Alliance Health's needs, such as holding video meetings in the conference room or accessing centralized databases across branches.

Performance issues

- Modified Extended star topology

Extended star topology can lead to large broadcast domains and performance problems, and a modified version can solve these problems. A hierarchical structure within each branch (department) can better manage network traffic, reduce congestion and improve performance by implementing a switch connecting each department and a central core switch or router connecting the branches.

Hierarchical topology, especially modified extended star topology, along with Ethernet and TCP/IP protocols, offers an efficient and scalable solution for Alliance Health's network architecture. It addresses requirements while optimizing performance, cost-effectiveness and maintainability.

Justification of hierarchical topology for efficient use

A hierarchical topology helps Alliance Health achieve a network that is efficient, scalable, secure, and easily adaptable to future growth. It is best suited to meet the company's current and future networking needs. A justification of the benefits of using this type of topology is given below.

Scalability

- One of the most important advantages of a hierarchical topology is that it can support growth. In the case of Alliance Health, as it expands, it becomes easier to add new departments, floors, or even branches without making major changes to the existing network structure.

  Ex: If a new department is introduced in the Matara branch, it can be easily integrated into the network by connecting it to a switch and assigning it to its subnet. This modular approach ensures growth without affecting the rest of the network. Scalability saves time, minimizes costs, and ensures that the network remains operational as it expands, without having to re-engineer the entire system.

Resource Allocation

- The hierarchical topology allows for effective management of network traffic using VLANs, Virtual Local Area Networks. Each department is assigned to its own VLAN, so network traffic is segmented, preventing unnecessary data transfer between departments.

  Ex: Traffic from the Human Resources department in the Colombo head office is segregated from data from the accounting department. This helps to avoid network congestion and optimize bandwidth usage. Employees in each department can access the resources they need without being interrupted by traffic from other departments. This bandwidth optimization improves overall network performance and user experience.

Security

- Another important advantage of the hierarchical topology is the added security to the network. Segmenting departments into subnets limits excessive data flow. The accounting department's financial data is restricted to its own subnet and is accessible only to its users.

  Ex: This prevents unauthorized access and reduces the damage caused by any eventual breach. The hierarchical topology facilitates the easy implementation of firewalls, intrusion detection systems, and access controls for relevant departments, further enhancing the security posture of the network.

Flexibility

- This ensures that a hierarchical topology effectively meets both high-speed and wireless needs with a combination of wired and wireless connections.

  Ex: Fixed workstations in an IT department use fast and reliable wired connections to access servers and applications. Mobile employees who can do sales and marketing can stay connected

even when they are traveling up and down the offices or visiting their clients with the help of Wi-Fi. Wi-Fi access points installed in public areas such as reception and customer service areas ensure seamless connectivity for guests and employees with mobile devices. Such flexibility ensures that all users on the network have access to resources in a way that best suits their work style.

LO3 Design efficient networked systems

P5 Design a networked system to meet a given specification.

Logical Diagram for each two branches.

Below is the logical diagram that I drew in Alien's health branch.

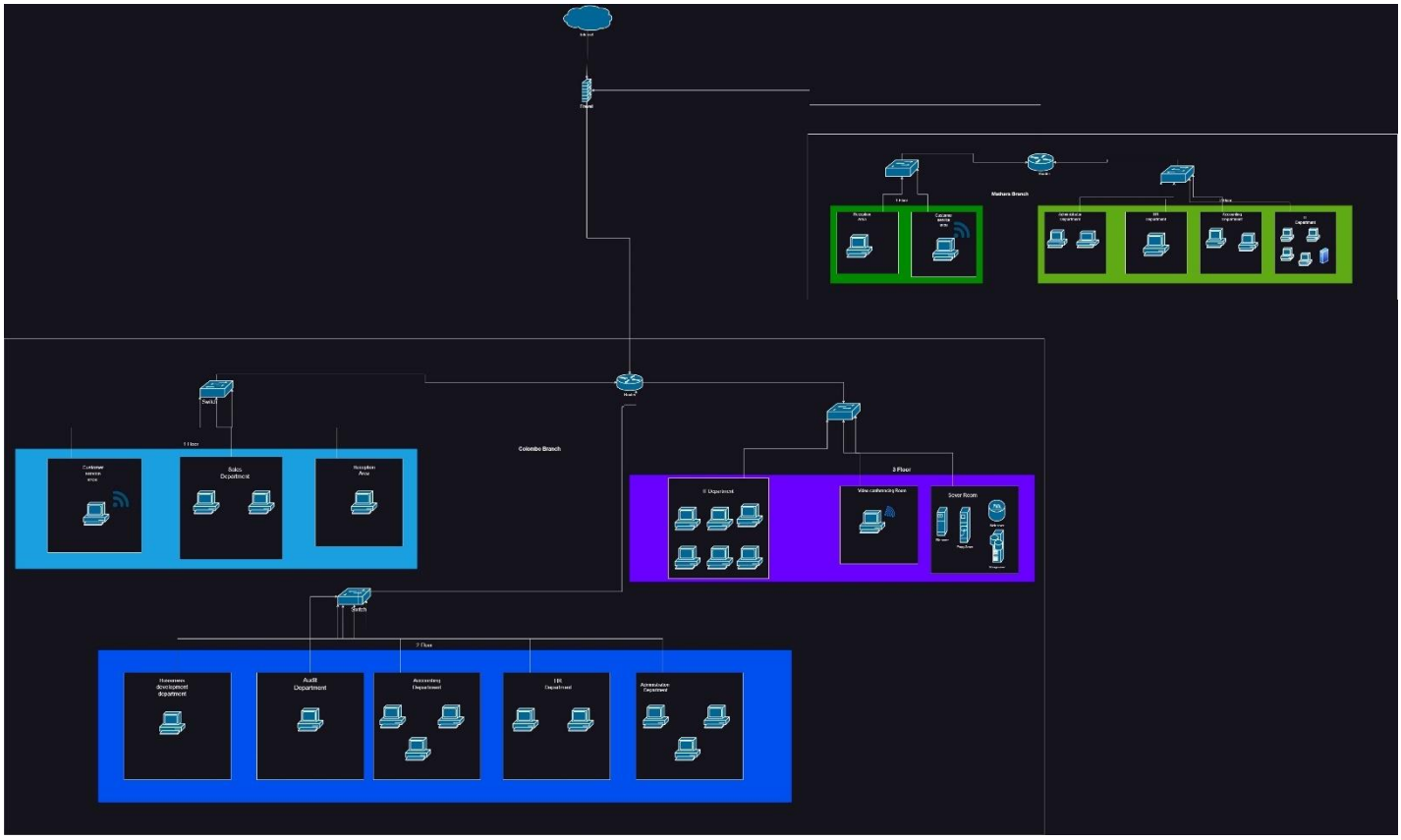


Figure 25 Logical diagram for Alien's health

Below is the logical diagram that I drew in Colombo branch.

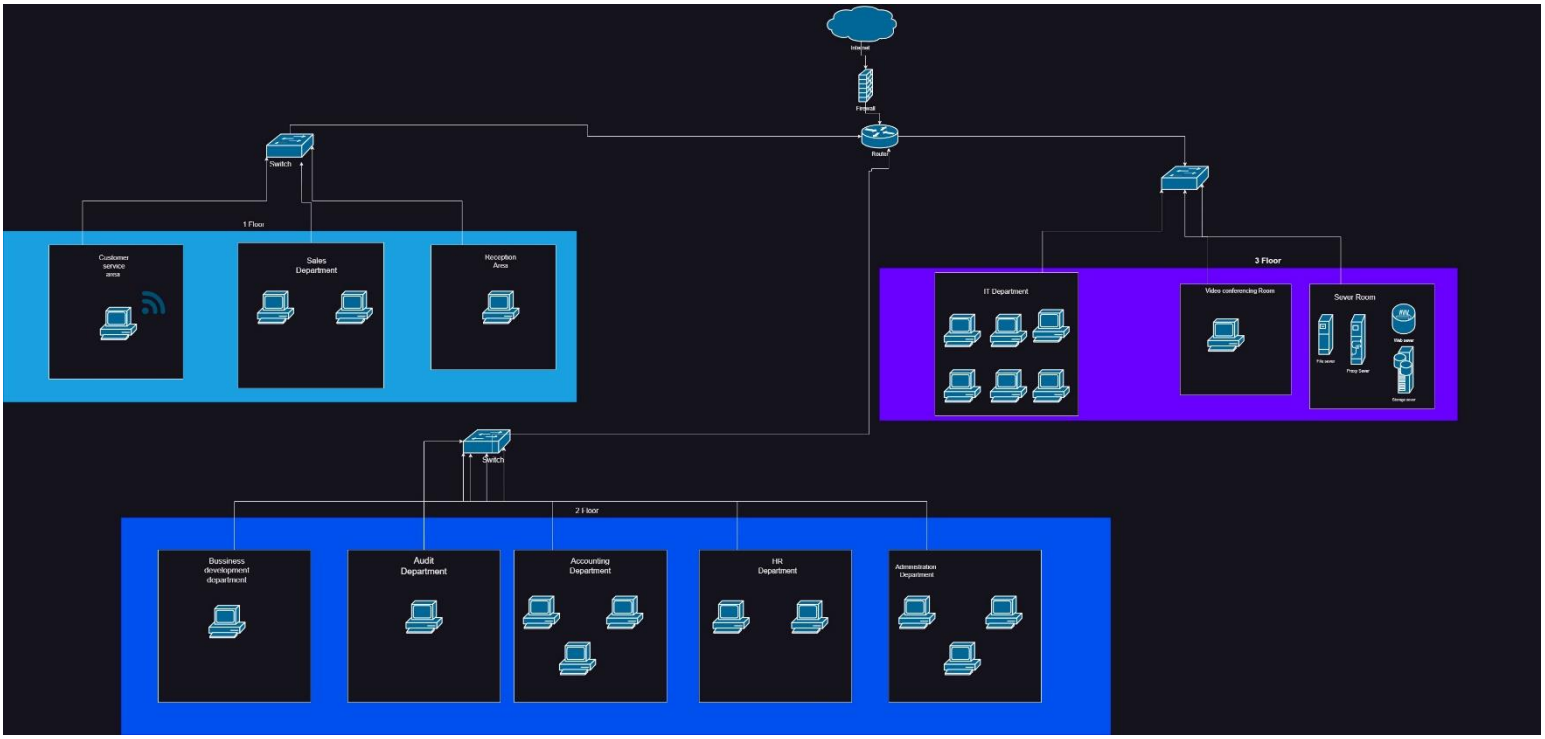


Figure 26 Colombo branch logical diagram

Below is the logical diagram that I drew in Mathara branch.

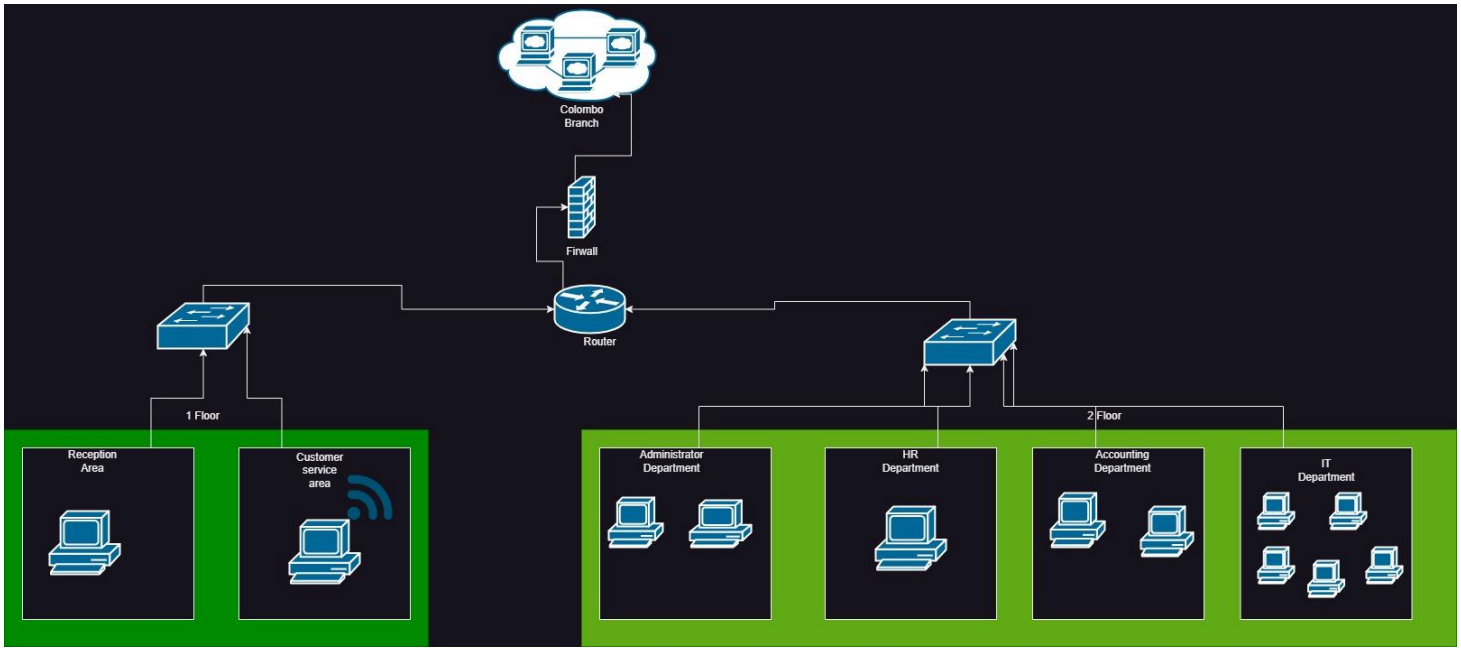


Figure 27 Mathara Branch logical diagram

Alliance Health's branch IP address

Colombo Branch

Table 10 Colombo branch IP

Floor 3 **IT**	Network address -192.168.10.0/26 Subnet mask-255.255.255.192 Gateway device-192.168.10.1 Frist device- 192.168.10.2 last device-192.168.10.62 broadcast ip-192.168.10.63 Users: 60
Floor 2 **Administrator**	Network address -192.168.10.64/27 Subnet mask-255.255.255.224 Gateway device-192.168.10.65 Frist device- 192.168.10.66 last device-192.168.10.94 broadcast ip-192.168.10.95 Users:30
Floor 2 **HR**	Network address -192.168.10.96/27 Subnet mask-255.255.255.224 Gateway device-192.168.10.97 Frist device-192.168.10.98 last device-192.168.10.126 broadcast ip-192.168.10.127 Users:20
Floor 2 **Account**	Network address -192.168.10.128/27 Subnet mask-255.255.255.224 Gateway device-192.168.10.129 Frist device-192.168.10.130 last device-192.168.10.158 broadcast ip-192.168.10.159 Users: 15
Floor 1 **Sales**	Network address-192.168.10.160/28 Subnet mask-255.255.255.240 Gateway device-192.168.10.161 Frist device-192.168.10.162 last device-192.168.10.174 broadcast ip-192.168.10.175 Users:10
Floor 2 **Audit**	Network address-192.168.10.176/29 Subnet mask-255.255.255.248 Gateway device-192.168.10.177 Frist device- 192.168.10.178 last device-192.168.10.182 broadcast ip-192.168.10.183 Users:5

Floor 2 **Business**	Network address-192.168.10.184/29 Subnet mask-255.255.255.248 Gateway device-192.168.10.185 Frist device- 192.168.10.186 last device-192.168.10.190 broadcast ip-192.168.10.192 Users: 5
Floor 1 **Reception Area**	Network address-192.168.10.193/29 Subnet mask-255.255.255.248 Gateway ip-192.168.10.194 Frist device- 192.168.10.195 last device-192.168.10.198 broadcast ip-192.168.10.199 Users: 4
Floor 1 **Customer service**	Network address-192.168.10.200/29 Subnet mask-255.255.255.248 Gateway ip-192.168.10.201 Frist device- 192.168.10.202 last device-192.168.10.206 broadcast ip-192.168.10.207 Users:4
Floor 3 **Video conferencing**	Network address- 192.168.10.208/29 Subnet mask-255.255.255.248 Gateway ip-192.168.10.209 Frist device- 192.168.10.210 last device-192.168.10.214 broadcast ip-192.168.10.215 Users: 4
Sever Room	Network address-192.168.10.224/27 Subnet mask-255.255.255.224 Gateway ip-192.168.10.225

Mathara Branch

Floor 2 **IT**	Network address -192.168.11.0/26 Subnet mask-255.255.255.192 Gateway device-192.168.11.1 Frist device- 192.168.11.2 last device-192.168.11.62 broadcast ip-192.168.11.63 Users:50
Floor 2 **Administrator**	Network address-192.168.11.64/28 Subnet mask-255.255.255.240 Gateway device-192.168.11.65 Frist device-192.168.11.66 last device-192.168.11.78 broadcast ip-192.168.11.79 Users:10
Floor 2 **Account**	Network address -192.168.11.80/28 Subnet mask-255.255.255.240 Gateway device-192.168.11.81 Frist device-192.168.11.82 last device-192.168.11.94 broadcast ip-192.168.11.95 Users:8
Floor 1 **HR**	Network address-192.168.11.96/28 Subnet mask-255.255.255.240 Gateway device-192.168.11.97 Frist device-192.168.11.98 last device-192.168.11.110 broadcast ip-192.168.11.111 Users:7
Floor 1 **Reception Area**	Network address-192.168.11.112/29 Subnet mask-255.255.255.248 Gateway device-192.168.11.113 Frist device-192.168.11.114 last device-192.168.11.118 broadcast ip-192.168.11.119 users: 4

Floor 1
Customer service

Network address- 192.168.11.120/29
Subnet mask-255.255.255.248
Gateway ip-192.168.11.121
Frist device-192.168.11.122
last device-192.168.11.126
broadcast ip-192.168.11.127
Users:4

Table 11 Mathara Branch IP

P6 Design a maintenance schedule to support the networked system.

Maintenance schedule for Alliance Health's branch

To create a network maintenance schedule table for Alliance Health's networked system, we outline key maintenance tasks, their frequency, and responsible personnel. Below is the maintenance schedule.

Table 12 Maintenance schedule

No	Procedure	Daily	Weekly	Monthly	6 Month	1 Year	Responsible Person
Severs & Systems							
S1	Backup configuration		✓				System Admin
S2	OS update			✓			
S3	Application updates			✓			
S4	Disk space monitoring		✓				
S5	Performance monitoring	✓					
S6	Log file analysis		✓				
S7	Disaster recovery testing					✓	
Security							
SE1	Firewall configuration			✓			Security Admin
SE2	Anti-virus update		✓				
SE3	Intrusion detection	✓					
SE4	Security patch management			✓			
SE5	User access review				✓		

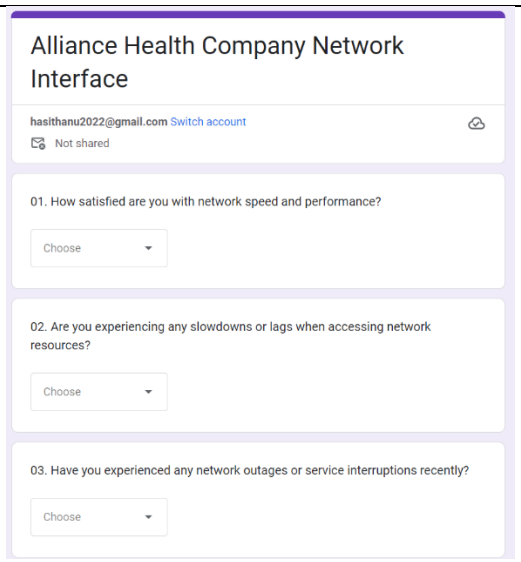
Network Hardware							
N1	Firmware updates			✓			Network Admin
N2	Configuration backups		✓				
N3	Interface monitoring	✓					
N4	Cable Inspection					✓	
Active directory							
AD1	User account management	As needed					System Admin
AD2	Group policy update				✓		
AD3	Security group review				✓		Security Admin
AD4	Domain controller health			✓			System Admin

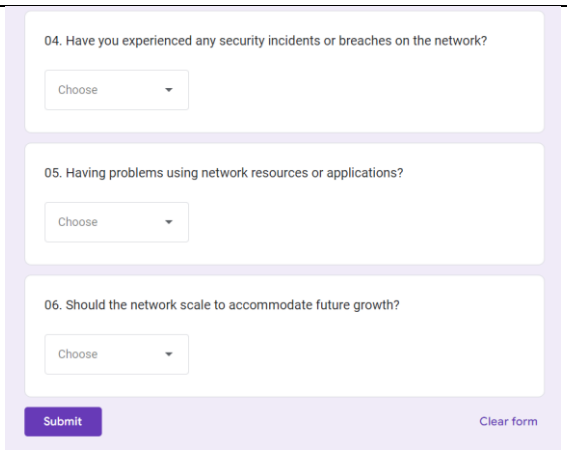
This maintenance schedule includes regular checks and updates to keep the network running smoothly and safely. It also allows proactive steps to be taken to address potential issues before they impact operations. In addition, the assignment of responsible personnel ensures timely execution of warranty and maintenance tasks.

M3 Analyse user feedback on your designs with the aim of optimizing your design and improving efficiency.

Below is the feedback form designed to gather peer feedback on the network design and improve its availability/reliability and security.

Table 13 User feedback





Result of the Google form

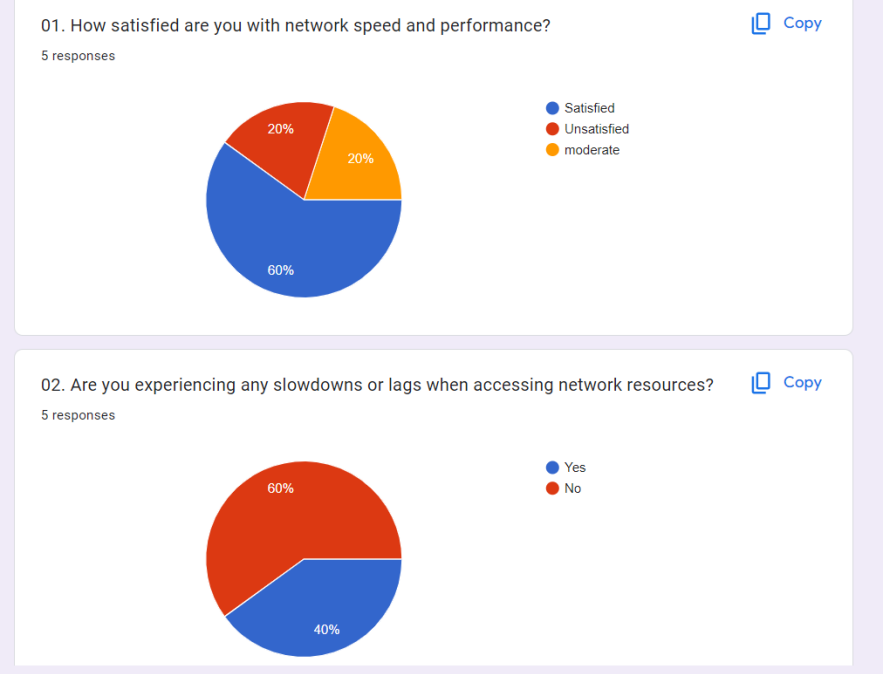


Figure 28 User feedback evidence 1

Analysis

1. The majority of users (60%) are satisfied with the network speed and performance, indicating that the current setup meets expectations for most users. However, the remaining 40% (neutral and dissatisfied) emphasize the room for improvement. Network performance may vary by department or location, suggesting that specific areas such as hardware upgrades or traffic flow reconfiguration may require optimization.

2. 60% of users do not experience slowdowns, while 40% report significant lag when accessing network resources. This feedback indicates isolated performance issues, which can arise due to congestion on specific subnets, heavy usage during peak hours, or insufficient bandwidth allocation for certain departments. Addressing these issues will improve the overall user experience.

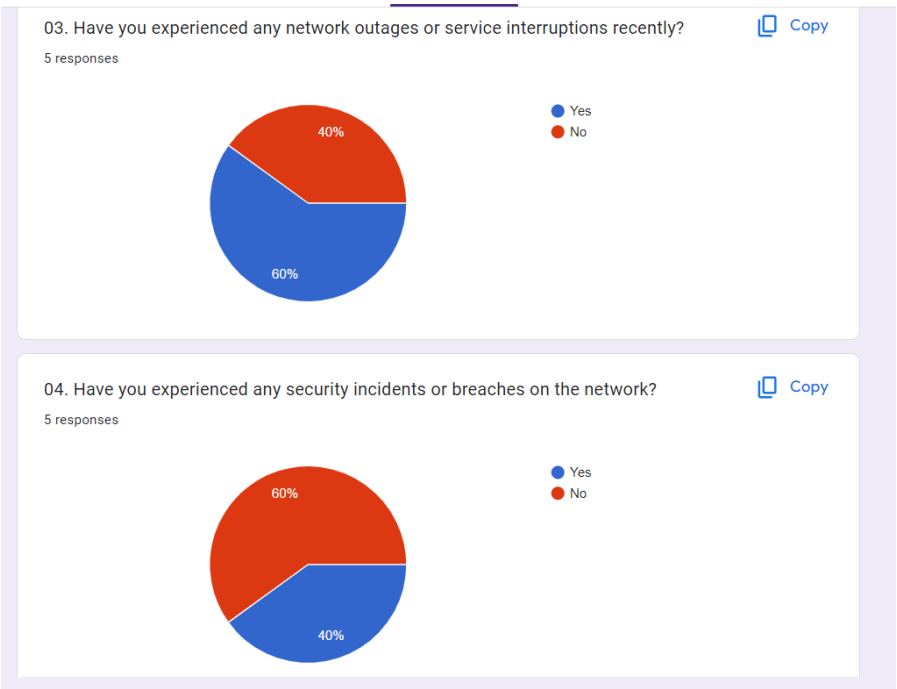


Figure 29 User feedback evidence 2

Analysis

3. A majority of users (60%) have experienced network outages or service interruptions. This suggests a significant problem with network reliability. Outages can be the result of hardware failures, insufficient redundancy, or poor fault tolerance in the current setup. Improving reliability should be a priority to ensure uninterrupted access to critical resources.

4. While 60% of users did not report any security incidents, the remaining 40% experienced breaches or related issues. This is especially relevant since security is critical to protecting sensitive data in a healthcare environment. Strengthening network security through firewalls, intrusion detection systems, and regular audits is essential to mitigate risks.

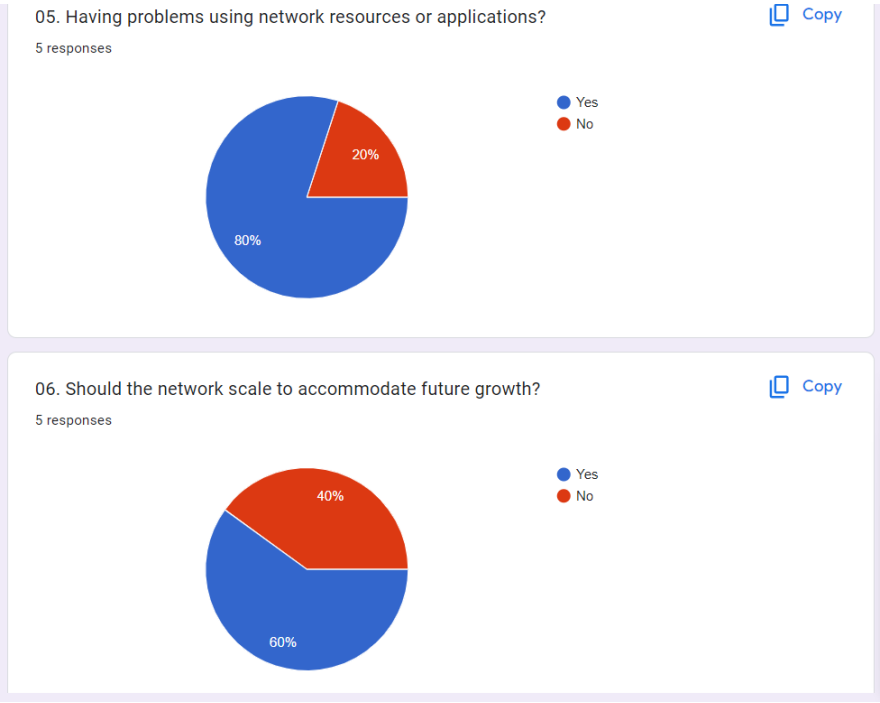


Figure 31 User feedback evidence 3

Analysis

5. A whopping 80% of users report problems using network resources or applications. This highlights a significant usability issue related to improper network configuration, software compatibility issues, or inadequate training. Urgent action is needed to identify and resolve these challenges to improve productivity.

6. 60% of users do not currently see a need for network scalability, while 40% believe it should accommodate future growth. This shows that while the existing network may be adequate for now, there is an awareness of the need for flexibility and planning to support expansion, especially with the addition of the Matara branch.

Summary of the google form

The feedback reveals mixed views on the current performance and usability of the network. While the network works well for the majority, there are significant issues with reliability, security, and usability for a portion of users. Key findings include.

- Performance - Network speeds are satisfactory for most users, but slowdowns and latency affect some, suggesting localized bottlenecks.

- Reliability - Frequent outages highlight the need for improved fault tolerance and redundancy.

- Security - Nearly half of respondents have experienced security incidents, underscoring the need for improved security.

- Usability - The majority of users face challenges accessing network resources, which significantly impacts productivity.

- Scalability - A significant minority emphasize the importance of preparing the network for future growth.

Conclusion

Alliance Health's current network meets basic needs for most users, but improvements in reliability, security, and usability are needed to address concerns raised by others. Improvements include hardware upgrades, configuration optimization, increased redundancy, and implementation of robust security measures. A proactive approach to scalability will ensure that the network can support future expansion and business growth.

By systematically addressing these issues, Alliance Health can create a robust and efficient network infrastructure that meets user expectations, supports operations, and aligns with the organization's goals.

These questions and answers provide valuable insight into user perceptions and experiences with the network. This helps to identify areas for network improvement, optimize network design for better performance availability, reliability and security.

LO4 Implement and diagnose networked systems.

P7 Implement a networked system based on a prepared design.

Below is the network diagram of Alliance Health's branch.

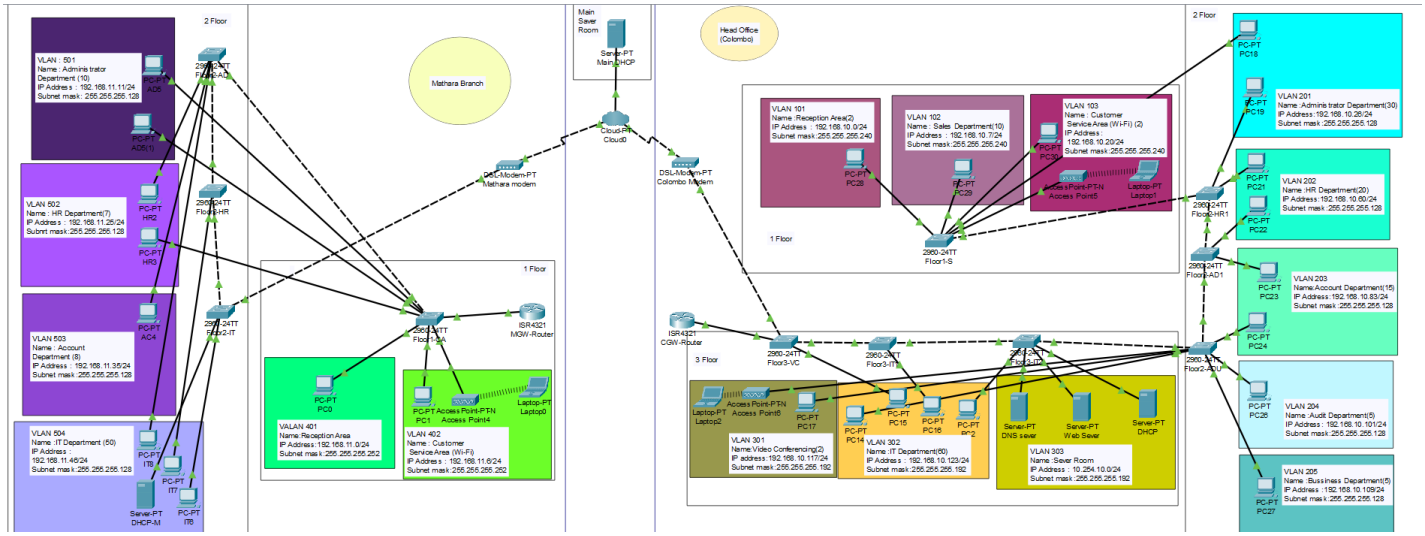


Figure 32 Network diagram of Alliance Health's branch

Below is the network diagram of Alliance Health's Mathara branch.

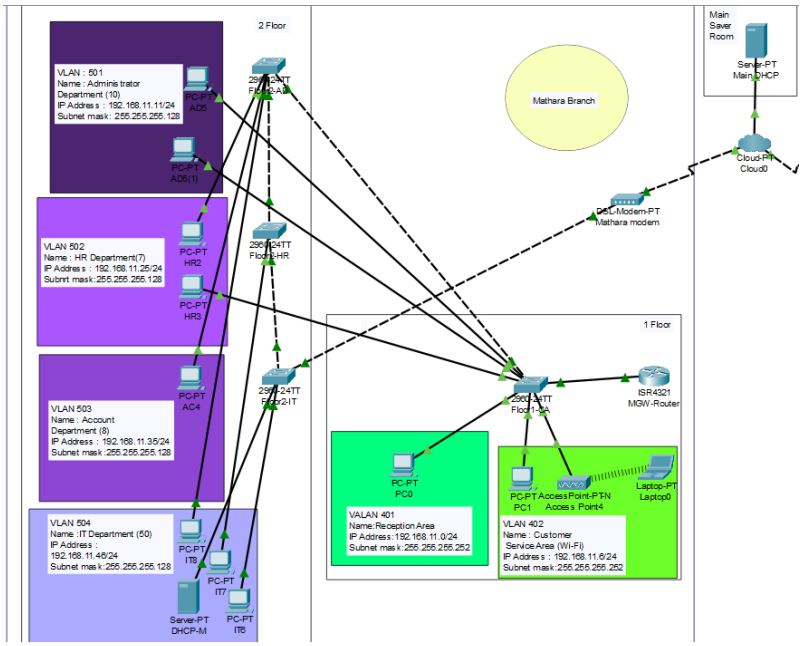


Figure 33 Network diagram of Alliance Health's Mathara branch

- In this case, I had to connect 4 switches, a router and DHCP server. Their settings are shown below.

Floor1-CA switch

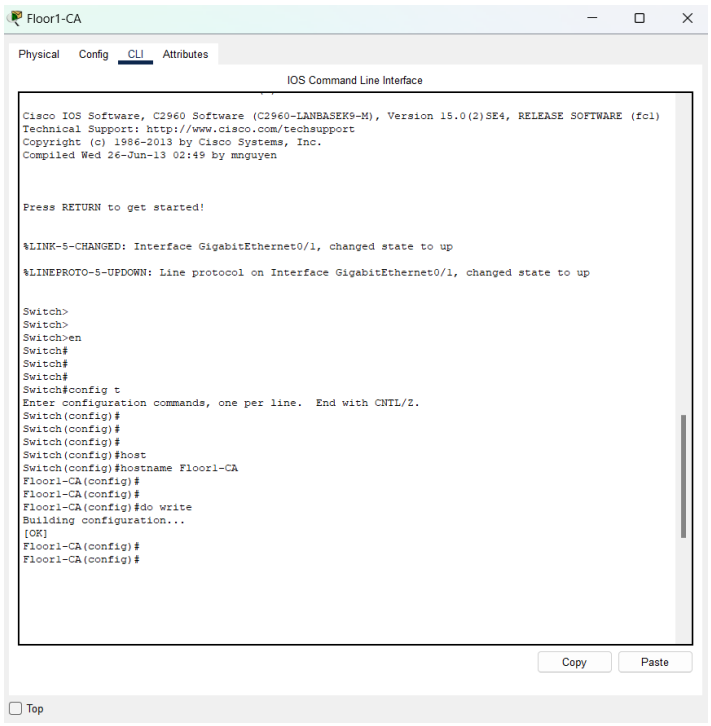


Figure 34 Switch 1 name

- This picture shows how to enter a name for switch 1.

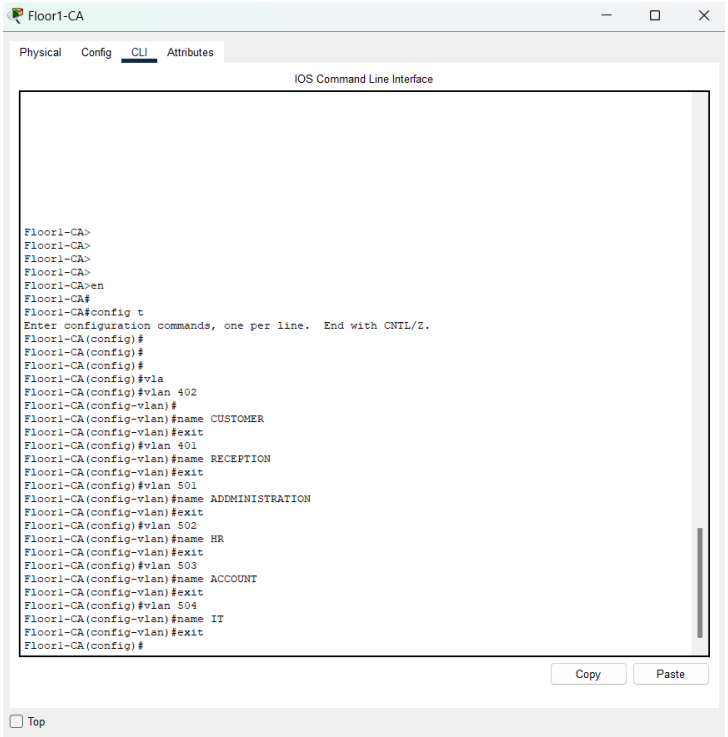


Figure 36 Switch 1 VLAN

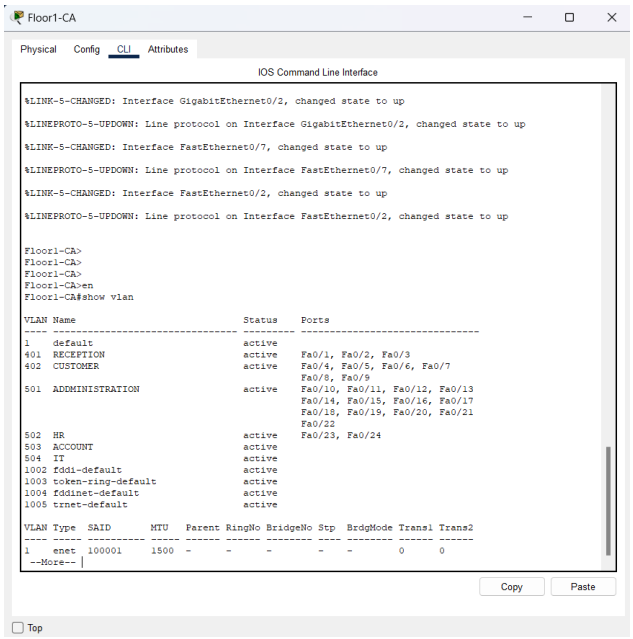


Figure 35 Switch1 Show VLAN

- This picture shows how VLAN and PCs are connected for switch 1.

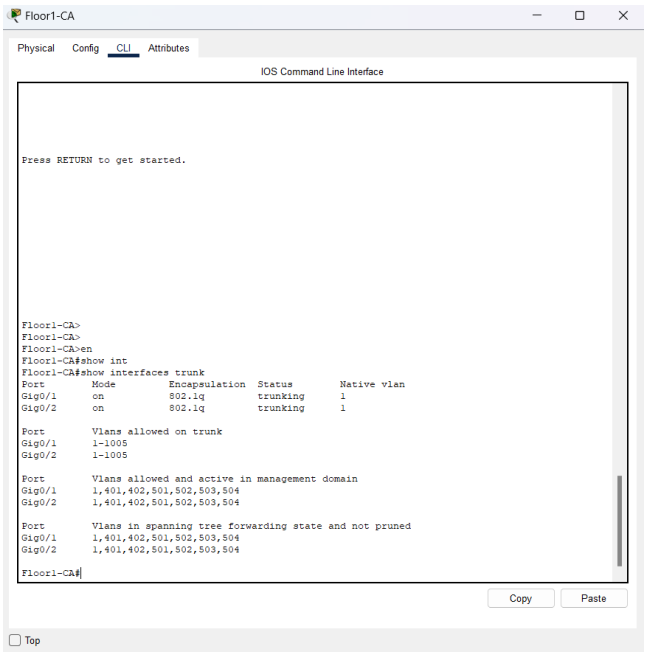


Figure 37 Trunk port switch 3

- This picture shows how switch 1 is trunked.

Floor2-AD switch

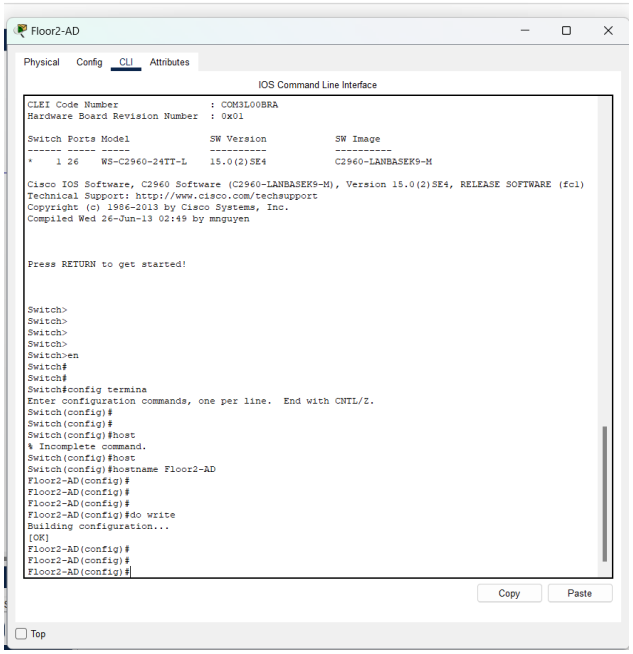


Figure 38 Switch 2 name

- This picture shows how to enter a name for switch 2.

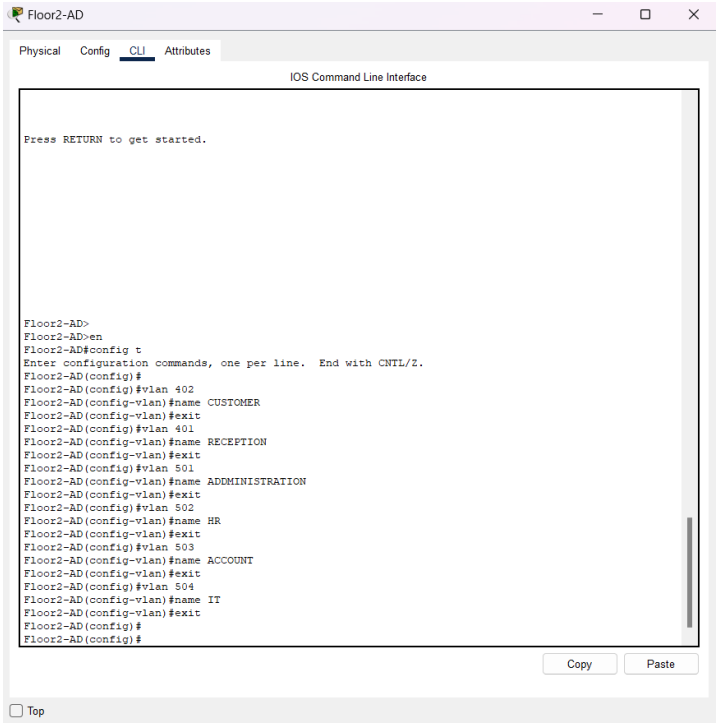


Figure 40 Switch 2 VLAN

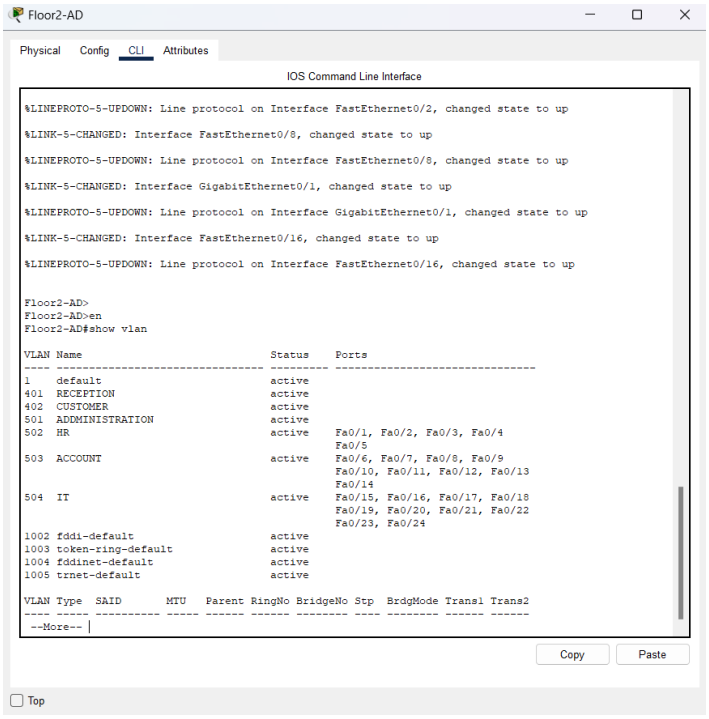


Figure 39 Switch 2 Show VLAN

- This picture shows how VLAN and PCs are connected for switch 2.

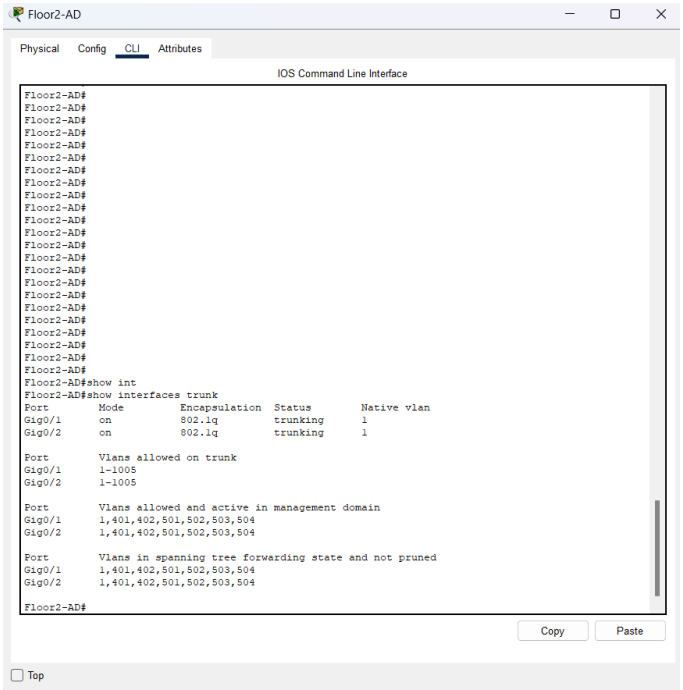


Figure 41 Switch 2 trunk

- This picture shows how switch 2 is trunked.

Floor2-HR switch

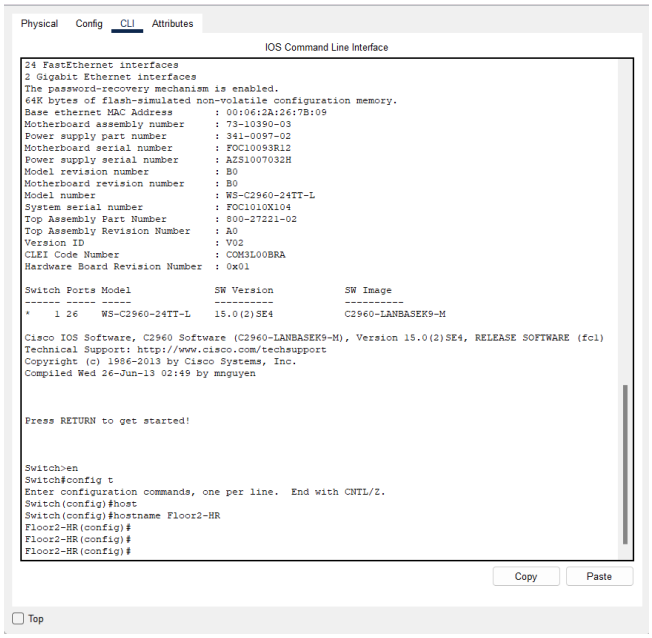


Figure 42 Switch 3 name

- This picture shows how to enter a name for switch 3.

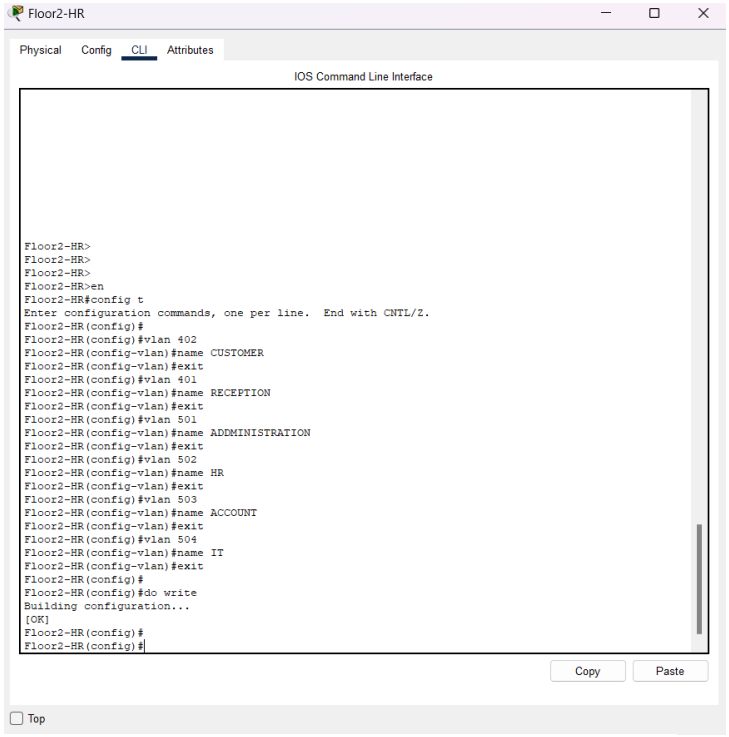


Figure 44 VLAN in Switch 3

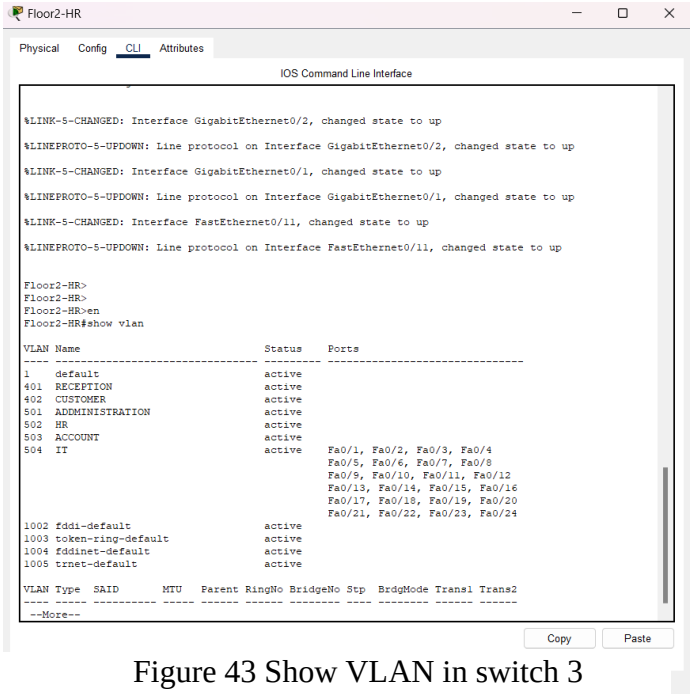


Figure 43 Show VLAN in switch 3

- This picture shows how VLAN and PCs are connected for switch 3.

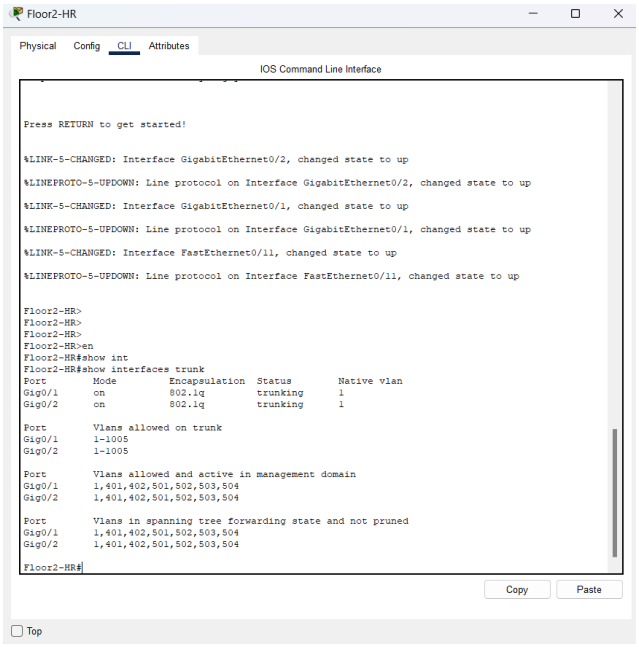


Figure 45 Trunk switch 3

- This picture shows how switch 3 is trunked.

Floor2-IT switch 4

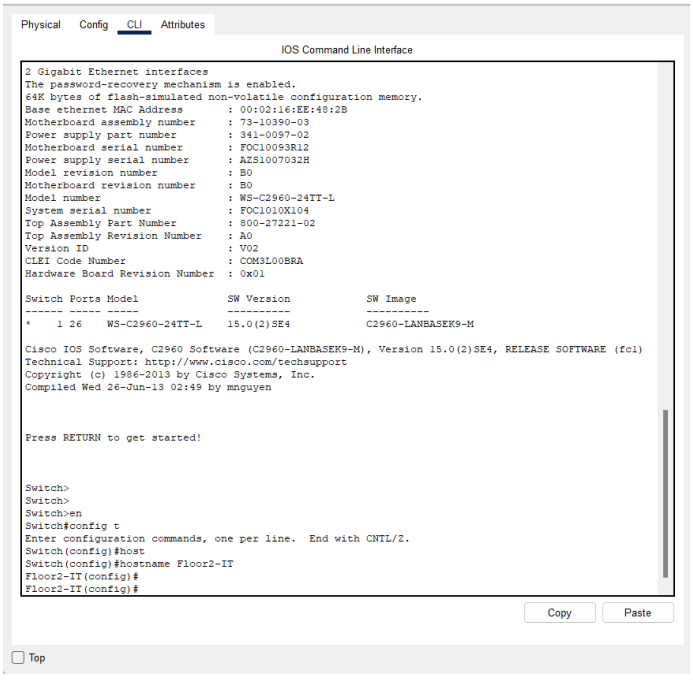


Figure 46 Switch 4 name

- This picture shows how to enter a name for switch 3.

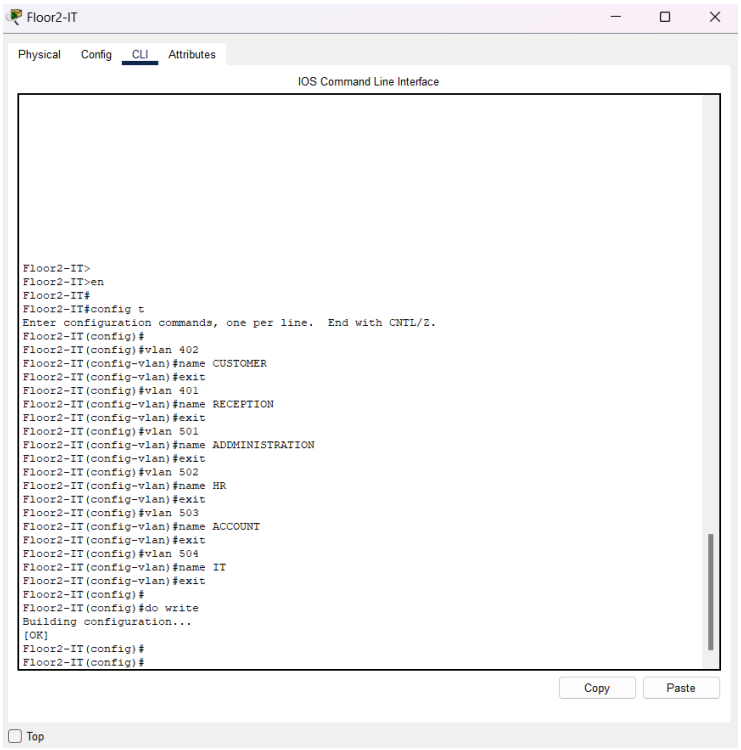


Figure 48 VLAN in switch 4

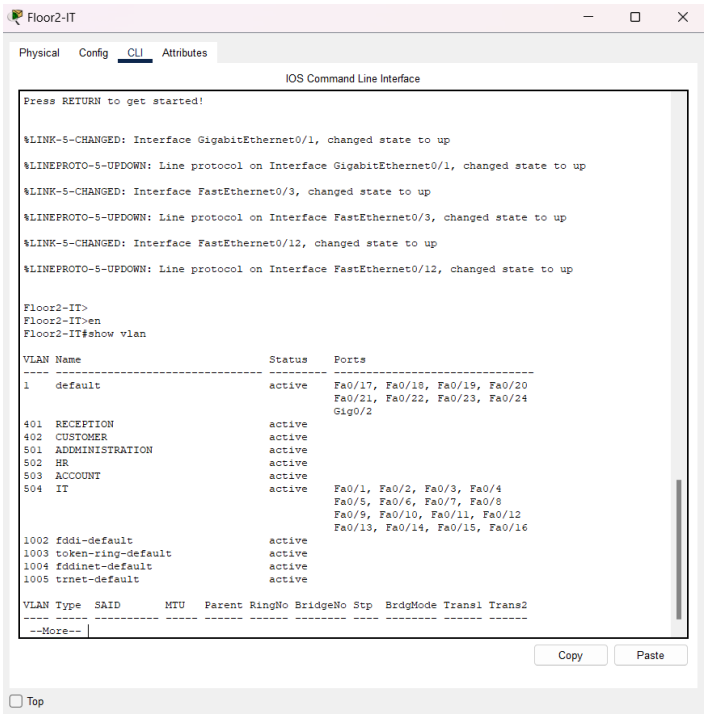


Figure 47 Show VLAN switch 4

- This picture shows how VLAN and PCs are connected for switch 4.

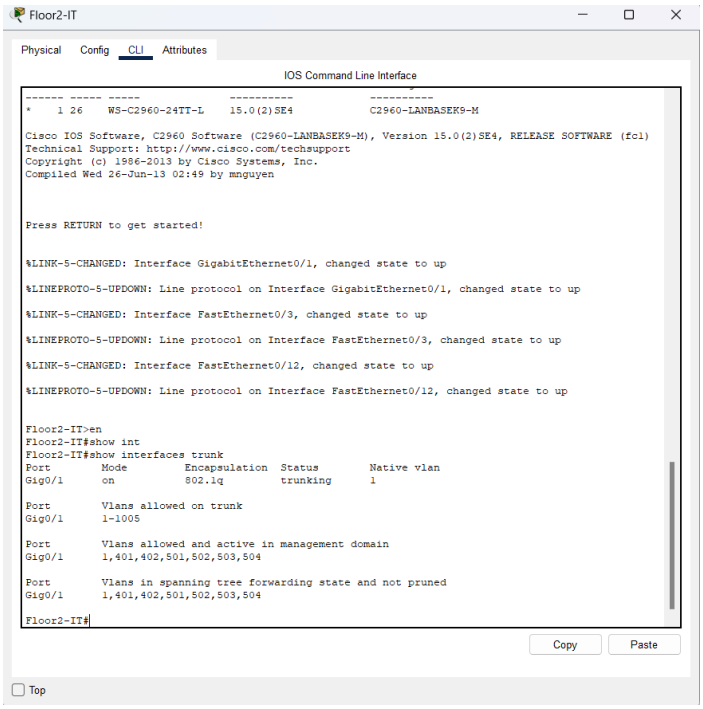


Figure 49 Switch 4 trunk

- This picture shows how switch 4 is trunked.

MGW-Router

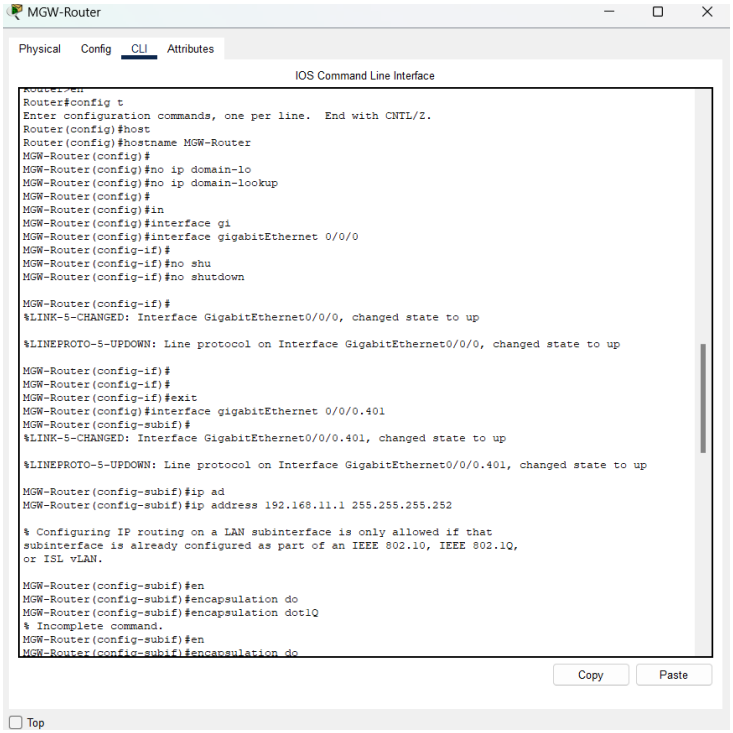


Figure 50 Router name

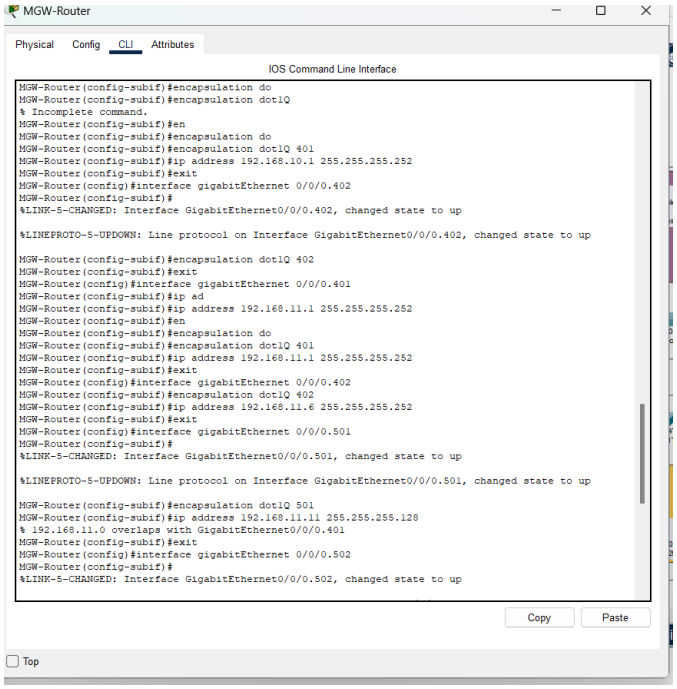


Figure 51 Router IP address

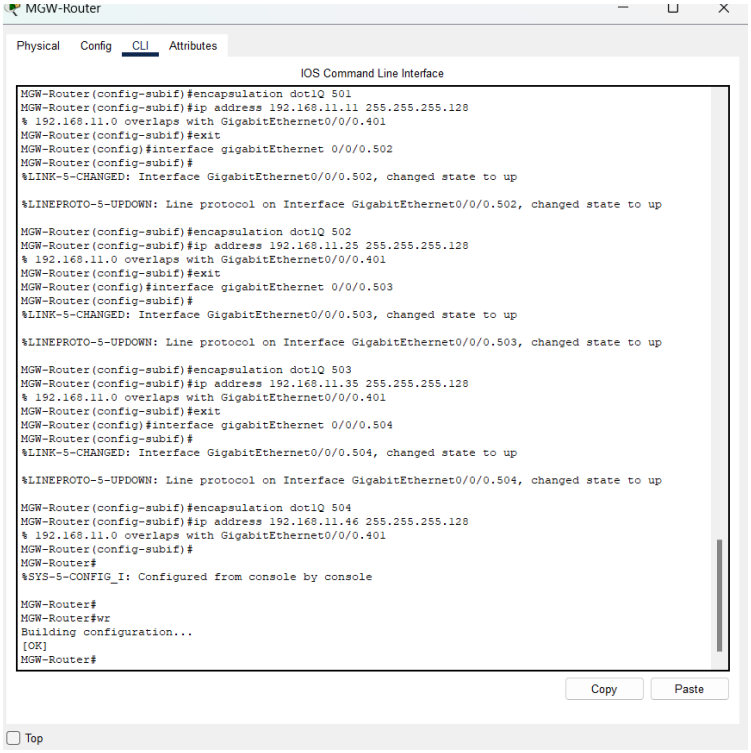


Figure 52 Router IP address

- These pictures show the hostname of the router and the IP address of the VLANs.

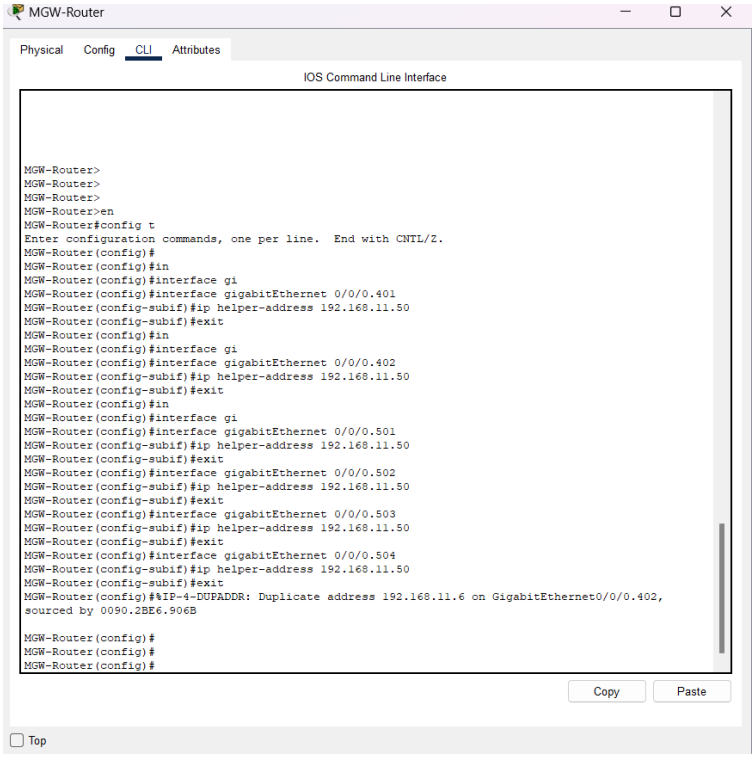


Figure 53 Router IP helper address

- This picture shows how to apply IP helper-address to the router after connecting the DHCP server.

DHCP-M sever

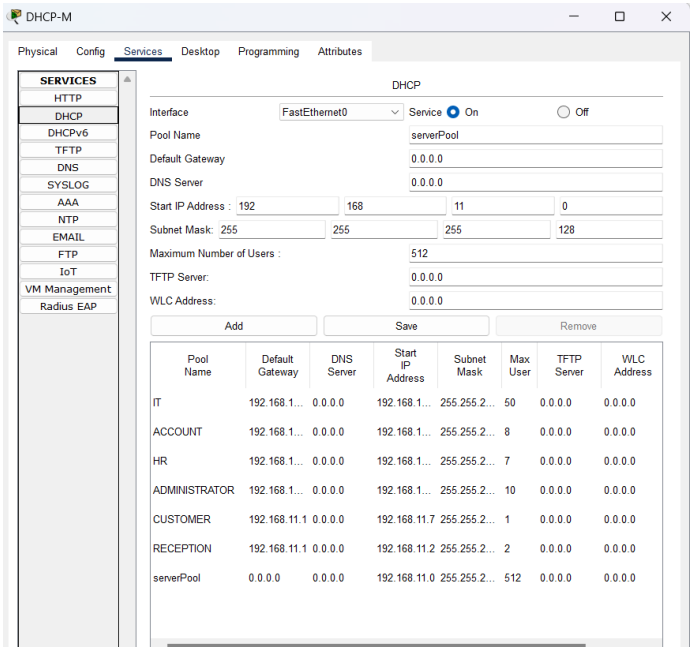


Figure 54 DHCP sever

- This picture shows how to connect the DHCP server.

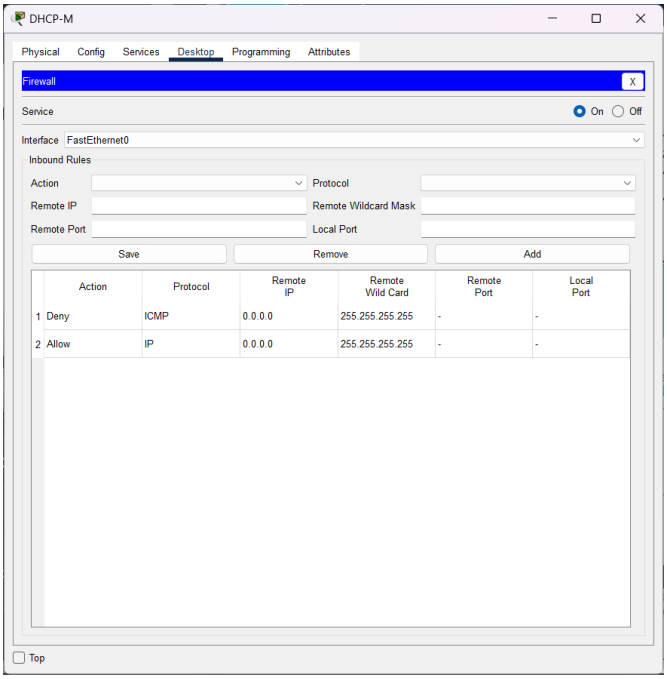


Figure 55 Firewall in DHCP sever

- This picture shows how the firewall of the Matara branch is connected through the DHCP server.

Below is the network diagram of Alliance Health's Colombo branch.

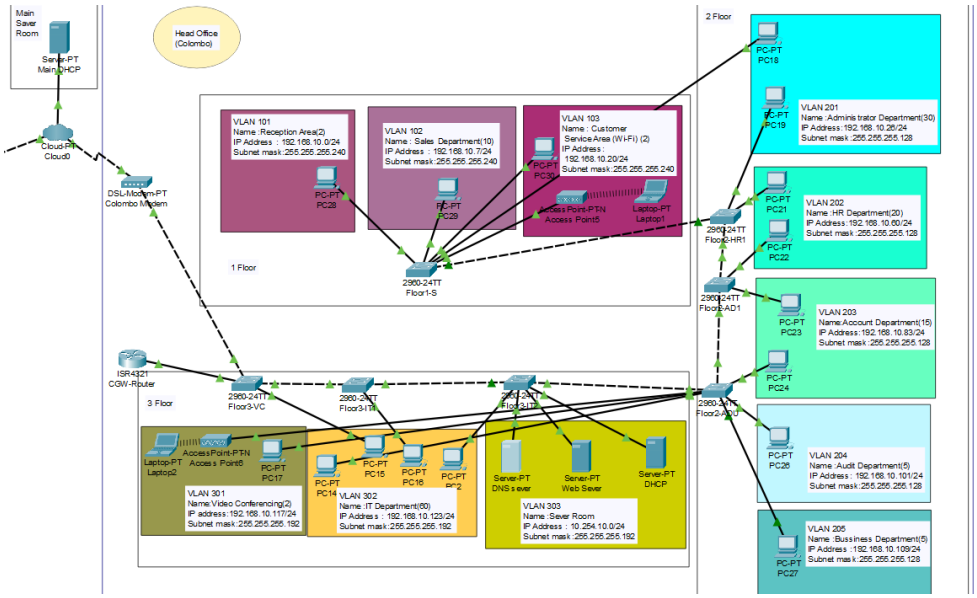


Figure 56 Network diagram of Alliance Health's Colombo branch

- In this case, I had to connect 4 switches, a router, DNS server, WEB server and DHCP server. Their settings are shown below.

Floor1-S

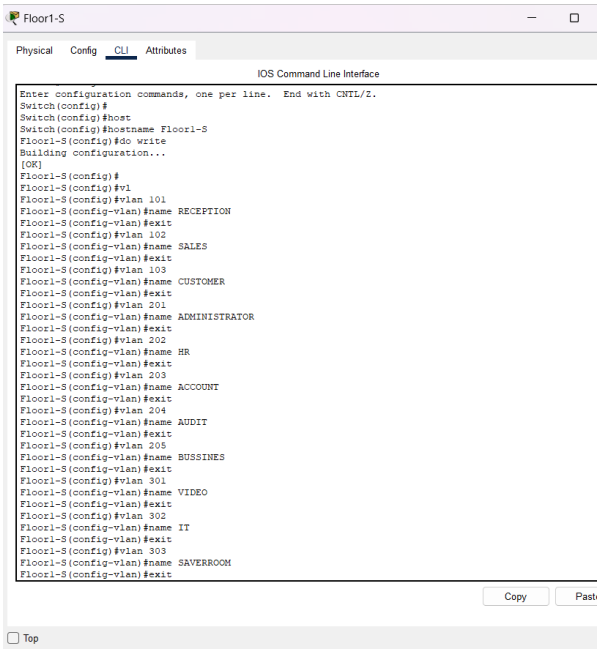


Figure 58 Switch 1 configurations Colombo

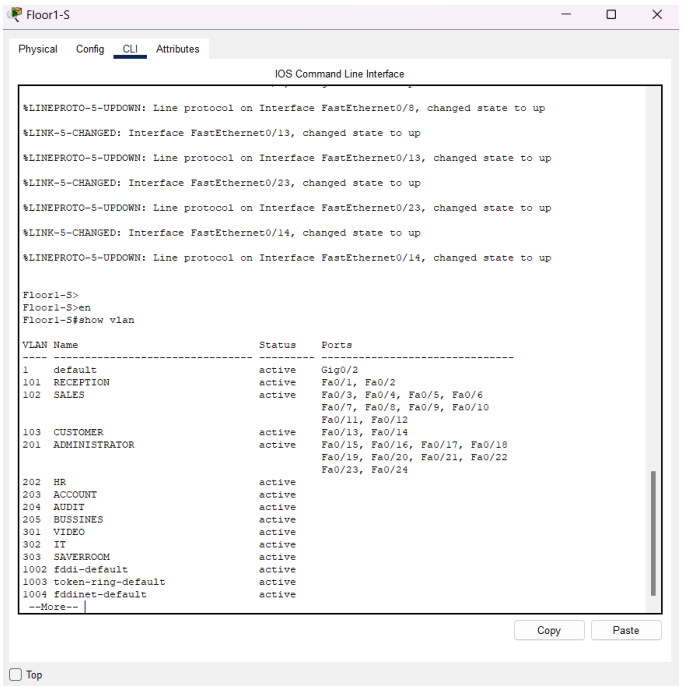


Figure 57 switch1 VLANs Colombo

- This picture shows how switch1's hostname, PCs and VLAN are connected.

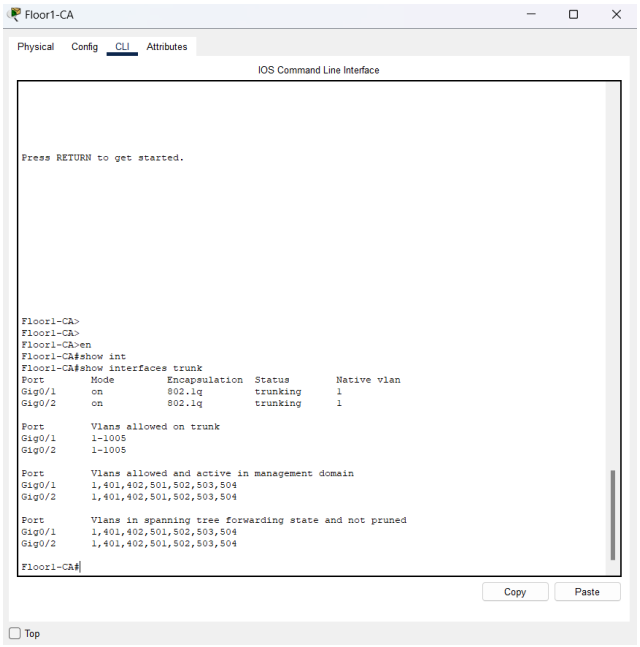


Figure 59 Switch 1 trunk

- This picture shows how switch 1 is trunked.

Floor2-HR1

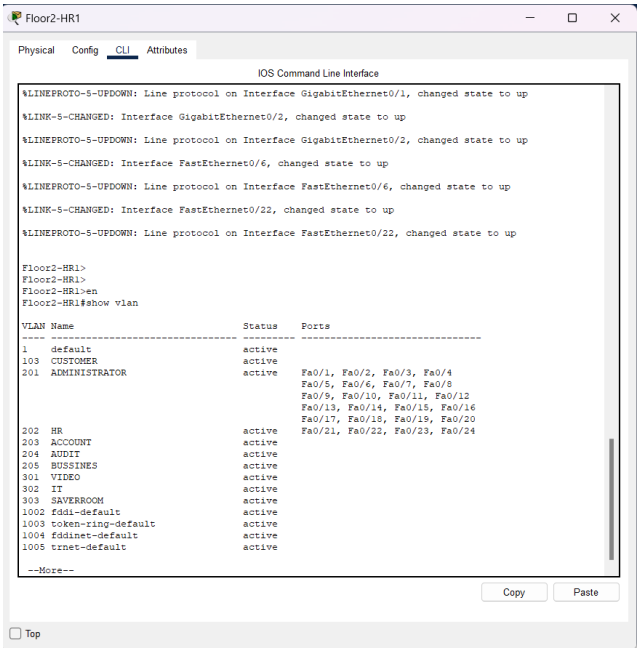


Figure 60 configuration switch2 Colombo

- This picture shows how switch2's hostname, PCs and VLAN are connected.

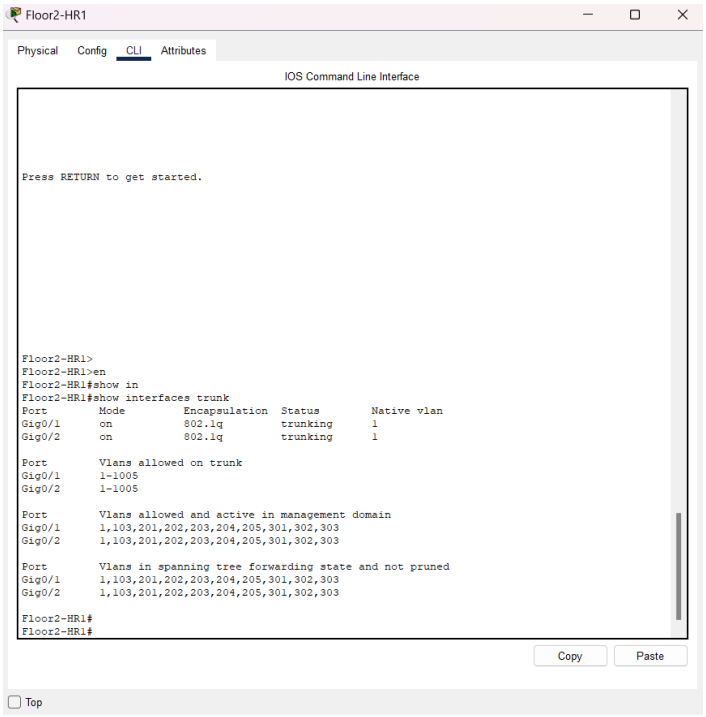


Figure 61 switch2 trunk

- This picture shows how switch 2 is trunked.

Floor2-AD1

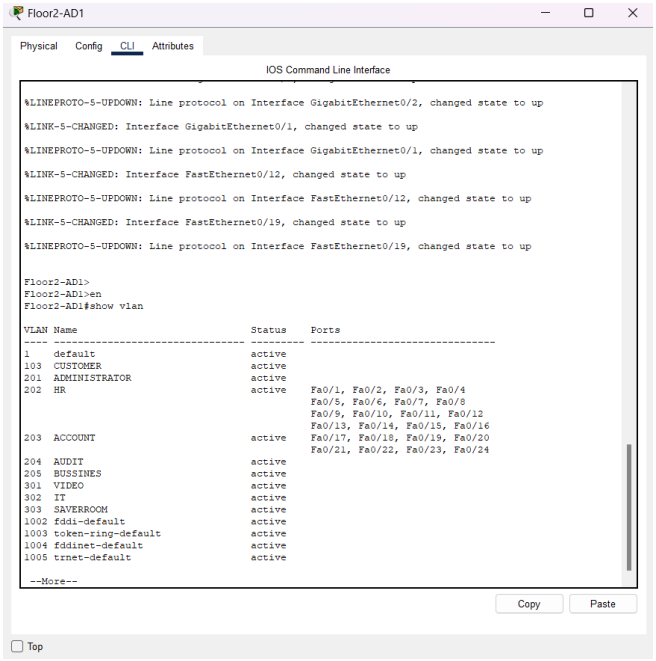


Figure 62 switch3 configuration Colombo

- This picture shows how switch3’s hostname, PCs and VLAN are connected.

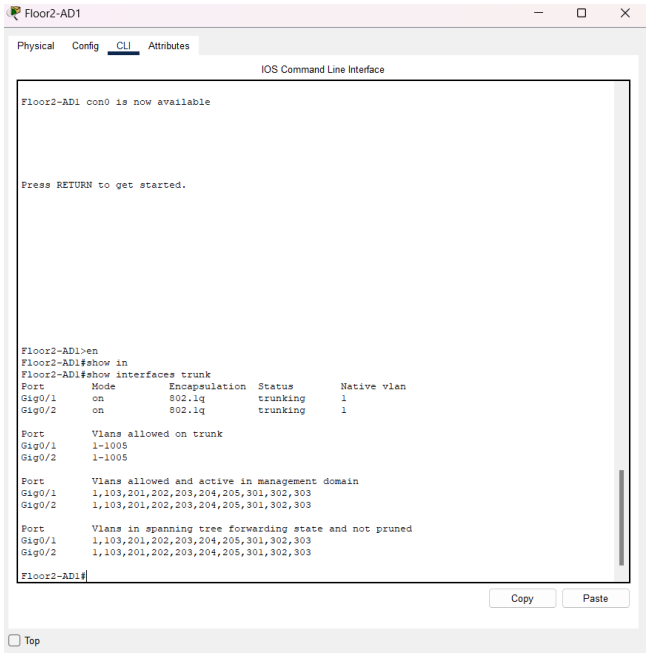


Figure 63 switch3 trunk

- This picture shows how switch 3 is trunked.

Floor2-ADU

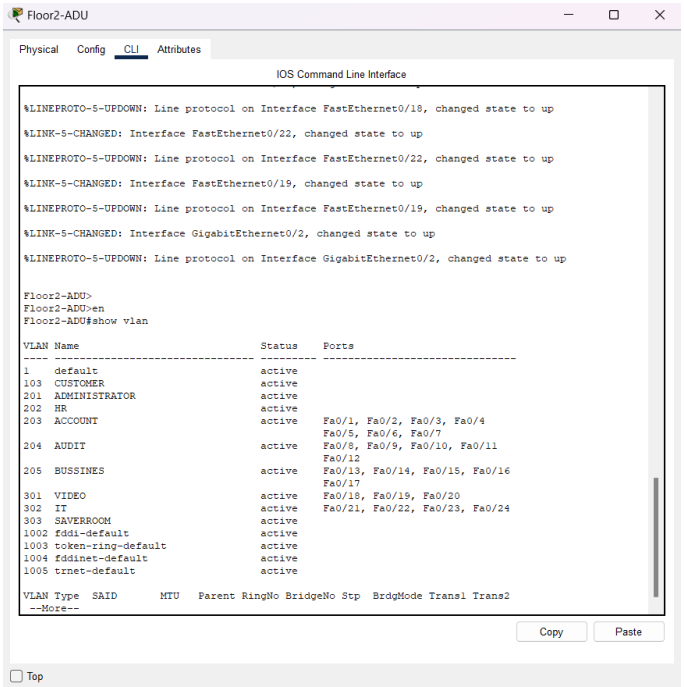


Figure 64 switch 4 configurations Colombo

- This picture shows how switch4’s hostname, PCs and VLAN are connected.

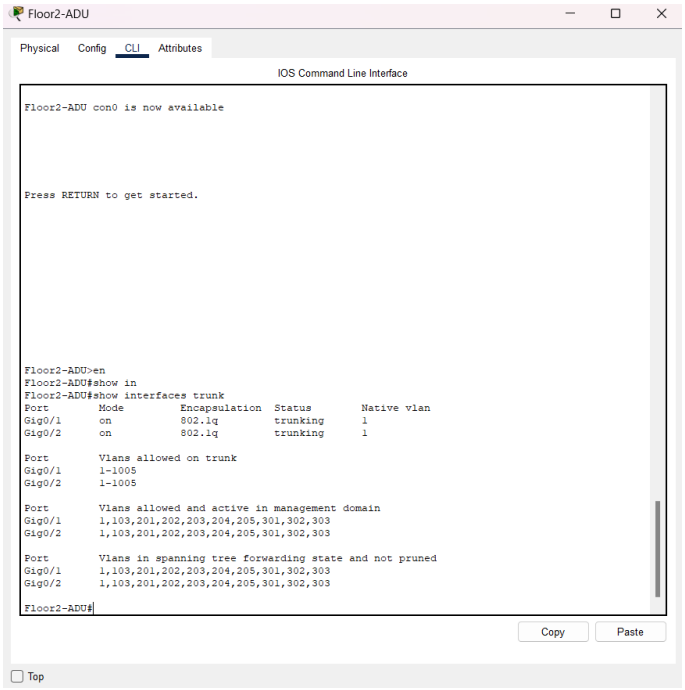


Figure 65 switch4 trunk

- This picture shows how switch 4 is trunked.

Floor3-IT1

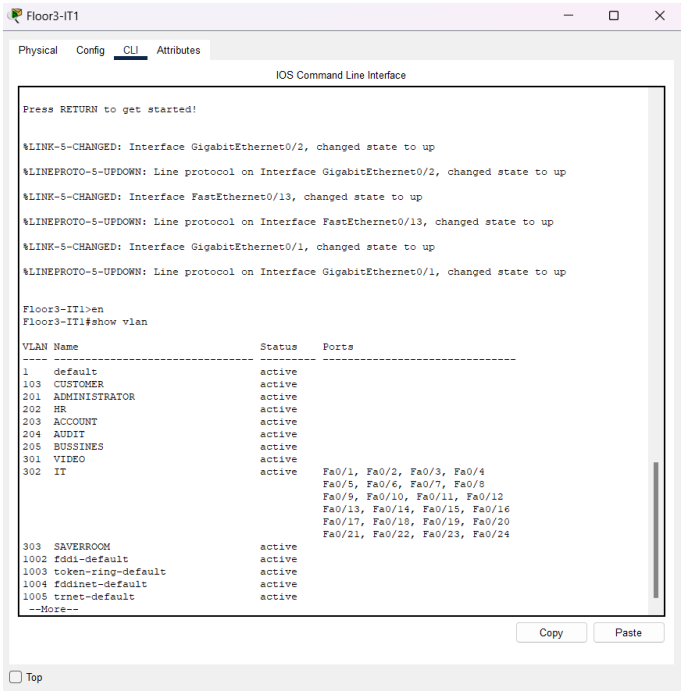


Figure 66 switch 5 configuration Colombo

- This picture shows how switch5's hostname, PCs and VLAN are connected**.**

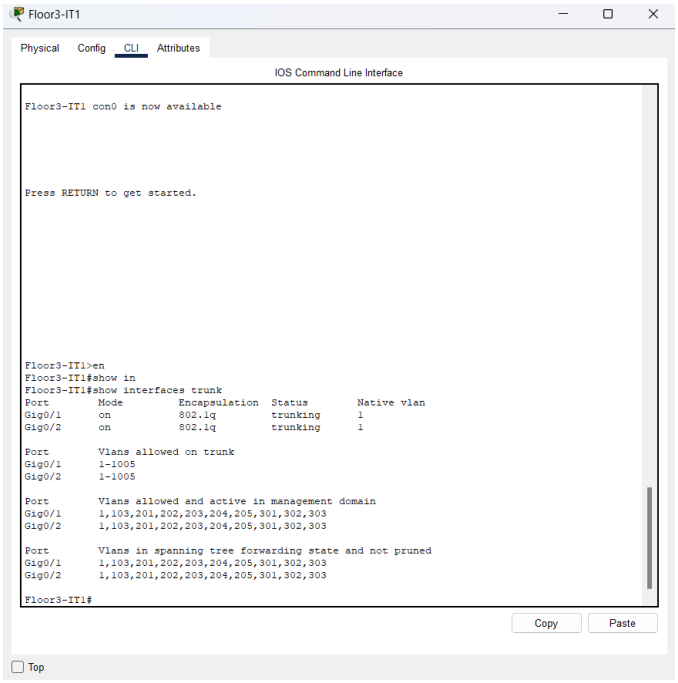


Figure 67 switch5 trunk

- This picture shows how switch 5 is trunked.

Floor3-IT2

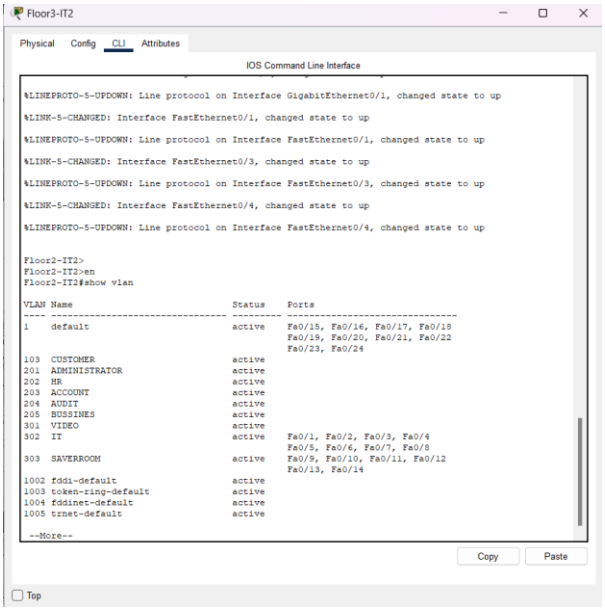


Figure 68 switch 6 configurations

- This picture shows how switch6's hostname, PCs and VLAN are connected.

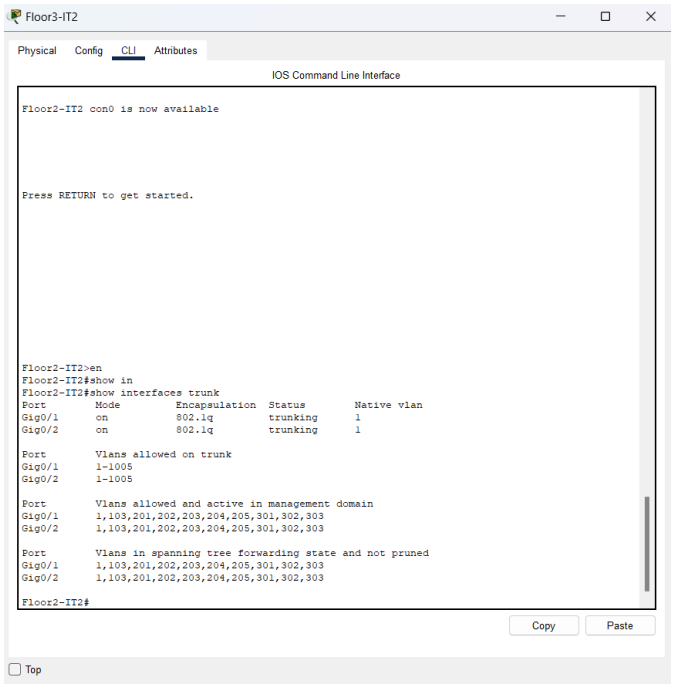


Figure 69 switch6 trunk

- This picture shows how switch 6 is trunked.

Floor3-VC

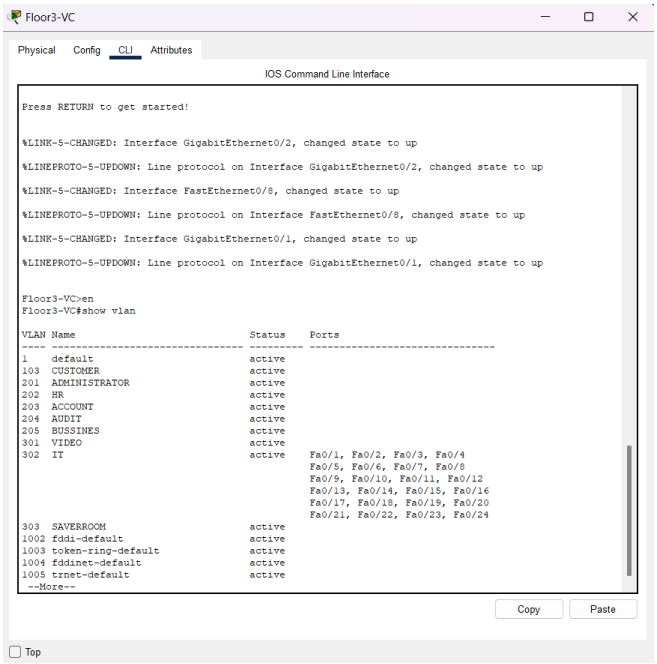


Figure 70 switch 7 configuration Colombo

- This picture shows how switch7's hostname, PCs and VLAN are connected.

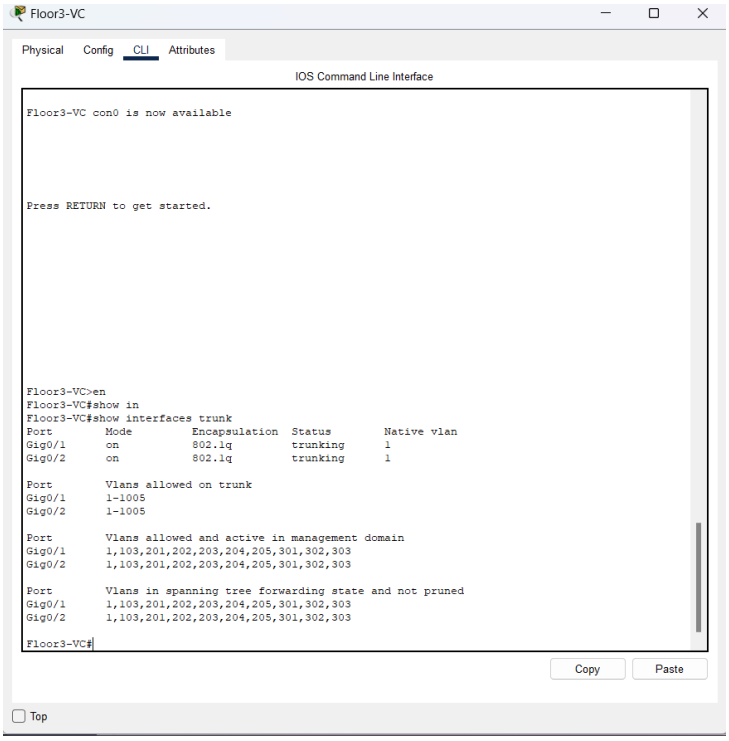


Figure 71 switch7 trunk

- This picture shows how switch 7 is trunked.

CGW-Router

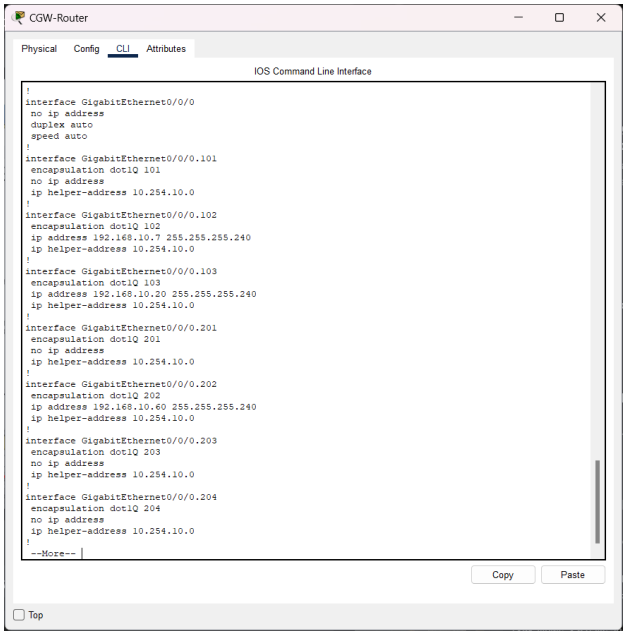


Figure 72 router configuration 1

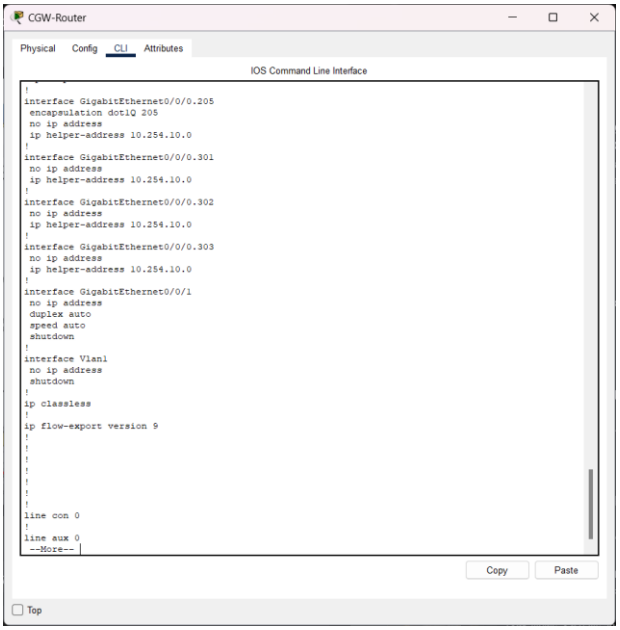


Figure 73 router configuration 2

- These images show how to apply the IP address, hostname and IP address to the router after connecting the DHCP server.

DHCP sever

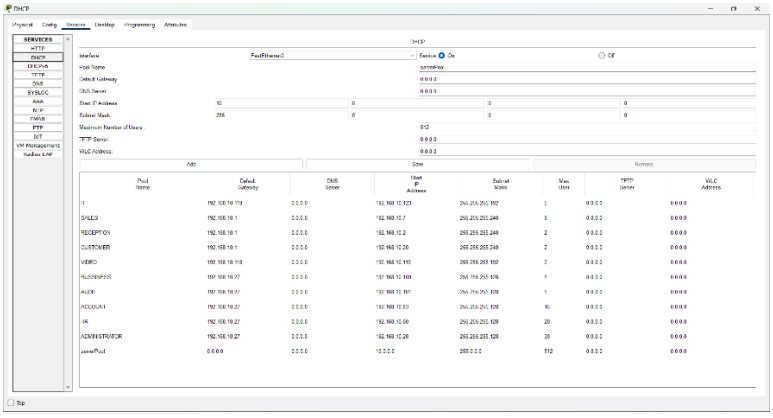


Figure 74 DHCP sever Colombo

- This picture shows how to connect the DHCP server.

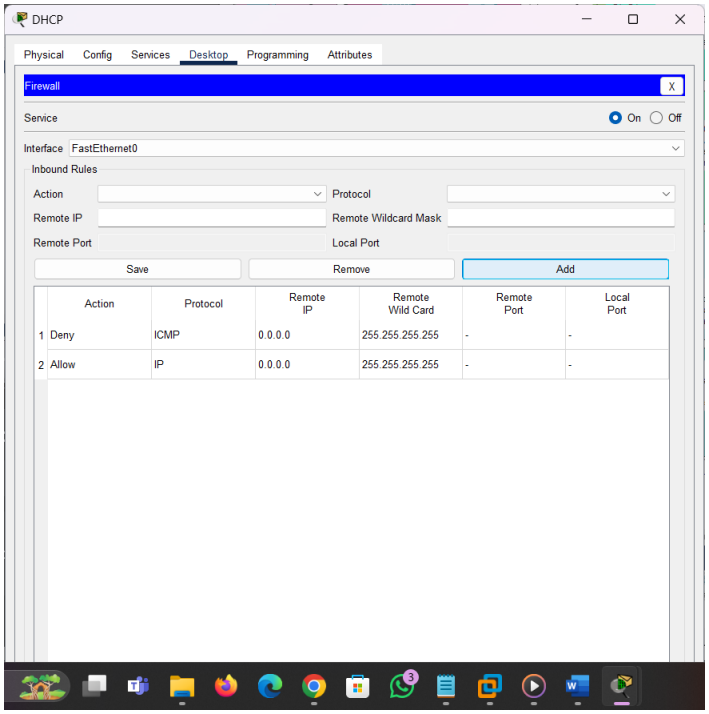


Figure 75

- This picture shows how the firewall of the Colombo branch is connected through the DHCP server.

DNS sever

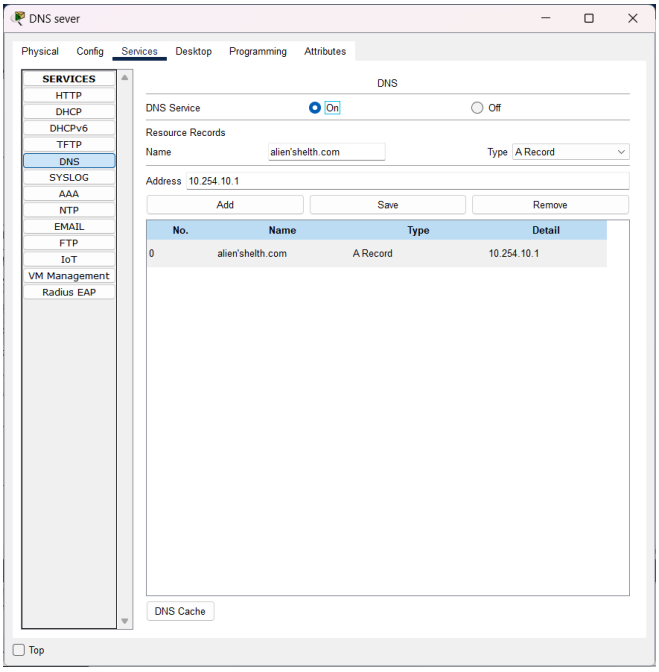


Figure 76 DNS sever Colombo

- This picture shows how to connect the DNS server.

WEB sever

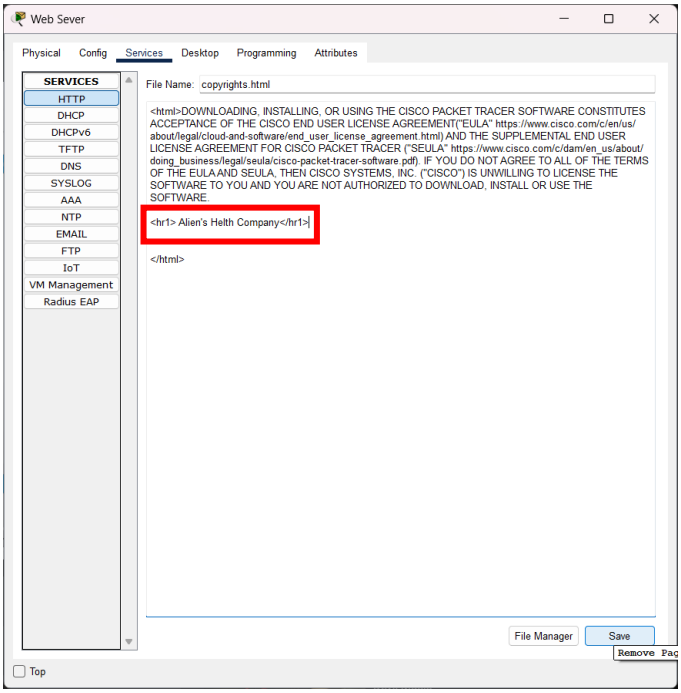


Figure 77 WEB server Colombo

- This picture shows how to connect the WEB server.

Cloud

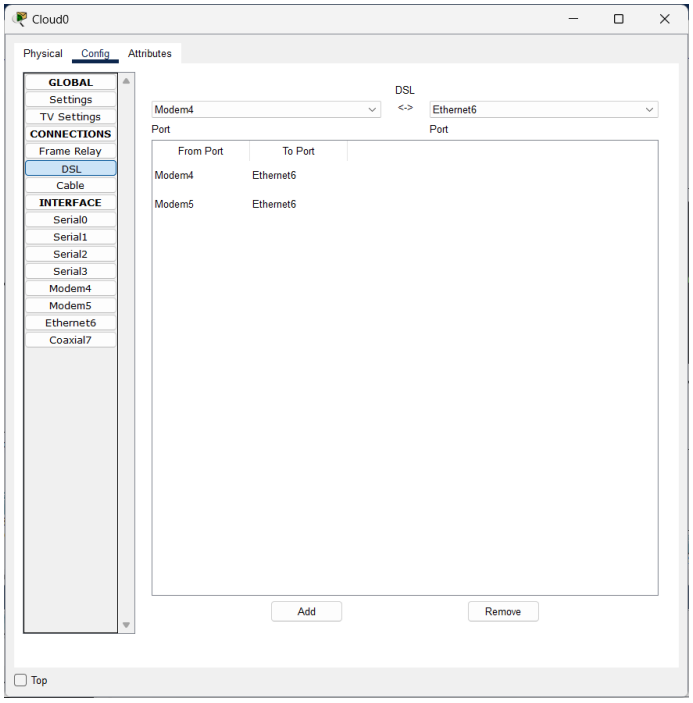


Figure 78 Cloud configuration

- This picture shows how a cloud was used to connect the two branches together. There I connected the cloud to the branches using two modems.

Main saver Room

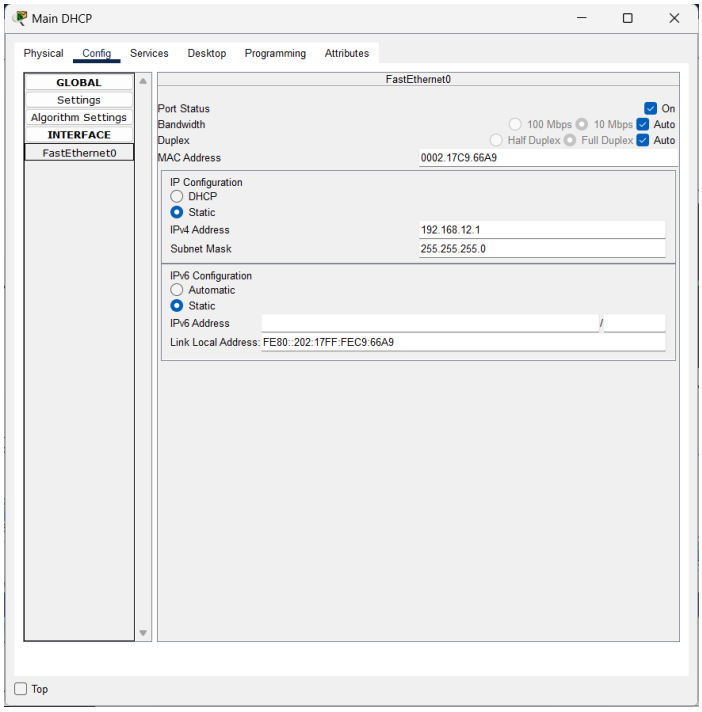


Figure 79 main saver room

- This picture shows how a server is deployed to the cloud.

Special facts

- I added two savers to Matara branch and Colombo branch. The reason for that is for convenience in adding a new device.
- I trunked the switch port to send the ping message from one department to another department.

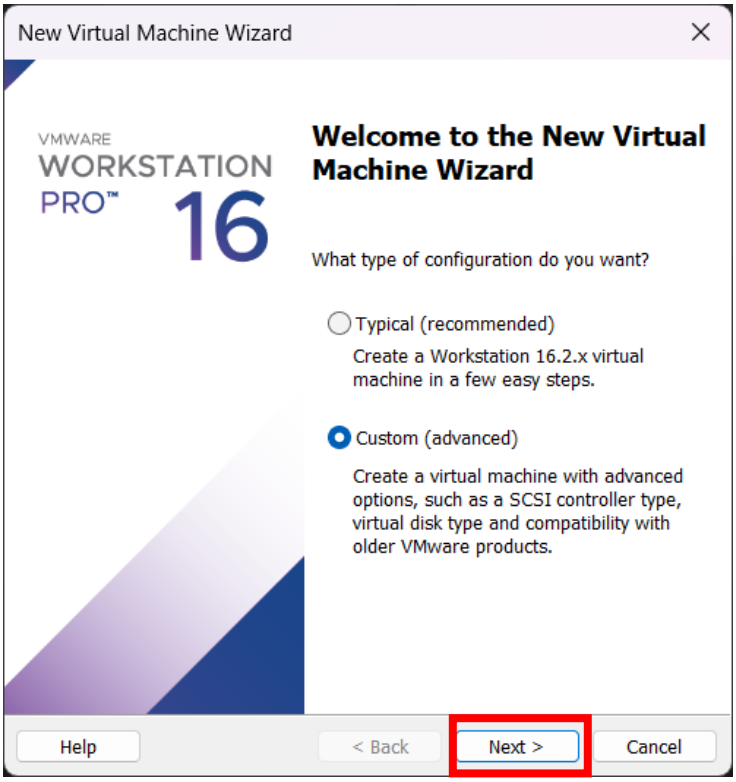


Figure 80 VMware step 1

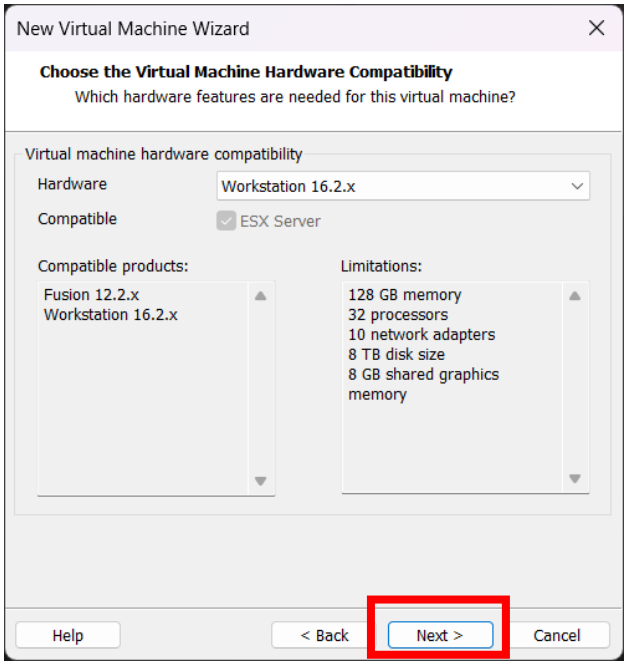


Figure 81 VMware step 2

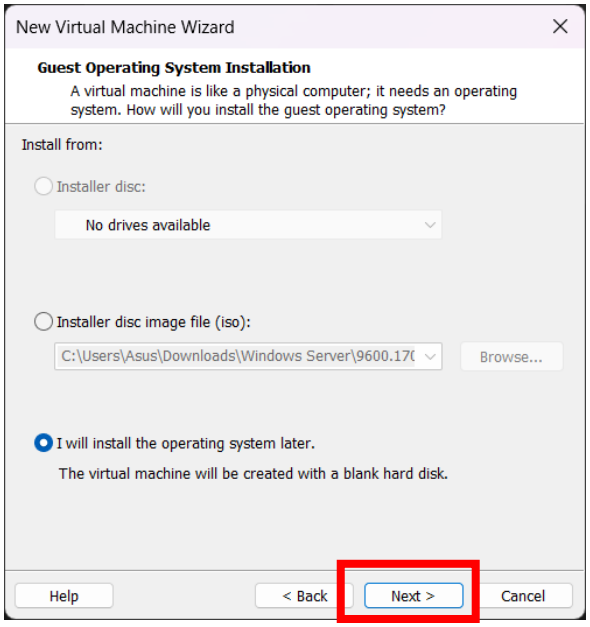


Figure 82 VMware step 3

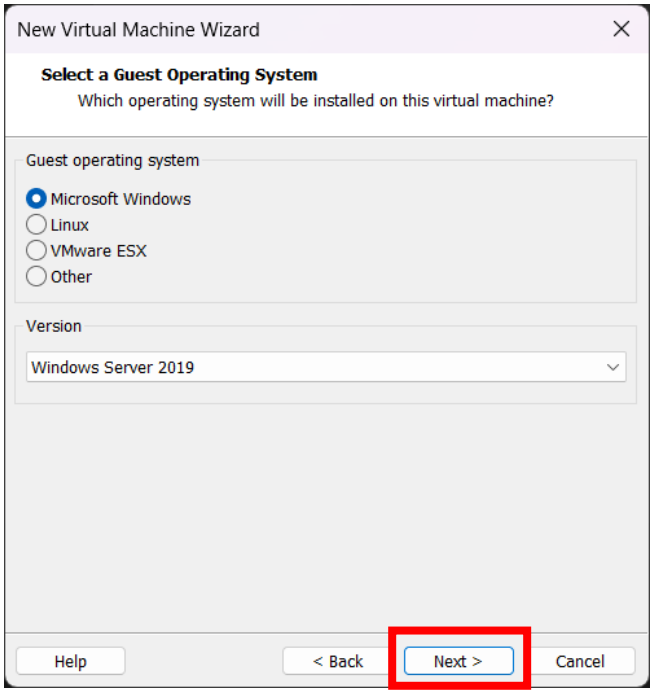


Figure 83 VMware step 4

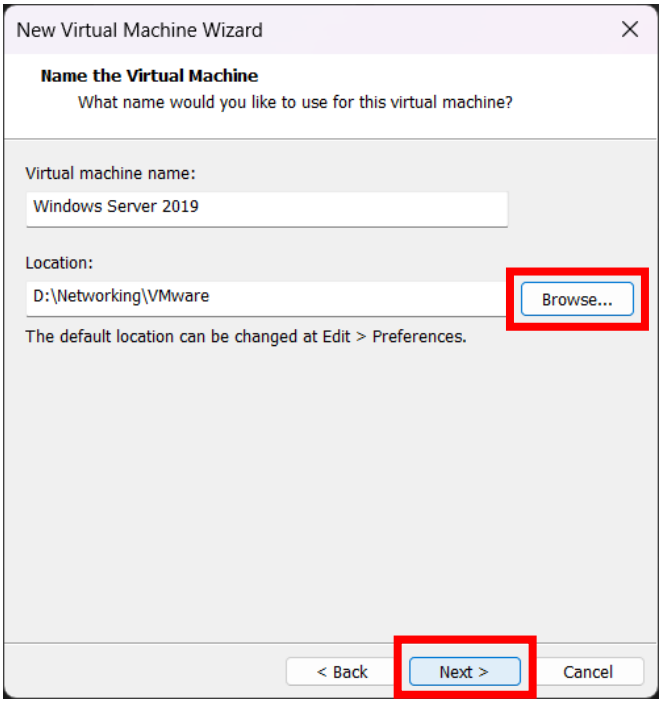


Figure 84VMware step 5

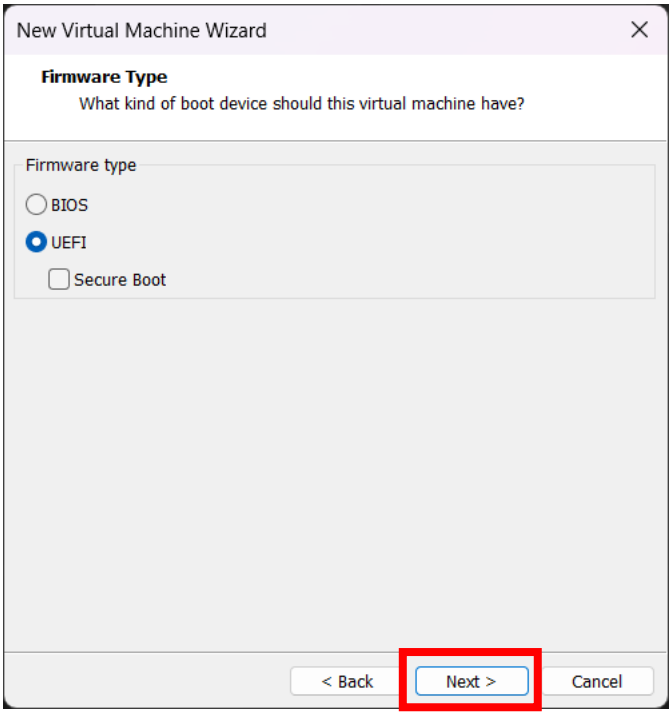


Figure 85 VMware step 6

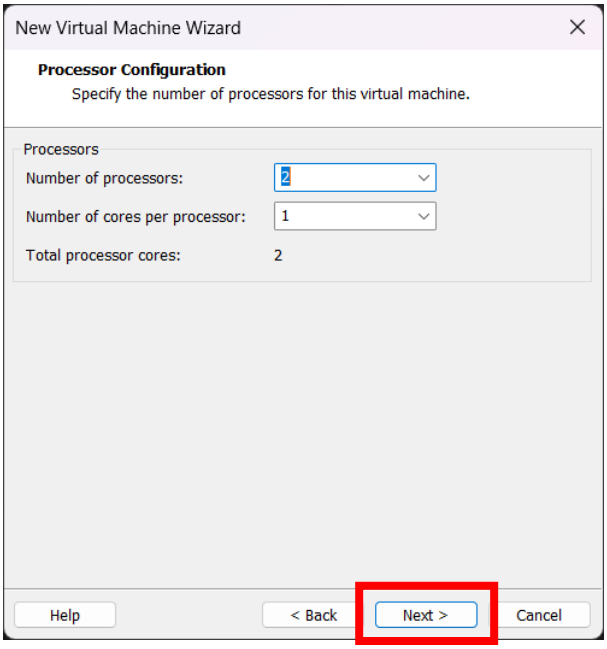


Figure 86 VMware step 7

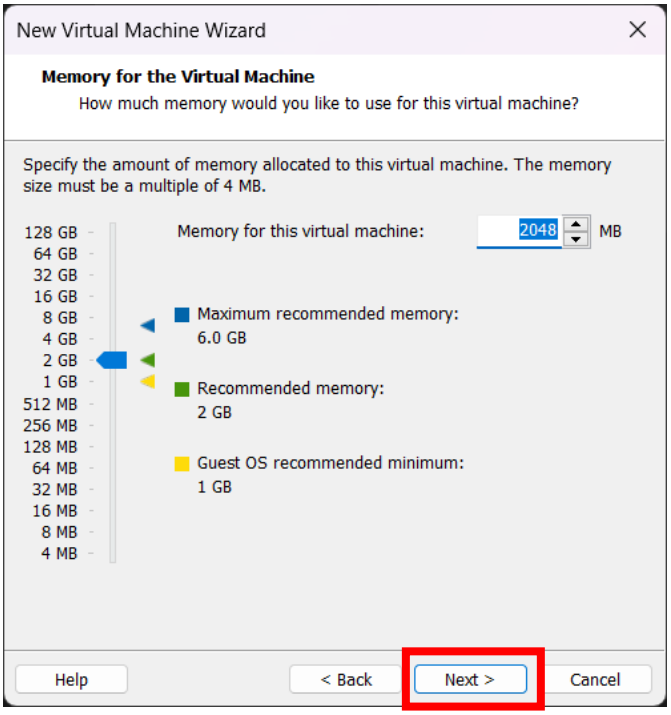


Figure 87 VMware step 8

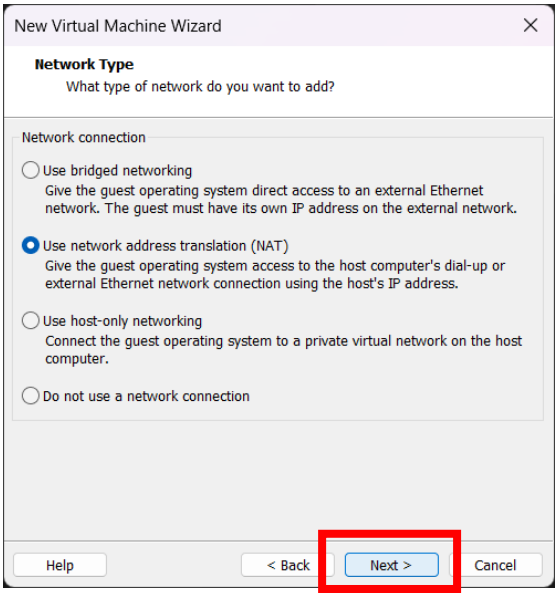


Figure 88 VMware step 9

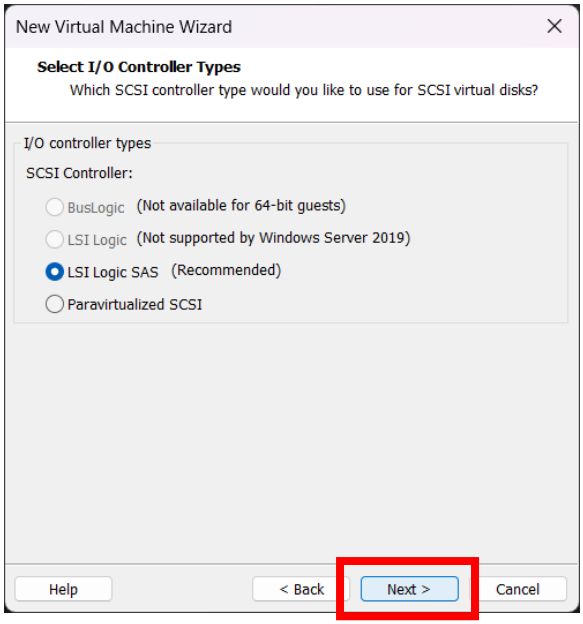


Figure 89 VMware step 10

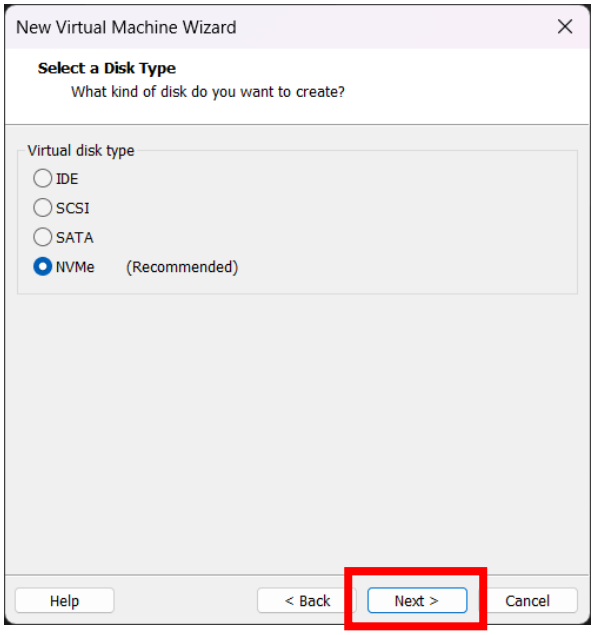


Figure 90 VMware step 11

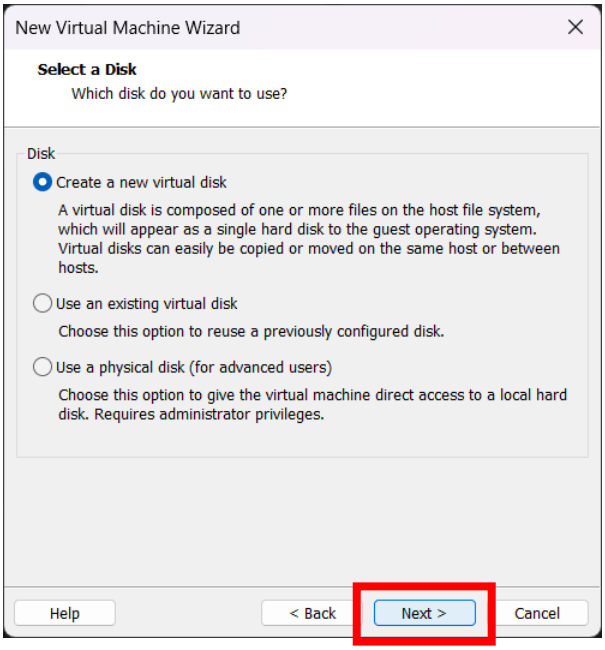


Figure 91 VMware step 12

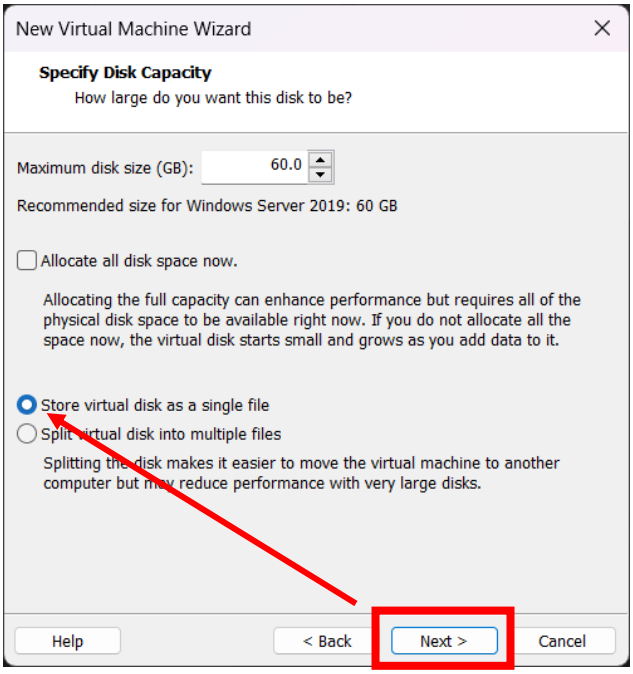


Figure 92 VMware step 13

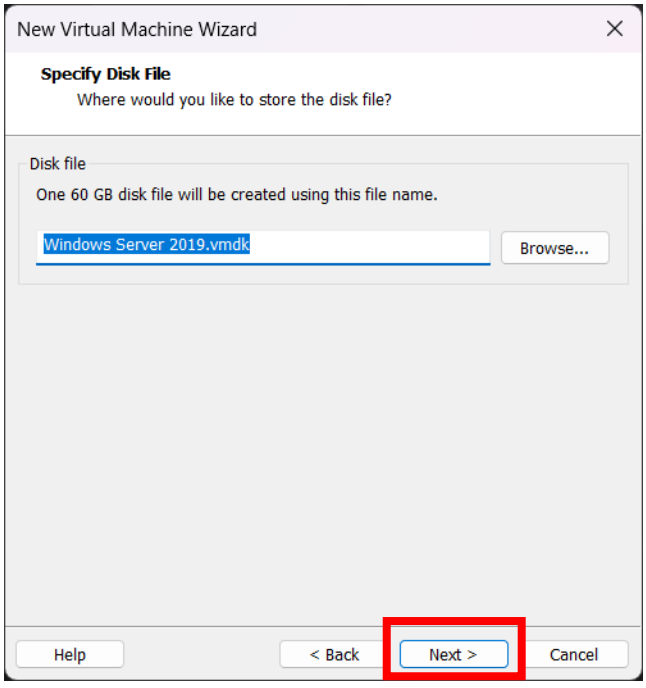


Figure 93VMware step 14

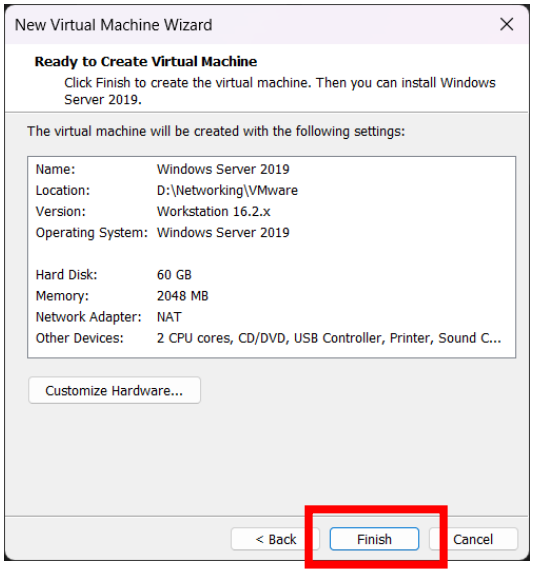


Figure 94 VMware step 15

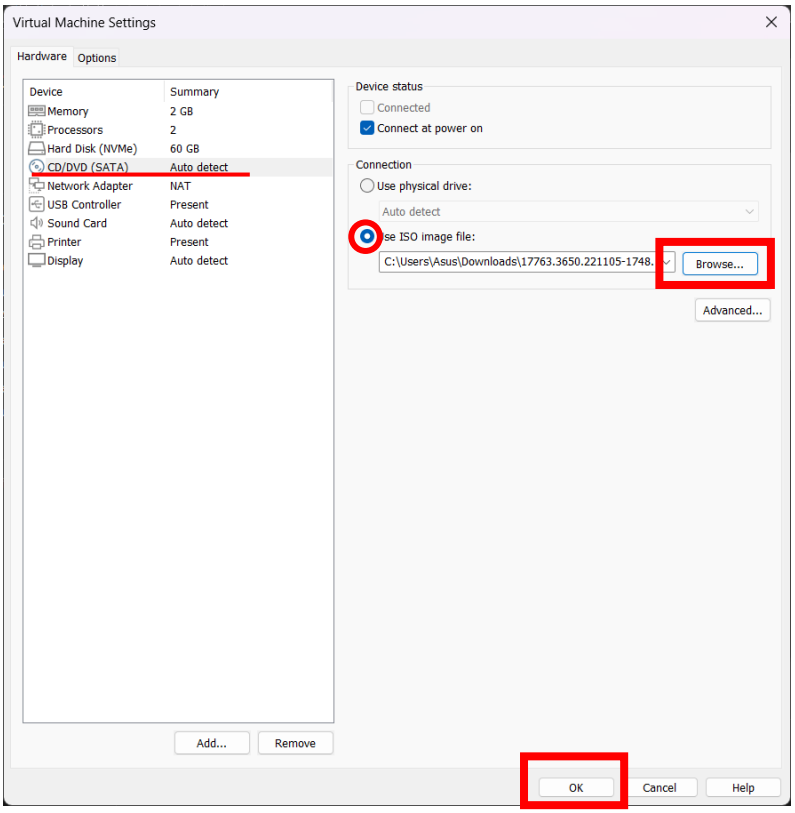


Figure 95 VMware step 16

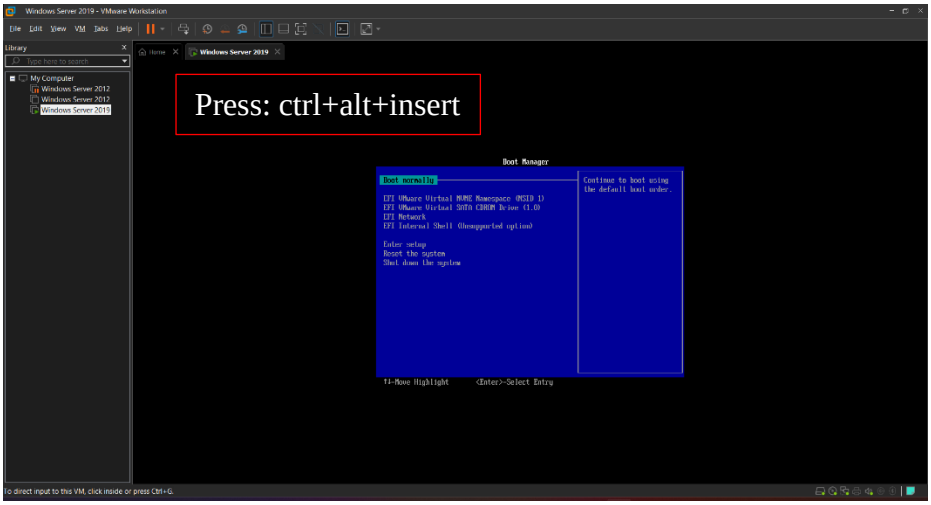


Figure 96 VMware step 17

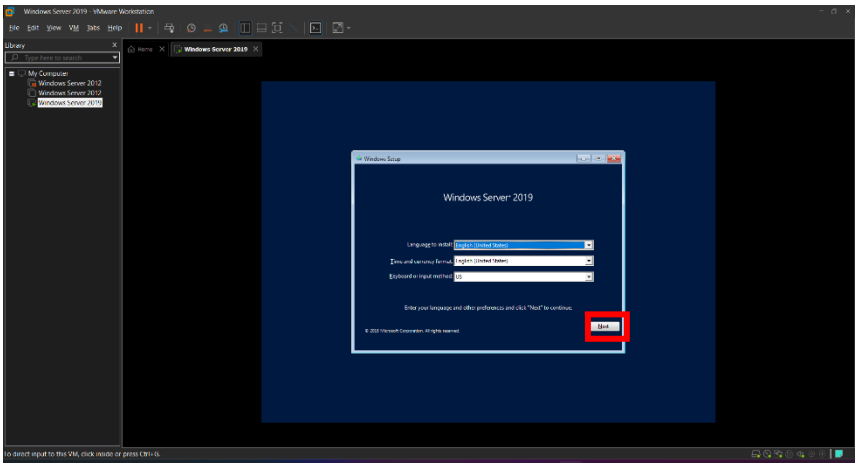


Figure 97 VMware step 18

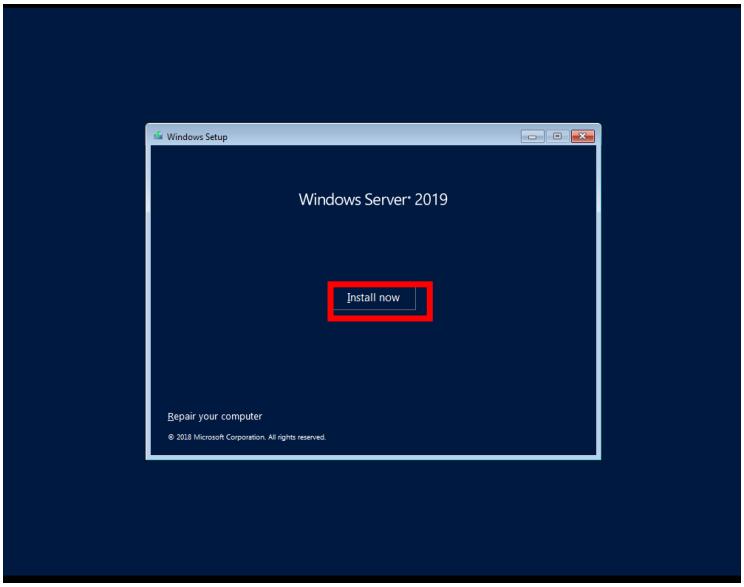


Figure 98 VMware step 19

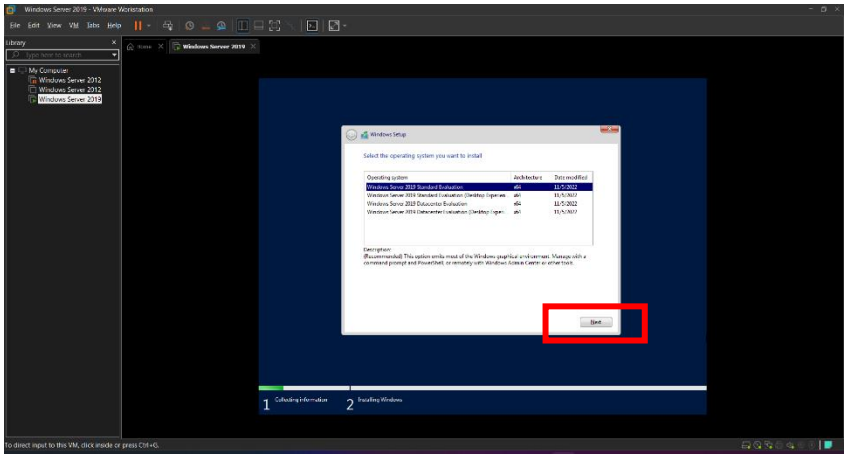


Figure 99 VMware step 20

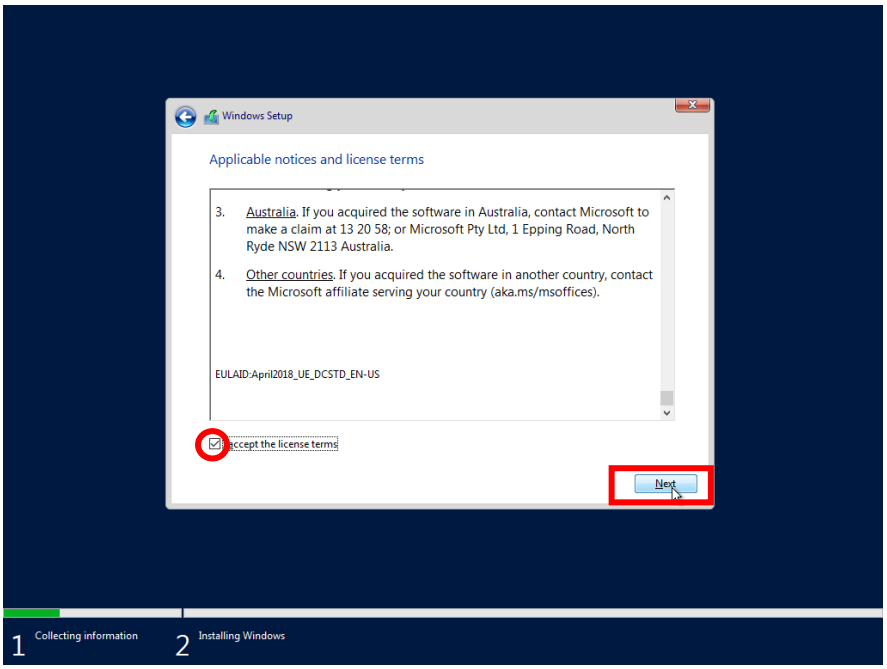


Figure 100 VMware step 21

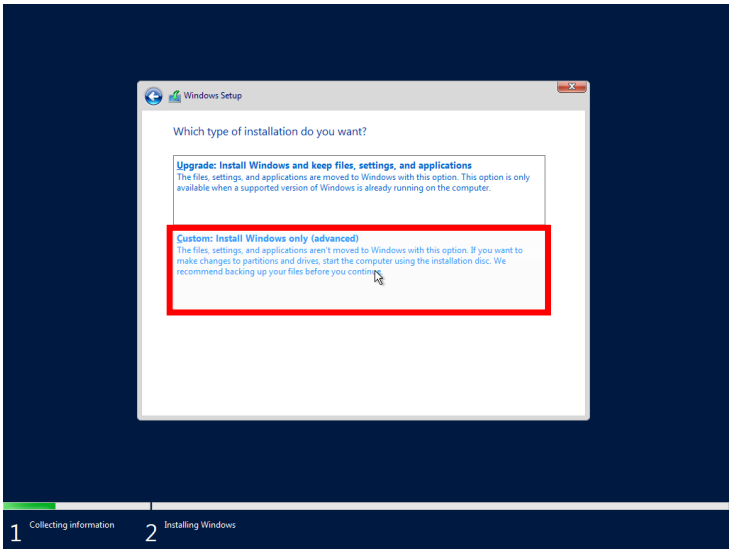


Figure 101 VMware step 22

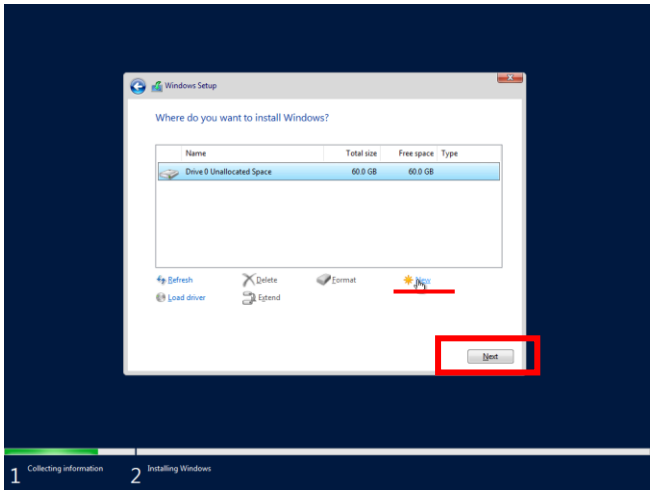


Figure 102 VMware step 23

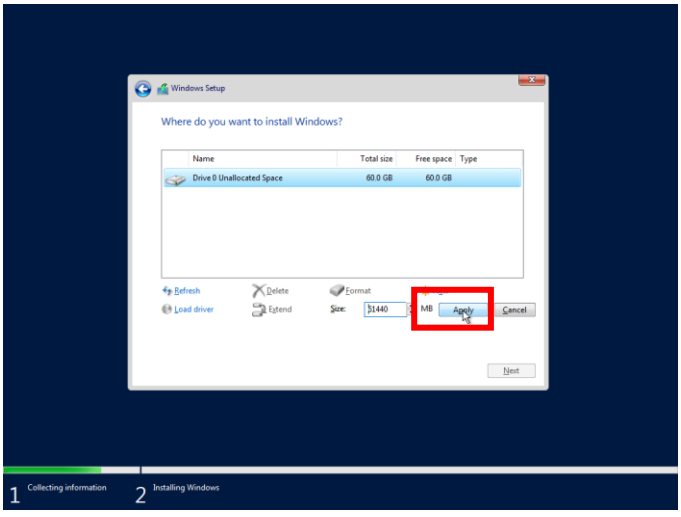


Figure 103 VMware step 24

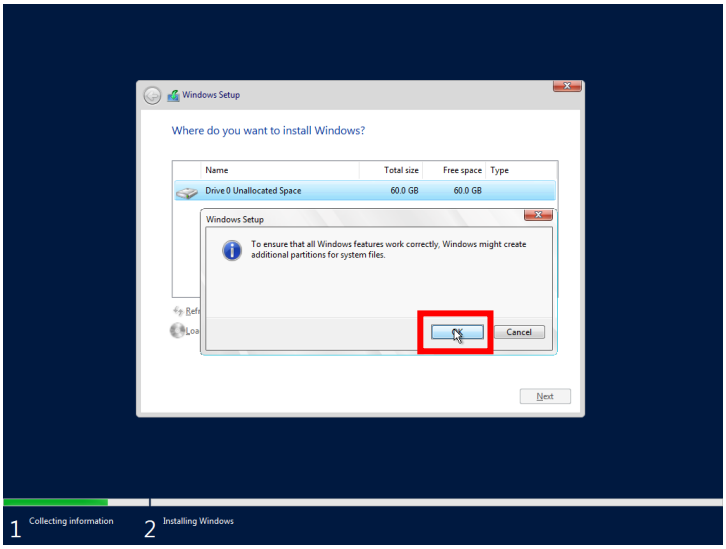


Figure 104 VMware step 25

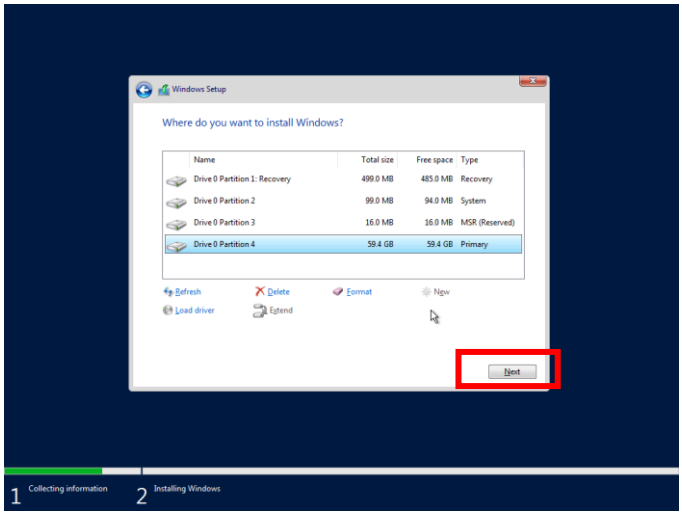


Figure 105 VMware step 26

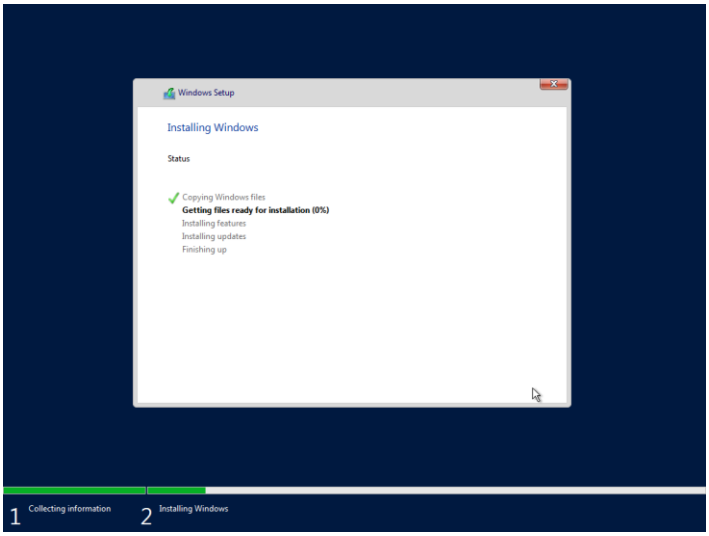


Figure 106 VMware step 27

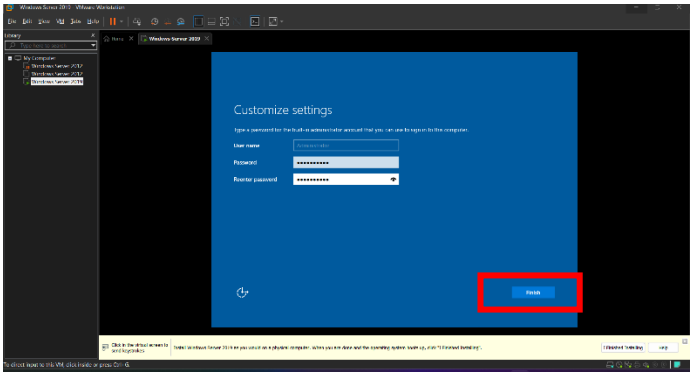


Figure 107 VMware step 28

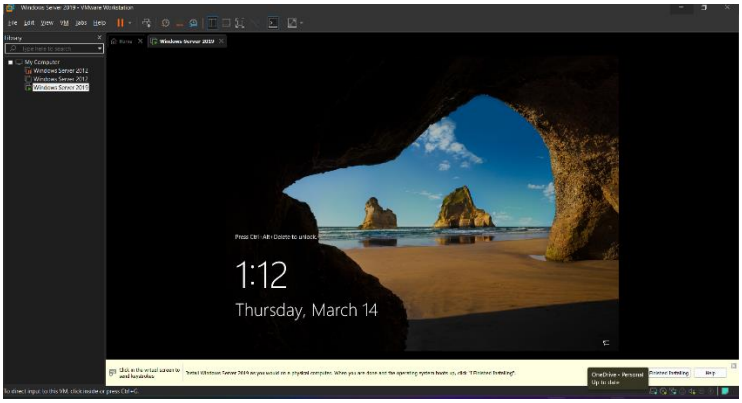


Figure 108 VMware step 29

- Here is the tools installation of VMware.

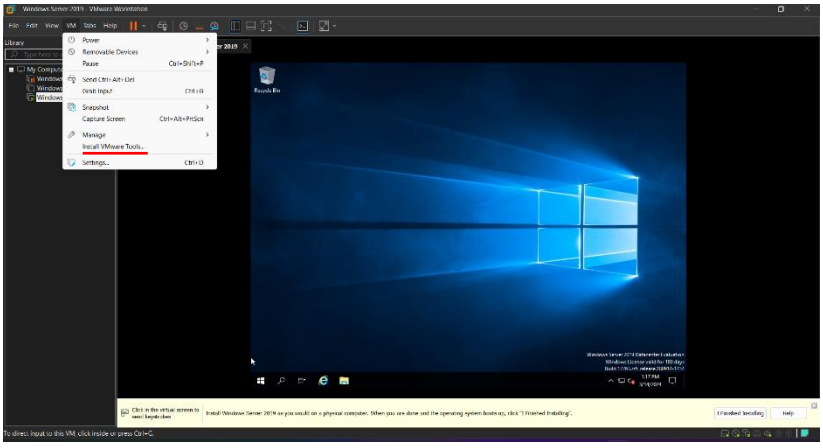


Figure 109 VMware step 30

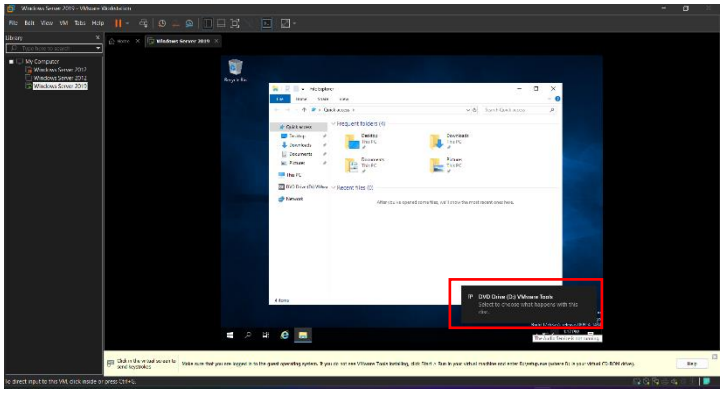


Figure 110 VMware step 31

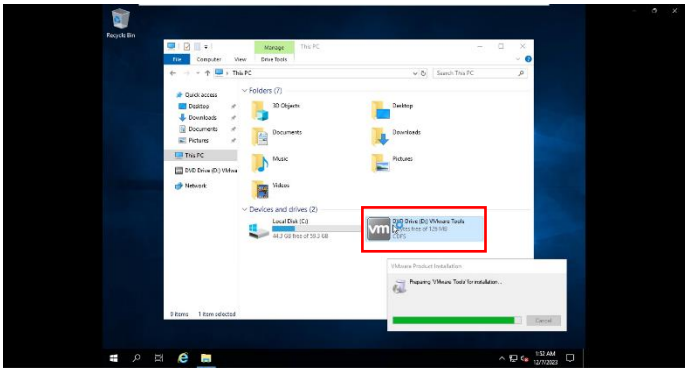


Figure 111 VMware step 32

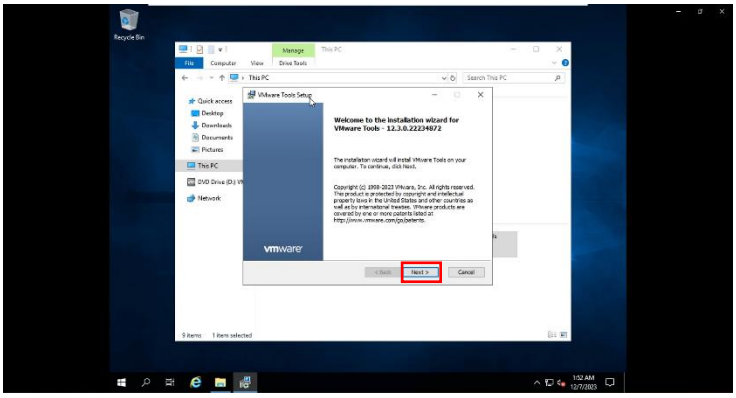


Figure 112 VMware step 33

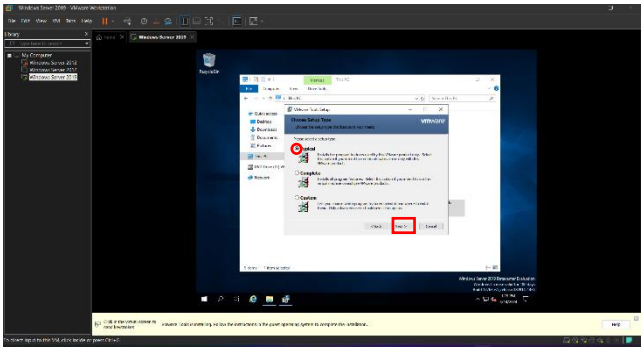


Figure 113 VMware step 34

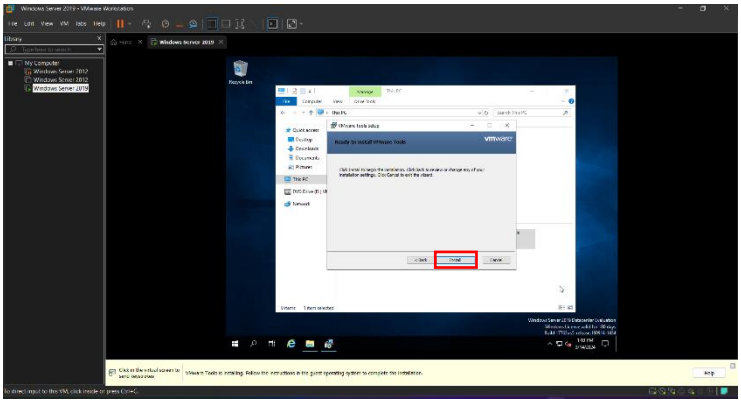


Figure 114 VMware step 35

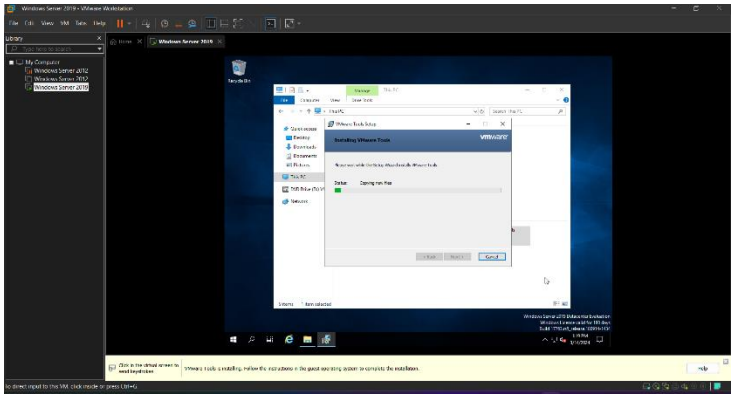


Figure 115 VMware step 36

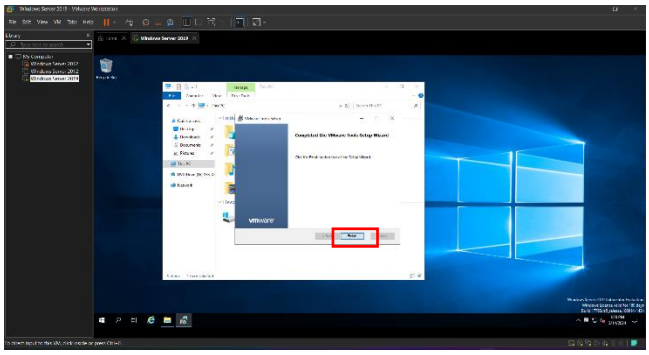


Figure 116 VMware step 37

Figure 117 VMware step 38

- Here is VMware's cleanup.

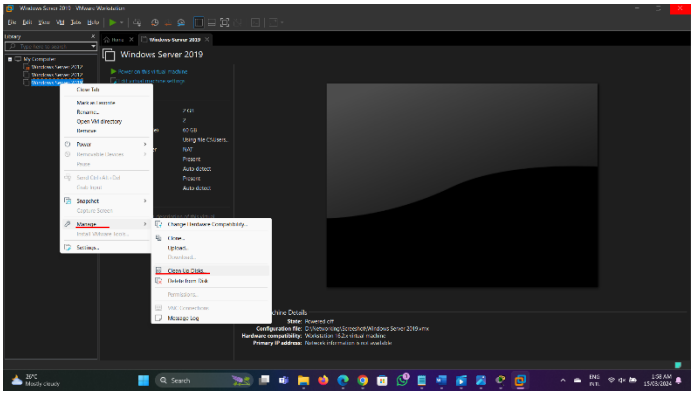


Figure 118 VMware cleanup Step 39

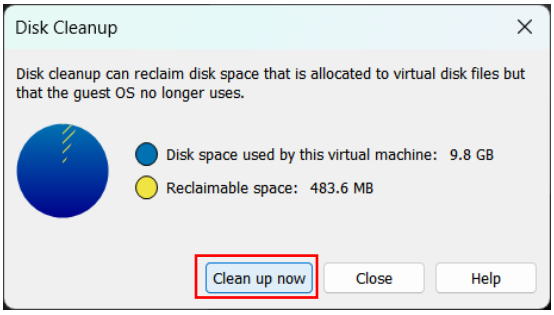


Figure 119 VMware cleanup Step 40

- Here is the VMware snapshot.

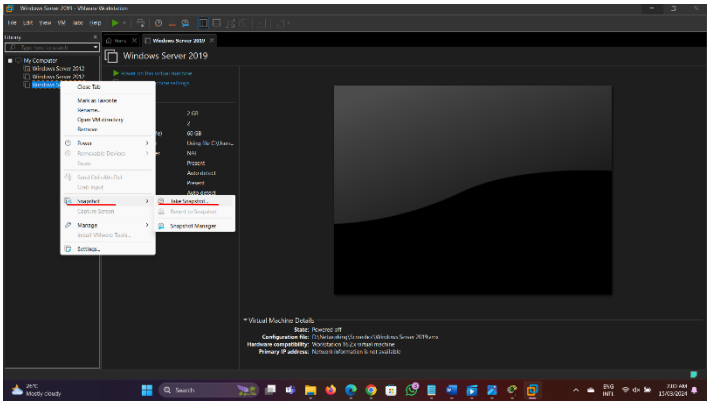


Figure 120 VMware snapshot Step 41

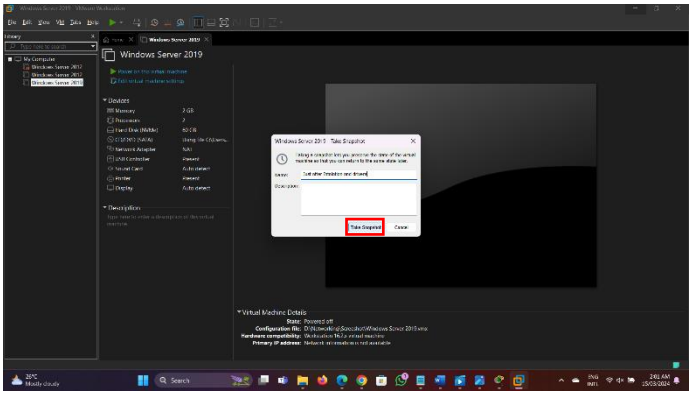


Figure 121 VMware snapshot Step 2

Server Name Configuration

Step 1: Go to This PCs properties.

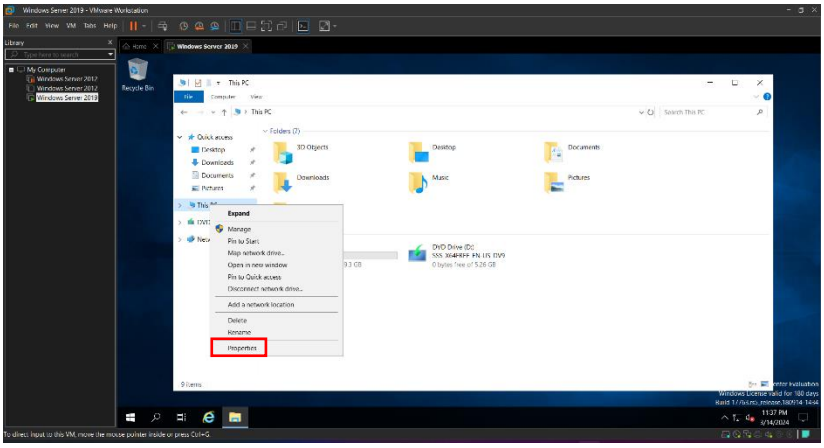


Figure 122 VMware configuration step 1

Step 2: Change setting

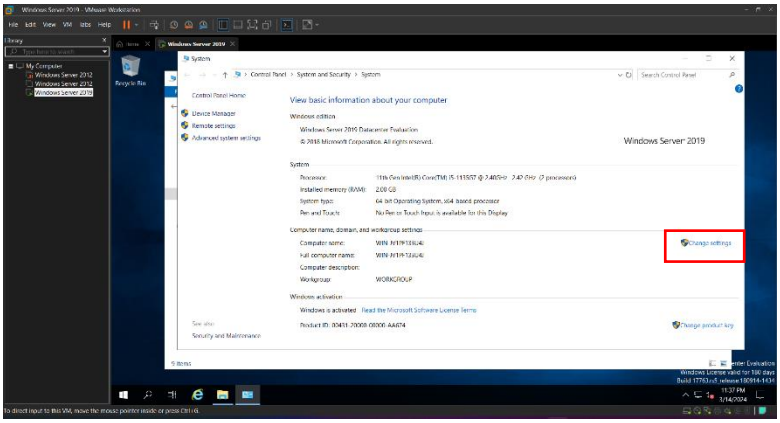


Figure 123 VMware configuration step 2

Step 3: click change button

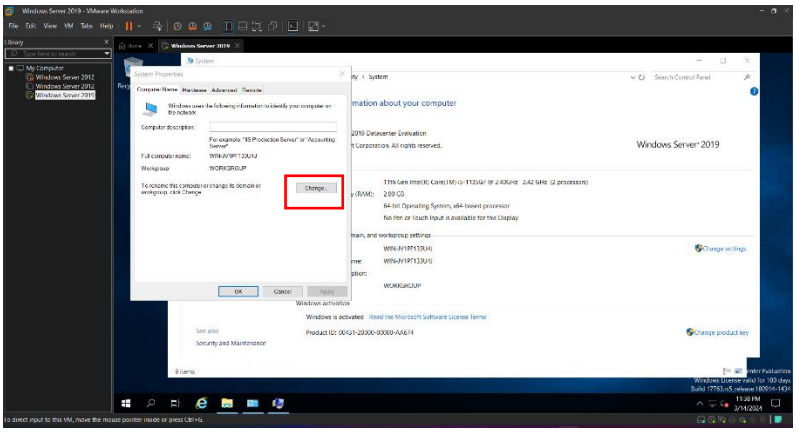


Figure 124 VMware configuration step 3

Step 4: type the name and click ok button

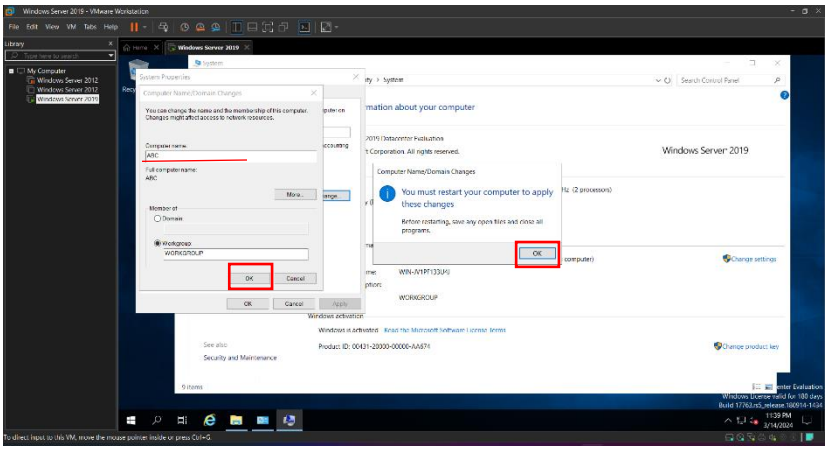


Figure 125 VMware configuration step 4

Step 5: Click close button

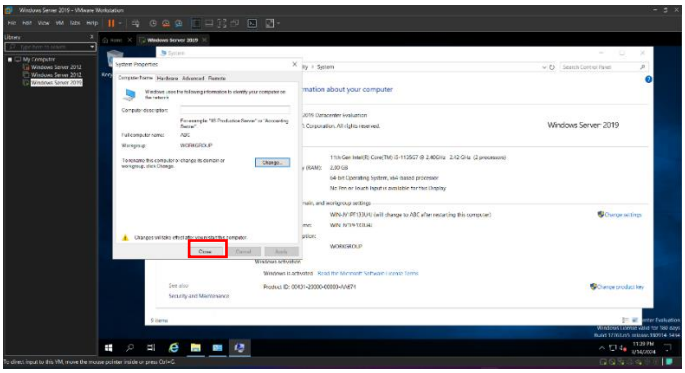


Figure 126 VMware configuration step 5

Step 6: Restart now

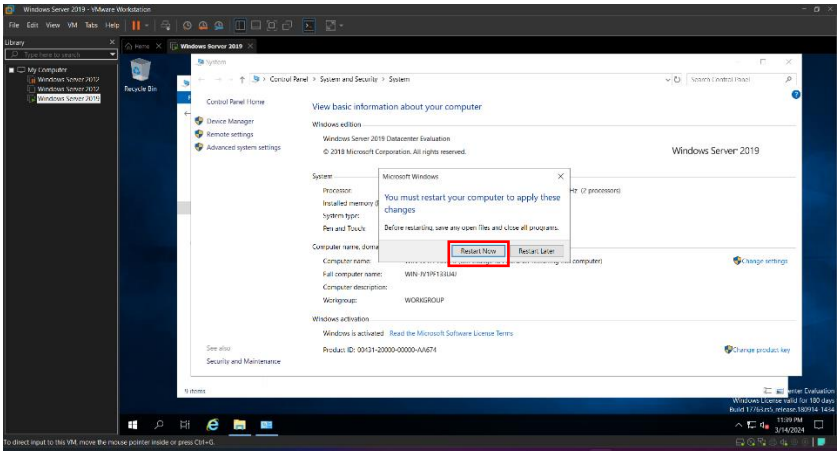


Figure 127 VMware configuration step 6

Step 7: Server name changing will be applied after the restart

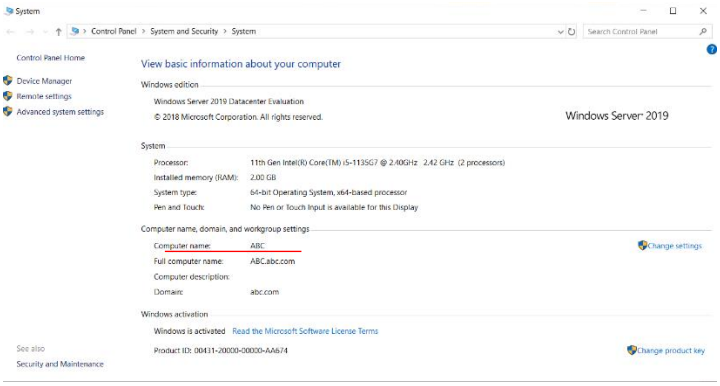


Figure 128 VMware configuration step 7

Server IP Configuration (GUI)

Step 1: Go to the Ethernet setting.

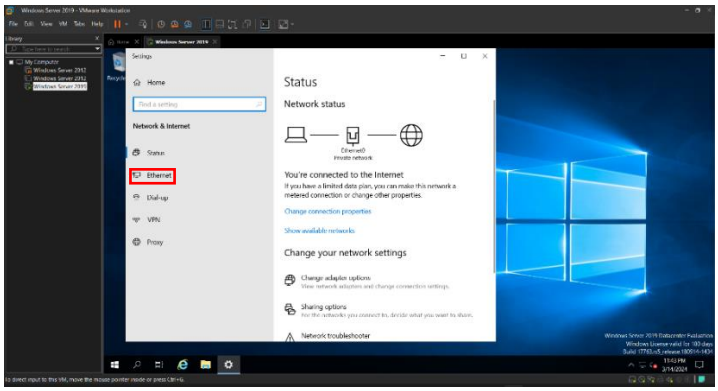


Figure 129 VMware configuration step 1

Step 2: Click advance sharing setting

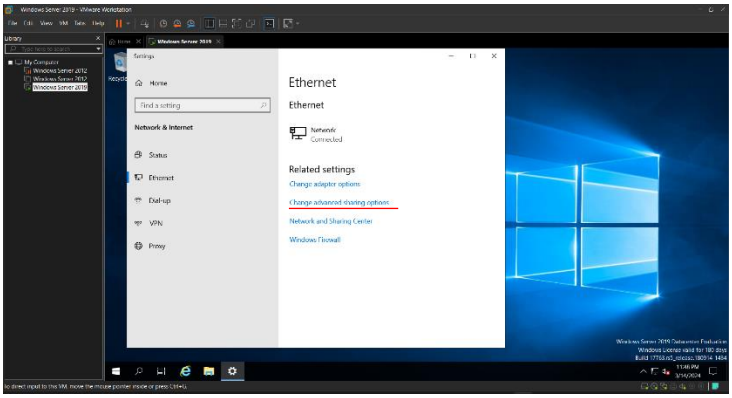


Figure 130 VMware configuration step 2

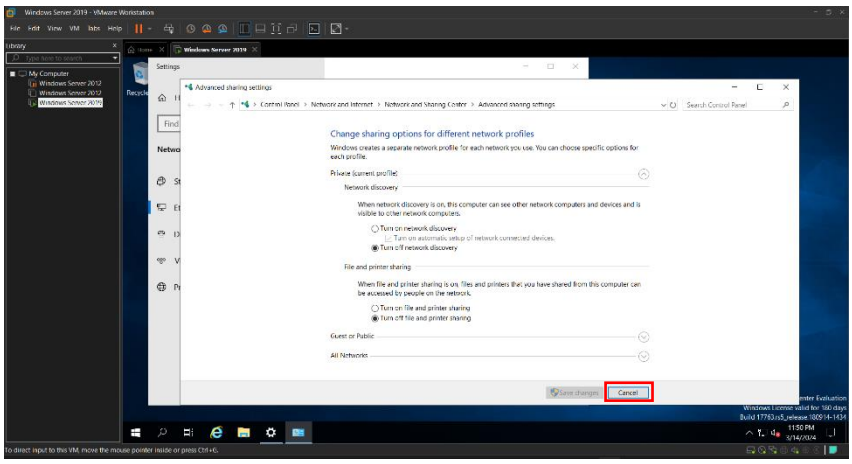


Figure 131 VMware configuration step 3

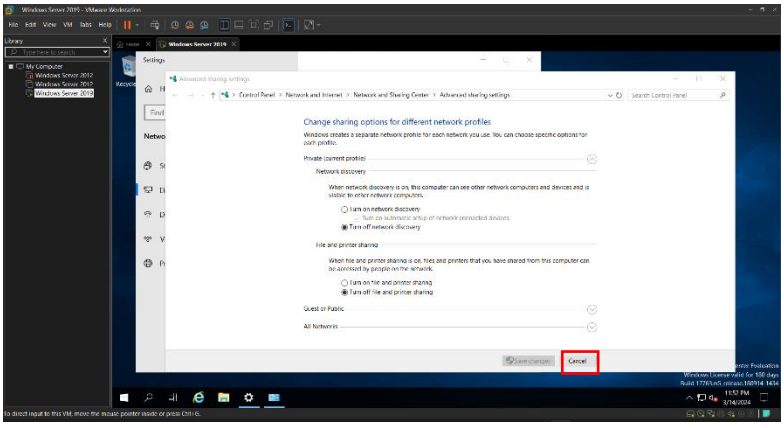


Figure 132 VMware configuration step 4

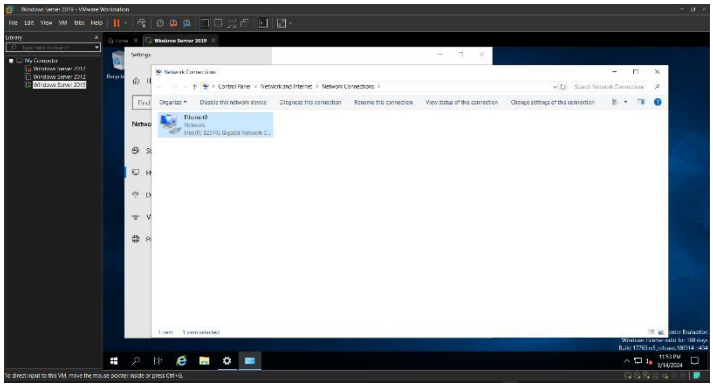


Figure 133 VMware configuration step 5

Step 3: Go to the properties of Ethernet card.

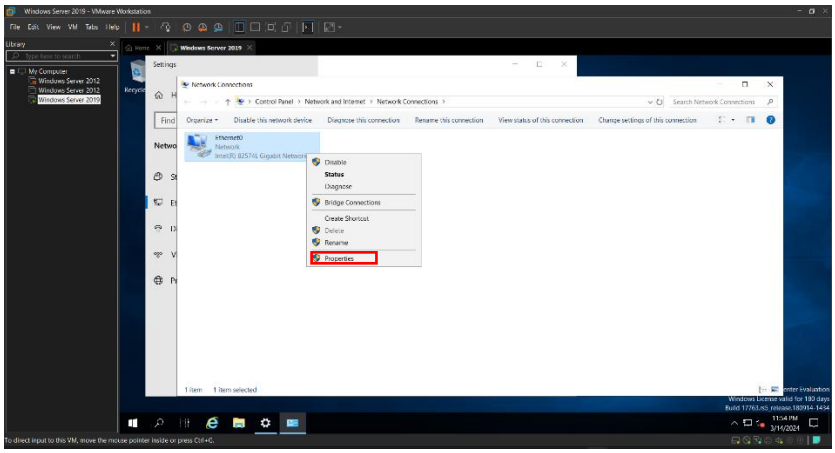


Figure 134 VMware configuration step 6

Step 4: Select ‘Internet Protocol Version 4’, and click on ‘Properties’ to access configuration window

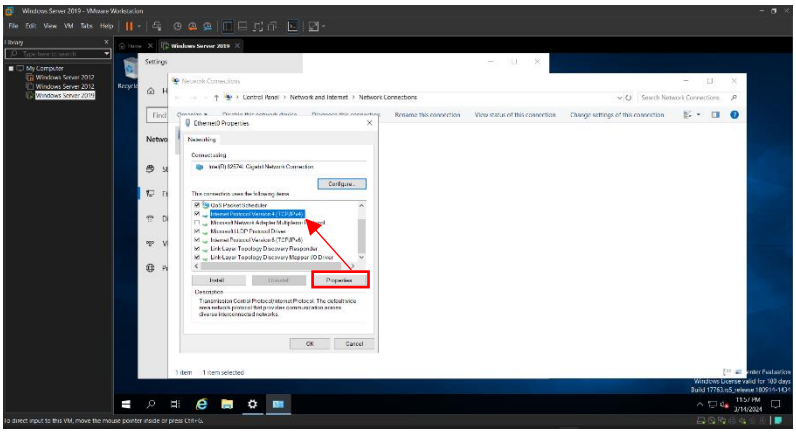


Figure 135 VMware configuration step 7

Step 5: To configure with static IP address, click on ‘Use the following IP address’ radio button, and set IP address, Subnet mask, and default gateway. Then click on ‘OK’ to apply the setting

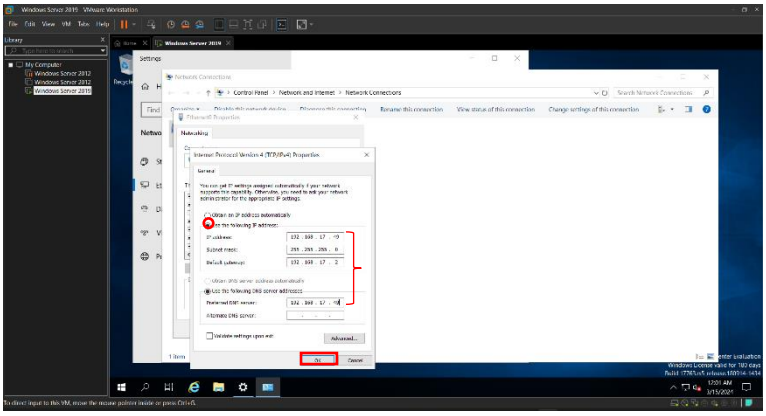


Figure 136 VMware configuration step 8

Step 6: Go to command prompt

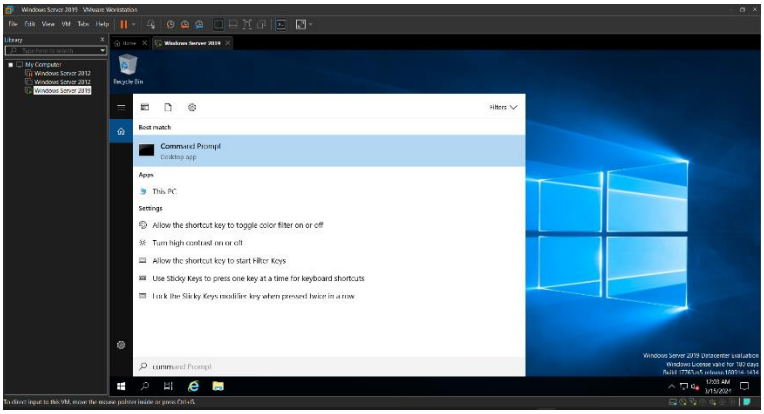


Figure 137 VMware configuration step 9

Step 7: Type ping message

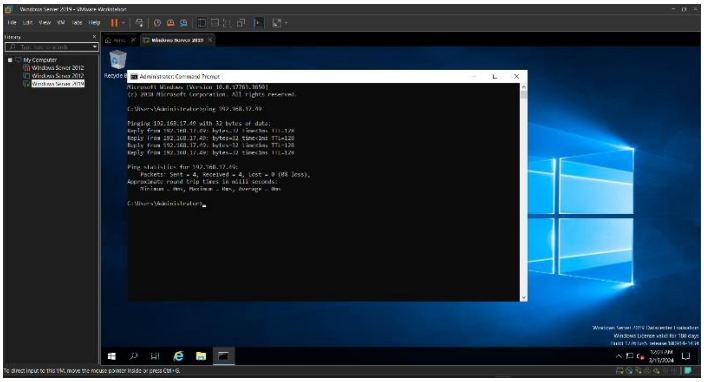


Figure 138 VMware configuration step 10

Step 8: IP setting will be applied on server

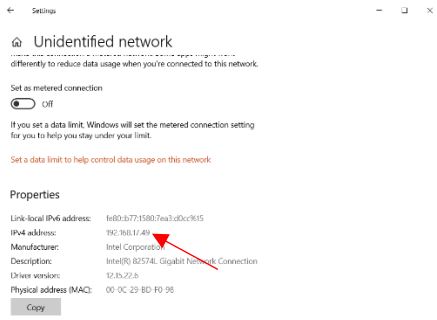


Figure 139 VMware configuration step 11

Installing Domain Controller on Server

Step 1: Open ‘Server Manager’, and open ‘Add Roles and Features’ wizard from Manage menu

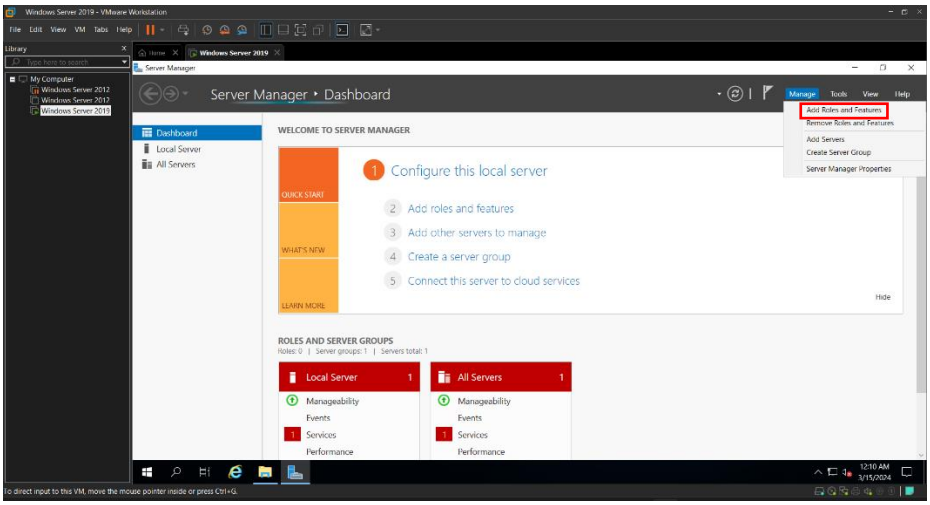


Figure 140 VMware Domain saver step 1

Step 2: In ‘Add Roles and Features’ wizard, click next to continue.

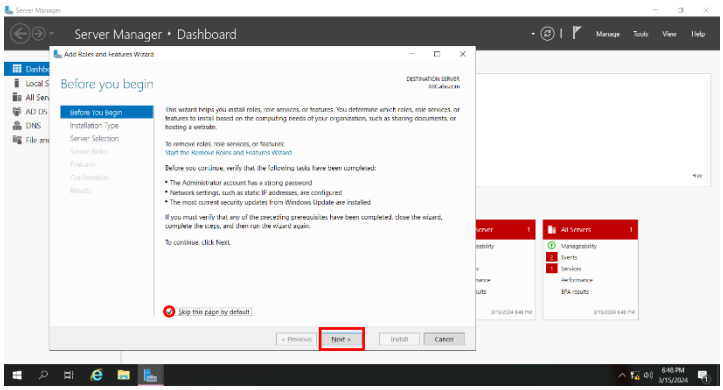


Figure 141 VMware Domain saver step 2

Step 3: Select ‘Role-based or feature-based installation’ as the installation type.

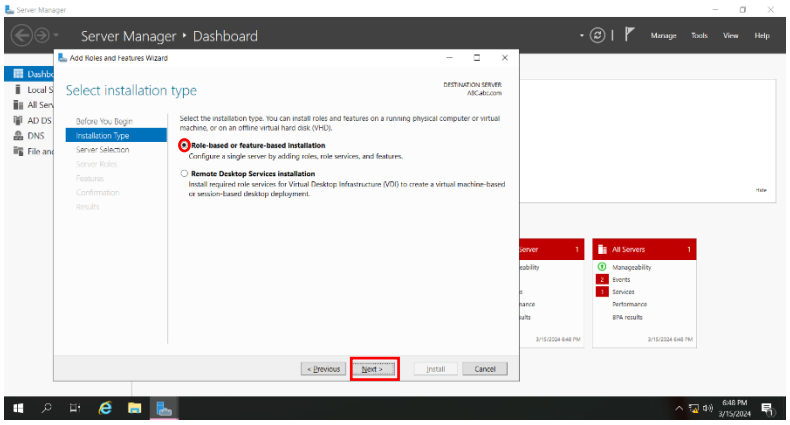


Figure 142 VMware Domain saver step 3

Step 4: Select the server from server pool. In this case, administrator select ‘ABC’ as the server. Then click next.

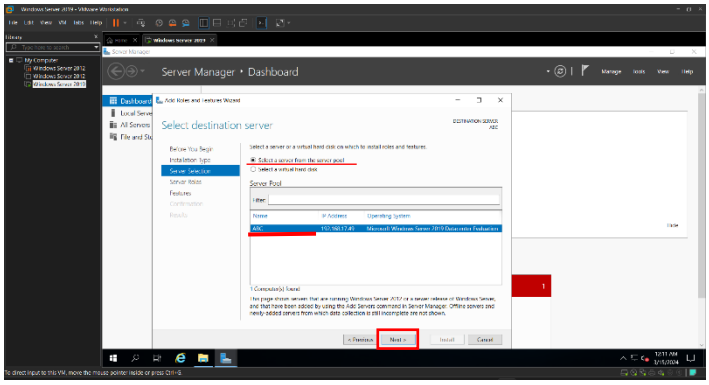


Figure 143 VMware Domain saver step 4

Step 5: Select the ‘Active Directory Domain Services’ as the server role, and click next.

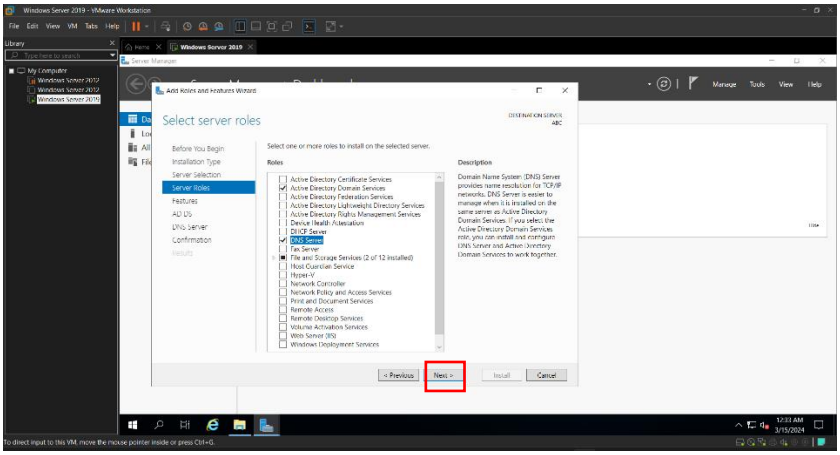


Figure 144 VMware Domain saver step 5

Step 6: Click on ‘Install’ to begin installation of selected features.

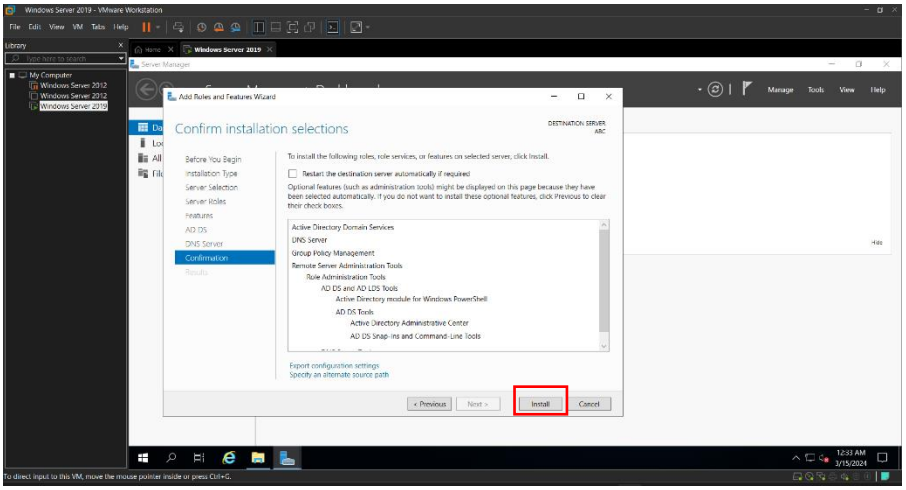


Figure 145 VMware Domain saver step 6

Step 7: Close the installation wizard after installation is completed.

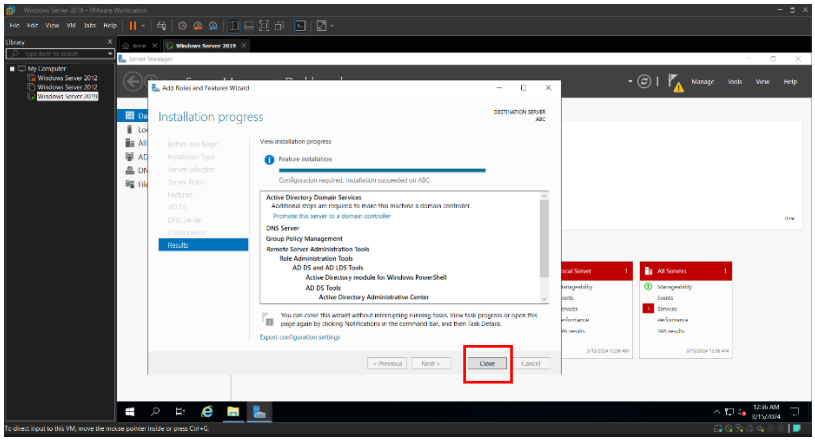


Figure 146 VMware Domain saver step 7

Configuring Active Directory Domain Services

Step 1: After the installation of AD DS feature, post deployment configuration notification will appear in ‘Server Manager’ dashboard. Click on ‘Promote this server to domain controller’ field to continue with configuration process.

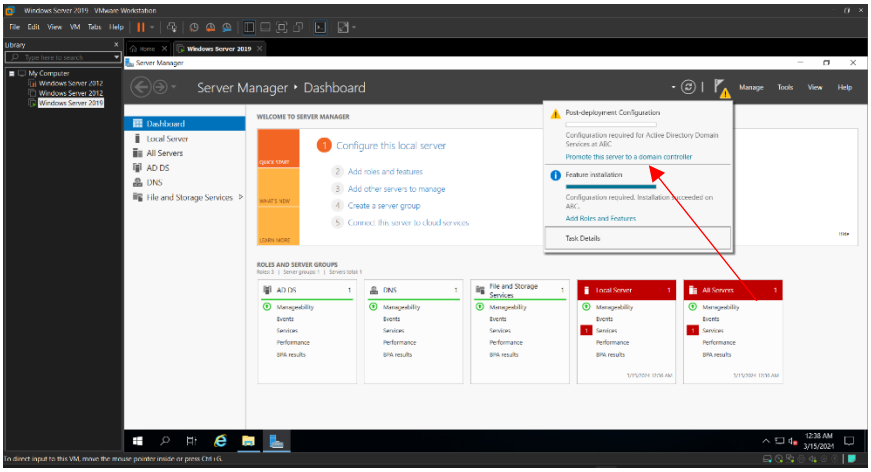


Figure 147 Configuring Active Directory Domain Services step 1

Step 2: Now the AD DS configuration wizard will appear. Click on ‘Add a new forest’ to create new root domain. Then specify the root domain name. Author used ‘abc.com’ as the root domain in this example.

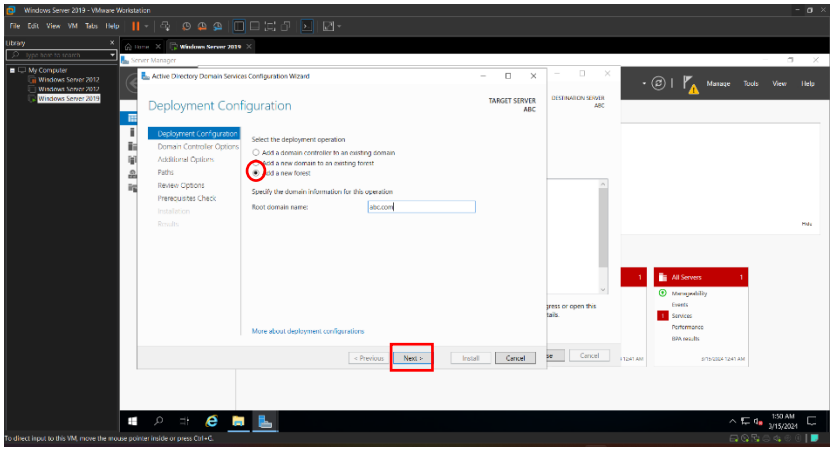


Figure 148 Configuring Active Directory Domain Services step 2

Step 3: In domain controller option pane, select DNS server in domain controller capabilities. Then specify the DSRM password, and click next

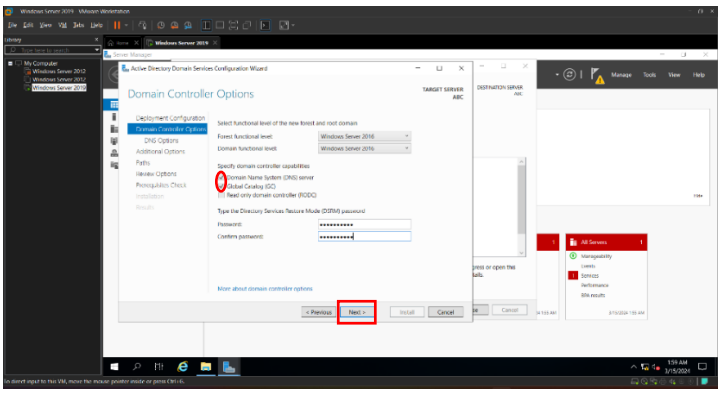


Figure 149 Configuring Active Directory Domain Services step 3

Step 4: Click ‘Next’ on DNS options pane to continue.

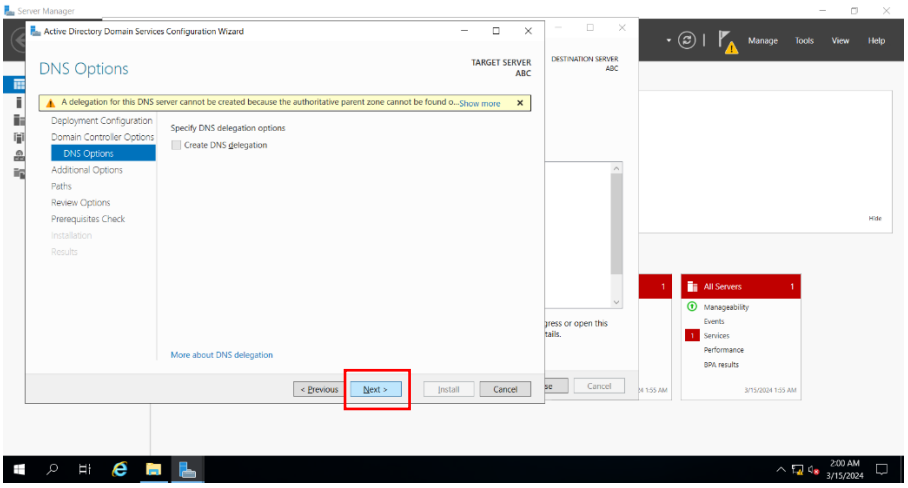


Figure 150 Configuring Active Directory Domain Services step 4

Step 5: Click ‘Next’ to verify the NetBIOS name in additional option pane.

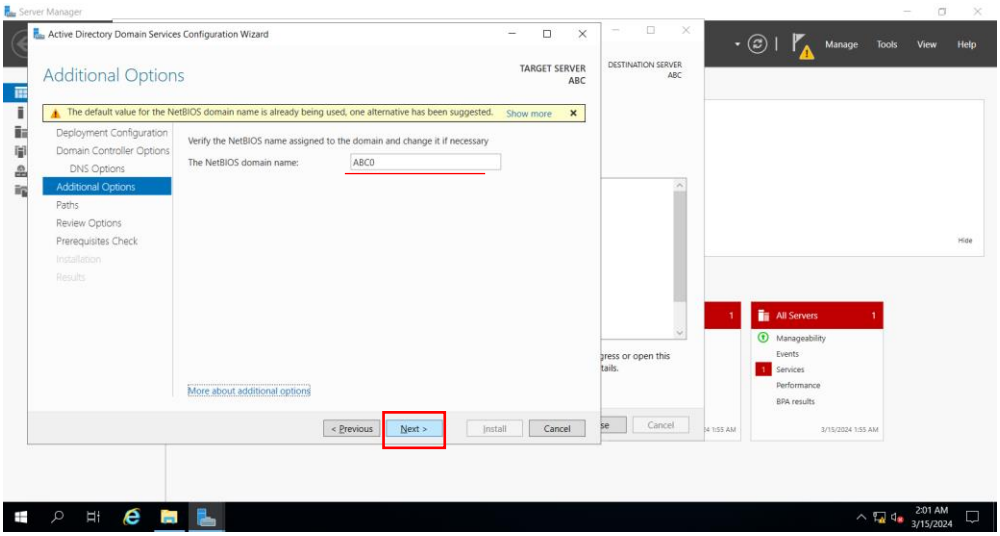


Figure 151 Configuring Active Directory Domain Services step 5

Step 6: In Review Option pane, click ‘Next’ to verify configurations.

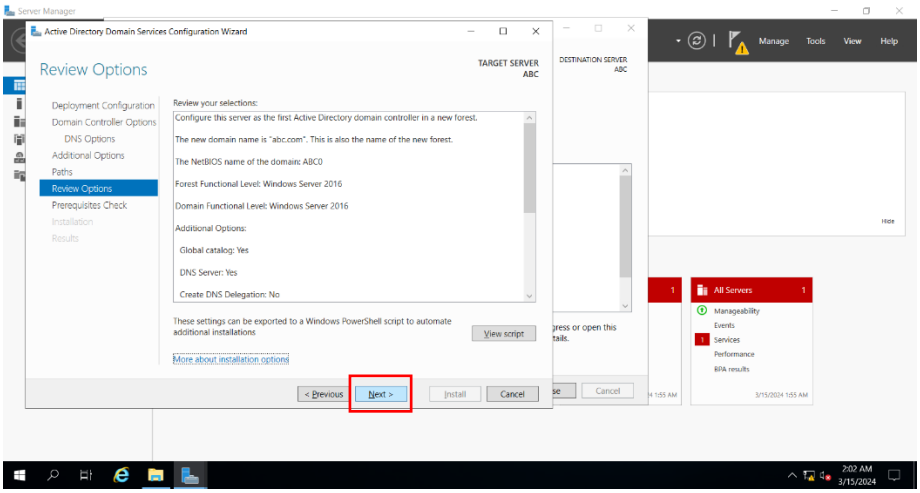


Figure 152 Configuring Active Directory Domain Services step 6

Step 8: After prerequisite check is completed, click ‘Next’ to install configurations.

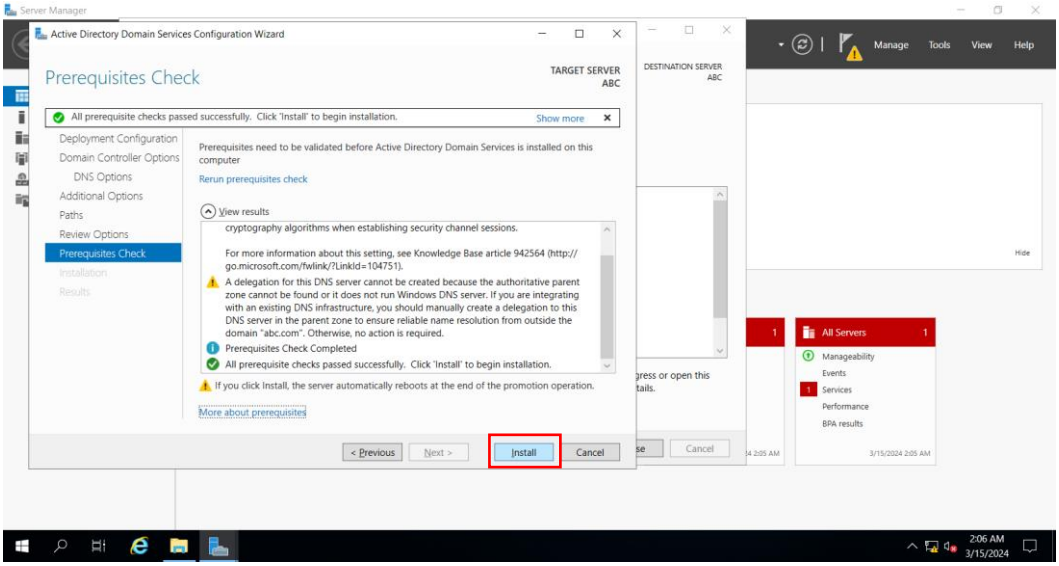


Figure 153 Configuring Active Directory Domain Services step 7

Creating Domain Users

Step 1: Go to ‘Active Directory Users and Computers’ in server, and right click on ‘Users’, then create ‘New user’ to open user creating wizard.

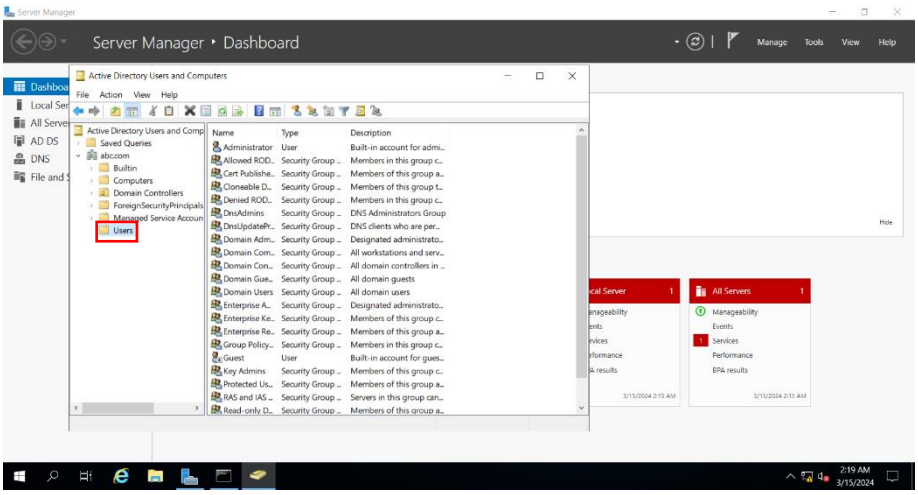


Figure 154 Creating Domain Users step 1

Step 2: Fill necessary fields and click next.

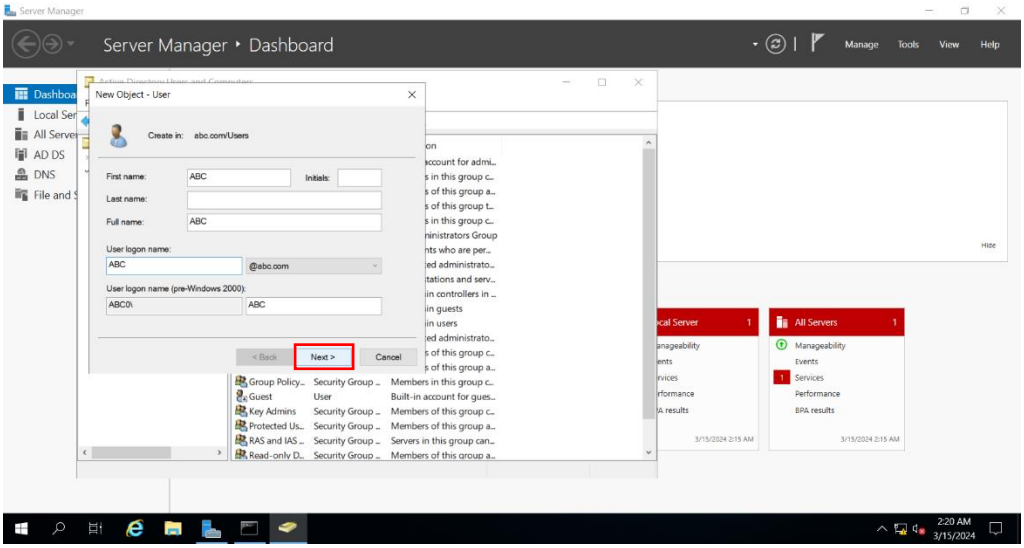


Figure 155 Creating Domain Users step 2

Step 3: Set password for the user account, and click next.

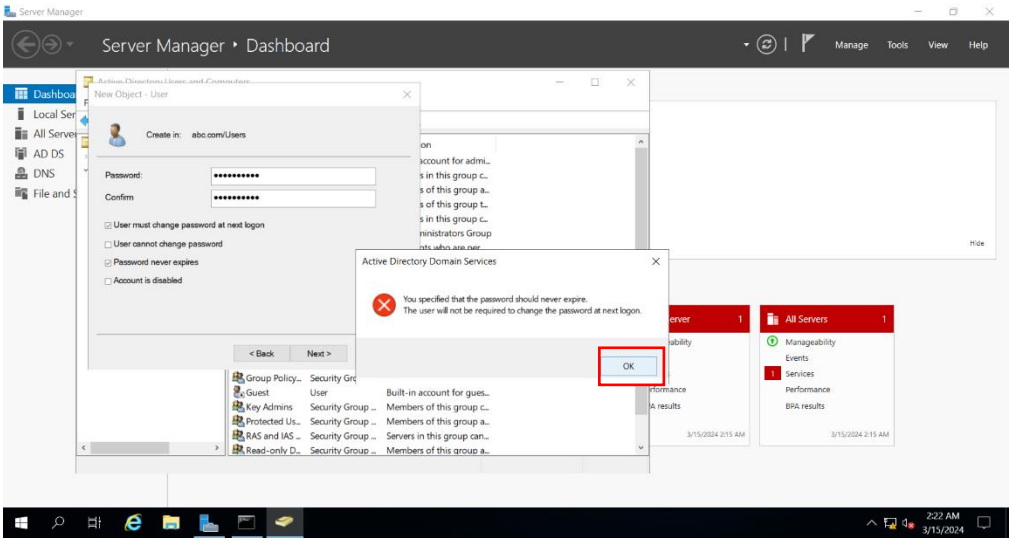


Figure 156 Creating Domain Users step 3

Step 4: Click on ‘Finish’ to create the account.

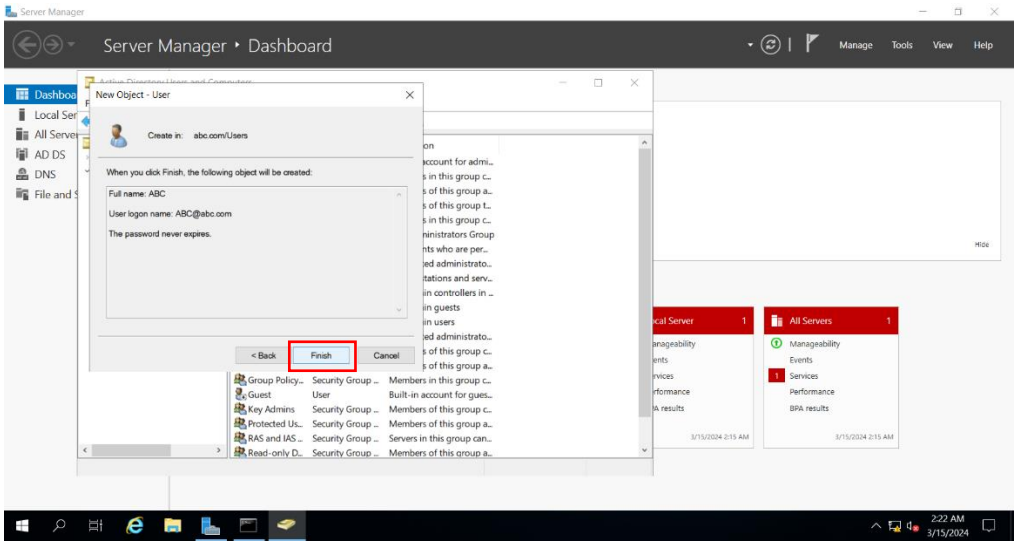


Figure 157 Creating Domain Users step 4

Step 5: User account will be appeared under Users in abc.com domain

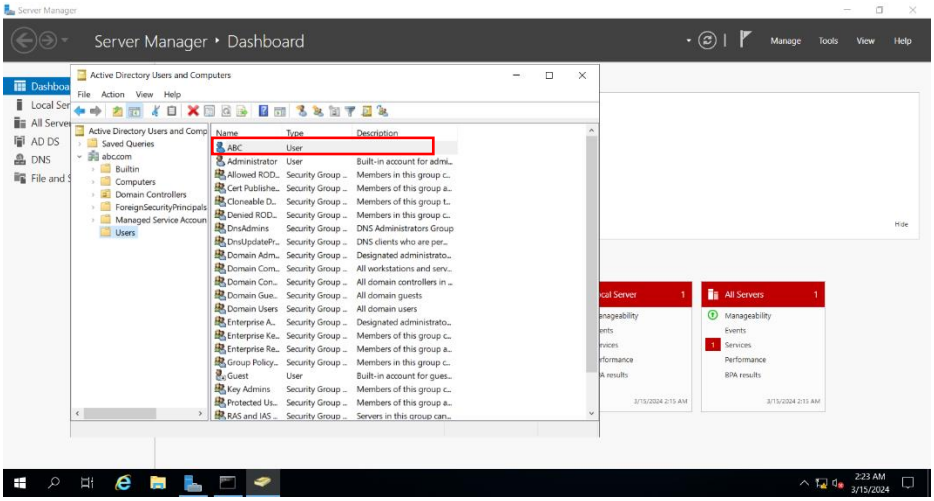
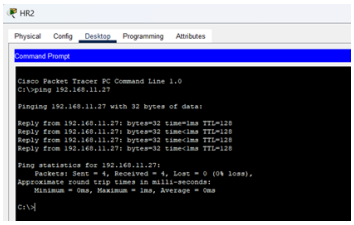


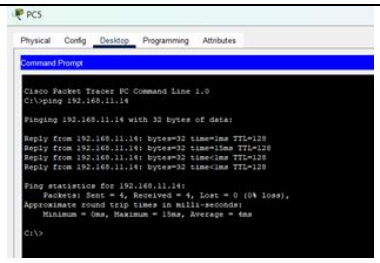
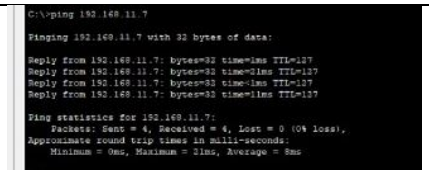
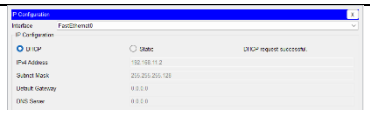
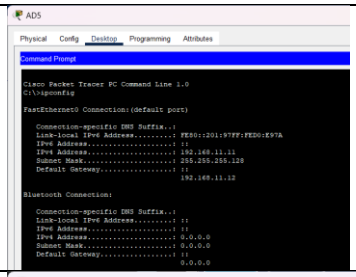
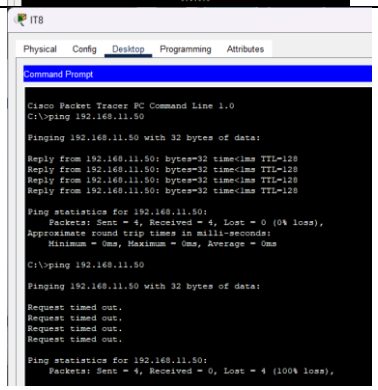
Figure 158 Creating Domain Users step 5

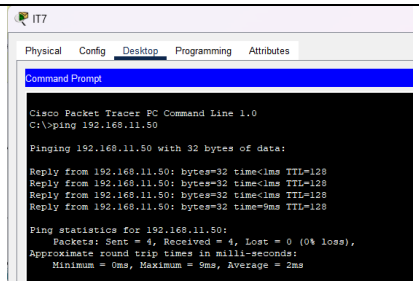
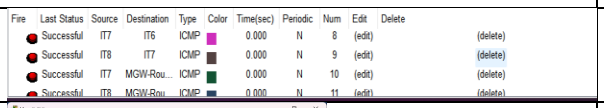
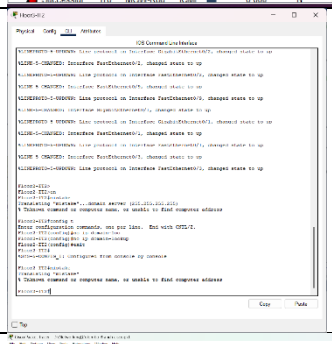
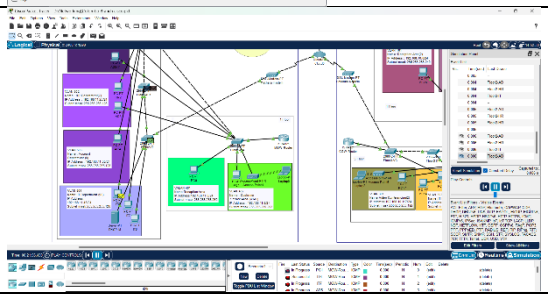
P8 Document and analyse test results against expected results.

Listed to document and analyse test results against expected results based on the provided network design. Given below is the analysis table which is proven with evidence.

Table 14 Test case table

Test ID	Test scenario	Screenshot	Expected Result	Actual result	Pass/fail
01	Ping from IP address 192.168.11.25 - 192.168.11.27 of the HR department of the Matara branch. But, these two IP addresses are connected to two switches.		Packets: Sent = 4, Received = 4, Lost=0 (0% loss)	Packets: Sent = 4, Received = 4, Lost=0 (0% loss)	Pass

02	Ping from IP address 192.168.11.11 - 192.168.11.14 of the administration department of the Matara branch.		Packets: sent = 4, Received=4, Lost=0(0% loss)	Packets: sent = 4, Received=4, Lost=0(0% loss)	Pass
03	Ping from Administration Department Matara to HR Department Matara		Packet: sent=4, Received=4, Lost=0(0% loss),	Packet: sent=4, Received=4, Lost=0(0% loss),	Pass
04	ID department IT8 PC getting IP from DHCP server				Pass
05	Check IP configuration in PC		Configure	Configured	Pass
06	The configuration above shows how the ping message went before the firewall was applied to the DHCP server and the configuration below shows how the ping message did not go after the firewall was applied. It indicates that the network is secure.		Packets: sent = 4, Received = 4, Lost = 0(0% loss),	Packets: sent = 4, Received = 4, Lost = 0(0% loss),	Pass

07	how the ping message went to the DHCP server from the IP address 192.168.11.47 of the IT department of the Matara branch.		Packets: sent = 4, Received = 4, Lost = 0(0% loss),	Packets: sent = 4, Received = 4, Lost = 0(0% loss),	Pass
08	PCs last status		Successful	Successfuled	Pass
09	DNS server lookup		Configure	Configure	pass
10	packet went from the switch to the PC		Successful	Successfuled	Pass

M4 Recommend potential enhancements for the networked systems.

Recommended Improvements for Networked Systems

Alliance Health's networked systems are proposed to be improved in various aspects to make them robust, efficient, and support the growth of the organization. These areas of improvement include performance optimization, increased availability, scalability, and security hardening. Each of these improvements is discussed in detail below.

Improving Performance

Quality of Service (QoS) Policies

QoS policies enforce priority for critical applications such as patient record systems or video conferencing over the network. This reduces latency and ensures sufficient bandwidth for essential operations during peak usage periods. Suppose there is an important video call between the Colombo head office and the Matara branch. QoS ensures that this traffic receives a higher priority compared to less critical activities such as file downloads.

Network Infrastructure Upgrade

Replacing older network components, including switches, routers, and access points, with higher-performance versions enables faster speeds and lower latency. In particular, gigabit or multi-gigabit switches can fully support higher traffic without significant delays for users accessing shared resources.

Proactive Network Monitoring

Implementing tools like SolarWinds or Nagios monitors network performance in real-time. These tools can help detect bottlenecks, track bandwidth usage, and alert the administrator to potential problems before they become critical. Proactive monitoring ensures that problems are resolved quickly, thereby maintaining smooth network operations.

Availability Enhancements

Redundant Network Paths and Devices

Introducing redundancy in paths and devices provides a minimal possibility of a single point of failure, such as backup links, switches, and routers.

Ex: When a primary router in Colombo fails, a backup router can automatically take over to ensure uninterrupted connectivity. This is very important and key for mission-critical applications that require continuous network availability.

High Availability for Critical Services

High availability should be ensured for DHCP, DNS, and database servers. This can be done through failover clustering, which automatically switches to the backup server in the event of a failure of the primary server. If there is a failure of the database server,

Ex: The failed server will provide uninterrupted service to users without significant downtime.

Scalability Enhancements

Scalable Network Design

The scalability of the network infrastructure means that new devices, users, or applications can be easily integrated into the organization.

Ex: Since VLANs are configured to accommodate them, an organization may not need to re-engineer the entire network to add more departments. Modular switches allow ports to be expanded to connect more devices without changing the hardware.

Cloud-based solutions

Integrating cloud-based services can offload resource-intensive tasks such as file storage or application hosting from on-premises servers. Cloud platforms such as Microsoft Azure or Amazon Web Services provide resources on demand, enabling the network to scale rapidly without heavy investment in physical infrastructure. This is especially useful for seasonal increases in workload or unexpected peaks in user activity.

Security Enhancements

Advanced Security Measures

Advanced deployment of firewall rules, intrusion detection and prevention systems add another layer of defines against unauthorized access and cyber threats.

Ex: An IDS can monitor network traffic to look for suspicious activity, while an IPS can automatically block malicious attempts.

Encryption Technology

Technologies such as VPN and SSL/TLS encryption enable secure communication over public networks.

Ex: Employees connecting to the network from the outside can use a VPN, which protects sensitive data from interception by unauthorized parties.

Regular Security Audits

Periodic security audits and risk assessments help identify vulnerabilities before they are exploited.

Ex: Outdated software, weak passwords, or misconfigured devices can be updated through regular checks to reduce the risk of data breaches.

D2 Critically reflect on the implemented network, including the design and decisions made to enhance the system.

Critical reflection of the network has been implemented

The network design for Alliance Health, including the new branch in Matara, targeted the organization's needs related to connectivity, security, scalability, and performance. During the design process, several strategic decisions were made to increase its efficiency and usability. Although justified, it is very important to critically reflect on these decisions by considering the potential weaknesses and design limitations.

Subnetting departments

This was done to ensure network segmentation for improved security. Since traffic is isolated within each department, this prevents unnecessary data exchange between unrelated departments, therefore reducing congestion and increasing performance. Subnetting allows for granular access to resources, therefore improving data security.

- Contraindications and limitations

While subnetting improves security and performance, it introduces complexity in network management, especially as the organization grows. Managing multiple subnets requires advanced expertise and ongoing administrative efforts. Subnet configuration errors can lead to connectivity issues or inefficiencies. These challenges can be addressed by providing proper training to network administrators and implementing automated subnet management tools.

Equipping conference rooms and customer service areas with Wi-Fi

Ex: Wi-Fi connectivity in conference rooms and service areas enhances collaboration and customer experience. Employees can easily share any resource during a meeting or discussion, and customers do not have to experience delays in receiving essential services.

- Contraindications and Limitations

Wi-Fi brings with it a number of potential security vulnerabilities, such as unauthorized access and interference. This is very critical in a healthcare organization where data privacy is of utmost importance. Wi-

Fi performance can degrade in areas with high traffic. While encryption, strong passwords, and access controls can mitigate risks, ensuring reliable Wi-Fi performance may require investment in high-quality access points and constant monitoring.

Intra-branch connectivity

It was also important to establish a seamless connection between the head office and the Matara branch for easy sharing of resources and collaboration. This decision increases productivity as employees can easily access resources such as databases and shared applications from any location.

- Contraindications and limitations

While inter-branch connectivity enables collaboration, it introduces latency and bandwidth constraints, especially during peak hours. Relying on inter-branch communication can lead to loss of productivity if that connectivity goes down. This can be mitigated with strategies such as bandwidth optimization, QoS policies, and redundancy, but requires ongoing administration.

Static IP assignment for servers

The servers in the server room were assigned static IP addresses for consistency in access and management. Static IPs avoid conflicts and ensure reliable access to critical resources such as databases and web servers.

- Contraindications and Limitations

Static IP management involves planning and proper documentation. A large pool of static IP addresses becomes difficult to manage as the network expands. When records are not well maintained, mismanagement can easily lead to network waste or even conflicts. This can be mitigated by using IP management tools and proper documentation procedures.

On-Site Wi-Fi Accessibility for Sales and Marketing Teams

Wi-Fi access for sales and marketing teams increases their mobility and productivity by enabling them to work efficiently in different office locations. This flexibility is important for teams that need to interact with clients frequently or need quick access to resources while on the go.

- Contraindications and Limitations

Wireless networks are inherently less secure than wired connections, which puts sensitive company data at risk. Wi-Fi signals can be affected by interference or poor coverage in certain areas, leading to inconsistent connectivity. Addressing these challenges requires implementing strong encryption protocols like WPA3, regular signal strength assessments, and deploying additional access points to eliminate dead zones.

Critical reflection on proposed improvements

Improve performance

Network performance bottlenecks should be overcome by implementing QoS policies and adding infrastructure components such as high-performance switches and routers. These improvements are often budget-constrained or their compatibility with existing systems may prevent them. Hardware upgrades should generally be planned carefully so that they do not disrupt operations. These can be mitigated by a phased implementation plan.

Improve availability

Unnecessary network paths and failover mechanisms help make the network more available. However, these call for additional investment and add complexity to the configuration. Over-reliance on redundancy can lead the team to become complacent about proactive maintenance, assuming that the failed systems will always be operational. Regular schedules and redundant system checks prevent this pitfall.

Scalability

The scalability of the design ensures that the network can handle future growth, whether it is more users or additional applications. There are many upfront costs and challenges in allocating resources for scalability, especially when over-engineering the network for hypothetical scenarios. A balance must be struck between current needs and projections for future growth to avoid underutilization of resources.

Security hardening

Advanced firewalls, intrusion detection systems, and regular audits are some of the important elements of enhanced security measures required to protect sensitive data. However, the need for dedicated staff to

constantly monitor such measures can increase operational costs. Overly restrictive protocols can limit user productivity due to employee frustration. Balancing this, a set of policies should be established that emphasize security without sacrificing usability in any way.

Design Weaknesses Acceptance

While this design meets most of Alliance Health's needs, the following limitations are considered:

1. Complexity- High-level configurations that include subnetting and redundancy add significant complexity to the network. This requires proper training and tools to handle it properly.

2. Cost Considerations- Certain upgrades, such as infrastructure upgrades and provision of failover mechanisms, can be stressful if not planned well within a budget.

3. Security-Usability Balance- Increasing security can have a negative impact on usability, as controls may be too restrictive for employees to easily access information. Usability must be balanced with security.

4. Adaptability- Although the network is scalable, it may require additional resources and quick decision-making to adapt to unexpected challenges such as spikes in traffic or new compliance requirements.

Google Drive link

E211307-Hasara Sesadi - Networking.zip

References

1. admin., 2023. *"OSI Model vs DoD Model (TCP/IP Model) – CCNA-Classes."* *Ccna-Classes.com,*. [Online]
   Available at: ccna-classes.com/ccna-study-resources/osi-model-vs-dod-model-tcp-ip-model/. [Accessed 11 June 2023].
2. Gaurav., S., 2022. *"IEEE Standards in Computer Networks - Scaler Topics."* *Scaler Topics, Scaler Topics,*. [Online]
   Available at: www.scaler.com/topics/computer-network/ieee-standards-in-computer-networks/ [Accessed 4 March 2024].
3. GfG., 2020. *"Difference between Physical and Logical Topology."* *GeeksforGeeks, GeeksforGeeks,*. [Online]
   Available at: www.geeksforgeeks.org/difference-between-physical-and-logical-topology/. [Accessed 4 March 2024].
4. Gillis, A. S. a. T. N., 2024. *"Network Topology."*. [Online]
   Available at: www.techtarget.com/searchnetworking/definition/network-topology.
5. Kapoor, A., 2022. *"Study the Importance of Types of Networks - LAN, MAN, and WAN."* *Simplilearn.com,Simplilearn,*. [Online]
   Available at: www.simplilearn.com/tutorials/networking-tutorial/importance-of-types-of-networks-lan-man-wan.
   [Accessed 4 March 2024].
6. Kinza Yasar, e. a., 2023. *"Network Protocol."* *Networking, TechTarget,*. [Online]
   Available at: www.techtarget.com/searchnetworking/definition/protocol. [Accessed 15 March 2024].