Higher Nationals

Internal verification of assessment decisions – BTEC (RQF)

INTERNAL VERIFICATION – ASSESSMENT DECISIONS				
Programme title	BTEC Higher National Diploma in Computing			
Assessor	Mrs.Anjula	**Internal Verifier**		
Unit(s)	**Unit 02: Networking**			
Assignment title	LAN Design & Implementation for Alliance Health			
Student's name				
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		**Dat**	
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	E13113		
Unit Title	Unit 02: Networking		
Assignment Number	1	**Assessor**	
Submission Date		**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 ☐ ☐
Descripts
M1 ☐ **D1** ☐

LO2 Explain networking devices and operations.
Pass, Merit & Distinction P3 P4 ☐ ☐
Descripts
M2 ☐

LO3 Design efficient networked systems.
Pass, Merit & Distinction P5 P6 ☐ ☐
Descripts
M3 ☐ **D2** ☐

LO4 Implement and diagnose networked systems.
Pass, Merit & Distinction P7 P8 ☐ ☐
Descripts
M4 ☐

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		**Date**	

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.

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

Date:
(*Provide Submission Date*)

Student Name /ID Number	
Unit Number and Title	**Unit 2: Networking**
Academic Year	2022/23
Unit Tutor	
Assignment Title	**LAN Design & Implementation for Alliance Health**
Issue Date	
Submission Date	
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.)

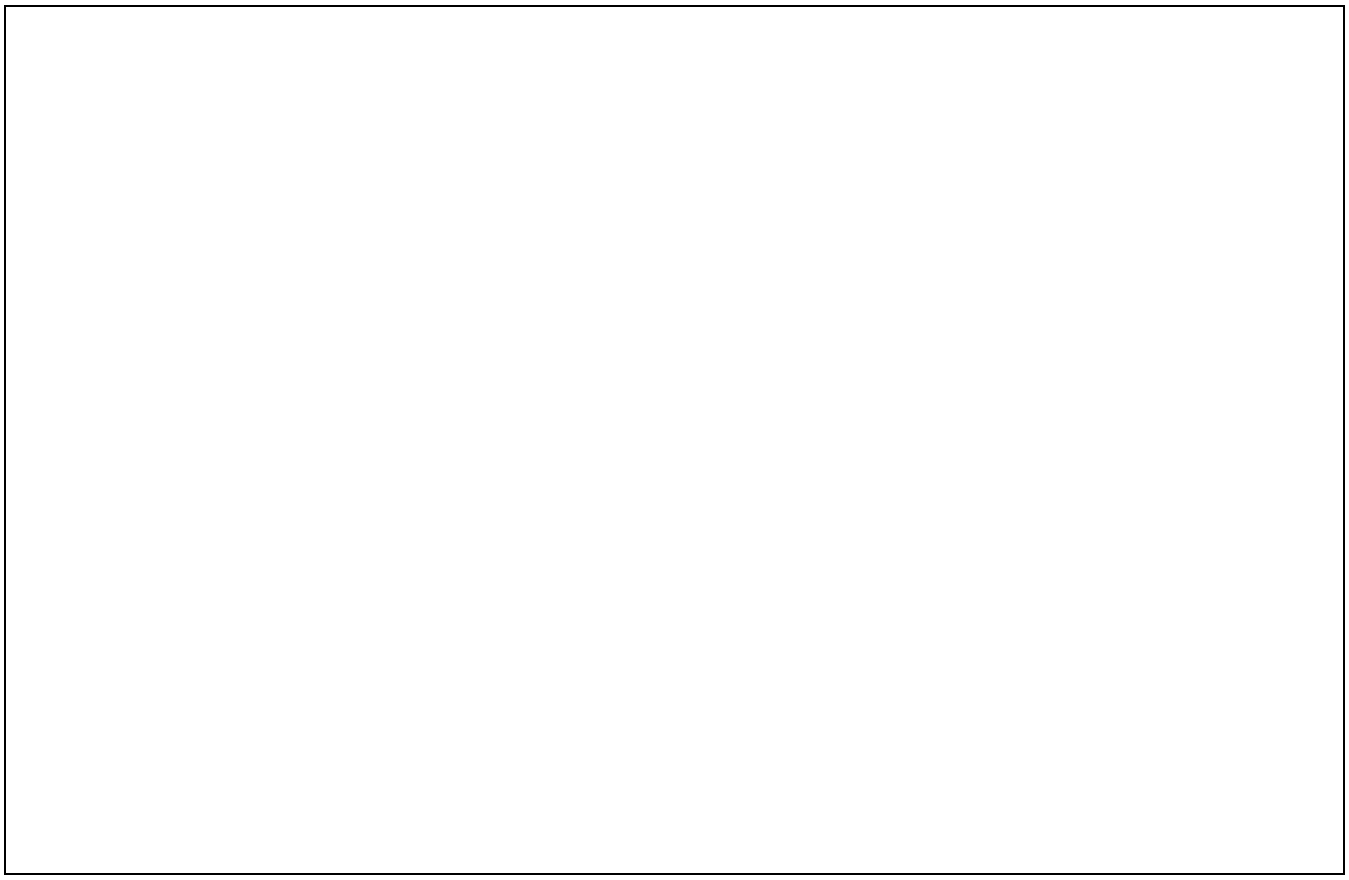
- Install and configure Network services, devices and applications (Ex: VLAN,WiFi, DNS,Proxy, Web, Etc.) according to the proposed design to accomplish the user requirements and design a detailed Maintenance schedule for above Network.

***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 protoco		
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

U.D LAHIRU SANDARUWAN E131113

Table of Contents

Table of figure

Acknowledgment

First of all, a special thanks to my parents.
I would like to sincerely thank my HND lecturers. I would like to thank the Esoft metro campus staff. because of their significant role in the accomplishment of the assignment. I have been guided by lots of my friends' valuable suggestions and experience throughout the process of completing the assignment. therefore
I would also like to express my gratitude to my all friends, without their support and cooperation this assignment could not have been accomplished. Finally, I would like to thank the people who helped me guide and blessings.
I could finish my assignment successfully.

2 Introduction

Computer networks are the backbone of modern communication systems, connecting devices and enabling the exchange of information across the world. A computer network is a collection of interconnected devices, such as computers, servers, routers, switches, and other networking hardware and software, that can communicate with each other and share resources.

The fundamental concepts of computer networks include protocols, topologies, network models, addressing, and routing. Protocols define the rules and standards for communication between devices on a network, while network topologies describe the physical or logical layout of devices in a network. Network models, such as the OSI (Open Systems Interconnection) model, provide a framework for understanding the different layers of communication in a network.

Addressing and routing are crucial components of network communication. Addressing involves assigning unique identifiers to devices on a network, such as IP (Internet Protocol) addresses. Routing is the process of directing data packets through a network to their intended destination, using protocols such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Other important concepts in computer networks include security, performance, and scalability. Security measures such as firewalls and encryption are used to protect networks from unauthorized access and data breaches. Performance considerations involve optimizing network speed, reliability, and bandwidth utilization. Scalability involves designing networks that can handle increasing amounts of traffic and accommodate new devices and applications.

This assignment will explore these fundamental concepts in more detail, examining the key components of computer networks and their roles in enabling modern communication and information exchange.

now this assignment is for planning and designing a network system for With its global delivery center in Colombo and Matara, Alliance Health

3 Contents

4 List Of Figure

5 List of Table

6 Activity 01:

6.1 NETWORKING PRINCIPLES

Network system types

What is the network system?

A network system is a collection of interconnected devices that communicate with each other to exchange data and resources. The devices in a network can be computers, servers, printers, routers, switches, or any other device that is capable of transmitting or receiving data.

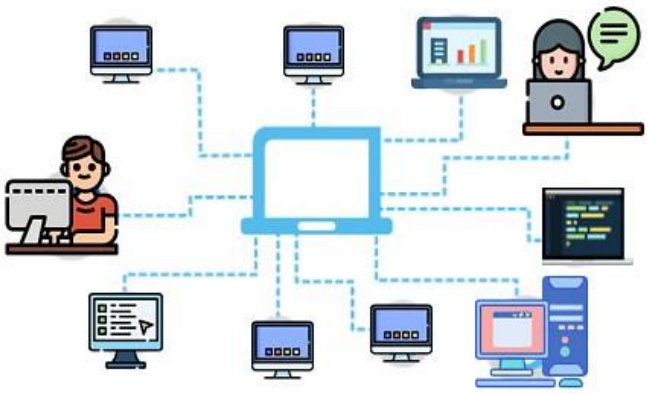


Figure 1network system

The basic components of a network system are:

1. Network devices: These include routers, switches, hubs, and other devices that are used to connect the various components of the network.

2. Transmission media: This includes cables, fibre optics, or wireless communication channels that are used to transmit data between devices.

3. Network protocols: These are a set of rules and procedures that govern the communication between devices in a network. Common network protocols include TCP/IP, HTTP, FTP, and SMTP.

4. Network services: These are applications that run on the network and provide services to users. Examples of network services include email, file sharing, and remote access.

5. There are several types of network systems, including: Local Area Network (LAN): This is a network that covers a small geographic area, such as an office building or school.

6. Wide Area Network (WAN): This is a network that covers a larger geographic area, such as a city or country. The internet is an example of a WAN.

7. Metropolitan Area Network (MAN): This is a network that covers a metropolitan area, such as a city.

8. Wireless Network: This is a network that uses wireless communication channels to transmit data between devices.

Network systems are used in many different industries, including business, healthcare, education, and government. They are essential for enabling communication and collaboration between devices and users across different locations.

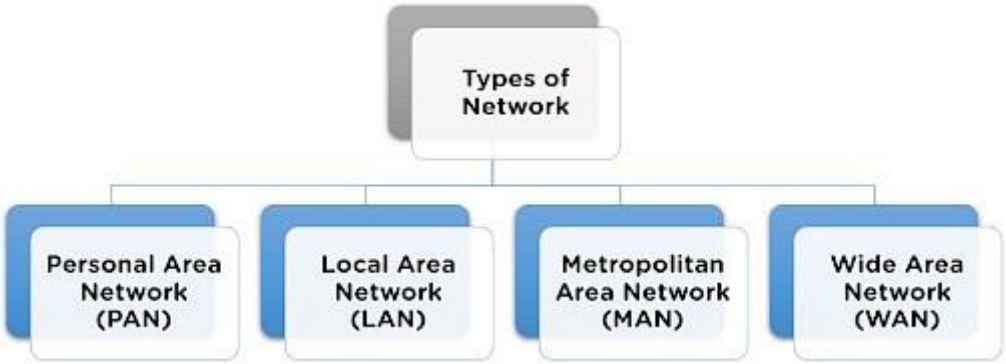


Figure 2 network types

Kapoor, A. (2022). *Importance of Types of Networks: LAN, MAN, and WAN | Simplilearn*. [online] Simplilearn.com.

Bourgeois, S. (2016). *Network-types*. [online] belden.com

javaTpoint (2011). *Types of Computer Network - JavaTpoint*. [online] www.javatpoint.com.

6.1.2 peer to peer

Peer-to-peer (P2P) networking is a type of network system in which every node in the network can act as both a client and a server. In other words, each node in the network can both receive and send data to other nodes in the network without relying on a central server or authority. Here are a few types of P2P network systems:

Pure P2P network: In this type of network, all nodes in the network are equal and have the same responsibilities. Each node can communicate directly with any other node in the network and can also store and share files.

Hybrid P2P network: This type of network combines the P2P model with a client-server model. Some nodes in the network act as servers, while others act as clients. The servers provide the initial content or files, while clients access these files from the servers.

Overlay network: This is a network that is built on top of an existing network, such as the internet. Nodes in the overlay network can communicate with each other and use the underlying network to send and receive data.

Distributed hash table (DHT) network: This type of network is used for searching and retrieving files. Nodes in the network store and index data, making it easier to search for specific files or pieces of data.

P2P networks are popular for their ability to distribute resources, improve fault tolerance, and increase network scalability. They are commonly used in file-sharing, messaging, and gaming applications.

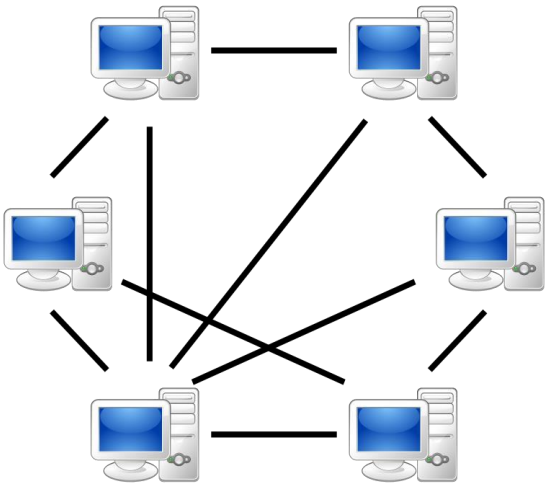


Figure 3 peer to peer

Anon, (2022). *What is Peer to Peer Network, and How does it work?[online]*

6.1.3 Client server

Client-server networking is a type of network system in which clients, or end-users, communicate with servers to access shared resources, such as files, applications, and data. The client sends requests to the server, and the server responds with the requested information. Here are a few types of client-server network systems:

File server: In this type of network, a central file server stores all shared files, which can be accessed by clients on the network. The file server manages file access and ensures that multiple clients do not access the same file simultaneously, which can cause data conflicts.

Print server: This type of network allows multiple users to access a shared printer. The print server manages print jobs and ensures that multiple users do not print to the same printer at the same time.

Web server: This type of network hosts web pages and web applications that can be accessed by clients via a web browser. The web server processes client requests and sends back the requested web pages.

Database server: In this type of network, a central database server stores all data, which can be accessed and manipulated by clients on the network. The database server manages data access and ensures that multiple clients do not modify the same data simultaneously, which can cause data inconsistencies.

Client-server networks are popular for their ability to centralize resources, manage access and security, and provide scalability. They are commonly used in business applications, such as email, file sharing, and database management.

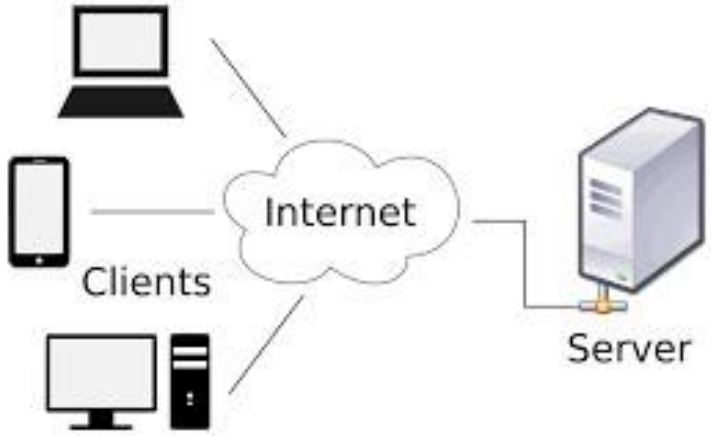


Figure 4 client server network

Computer Science GCSE GURU. (n.d.). *Client-Server Networks*. [online]

Code Institute Global. (2022). *What is a Client-Server Network?* [online]

Table 1 peer to peer and client server comparison

BASIS FOR COMAPAISON	CLIENT-SERVER	PEER-TO-PEER
Basic	There is a specific server and specific clients connected to the server.	Clients and server are not distinguished; each node act as client and server.
Service	The client request for service and server respond with the service.	Each node can request for services and can also provide the services.

BASIS FOR COMAPAISON	CLIENT-SERVER	PEER-TO-PEER
Focus	Sharing the information.	Connectivity.
Data	The data is stored in a centralized server.	Each peer has its own data.
Server	When several clients request for the services simultaneously, a server can get bottlenecked.	As the services are provided by several servers distributed in the peer-to-peer system, a server in not bottlenecked.
Expense	The client-server are expensive to implement.	Peer-to-peer are less expensive to implement.
Stability	Client-Server is more stable and scalable.	Peer-toper suffers if the number of peers increases in the system.

6.1.4 Cloud

Cloud computing is the delivery of computing services-servers ,storage, database, networking, software, analytics, and more- over the internet ("the cloud"). Computing offering these computing services are call typically charge for computing Loud computing services based on usage, like how you're billed for water or electricity at home.

(divition, the panel of lecturers HND;, 2022, p. page 5)

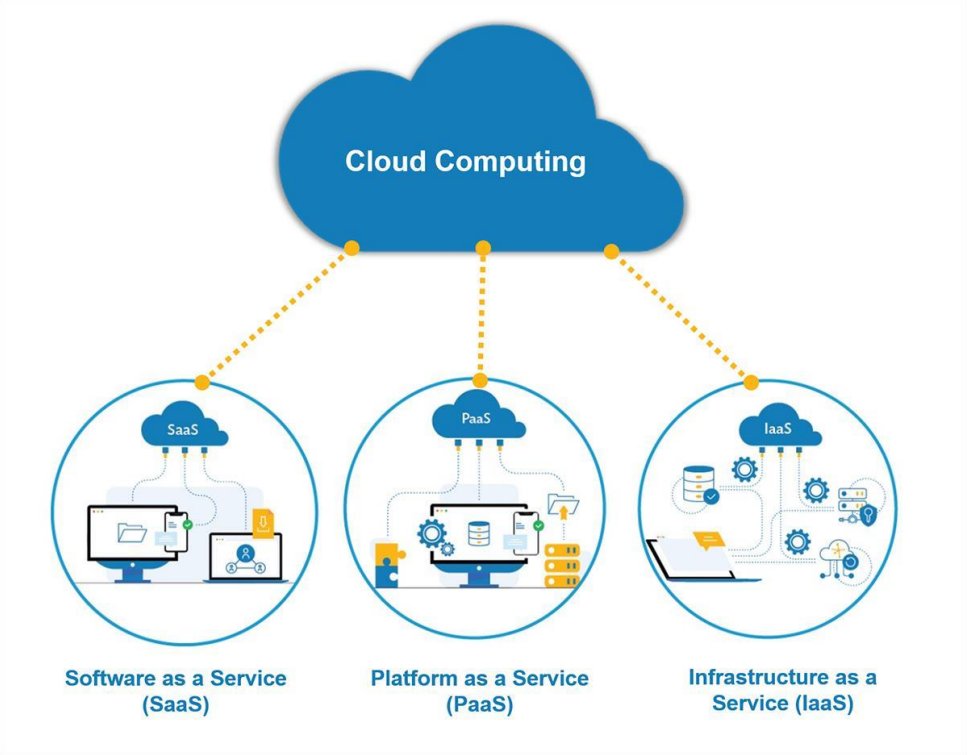


Figure 5 cloud serves.

Cloud computing is a model of delivering computing services over the internet. Instead of storing data and running applications on local servers or personal computers, users can access computing resources from remote servers located in data centers provided by a third-party service provider.

Cloud computing services are typically provided through a pay-as-you-go or subscription-based model, where users pay for the computing resources they use. This allows for flexibility in scaling up or down based on the demand for computing resources.

There are different types of cloud computing services, including:

Infrastructure-as-a-Service (IaaS): Provides virtualized computing resources such as servers, storage, and networking. Users can deploy and run their own software on the infrastructure provided by the cloud provider.

Platform-as-a-Service (PaaS): Provides a platform for building, deploying, and managing applications. The cloud provider manages the underlying infrastructure and users focus on developing and deploying their applications.

Software-as-a-Service (SaaS): Provides software applications that are hosted by the cloud provider and accessed by users over the internet. Users do not need to install the software on their local computers and can access it through a web browser or mobile app.

Cloud computing has several **benefits**, including:

Scalability: Cloud computing services can easily scale up or down to meet the changing demand for computing resources.

Cost-effective: Users can pay for the computing resources they use, eliminating the need for upfront investments in hardware and infrastructure.

Accessibility: Cloud computing services can be accessed from anywhere with an internet connection, making it easy for users to access their applications and data.

Reliability: Cloud computing providers typically offer high availability and reliability, with multiple servers and data centres to ensure continuity of service.

However, there are also some potential drawbacks, such as concerns around data privacy and security, dependency on third-party providers, and the potential for service disruptions due to internet connectivity issues. It is important for users to carefully evaluate their cloud computing needs and choose a provider that meets their specific requirements.

Frankenfield, J. (2022). *Cloud Computing*. [online
Google (n.d.). *What is Cloud Computing?* [online] Google Cloud

6.1.5 Cluster

In computer networking, a cluster is a group of computers, servers, or other networkconnected devices that work together to provide a service or run an application.

In a clustered network, the devices are interconnected and can communicate with each other to distribute workloads, share resources, and provide fault tolerance. The main purpose of clustering is to improve the availability and performance of network services, by distributing the load across multiple devices and ensuring that a single point of failure does not disrupt the entire network.

Clustering can be implemented in various ways, such as load balancing, failover clustering, and parallel processing. Load balancing involves distributing network traffic across multiple devices to prevent any one device from becoming overloaded. Failover clustering involves setting up redundant devices that can take over the workload of a failed device to ensure continuous service availability. Parallel processing involves breaking up a large task into smaller parts and distributing them across multiple devices to speed up the processing time.

Clustering can also be used in data centres and cloud computing environments to provide high availability and scalability for applications and services. Overall, clustering is an important technique in network design and management that helps to ensure reliable and efficient network operation.

The following are the programming interfaces for windows clustering technologies:

1. **The network load balancing provider (NLB)** is a software component of Microsoft Windows Server that provides a distributed load balancing mechanism for network traffic across multiple servers or network devices.

2. **The failover cluster APIs** is a group of two or more computers that work together to provide high availability for applications and services. In a failover cluster, if one node (computer) fails, another node takes over the workload automatically, without interruption, ensuring continuous service availability.

Virtana. (n.d.). *What are computer clusters?* [online]

Capital One. (n.d.). *What is a Cluster? An Introduction to Clustering in the Cloud*. [online]

(divition, the panel of lecturers HND;, 2022, p. page 7)

REDMOND\\markl (n.d.). *Network Load Balancing Provider*. [online]

REDMOND\\markl (n.d.). *Failover Cluster APIs*. [online]

6.1.6 Centralized

Centralized network architecture refers to a type of network design in which all network devices, resources, and services are located in a single central location or data center.

In a centralized network, all devices are connected to a central switch or router, which is responsible for managing the traffic and directing it to the appropriate destinations. The central location typically contains servers, storage devices, and other network resources, which are shared by all network users and devices.

Figure 6 explain centralized clipart.

Centralized network architecture has several advantages, including simplified network management, improved security, and easier resource allocation. By having all network devices and resources in a single location, network administrators can easily monitor and manage the network, apply security policies, and allocate resources to different users and applications.

Centralized networks can also reduce network costs by consolidating resources and reducing the number of devices required to support the network. Additionally, centralized network architecture can improve network performance by reducing the distance that network traffic needs to travel, and by providing a single point of control for network routing and switching.

However, centralized network architecture also has some drawbacks, such as the risk of a single point of failure, which could potentially bring down the entire network. Centralized networks can also be more complex and costly to set up and maintain than other types of network architectures.

Overall, centralized network architecture is a common approach to network design, particularly in enterprise environments, where centralized management and control are essential.

N-Able (2018). *The Difference Between Centralized and Decentralized Networks*. [online]

EasyTechJunkie. (n.d.). *What Is Centralized Network Management? (with pictures)*. [online]

6.1.7 Virtualized

Virtualized network architecture refers to a type of network design in which network services and resources are abstracted from their underlying hardware and presented to users and applications as virtual entities.

In a virtualized network, network devices, such as servers, switches, and routers, are abstracted from their physical hardware and presented as virtual machines or virtual appliances. Network resources, such as storage, bandwidth, and computing power, are also abstracted from their underlying hardware and presented as virtual entities.

Virtualized network architecture enables network administrators to create and manage network services and resources more efficiently and flexibly. By virtualizing network resources, administrators can allocate them dynamically to different applications and users, based on their needs. This can help to reduce costs, increase scalability, and improve network performance.

Virtualized network architecture also enables the creation of virtual private networks (VPNs), which can provide secure and private connectivity between different locations or remote users. VPNs can be created by using virtual appliances or software-defined networking (SDN) technologies, which can abstract the network infrastructure and create virtual network segments that can be isolated from other network traffic.

Another benefit of virtualized network architecture is that it can help to simplify network management by centralizing the control and management of network resources. By using management software and tools, administrators can monitor and manage the virtualized network resources from a single location, and apply policies and configurations to the entire network, rather than individual devices.

Overall, virtualized network architecture is becoming increasingly popular in modern network design, particularly in cloud computing environments, where flexibility, scalability, and cost efficiency are important considerations.

www.redhat.com. (n.d.). *What is network virtualization*. [online]

www.sciencedirect.com. (n.d.). *Network Virtualization - an overview | ScienceDirect Topics*. [online]

6.1.8 Personal Area Network (PAN)

A Personal Area Network (PAN) is a type of network system that is used for communication and data exchange between personal devices that are in close proximity to each other. A PAN can be established wirelessly or through a wired connection and is typically used for personal use rather than for business or enterprise applications.

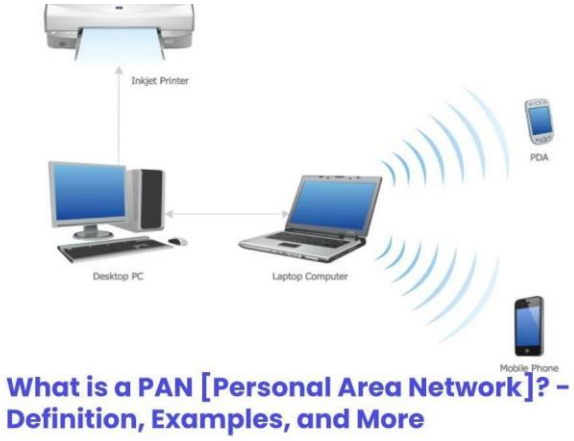


Figure 7personal area network (PAN)

The key characteristics of a PAN include:

Limited coverage area: A PAN typically covers a very small geographic area, typically a few meters, and is designed for use by a single person or device.

Low power consumption: Devices in a PAN typically have low power requirements and are designed to conserve battery life.

Short-range connectivity: PANs use wireless communication technologies such as Bluetooth, Zigbee, or Wi-Fi Direct, which have a short range of coverage.

Personal use: PANs are designed for personal use, typically for communication and data exchange between personal devices such as smartphones, laptops, tablets, and wearable devices.

Security: PANs can be secured by implementing authentication and encryption protocols to protect against unauthorized access and data theft.

Some common examples of devices that can be connected in a PAN include:

1. Smartphones and other mobile devices
2. Laptops and desktop computers
3. Wireless headphones and earbuds
4. Fitness trackers and smartwatches
5. Wireless keyboards and mice

PANs can be used for a variety of purposes, such as transferring files between devices, streaming audio or video content, and controlling smart home devices. They are useful for enabling communication and data exchange between personal devices that are in close proximity to each other, without the need for an internet connection or other external network.

Kapoor, A. (2022). *Importance of Types of Networks: LAN, MAN, and WAN | Simplilearn*. [online] Simplilearn.com.

Bourgeois, S. (2016). *Network-types*. [online] belden.com

javaTpoint (2011). *Types of Computer Network - JavaTpoint*. [online] www.javatpoint.com.

Figure 8 PERSONAL AREA NETWORK

A PAN can be very convenient and easy to set up. The following are a few benefits of using a PAN.

There is no need for wiring. A PAN avoids the need for additional wires by simply requiring Bluetooth to be enabled on the connected devices. This eliminates the requirement for floor area wastage and cable management, making it a very cost-effective network.

We can see many different PAN network instances every day. Some of those are.

1. Ultra-wideband (Ultra band)
2. ZigBee
3. Bluetooth
4. IrDA

Some of the **advantages** of a personal Area Network are:

1. There is no need for wiring: A PAN avoids the need for additional wires by simply requiring Bluetooth to be enabled on the connected devices. This eliminates the requirement for floor area wastage and cable management, making it a very cost-effective network.

2. Reliable and secure: If the connection is made within a 10-meter radius, a PAN network offers a dependable and steady connection.

3. Easy data synchronization: Data synchronization between several devices is made simple by a PAN. A PAN, for instance, allows all of the devices linked inside it to share, download, and upload data with one another.

4. Portability: A PAN provides extreme portability, as its wireless, and users can transport devices and exchange data wherever they want.

Some of the **Disadvantages** of a personal Area Network are:

1. Short network range and slow data transfer: A PAN uses Bluetooth communication that doesn't span beyond the 10-meter range. This makes long-distance data sharing difficult and slows down the rate of data transfers.

2. Signal interference: The Bluetooth and IrDA rays used for transmission in a PAN can cause interference with radio signals, which can severely interrupt and degrade the quality of communication between devices.

3. Cost: Using a PAN can be expensive, as most built-in WPAN devices are costly. Also, most devices used for creating a PAN have a higher price tag, such as smartphones and laptops.

4. Line of sight propagation: PANs mostly operate on IrDA technology, which travels in a straight line from one point to another, also known as the lineof-sight propagation. Unlike radio-based communications, IrDA devices must be aligned to work. For example, a TV remote won't work unless it's beamed directly to the TV screen.

6.1.9 Local Area Network (LAN)

A Local Area Network (LAN) is a type of network system that covers a relatively small geographic area, such as an office building, school, or a home. In a LAN,

multiple devices, such as computers, printers, and servers, are connected to each other to share resources and communicate with each other.

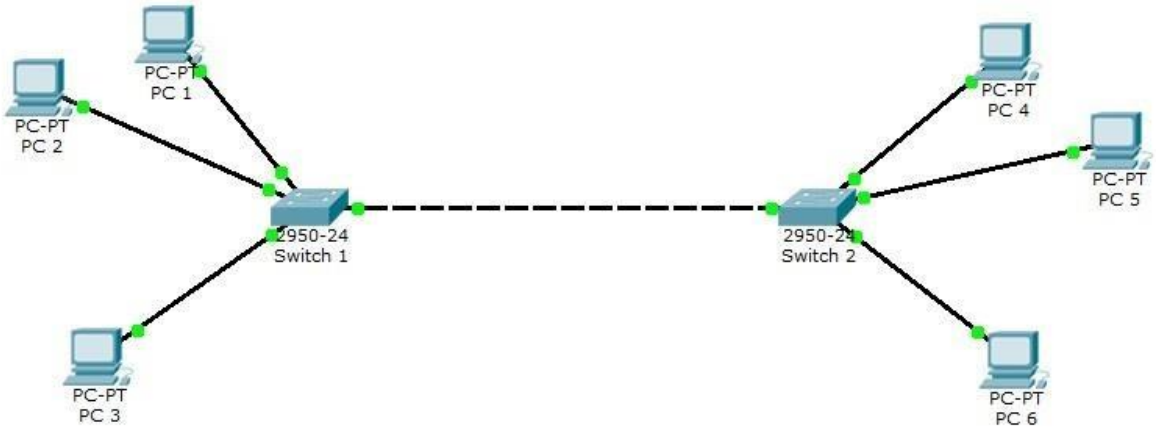


Figure 9 Example of the (LAN) NETWORK

The key characteristics of a LAN include:

Limited geographic area: A LAN typically covers a small geographic area, such as a building, floor, or campus.

1. High data transfer rates: LANs are designed to provide high-speed data transfer rates, which allow users to share data and resources quickly and efficiently.

2. Shared resources: In a LAN, devices can share resources such as printers, storage devices, and internet access.

3. Low cost: LANs are generally less expensive to set up and maintain than other types of network systems, such as WANs or MANs.

4. Security: LANs can be secured by implementing firewalls, passwords, and other security measures to protect against unauthorized access.

5. Common LAN topologies include:

   Bus Topology: In this topology, all devices are connected to a single cable or backbone. Data is transmitted from one end of the cable to the other.

6. Star Topology: In this topology, all devices are connected to a central hub or switch, which acts as a central point of communication.

7. Ring Topology: In this topology, devices are connected in a circular or ring-like configuration, with each device connected to the next in a chain.

LANs are used in a variety of settings, including homes, schools, businesses, and hospitals, to enable communication and resource sharing among devices and users in a localized area.

Kapoor, A. (2022). *Importance of Types of Networks: LAN, MAN, and WAN | Simplilearn*. [online] Simplilearn.com.

Bourgeois, S. (2016). *Network-types*. [online] belden.com

javaTpoint (2011). *Types of Computer Network - JavaTpoint*. [online] www.javatpoint.com.

www.javatpoint.com. (n.d.). *Advantages and Disadvantages of WAN - Javatpoint*. [online]

6.1.10 Wide Area Network (WAN)

A Wide Area Network (WAN) is a network that covers a large geographical area, such as a city, country, or even the entire world. It is used to connect multiple Local Area Networks (LANs) and other types of networks, allowing devices in different locations to communicate with each other.

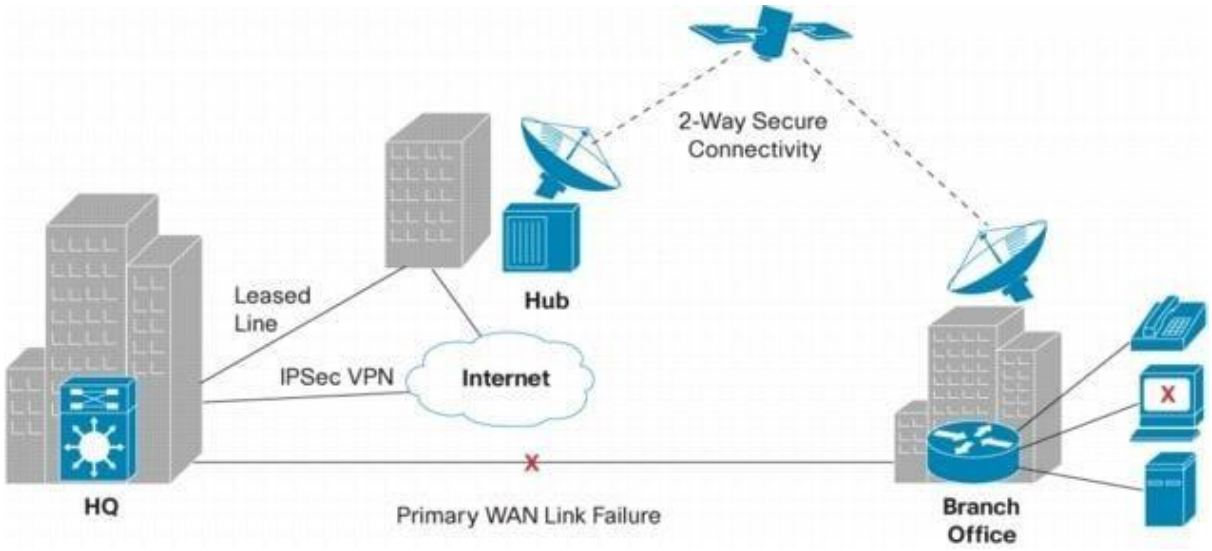


Figure 10 WAN area network (WAN)

WANs are typically used by businesses, organizations, and government agencies to connect their branch offices, data centers, and remote workers. WANs can use different types of communication technologies, including leased lines, satellite links, microwave links, and fiber-optic cables.

WANs can be privately owned, such as those used by large corporations or government agencies, or they can be provided by a telecommunications company as a service. The Internet itself can also be considered a WAN, as it connects millions of devices across the globe.

One of the key challenges of WANs is managing the latency and bandwidth limitations that come with transmitting data over long distances. This is usually addressed through various techniques such as optimizing data transmission protocols, caching frequently accessed data, and using content delivery networks (CDNs) to distribute data to multiple locations.

Kapoor, A. (2022). *Importance of Types of Networks: LAN, MAN, and WAN | Simplilearn*. [online] Simplilearn.com.

Bourgeois, S. (2016). *Network-types*. [online] belden.com

javaTpoint (2011). *Types of Computer Network - JavaTpoint*. [online] www.javatpoint.com

Cisco. (n.d.). *Cisco IP VSAT Satellite WAN Network Module for Cisco Integrated Services Routers*

We can see many different WAN network instances every day. Some of those are.

1. Mobile Internet
2. Last mile
3. Personal Network
4. Commercial Services
5. Internet

Some of the **advantages** of a Wide Area Network are.

1. Boost effectiveness: The centralized IT infrastructure can provide its customers with a better service because it can utilize all available bandwidth and capacity. This can help you convey information more swiftly and effectively.

2. simple interaction You don't need to worry about the speed of your network connection when communicating online with someone in a different country or even on a different continent. You can send communications quickly and easily using WAN technology while retaining a high level of confidentiality and anonymity.

3. The ability to communicate with anyone on the planet via a computer or cell phone at any time of day or night is made possible by the extensive geographic coverage provided by this technology. Using this technology, you can instantly connect with millions of people, no matter where they are in the world.

4. The WAN is the largest network, and it can also connect two countries.

5. We may securely store all our files and data on a single server computer with the aid of WAN. The information saved in this server is accessible by other computers linked to the WAN.

6. Since WANs have a wider coverage area than LANs and MANs, their bandwidth is also higher than other networks.

Some of the **Disadvantages** of a Wide Area Network are.

While Wide Area Networks (WANs) are an essential part of modern communication infrastructure, they also have a few disadvantages. Here are some of the major drawbacks of WANs:

1. High Cost: WANs typically require expensive hardware and software components to set up and maintain, making them more expensive than other types of networks. WANs may also require ongoing maintenance, upgrades, and support, which adds to their overall cost.

2. Limited Bandwidth: WANs can suffer from bandwidth limitations due to the distance between nodes, as well as the number of nodes on the network. This can result in slower data transfer speeds, which can be problematic for large files and real-time applications.

3. Security Risks: WANs can be vulnerable to security threats, such as hacking, data breaches, and malware attacks. The large scale of WANs makes it difficult to control access to network resources, which can lead to security breaches.

4. Dependency on Service Providers: WANs often rely on service providers to maintain the network infrastructure and provide internet connectivity. This can create a dependency on third-party providers and make it difficult to troubleshoot and resolve network issues.

5. Network Complexity: WANs can be complex to set up and manage, especially if they involve multiple locations or remote workers. This can make it challenging to troubleshoot network issues and ensure consistent performance across the network.

6. Overall, while WANs offer many advantages, they also come with a few significant disadvantages. Organizations must carefully consider their needs and requirements before deciding to implement a WAN.

6.1.11 Metropolitan area network (MAN)

A Metropolitan Area Network (MAN) is a type of computer network that spans a geographic area larger than a Local Area Network (LAN) but smaller than a Wide Area Network (WAN). MANs typically cover a city or a metropolitan area, hence the name.

A MAN is usually designed to interconnect a group of LANs or other networks within a city or a campus. It can be used to provide high-speed connectivity between multiple

locations within the same city or to provide Internet access to a group of buildings or organizations in the same area.

MANs can be built using various technologies, including fiber optic cables, wireless links, and leased lines. They can be owned and managed by a single organization, such as a university or a municipal government, or they can be owned and managed by a group of organizations that share the network infrastructure.

One of the key benefits of a MAN is its ability to provide high-speed connectivity over a relatively large geographic area. This makes it useful for businesses and organizations that need to transfer large amounts of data quickly between different locations. MANs can also be more cost-effective than WANs because they do not require as much infrastructure or equipment to set up and maintain.

Cisco. (n.d.). *Cisco IP VSAT Satellite WAN Network Module for Cisco Integrated Services Routers*. [online]

We can see many different MAN network instances every day. Some of those are.

- Cable TV network
- Telephone networks
- DSL line
- The IUB network
- IEEE 802.16
- WiMAX

Some of the **advantages** of a Metropolitan Area Network are.

1. Metropolitan Area Network allows people to connect LANs.
2. It improves data handling efficiency while increasing data transfer speed.
3. It can send data in both directions at the same time.
4. It increases WAN access by acting as a great backbone for a big network.
5. A Metropolitan Area Network's implementation costs are cheaper than WAN's since it uses fewer resources.
6. It makes it possible to share resources like printers at a low cost.
7. Metropolitan Area Network usually encompasses several city blocks or an entire city.

Some of the **disadvantages** of a Metropolitan Area Network are:

1. Compared to LAN, more cable is required to set up a Metropolitan Area Network.
2. The data rate is slow in a Metropolitan Area Network compared to LAN.
3. It makes it possible to share resources like printers at a low cost.
4. Because this network consists of several LANs, it is challenging to prevent hackers from entering.
5. Network administrators and experienced technicians are required to implement these networks.
6. The costs of setting up and maintaining this network are more than those of a local area network.
7. This network is complicated to operate since it is a vast network made up of multiple local area networks.
8. The overall installation and management costs increase since qualified technicians and network administrators are required to implement this network.

,

Kapoor, A. (2022). *Importance of Types of Networks: LAN, MAN, and WAN | Simplilearn*. [online]

Kapoor, A. (2022). *Importance of Types of Networks: LAN, MAN, and WAN | Simplilearn*. [online]

6.1.12 Virtual privet network (VPN)

An encrypted connection between a device and a network via the Internet is known as a virtual private network, or VPN. Secure transmission of sensitive data is aided by the encrypted connection. It makes it impossible for unauthorized parties to eavesdrop on the traffic and enables remote work for the user. The use of VPN technology is common in business settings.

6.1.13 STRONGE AREA NETWORK (SAN)

The Storage Area Network is referred to by the acronym SAN. Block-level data storage is offered via the dedicated, specialized, and fast Storage Area Network. It provides several servers with access to the pool of shared storage devices.

6.1.14 Controller area network (CAN)

A high-integrity serial bus system for networking intelligent devices is called a controller area network (CAN) bus. Devices and CAN busses are frequently found in industrial and automotive systems. You can create LabVIEW applications to interact with a CAN network using a CAN interface device.

We have discussed one categorization of network types above. Networks can be categorized as intranet and extranet as well.

6.1.15 Intranet

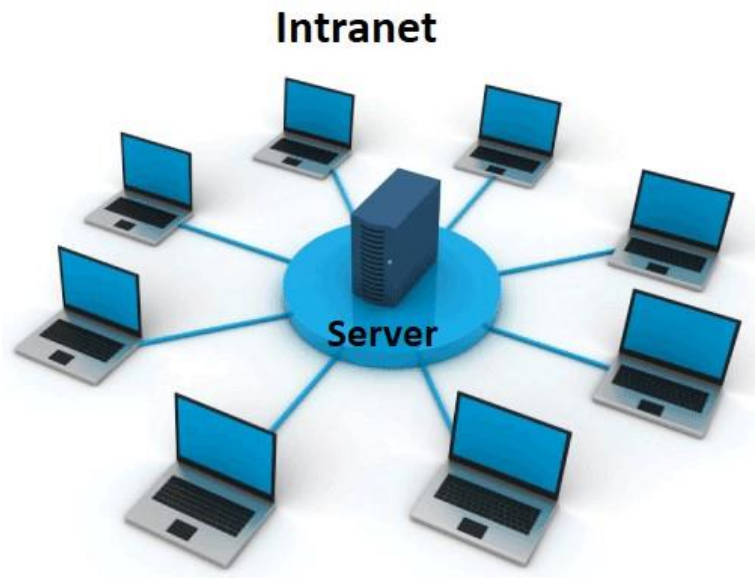


Figure 11 intranet

An intranet is a personal network that is exclusive to a specific company. It is intended for for usage by a company and those connected to it, including customers, employees, and other authorized individuals. It provides a safe environment for sharing data and information with authorized users. The staff can be given access to confidential data, databases, links, forms, and apps via the intranet. In order to give access to information and documents within an organization to its employees, it functions like a private internet or an internal website. An individual IP Address is used to identify each computer on the intranet.

An intranet is a private network that is used by an organization to share information, resources, and communication among its members. Here are some advantages and disadvantages of using an intranet:

Advantages:

1. Improved Communication: Intranets provide a platform for better communication within the organization. Members can share information and collaborate easily, regardless of their location.

2. Centralized Information: Intranets provide a centralized location for information and resources, making it easier for members to find what they need.

3. Increased Productivity: Intranets can help increase productivity by providing easy access to information and resources, reducing the time spent on searching for information.

4. Enhanced Security: Intranets are private networks, so they are more secure than the internet. This can help protect sensitive information and prevent unauthorized access.

5. Cost-effective: Intranets can be more cost-effective than other forms of communication, such as paper-based systems or traditional mail.

Disadvantages:

1. Initial Setup Cost: The initial setup cost for an intranet can be high, especially for small organizations.

2. Maintenance Cost: Intranets require ongoing maintenance and updates to keep them functioning properly.

3. Dependence on Technology: Intranets rely on technology, which can be subject to failures or malfunctions.

4. Training and Support: Members may require training and support to effectively use the intranet.

5. Limited Accessibility: Intranets are only accessible within the organization, so members who work remotely may have limited access to information and resources.

www.javatpoint.com. (n.d.). *Intranet - javatpoint*. [online]

6.1.16 Extranet

An extranet is a private network that is only accessible to specific people within an organization. It provides a safe and secure means to communicate with partners, consumers, and other third parties. To access the network, users typically use a login method like a username and password. Simply put, an extranet offers a secure network so that a company can communicate information with pertinent people outside the company. It is a section of an intranet that is divided by a firewall.

An extranet is a private network that allows authorized users to access information and resources from outside an organization, such as customers, partners, or suppliers. Here are some advantages and disadvantages of using an extranet:

Advantages:

1. Improved Collaboration: Extranets allow organizations to collaborate with their partners, customers, or suppliers more effectively, sharing information and resources in real-time.

2. Increased Productivity: Extranets can help increase productivity by providing easy access to information and resources, reducing the time spent on searching for information.

3. Enhanced Security: Extranets are private networks, so they are more secure than the internet. This can help protect sensitive information and prevent unauthorized access.

4. Cost-effective: Extranets can be more cost-effective than other forms of communication, such as paper-based systems or traditional mail.

5. Scalability: Extranets can be scaled up or down depending on the needs of the organization.

Disadvantages:

1. Initial Setup Cost: The initial setup cost for an extranet can be high, especially for small organizations.

2. Maintenance Cost: Extranets require ongoing maintenance and updates to keep them functioning properly.

3. Dependence on Technology: Extranets rely on technology, which can be subject to failures or malfunctions.

4. Training and Support: Authorized users may require training and support to effectively use the extranet.

5. Security Risks: Extranets can be susceptible to security breaches, especially if users are not careful with their login credentials or if the network is not properly secured.

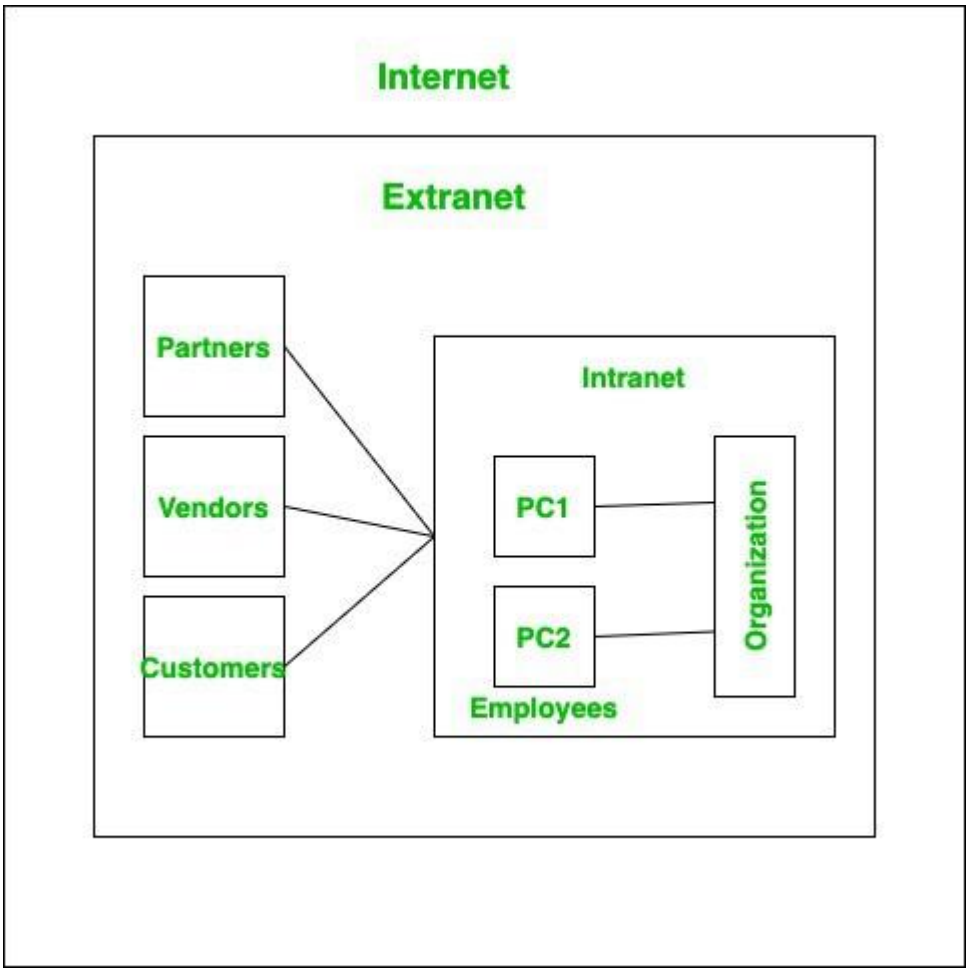


Figure 12 extranet explain.

GeeksforGeeks. (2021). *What is Extranet? Definition, Implementation, Features*. [online

6.2 NETWORKING STANDARDS

6.2.1 Network Standards and Standardization Bodies

Networking standards are a set of guidelines and rules that ensure interoperability and compatibility between networking devices and systems. These standards are developed by various organizations such as the Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), and the Internet Engineering Task Force (IETF).

Networking standards cover a wide range of aspects of networking, including protocols, hardware interfaces, and data formats. They are essential for ensuring that devices from different manufacturers can communicate and work together seamlessly, as well as for ensuring the security and reliability of networks.

Some of the most commonly used networking standards include Ethernet, Wi-Fi, TCP/IP, DNS, HTTP, and SSL/TLS. Ethernet is a wired networking standard that is used for local area networks (LANs), while Wi-Fi is a wireless networking standard that is used for wireless LANs. TCP/IP is a set of protocols that governs how data is transmitted across the internet, while DNS is a protocol that translates domain names into IP addresses. HTTP is a protocol that governs how web pages are requested and served, while SSL/TLS is a protocol that provides secure communication over the internet.

Overall, networking standards are essential for ensuring the smooth and reliable operation of networks and for enabling the communication and sharing of information between devices and systems.

6.2.2 Standards Organizations

Some of the noted standard's organizations are:

6.2.2.1 International Standards Organization (ISO)

The International Organization for Standardization, commonly known as ISO, is an independent, non-governmental international organization that develops and publishes standards for various industries and sectors. The ISO was founded in 1947 and is headquartered in Geneva, Switzerland.

Figure 13 ISO logo

The ISO develops and publishes a wide range of international standards that cover many areas of industry and commerce,

including quality management, environmental management, information security, and many others. The standards are developed by technical committees that are made up of experts from around the world and are designed to ensure consistency and compatibility across industries and borders.

ISO standards are recognized globally and are used by organizations of all sizes, from small businesses to multinational corporations. Compliance with ISO standards is often a requirement for doing business in certain industries and regions, and can provide organizations with a competitive advantage by demonstrating their commitment to quality, safety, and environmental responsibility.

Overall, the ISO plays an important role in developing and promoting international standards that support innovation, trade, and economic growth while also protecting consumers and the environment. ISO (2022). *About us*. [online]

www.creativesafetysupply.com. (n.d.). *International Standards Organizations (ISO)*. [online]

6.2.2.2 Institute of Electronics and Electrical Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is a professional organization that is dedicated to advancing technology in the fields of electrical and electronics engineering. It is the world's largest technical professional organization with over 400,000 members in more than 160 countries. The IEEE is responsible for developing and publishing technical standards related to a wide range of technologies, including telecommunications, power generation and distribution, computing, biomedical engineering, and many others. The organization also provides educational and professional development opportunities for its members and plays a leading role in shaping the future of technology.

Figure 14 IEEE logo

6.2.2.3 American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) is a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States. Founded in 1918, ANSI is responsible for accrediting standards development organizations, developing accreditation programs, and promoting the use of standards to improve safety, quality, and competitiveness across all industries. ANSI is also the U.S. member body to the International Organization for Standardization (ISO), ensuring that American interests

are represented in the development of international standards. ANSI plays a key role in promoting standardization in the United States and around the world.

Figure 15 ANSI logo

American National Standards Institute - ANSI. (n.d.). *ANSI Introduction*. [online] Available at: https://www.ansi.org/about/introduction.

6.2.2.4 Internet Research Task Force (IETF)

The Internet Research Task Force (IETF) is a large open international community of network designers, engineers, and researchers that promotes the development of Internet standards and protocols. The IETF is responsible for the development of the technical standards that govern how the internet operates, including the TCP/IP protocol suite, HTTP, DNS, and many others. The IETF works through a number of working groups, each focused on a specific area of Internet technology, and is committed to an open, collaborative, and consensus-driven approach to standardization. The IETF plays a crucial role in the development and evolution of the internet, ensuring that it remains an open, interoperable, and secure platform for communication and innovation.

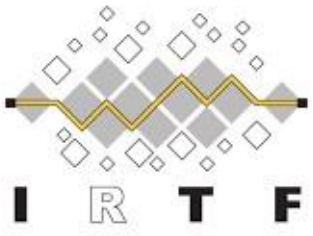


Figure 16 IETF logo

irtf.org. (n.d.). *Internet Research Task Force*. [online]

6.2.2.5 world wide web consortium(w3c)

The World Wide Web Consortium (W3C) is an international community dedicated to developing open web standards and protocols. Founded in 1994 by Tim Berners-Lee, the inventor of the World Wide Web, the W3C is made up of member organizations from around the world, including companies, universities, government agencies, and non-profits. The W3C works to create technical standards for the web that promote interoperability, accessibility, and usability, and its work includes the development of HTML, CSS, and other web technologies. The W3C is committed to an open and transparent standards development process, and its standards are widely used by web developers and browser vendors around the world.

Figure 17 W3C Logo

W3C (2008). *World Wide Web Consortium (W3C)*. [online]

Some more of the noted standards organizations are:

1. Electronic Industries Association (EIA)

2. International Telecommunication Union (ITU)

Anon, (n.d.). *4.6. Network Standards and Standardization Bodies – Wachemo University e-Learning Platform*. [online]

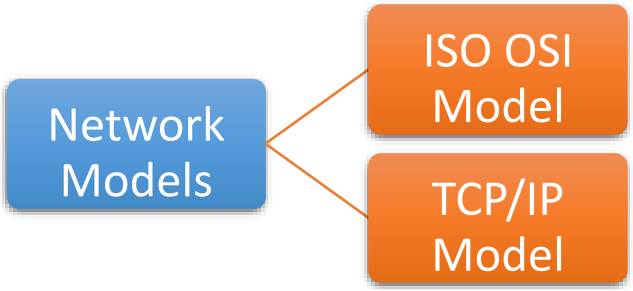
Organization web site
ANSI (WWW.ansi.org)
EEE (WWW.ieee.org)
ISO (WWW.iso.org)
IETF (WWW.ieft.org)
W3C (WWW.w3c.org)

6.2.3 NETWORK MODELS

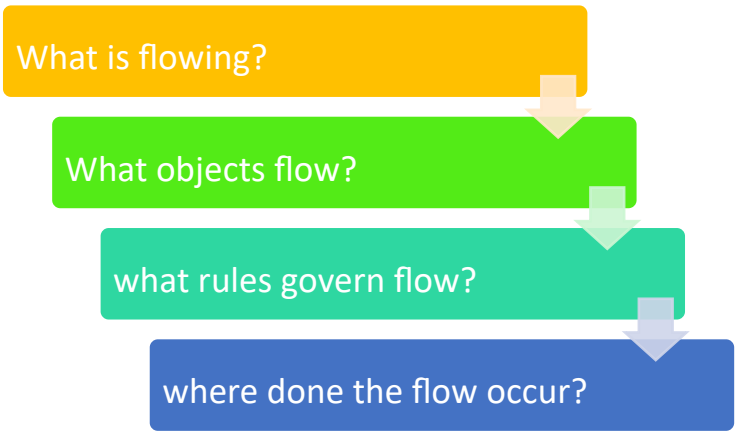
In computer networking, a network model is a conceptual framework that describes the various layers of communication and protocols that make up a computer network. The most widely used network model is the OSI (Open Systems Interconnection) model, which divides network communication into seven distinct layers. The layers of the OSI model, from top to bottom, are application, presentation, session, transport, network, data link, and physical.

Another popular network model is the TCP/IP (Transmission Control Protocol/Internet Protocol) model, which is based on a four-layer conceptual framework. The layers of the TCP/IP model, from top to bottom, are application, transport, internet, and network access.

Network models provide a structured way of understanding the complex interactions between the different layers of a network and can help network designers and administrators to troubleshoot and optimize network performance. They also provide a common language and reference point for developers working on network protocols and applications.



NOTE: network models are conceptual models that help to explain the data communication within a computer network



(divition, the panel of lecturers HND;, 2022, p. page 17)

6.2.3.1 ISO OSI Model

The ISO OSI model (Open Systems Interconnection model) is a conceptual framework that describes how network communications should occur between computers. It was developed by the International Organization for Standardization (ISO) in the early 1984s to standardize network communications.

The OSI model consists of seven layers, each with a specific function that facilitates communication between devices. These layers are:

1. **Physical Layer:** This layer deals with the physical transmission of data over the network. It includes specifications for the cables, connectors, and other hardware used for communication.

2. **Data Link Layer:** This layer ensures the reliable transmission of data over the physical layer. It is responsible for error detection and correction and also manages flow control between devices.

3. **Network Layer:** This layer provides the ability to route data between networks. It determines the best path for data to travel across multiple networks.

4. **Transport Layer:** This layer ensures that data is transmitted reliably between applications. It manages end-to-end communication and provides error recovery and flow control.

5. **Session Layer**: This layer establishes, manages, and terminates communication sessions between applications.

6. **Presentation Layer**: This layer ensures that data is presented in a format that can be understood by the receiving application. It handles tasks such as data compression, encryption, and decryption.

7. **Application Layer:** This layer provides the interface between the user and the network. It includes application protocols such as HTTP, FTP, and SMTP.

The OSI model is widely used as a reference model for understanding how network communication works.

Gaurav, S. (2022). *What is the OSI Model? Layers of OSI Model*. [online]

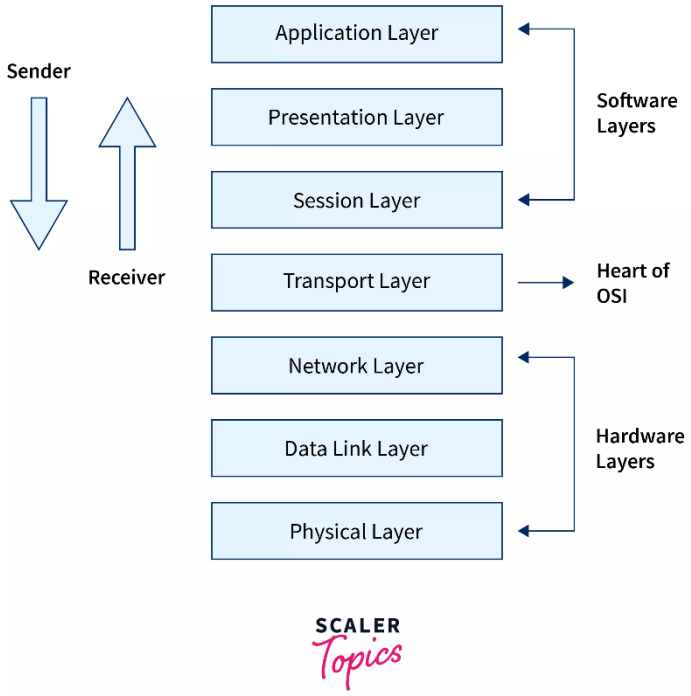


Figure 18 ISO OSI model

6.2.3.2 TCP/IP Model

The TCP/IP model is a networking model that was developed in the 1970s by the US Department of Defense. It is the foundation for the Internet and is widely used as a networking standard.

The TCP/IP model consists of four layers, each with a specific function that facilitates communication between devices. These layers are:

1. **Network Access Layer**: This layer deals with the physical transmission of data over the network. It includes specifications for the cables, connectors, and other hardware used for communication. This layer is similar to the Physical and Data Link layers in the OSI model.

2. **Internet Layer:** This layer provides the ability to route data between networks. It determines the best path for data to travel across multiple networks. This layer is similar to the Network layer in the OSI model.

3. **Transport Layer:** This layer ensures that data is transmitted reliably between applications. It manages end-to-end communication and provides error recovery and flow control. This layer is similar to the Transport layer in the OSI model.

4. **Application Layer:** This layer provides the interface between the user and the network. It includes application protocols such as HTTP, FTP, and SMTP. This layer is similar to the Session, Presentation, and Application layers in the OSI model.

One of the key differences between the TCP/IP model and the OSI model is that the TCP/IP model has fewer layers. This makes it more efficient and easier to implement. Additionally, the TCP/IP model is more closely aligned with the way that the Internet works, which makes it a more practical networking model for modern-day networks.

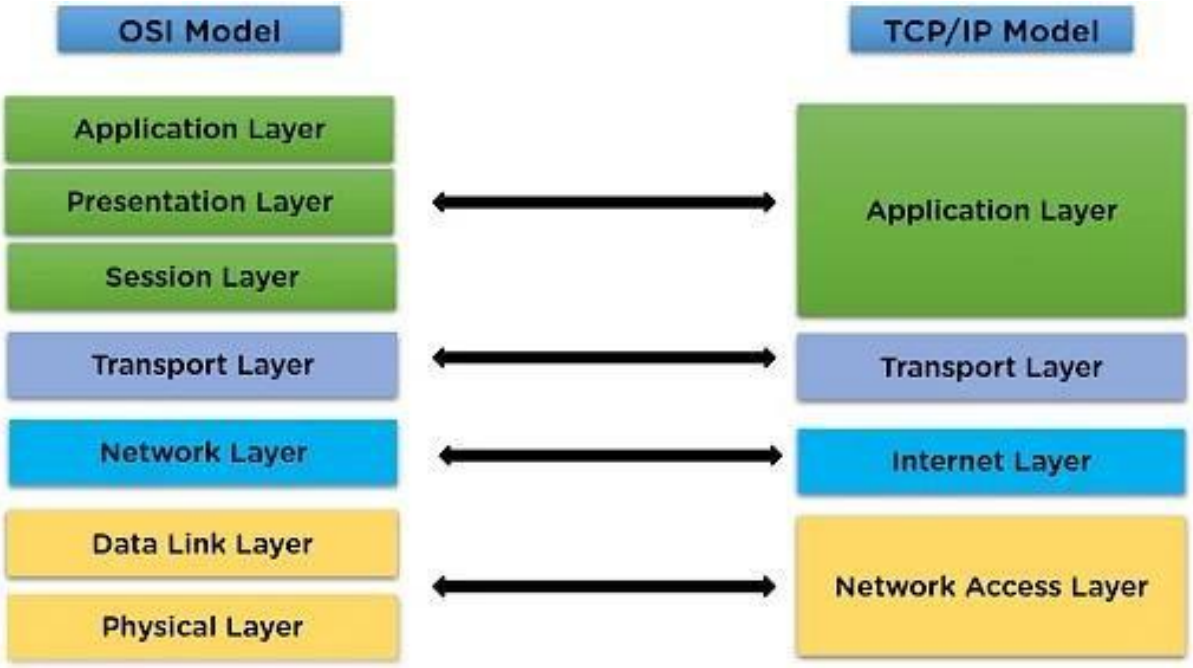


Figure 19 OSI to TCP/PI mapping

GeeksforGeeks (2019). *TCP/IP Model - GeeksforGeeks*. [online]

6.2.4 PROTOCOLS

Protocols in networking are a set of rules and guidelines that govern the communication between devices on a network. These protocols define the format and sequence of messages transmitted between devices and specify how errors and other issues are handled during the communication process.

There are numerous protocols used in networking, but some of the most commonly used protocols include:

1. The Internet's foundational protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), is used to transmit data over a network. While IP is in charge of addressing and routing data across the Internet, TCP is in charge of making sure that data is transmitted reliably.

2. Data is transferred over the World Wide Web using the Hypertext Transfer Protocol (HTTP). It describes how web browsers and web servers interact to send and receive requests for web pages and other resources.
3. File Transfer Protocol (FTP): This protocol is used for transferring files between devices on a network. It is often used for downloading files from a server or uploading files to a website.

4. Simple Mail Transfer Protocol (SMTP): This protocol is used for transmitting email messages over a network. It defines how email servers communicate with each other to send and receive email messages.

5. Domain Name System (DNS): This protocol is used to translate domain names into IP addresses, which allows devices to locate and communicate with each other on a network.

6. Dynamic Host Configuration Protocol (DHCP): This protocol is used to assign IP addresses to devices on a network automatically.

7. These protocols, along with others, provide the foundation for communication between devices on a network. They ensure that data is transmitted accurately, securely, and efficiently, allowing users to access the resources and information they need.

communications @manageengine.com, M. (n.d.). *Network Monitoring Software by ManageEngine OpManager*. [online]

Default. (n.d.). *Network Protocol Definition | Computer Protocol | Computer Networks | CompTIA*. [online]

6.2.4.1 File Transfer Protocol (FTP)

A TCP/IP network, such as the internet, uses the File Transfer Protocol (FTP) to move files from one host to another. A client device (the client) requests data from a server device (the server) via the client-server protocol known as FTP (the server)

Users can download and upload files to and from a distant server using FTP. It can be utilized for a number of things, including downloading software updates, posting files to websites, and backing up data to a distant server.

FTP uses two channels to transfer data between the client and server: a control channel and a data channel. The control channel is used for sending commands and receiving responses between the client and server. The data channel is used to transfer files between the client and server.

FTP has several commands that allow users to interact with remote servers, including:

1. CONNECT: This command is used to establish a connection to a remote server.
2. LOGIN: This command is used to log in to a remote server.
3. CD: This command is used to change the current directory on the remote server.
4. GET: This command is used to download a file from the remote server to the client.
5. PUT: This command is used to upload a file from the client to the remote server.

FTP can be used with a variety of operating systems and supports a range of security options, such as SSL/TLS encryption and username/password authentication. However, FTP is considered to be an insecure protocol, as it transmits login credentials and data in plaintext, making it vulnerable to interception and hacking. As such, alternative protocols such as SFTP and FTPS are often used instead.

Mitchell, C. (n.d.). *File Transfer Protocol (FTP) Definition*. [online]

6.2.4.2 SSH – Secure Shell

SSH (Secure Shell) is a network protocol used for secure communication between two devices over an unsecured network, such as the internet. SSH is designed to provide a secure remote access to a device, allowing users to securely log in and access files, applications, and services on remote devices.

SSH works by establishing an encrypted connection between two devices, allowing secure communication to take place. This is achieved through the use of cryptographic techniques, such as public key cryptography and symmetric encryption. SSH provides a number of security features, including:

1. Authentication: SSH requires users to authenticate themselves using a username and password, or by using public key authentication, which is a more secure method.

2. Encryption: SSH uses encryption to protect the confidentiality of data transmitted between devices. This ensures that data cannot be intercepted or read by unauthorized users.

3. Integrity: SSH provides data integrity by using cryptographic checksums to verify that data has not been tampered with during transmission.

4. Port forwarding: SSH allows users to forward network traffic from one device to another, providing a secure way to access remote services.

SSH is widely used in the IT industry for remote server management, software development, and system administration. It is also used for secure file transfer, with protocols such as SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol) built on top of the SSH protocol. Overall, SSH provides a secure and reliable way to access and manage devices over unsecured networks.

www.ssh.com. (n.d.). *SSH Secure Shell home page, maintained by SSH protocol inventor Tatu Ylonen. SSH clients, servers, tutorials, howtos.* [online]

6.2.4.3 Telnet

Telnet is a network protocol that allows for two-way, collaborative, text-based communication between two computers as well as remote computer access.

It uses the Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocol to create remote sessions in response to user commands. While Telnet allows users to log on as regular users with the access credentials they are permitted to the specific apps and data on that computer, HTTP and FTP on the web only allow users to request specific files from remote computers.

6.2.4.4 SMTP- Simple Mail Transfer protocol

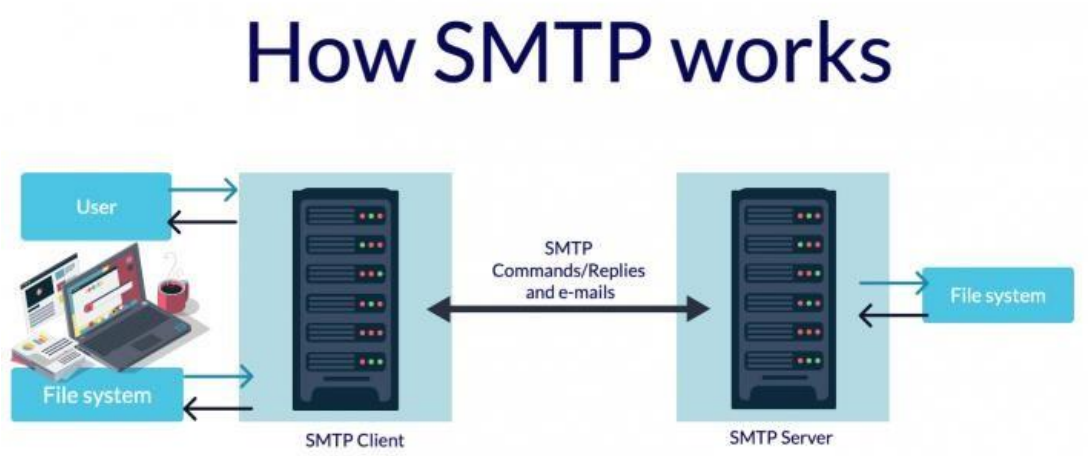


Figure 20 how to SMTP work

Email is sent and received using SMTP. IMAP or POP3 are sometimes used in conjunction with it (for instance, by a user-level application) to handle message retrieval, whereas SMTP is primarily used to send messages to servers for forwarding. Although SMTP can transmit and receive mail, it performs poorly at queuing incoming messages, which is why other protocols are frequently delegated in its place. While using their own servers, proprietary systems like Gmail have their own mail transfer protocols; however, beyond that, they continue to use the trusted SMTP protocol.

1. Simple Mail Transmission Protocol is known as SMTP.
2. The Simple Mail Transmission Protocol (SMTP) is a set of rules for communication that enables applications to send electronic mail over the internet.
3. Based on email addresses, it is an application used to deliver messages to other computer users.
4. Amongst users using the same or other computers, it offers mail exchange, and it also supports:
5. One message may be sent to one or many recipients.
6. Messages can be sent using text, voice, video, or graphics.
7. The communications may also be sent via networks other than the Internet.

6.2.4.5 POP3-Post Office Protocol

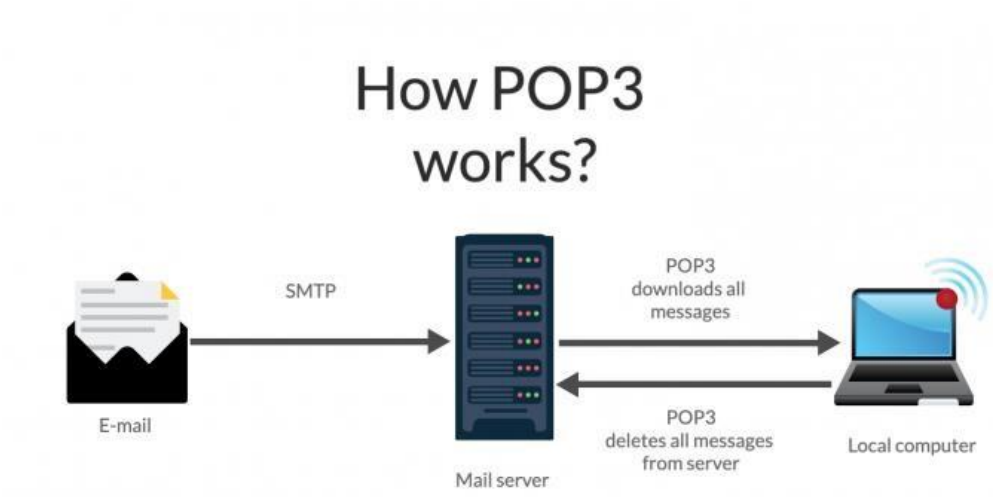


Figure 21 how to POP3 works?

Post Office Protocol version 3 is known as POP3, and it allows access to an inbox that is kept on a mail server. It carries out the download and message deletion actions. Hence, a POP3 client obtains all messages from the mailbox when it establishes a connection with the mail server. Once they are deleted from the remote server, it stores them on your local computer.

You can access the messages locally and in offline mode because of this protocol.

If you specifically choose this option, modern POP3 clients allow you to keep a duplicate of your messages on the server.

6.2.4.6 DNS- Domain name service

The POP3 protocol is straightforward and has only a few features. While using the POP3 protocol, the recipient's machine must have the POP3 client installed, and the recipient's mail server must have the POP3 server installed.

1. The emails are quick and simple to obtain because they are already on our PC.
2. The size of the emails we transmit or receive has no size restriction.

3. As every email is saved locally, the server needs less storage space.
4. The size of the hard disk places a cap on the mailbox's maximum size.
5. It is one of the most widely used protocols in use today because it is straightforward.
6. It is simple to set up and utilize.

6.2.4.7 HTTP- Hyper Text Transfer Protocol

1. Here are some key points about HTTP (Hyper Text Transfer Protocol):

2. HTTP is a client-server protocol used for transferring hypertext (text with embedded links) over the internet.

3. It is the foundation of data communication on the World Wide Web (WWW) and is responsible for handling the communication between a client and a server.

4. HTTP is a stateless protocol, meaning that each request/response pair is independent of any previous requests or responses.

5. HTTP operates on top of the TCP/IP protocol, which provides reliable, ordered, and error-checked delivery of data.

6. HTTP requests are initiated by the client, which sends a request message to the server, specifying the method (such as GET or POST) and the resource (such as a web page or file) being requested.

7. The server responds to the request with an HTTP response message containing the requested data, such as the HTML, images, and other resources.

8. HTTP supports several methods, including GET, POST, PUT, DELETE, and others, each with its own specific purpose.

9. HTTP is extensible, meaning that new features can be added to the protocol over time.

10. HTTP is the basis for the modern web and is used in virtually all web applications and services, including web browsers, web servers, APIs, and more.

11. Overall, HTTP is a crucial component of the internet and the web, providing a standardized way for clients and servers to communicate and transfer data in a reliable, efficient, and extensible manner.

6.2.4.8 DHCP-Dynamic Host Configuration Protocol

A network management technique called Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addresses and other network configuration

elements to devices on a network, including subnet mask, default gateway, and DNS server addresses.

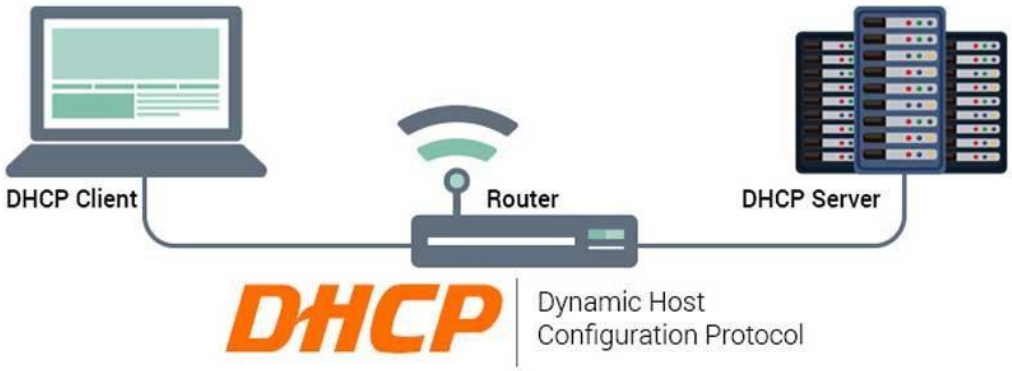


Figure 22 DHCP explain map

DHCP makes it simpler for network managers to expand and operate big networks by centralizing and automating IP address management. Network administrators would have to manually allocate IP addresses to each device absent DHCP, which would take time and be prone to mistakes.

A device that uses DHCP to connect to a network broadcasts a request for network configuration data. In response to the request, a DHCP server on the network offers an IP address and other configuration parameters. After accepting the offer, the device can finish the configuration procedure and start interacting with other networked devices.

In a process called as a lease, DHCP can also be used to dynamically assign IP addresses to devices. The device must ask the DHCP server for a new lease when the current one expires. By doing this, it is ensured that IP addresses are allotted effectively and are not thrown away when devices depart the network.

In conclusion, DHCP is an essential protocol for controlling IP addresses and network configuration on contemporary networks, enabling automation and scalability that would be challenging to achieve otherwise.

www.javatpoint.com. (n.d.). *POP Protocol | Post Office Protocol - javatpoint*. [online

6.2.4.9 IP

IP (Internet Protocol) is a protocol used for communicating data across networks, including the internet. It provides a standardized way for devices to send and receive

data packets, which can contain information such as text, images, and other types of data.

In networking, IP addresses are used to identify devices on a network. An IP address is a unique numerical identifier assigned to each device connected to a network, such as a computer, server, or router. IP addresses are used to route data packets to their intended destination, allowing devices on a network to communicate with each other.

There are two versions of IP currently in use: IPv4 and IPv6. IPv4 addresses are 32-bit numbers, expressed as four decimal numbers separated by periods, while IPv6 addresses are 128-bit numbers, expressed as hexadecimal values separated by colons. IPv4 addresses are more commonly used, but IPv6 is becoming increasingly important as the number of devices connected to the internet continues to grow.

In addition to identifying devices on a network, IP also provides a range of other features, including:

Fragmentation and reassembly of data packets to accommodate different network configurations and sizes.

Routing of data packets to their intended destination using routers and switches.

Error checking and correction to ensure that data is transmitted reliably and accurately.

Overall, IP is a fundamental protocol for networking, providing a standardized way for devices to communicate with each other across networks. IP addresses are a critical component of this, allowing devices to be uniquely identified and enabling data to be routed to its intended destination

Kaspersky (2021). *What is an IP Address – Definition and Explanation*. [online]

6.2.5 Network Topologies

Network topology is the arrangement of various components of a network, such as computers, routers, switches, and servers, and how they are interconnected. It is an essential concept in computer networking and is crucial to designing, building, and maintaining effective and efficient networks.

Network topology can be physical, such as the actual layout of cables, devices, and other physical components, or logical, which refers to the way data flows through the network. The choice of topology can significantly impact a network's performance,

reliability, and scalability, and therefore it is essential to select the appropriate topology for a given network.

There are several common network topologies, including the bus topology, star topology, ring topology, mesh topology, and tree topology. Each topology has its own advantages and disadvantages, and the selection of a specific topology depends on various factors such as network size, cost, fault tolerance, and performance requirements.

Understanding network topology is essential for network administrators, designers, and engineers to ensure that the network is optimized for its intended purpose, secure, and reliable. As networks continue to evolve and become more complex, network topology will remain a critical concept for managing and improving network performance.

A network's configuration can make or break its connectivity, functioning, and uptime protection. An explanation of the two categories in the network topology can provide an answer to the question, "What is network topology?"

1. **Physical** – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network.

2. **Logical** – The logical network topology is a higher-level idea of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources.

Contributor, S. (2019). *What is network topology? Best guide to types & diagrams - dnsstuff*.

6.2.6 Physical topology

6.2.6.1 BUS Topology

In a bus topology, all devices (such as computers, printers, and servers) in a network are connected to a single communication line called the bus. The bus acts as a shared communication medium, and data travels in both directions along the bus.

Each device in the network can "listen" to the communication on the bus and pick up any message that is intended for it. If a device wants to send a message, it "broadcasts" the message onto the bus, and all other devices on the bus receive the message. However, only the intended recipient device will actually process and act upon the message.

One of the advantages of a bus topology is that it is relatively simple and inexpensive to implement. However, it can be vulnerable to performance issues if many devices are connected to the bus, as they may compete for access to the communication medium. Additionally, if the bus itself fails, the entire network will be affected.

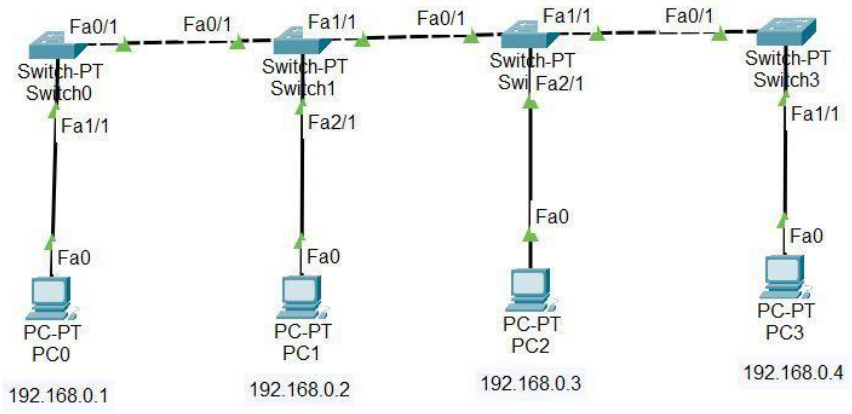


Figure 23 bus topology example

Table 2 Steps to Configure and Setup Bus Topology in Cisco Packet Tracer :

S.NO	Device	Model-Name
1.	PC	PC
2.	Switch	PT-Switch

Table 3IP bus topology Addressing Table

S.NO	Device	IPv4 Address	Subnet Mask
	pc0	192.168.0.1	255.255.255.0
	pc1	192.168.0.2	255.255.255.0
	pc2	192.168.0.3	255.255.255.0
	pc3	192.168.0.4	255.255.255.0

GeeksforGeeks (2020). *Advantages and Disadvantages of Bus Topology*.

6.2.6.2 Advantages of bus topology

Easy to connect a computer.

Easy to implement and extend. Suitable for small network It is flexible and scalable.

It is very simple and easy to install.

Require less cable length than a star topology.

It is less expensive.

If one node fails, other nodes are not to be affected.

When a node added or removed to and from the network, the network is not affected. Typically to cheapest topology to implement.

6.2.6.3 Disadvantages of bus topology

1. Entire network fail is there any problem in a central cable.
2. Difficult to administrator and troubleshoot.
3. Limited cable length and number of stations.
4. Performance degrades as additional computers are added.
5. Maintenance cost may be much higher in the long run.
6. A cable break can disable the entire network, and there is no redundancy.
7. Every workstation all the data on the network (security issues)
8. Used to connect 5 - 9 system only.
9. One virus in the network will affect all of the systems.
10. If many computers are attached, the amount of data flowing causes the network to suddenly slow down.
11. Proper termination is required.
12. The efficiency of the bus network reduces, at that time as the number of devices connected to it increases.
13. Data traffic is high.
14. Data collision is high.

6.2.6.4 Mesh Topology

Mesh topology is a type of network topology in which devices are connected to each other through multiple, redundant paths. In a mesh network, each device acts as a node that can transmit data to any other node in the network. This allows for high levels of reliability and fault tolerance, as data can be rerouted in the event of a connection failure or network congestion. Mesh networks are commonly used in wireless networks, such as Wi-Fi mesh networks, as well as in wired networks for applications that require high levels of reliability and redundancy.

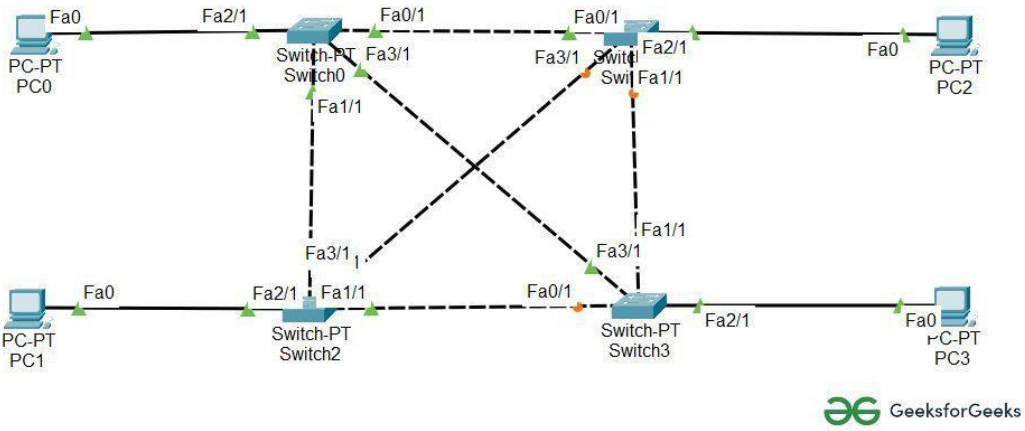


Figure 24 mesh topology example

Table 4 Steps to Configure and Setup Ring Topology in Cisco Packet Tracer

S.NO	Device	Model name
1.	PC	PC
2.	Switch	PT-switch

Table 5 IP Addressing Table:

S.NO	Device	IPv4 Address	Subnet Mask
1.	pc0	192.168.0.1	255.255.255.0
2.	pc1	192.168.0.2	255.255.255.0
3.	pc2	192.168.0.3	255.255.255.0
4.	pc3	192.168.0.4	255.255.255.0

GeeksForGeeks (2020). *Advantage and Disadvantage of Mesh Topology*

6.2.6.5 Advantages of Mesh Topology:

1. High Reliability: In a mesh topology, each node is connected to multiple nodes, so if one node fails or becomes unreachable, the data can still be transmitted through alternate paths. This high level of redundancy makes mesh topology very reliable.

2. Fault Tolerance: The redundancy of connections in a mesh topology also makes it very fault tolerant. Even if one or more nodes fail, the network can continue to function.

3. Scalability: Mesh topology can be easily scaled up or down by adding or removing nodes. It is easy to expand the network as needed.

4. Privacy and Security: Mesh topology provides a high level of privacy and security because data is transmitted only between the nodes that need to communicate with each other.

5. High Bandwidth: Mesh topology can provide high bandwidth because each node can communicate directly with any other node in the network.

6.2.6.6 Disadvantages of Mesh Topology:

1. Cost: Mesh topology can be expensive to implement because each node needs to be connected to every other node in the network. The cost of wiring and hardware can be high.

2. Complexity: The complexity of the mesh topology increases as the number of nodes in the network grows. Managing and configuring a large mesh network can be difficult.

3. Network Traffic: In a mesh topology, each node must transmit and receive data from multiple nodes, which can cause network traffic congestion.

4. Performance: The performance of a mesh topology can be impacted by the number of nodes in the network, the quality of the connections between the nodes, and the amount of data being transmitted.

5. Maintenance: Troubleshooting and maintaining a mesh network can be difficult due to the complexity of the network

6.2.6.7 Star topology

A star topology is a network topology where all devices are connected to a central hub or switch. In a star network, all devices communicate with each other through the hub or switch, which acts as a central point of communication.

Each device in a star topology has a dedicated connection to the hub or switch, which provides a high level of reliability and fault tolerance. If one device fails or goes offline, it does not affect the rest of the network.

Star topology is one of the most commonly used network topologies in local area networks (LANs) because it is easy to set up, maintain, and troubleshoot. It is also a scalable topology, which means that new devices can be added to the network easily by connecting them to the hub or switch.

The main disadvantage of a star topology is that it relies heavily on the hub or switch. If the hub or switch fails, the entire network can become unusable. Additionally, the cost of implementing a star topology can be higher than other topologies due to the need for a central hub or switch.

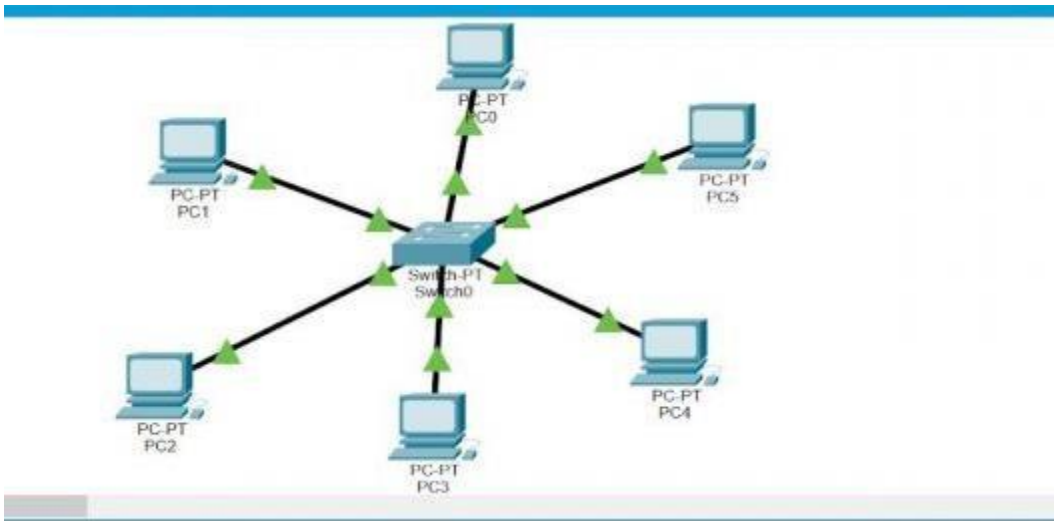


Figure 25 star topology example

6.2.6.8 Advantages of Star Topology:

1. Centralized Management: A star topology allows for centralized management, making it easy to monitor and manage the network from a single location.

2. High Reliability: In a star topology, if one device fails or goes offline, it does not affect the rest of the network. This provides a high level of reliability and fault tolerance.

3. Scalability: Star topology is a scalable topology, which means that new devices can be added to the network easily by connecting them to the hub or switch.

4. Easy to Troubleshoot: Troubleshooting a star network is relatively easy because the failed device can be isolated from the network, and the rest of the network can continue to function.

5. High Performance: In a star topology, each device has a dedicated connection to the hub or switch, which provides a high level of performance and bandwidth.

6.2.6.9 Disadvantages of Star Topology:

1. Single Point of Failure: The hub or switch in a star network is a single point of failure. If the hub or switch fails, the entire network can become unusable.

2. Cost: The cost of implementing a star topology can be higher than other topologies due to the need for a central hub or switch.

3. Limited Distance: Star topology has a limited distance between the hub or switch and the devices. If the distance is too far, signal degradation can occur, and the network's performance can suffer.

4. Network Traffic: In a star topology, all data must pass through the hub or switch, which can cause network traffic congestion.

5. Dependency on Hub or Switch: The performance of the network is dependent on the hub or switch's capability, which can limit the network's overall performance.

6.2.6.10 Tree topology

Tree topology is a network topology that combines the characteristics of bus topology and star topology. In a tree network, the nodes are arranged in a hierarchy, where each level of the hierarchy is connected to a central bus or backbone.

The tree topology is similar to the structure of a tree, where the root of the tree is connected to the main backbone, and the branches are connected to the root. This hierarchical structure allows for easy expansion of the network by adding additional branches or nodes to the existing network.

In a tree topology, each device has its own dedicated connection to the central bus or backbone, which provides high levels of reliability and fault tolerance. If one branch or device fails, the rest of the network can still function.

The main advantage of a tree topology is its scalability. New devices and branches can be added to the network easily, making it suitable for large-scale networks. However, the disadvantage of a tree topology is that it can be expensive to implement and maintain, especially in larger networks. Additionally, the failure of the central backbone can cause the entire network to fail.

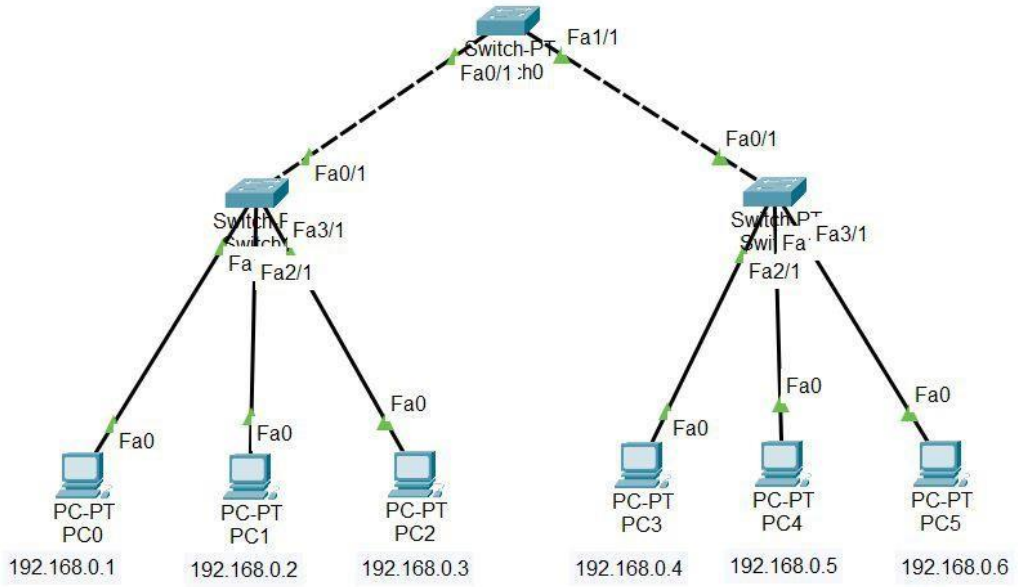


Figure 26 tree topology example

Table 6 Steps to Configure and Setup Tree Topology in Cisco Packet Tracer

S.NO	Device	Model-Name
1.	PC	PC
2.	switch	PT-switch

Table 7 IP Addressing Table

S.NO	Device	IPv4 Address	Subnet Mask
1.	pc0	192.168.0.1	255.255.255.0
2.	pc1	192.168.0.2	255.255.255.0
3.	pc2	192.168.0.3	255.255.255.0
4.	pc3	192.168.0.4	255.255.255.0
5.	pc4	192.168.0.5	255.255.255.0
6.	pc5	192.168.0.6	255.255.255.0

6.2.6.11 Advantages of Tree Topology:

1. Scalability: Tree topology is a scalable topology, which means that new devices and branches can be added to the network easily. This makes it suitable for large-scale networks and allows for future expansion.

2. Centralized Management: The hierarchical structure of a tree network allows for centralized management, making it easy to monitor and manage the network from a single location.

3. High Reliability: Each device in a tree topology has its own dedicated connection to the central backbone, which provides high levels of reliability and fault tolerance. If one branch or device fails, the rest of the network can still function.

4. Improved Performance: The use of dedicated connections in a tree topology provides improved network performance compared to other topologies.

5. Flexible: Tree topology is a flexible topology that can be used in a variety of network setups, including LANs and WANs.

6.2.6.12 Disadvantages of Tree Topology:

1. Cost: Tree topology can be expensive to implement and maintain, especially in larger networks.

2. Complexity: The hierarchical structure of a tree network can make it more complex to design, install, and manage compared to other topologies.

3. Single Point of Failure: The central backbone in a tree network is a single point of failure. If the backbone fails, the entire network can become unusable.

4. Network Traffic: In a tree topology, all data must pass through the central backbone, which can cause network traffic congestion and affect the network's performance.

5. Limited Distance: Tree topology has a limited distance between the central backbone and the devices. If the distance is too far, signal degradation can occur, and the network's performance can suffer.

Computer Hope (2017). *What is a Tree Topology?*
www.javatpoint.com. (n.d.). *What is Tree Topology - javatpoint*.

6.3 recommendation network topology

Recommending a Networking Topology and Protocols for the efficient utilization of a networking system.

1. The task of designing a network for the Matara Branch has been delegated to us under the aforementioned circumstance.
2. in the above scenario Alliance Health. The most suitable topology for the networking of departments is star topology. departments. These departments can be divided into different subnets using VLANs. By
3. the various of departments work with the central switch to establish distinct Subnets for the
4. Using a tree topology for client devices in a company's branch network can offer several benefits, including.
    a. Scalability: A tree topology can be easily scaled by adding or removing branches or levels, without disrupting the rest of the network.

    b. Robustness: Tree topology offers a high degree of robustness, as it provides multiple paths between nodes, allowing for alternative routes in case of link or node failure.

    c. Flexibility: The tree topology can accommodate various devices with different bandwidth requirements, allowing the network to handle diverse traffic types and support various applications.

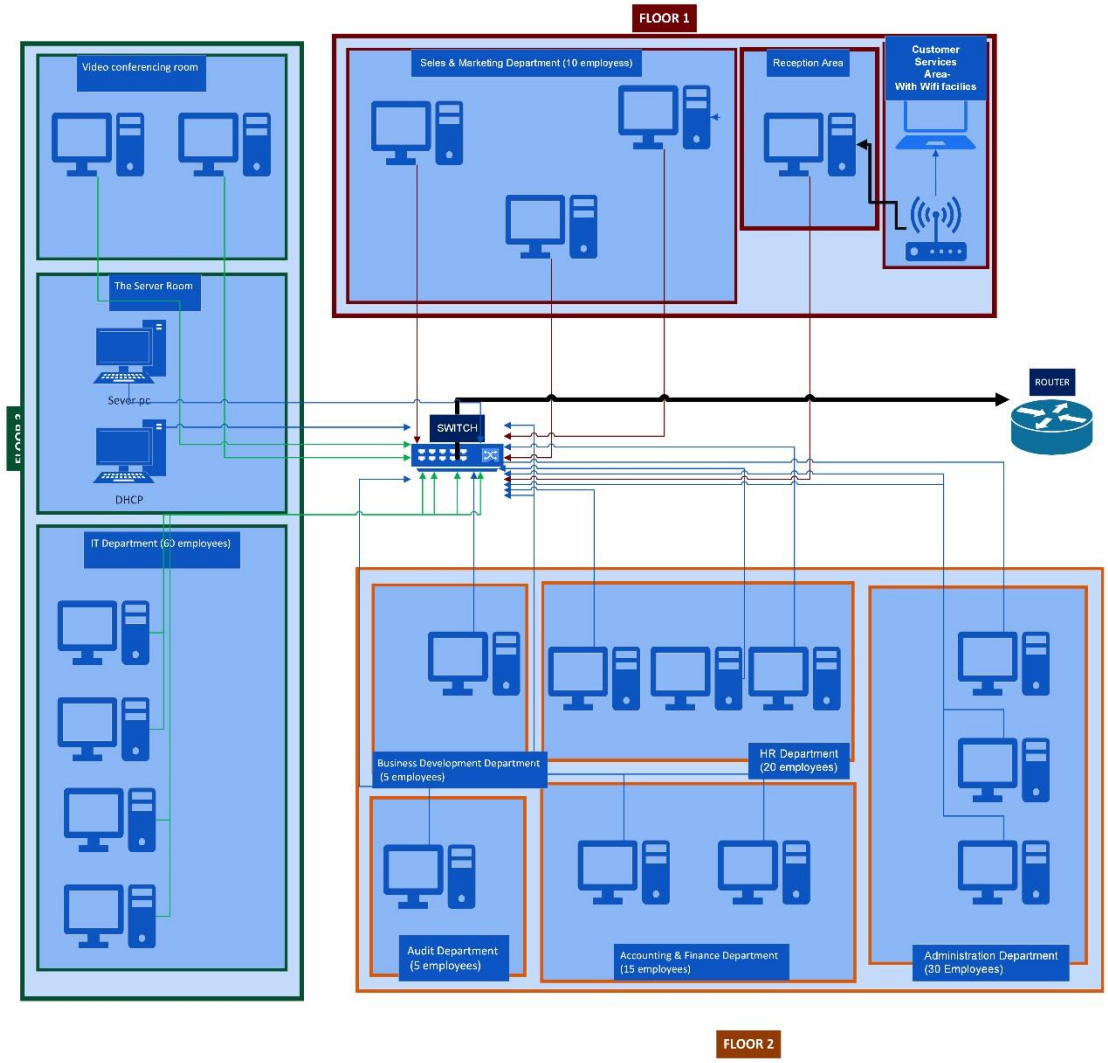
    d. Easy to manage: With a hierarchical structure, a tree topology is easy to manage and troubleshoot, as each branch or level can be monitored independently.
    e. Cost-effective: Tree topology can be a cost-effective solution for large networks, as it reduces the amount of cabling and the number of devices required compared to other topologies, such as mesh or ring topologies

By utilizing only one network switch per branch, a company can save on expenses related to purchasing and

maintaining multiple switches. This approach simplifies the network design and reduces the complexity of the network, making it easier to manage and troubleshoot

Moreover, having only one switch per branch reduces the amount of cabling and the number of network ports required, which in turn, reduces the cost of purchasing and installing network equipment. Additionally, a single switch is easier to configure, secure, and manage compared to multiple switches, which reduces the need for IT staff and their associated costs.

Overall, utilizing only one network switch per branch is a cost-effective approach to network design, especially for smaller companies or branches with limited budgets or technical resources. However, it's important to ensure that the single switch is of sufficient capacity and performance to meet the network requirements and provide reliable connectivity for all devices on the network.



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

Figure 27 recommendation COLOMBO branch network topology

The floor plan of the head office in Matara is as follows NETWORK Blueprint

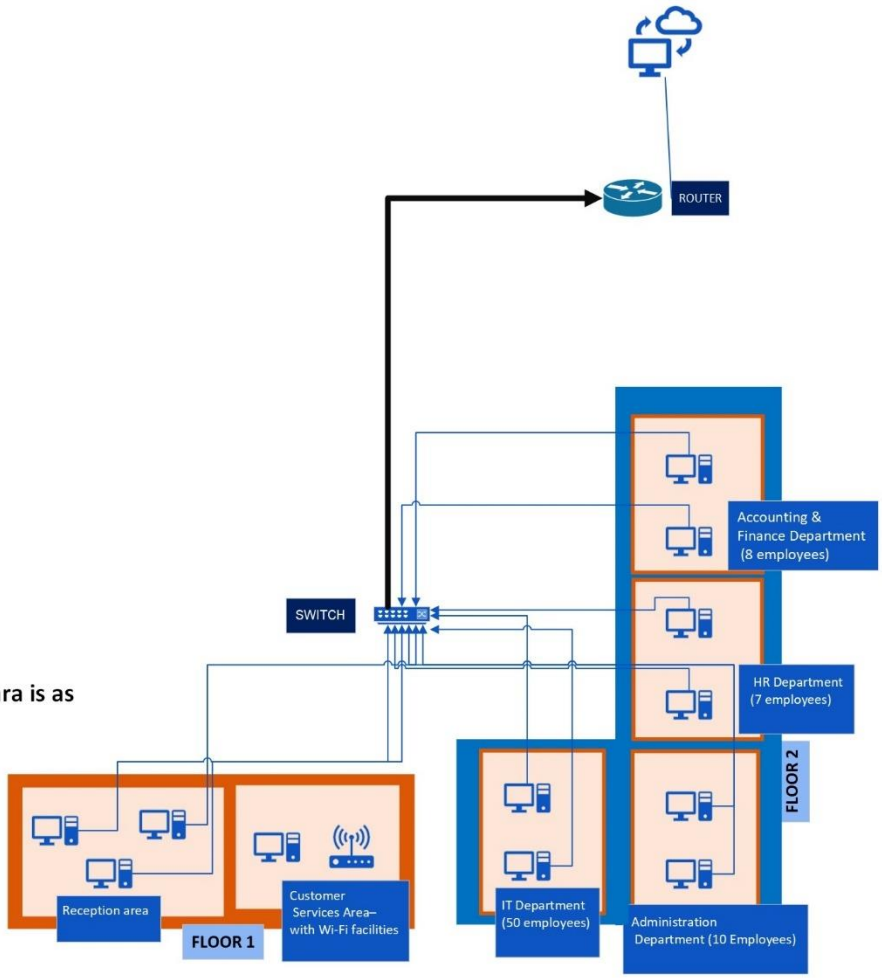
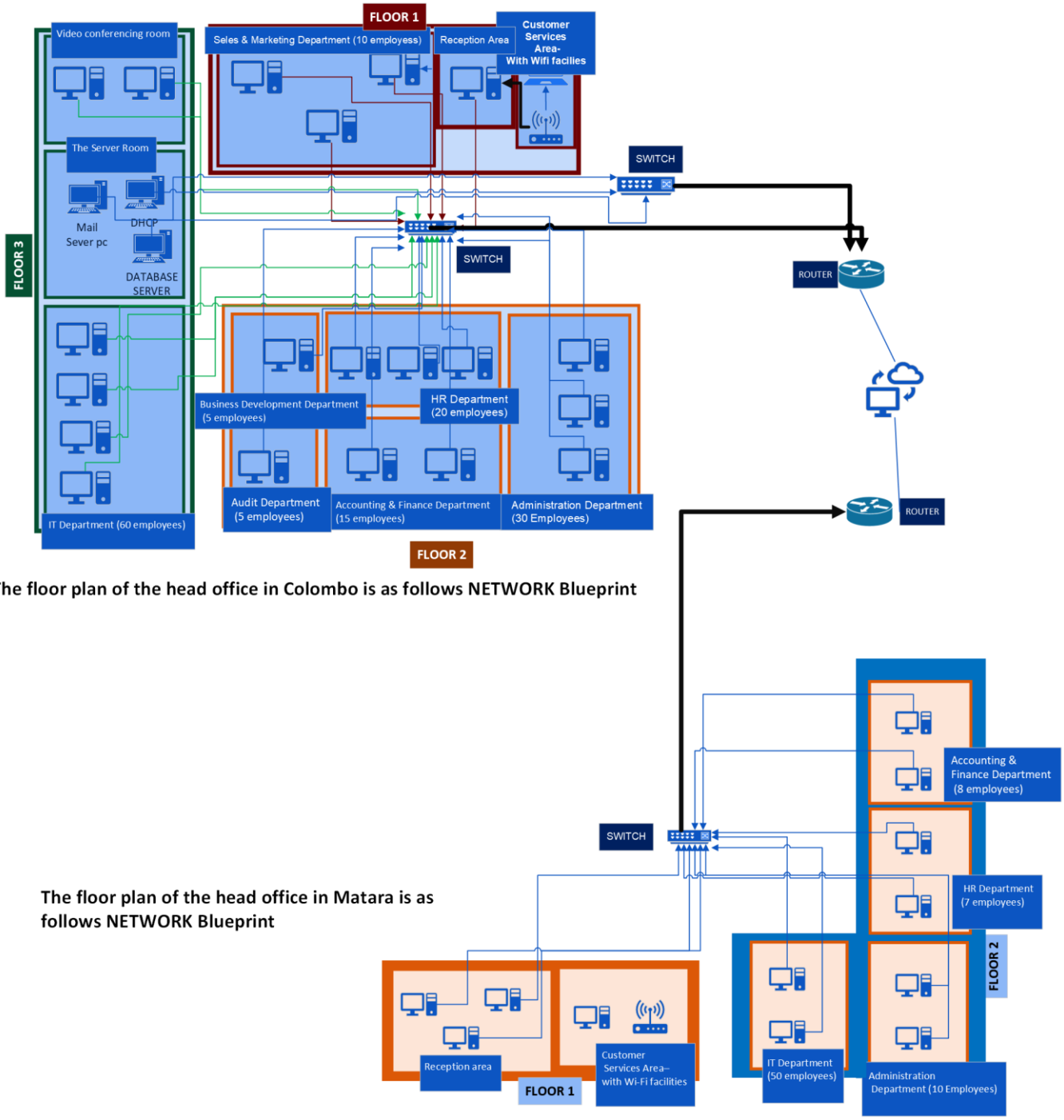


Figure 1 The floor plan of the head office in Matara is as



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

The floor plan of the head office in Matara is as follows NETWORK Blueprint

Figure 2 fully funational netowrk diagraom.

7 Activity 2

7.1 network devices and operations

Network devices are hardware components that are used to facilitate communication between devices on a network. These devices work together to ensure that data is transmitted between devices efficiently and securely. Some common network devices include routers, switches, hubs, firewalls, and modems.

Routers are used to connect different networks together, such as connecting a home network to the internet. They use routing protocols to determine the most efficient path for data to travel between networks.

Switches are used to connect devices within a network. They use MAC addresses to forward data to the correct device.

Types of network devices

Here is the common network device list:

1. Hub
2. Switch
3. Router
4. Bridge
5. Gateway
6. Modem
7. Repeater
8. Access Point

www.javatpoint.com. (n.d.). *What is Tree Topology - javatpoint*.

GeeksforGeeks (2018). *Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter) - GeeksforGeeks*.

7.1.1 Hub

A hub is a networking tool that connects several networked devices. In the physical layer of the OSI model, or layer 1, hubs work by receiving incoming data and broadcasting it to all associated devices. In other words, the hub will broadcast data to all other devices linked to it when a device provides data to the hub.

In comparison to switches and routers and other network hardware, hubs are straightforward and affordable. They are less effective, though, because they send all data to every connected device, even if it is not the device for which the data was intended. This may result in network sluggishness and reduced data transfer speeds.

Small networks with a constrained number of devices can use hubs. Hubs can, however, turn into a bottleneck as network traffic rises, degrading network performance. Because of this, hubs are rarely utilized in current networks; instead, switches have mainly taken their place.

It's worth noting that there are two types of hubs: passive and active. Passive hubs simply pass incoming data along to all connected devices without any additional processing, while active hubs amplify the signal and regenerate the data before forwarding it to the connected devices. Active hubs are more expensive than passive hubs but can provide better performance.

7.1.1.1 Features of Hub

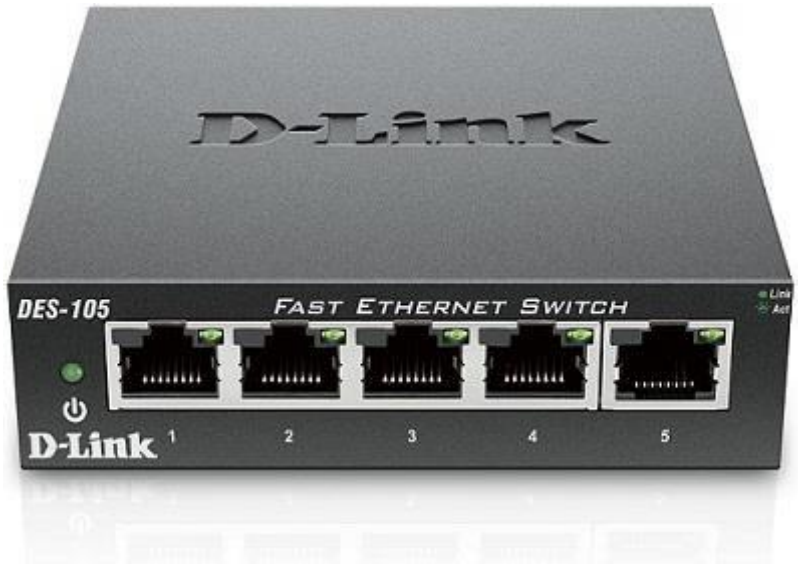
1. It acts with shared bandwidth and broadcasting.
2. It includes only one collision domain and broadcast domain.
3. It works at the physical layer of the OSI model and also offers support for halfduplex transmission mode.
4. It cannot create a virtual LAN and does not support spanning tree protocol.
5. Furthermore, mainly packet collisions occur inside the hub.
6. It also has a feature of flexibility, which means it includes a high transmission rate to different devices.

7.1.1.2 Advantages of Hub

1. It provides support for different types of Network Media.
2. It can be used by anyone as it is very cheap.
3. It can easily connect many different media types.
4. The use of a hub does not impact on the network performance.
5. Additionally, it can expand the total distance of the network.

7.1.1.3 Disadvantages of Hub

1. t has no ability to choose the best path of the network.
2. It does not include mechanisms such as collision detection.
3. It does not operate in full-duplex mode and cannot be divided into the Segment.
4. It cannot reduce the network traffic as it has no mechanism.
5. It is not able to filter the information as it transmits packets to all the connected segments.
6. Furthermore, it is not capable of connecting various network architectures like a ring, token, and ethernet, and more



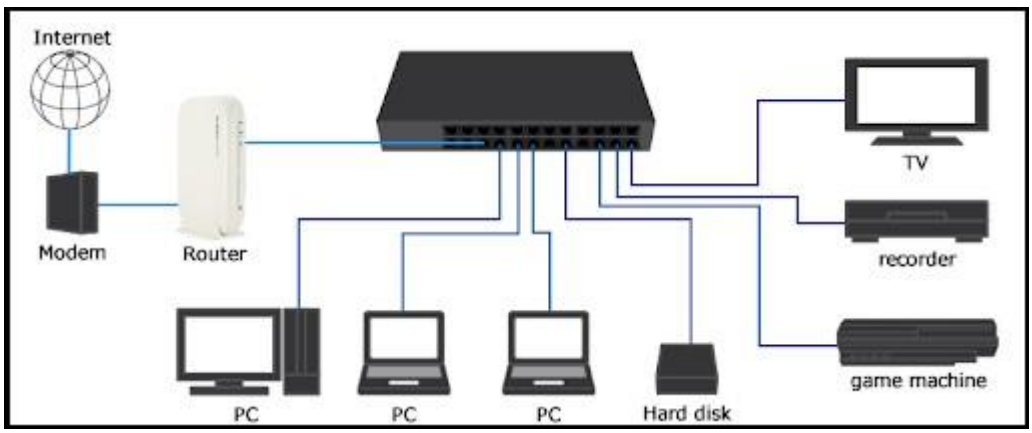


Figure 28Installing the Hub

7.1.2 Switch

A network switch is a computer networking device that connects devices together on a computer network, such as a local area network (LAN) or a wide area network (WAN). It works by receiving data packets from one device and forwarding them to the appropriate destination device, based on the destination address of each packet.

Switches operate at the data link layer (layer 2) of the OSI (Open Systems Interconnection) model, which is responsible for transmitting data between adjacent nodes on a network. They use a technique called packet switching to forward data, which involves storing incoming packets in memory and forwarding them to the appropriate output port based on the destination address.

Switches are typically used in Ethernet networks to provide connectivity between devices, such as computers, servers, printers, and other network-enabled devices. They are available in various configurations, including unmanaged switches, which are simple and easy to use, and managed switches, which offer more advanced features and configuration options.

Some of the advantages of using network switches include improved network performance, increased bandwidth, and better security. They can also help to reduce network congestion and improve network reliability by providing dedicated connections between devices.

7.1.2.1 Features of Switch

1. Versatility: The Switch can be used as a portable handheld device or docked to a TV to play games on a bigger screen. This flexibility allows players to seamlessly switch between playing at home or on-the-go.
2. Joy-Con controllers: The Switch's detachable Joy-Con controllers allow for a variety of gameplay options, including local multiplayer and motion control. They can also be used independently by two players for multiplayer games.
3. Amiibo compatibility: The Switch is compatible with Nintendo's Amiibo figurines, which can be used to unlock special content and features in various games.
4. Online play: The Switch offers online play through its Nintendo Switch Online subscription service, allowing players to compete or cooperate with others around the world in various games.
5. Parental controls: The Switch includes robust parental controls that allow parents to restrict content and set limits on playtime for their children.

Figure 30 Switch image

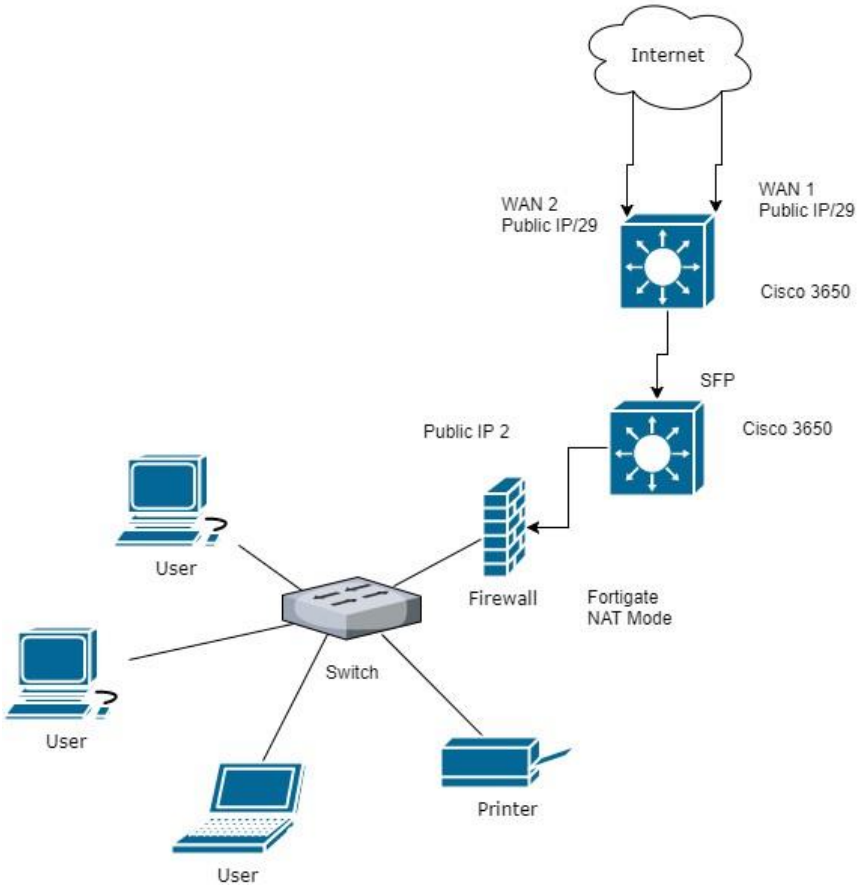


Figure 29 Switch installing in network

7.1.2.2 Advantages of Switch

1. Network switches improve network performance and speed.
2. They are scalable and can be expanded as needed.
3. Network switches provide better security than hubs or routers.
4. They support a wide range of devices and technologies.
5. Centralized management makes it easier to configure and monitor the network.

7.1.2.3 Disadvantages of Switch

1. Network switches can be expensive.
2. They can be complex to configure and manage.
3. A malfunctioning switch can bring down the entire network.
4. Switches have a limited range, which can be a disadvantage for large networks.
5. Some devices may not be compatible with certain types of network switches

Cloudflare (n.d.). What is a network switch? | Switch vs. router | Cloudflare. *Cloudflare*.

7.1.3 Deferent Features of Switch and Hub

HUB	SWITCH
A hub operates on the physical layer.	A switch operates on the data link layer.
Hubs perform frame flooding that can be unicast, multicast, or broadcast.	It performs broadcast, then the unicast and multicast as needed
Just a singular domain of collision is present in a hub.	Varied ports have separate collision domains.
Transmission mode is Half-duplex	Transmission mode is Full duplex

Hubs operates as a Layer 1 devices per the OSI model.	Network switches help you to operate at Layer 2 of the OSI model
To connect a network of personal computers should be joined through a central hub	Allow connecting multiple devices and ports.
Uses electrical signal orbits	Uses electrical signal orbits
Uses electrical signal orbits	Multiple Spanning-Tree is possible
Collisions occur mostly in setups using hubs	No collisions occur in a full-duplex switch.
Hub is a passive device	A switch is an active device
A network hub can't store MAC addresses.	Switches use CAM (Content Accessible Memory) that can be accessed by ASIC (Application Specific Integrated Chips)
Not an intelligent device	Intelligent device
Its speed is up to 10 Mbps	10/100 Mbps, 1 Gbps, 10 Gbps
Does not use software	Has software for administration

Figure 31 switch vs Hub of features table

Diffen.com. (2019). *Hub vs Switch - Difference and Comparison*

7.1.4 Router

A router is a network device that connects multiple computer networks together and directs traffic between them. It acts as a central hub for data communication, receiving data packets from different devices and forwarding them to their destination using routing protocols and tables. Routers play a crucial role in modern computer networks, enabling communication between devices on different networks and allowing access to the internet. They are essential for managing network traffic, ensuring security, and providing remote connectivity to networks and devices

Figure 32 network Router

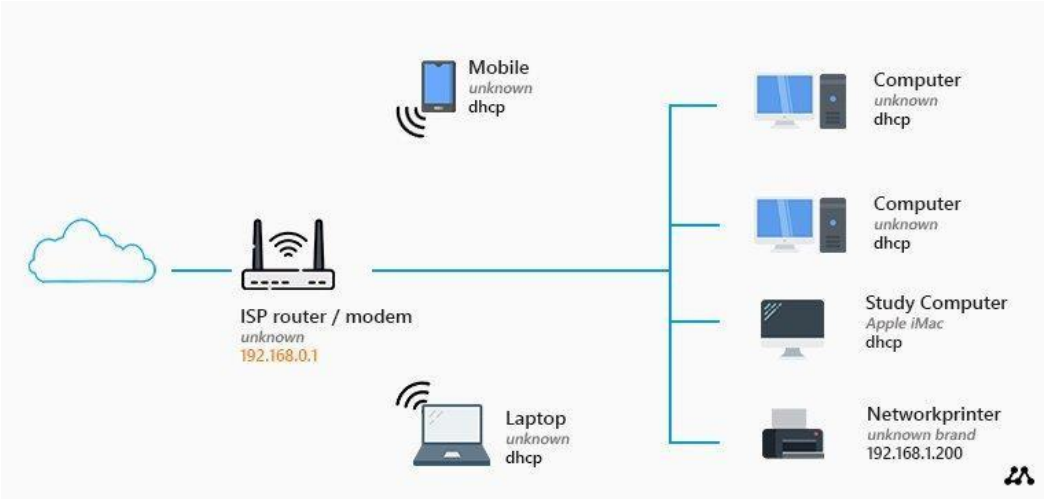


Figure 33 how to install by Router in network.

7.1.4.1 Features of Router

1. Packet forwarding: Routers forward data packets between networks, determining the best path for each packet based on routing tables and protocols.

2. Network address translation (NAT): Routers use NAT to translate private IP addresses into public addresses, enabling devices on a local network to access the internet.

3. Firewall and security: Routers can act as firewalls, filtering incoming and outgoing traffic to protect against malicious attacks and unauthorized access.

4. Quality of Service (QoS): Routers can prioritize traffic based on its type or source, ensuring that critical traffic like video or voice data is given priority over less important traffic.

5. VPN and remote access: Routers can provide virtual private network (VPN) functionality, allowing remote users to securely access the network over the internet.

6. Wireless connectivity: Many routers include built-in wireless access points, allowing devices to connect to the network wirelessly.

7. Management and monitoring: Routers can be managed and monitored using web-based interfaces or specialized software, allowing network administrators to configure, troubleshoot, and optimize the network.

7.1.4.2 Advantages of Router

1. Routers forward data packets between networks, enabling communication across different networks.
2. Network address translation (NAT) allows devices on a local network to access the internet.
3. Routers can act as firewalls, providing network security and filtering traffic.
4. Quality of Service (QoS) ensures that critical traffic is given priority over less important traffic.
5. Routers can provide VPN functionality for secure remote access.

7.1.4.3 Disadvantages of Router

1. Routers can be expensive, especially for high-end models.
2. They can be complex to configure and manage, requiring skilled IT personnel.
3. Routers can become a single point of failure if they malfunction or lose power.
4. Wireless routers may have limited range or interference issues.

5. Compatibility issues may arise with certain devices or networks.

Diffen.com. (2019).

www.javatpoint.com. (n.d.). *What is Router - javatpoint*.

7.1.5 Repeater

A network repeater is a device that regenerates or amplifies network signals to extend the range of a network. It receives signals from a source, such as a router or switch, and retransmits them to increase their reach. Repeaters are often used in environments where network signals degrade over long distances, such as in large buildings or outdoor areas. They play a critical role in maintaining network quality and reliability, helping to improve signal strength and reduce data loss. Repeaters are a simple and cost-effective way to enhance network performance and coverage.

Figure 35 repeaters

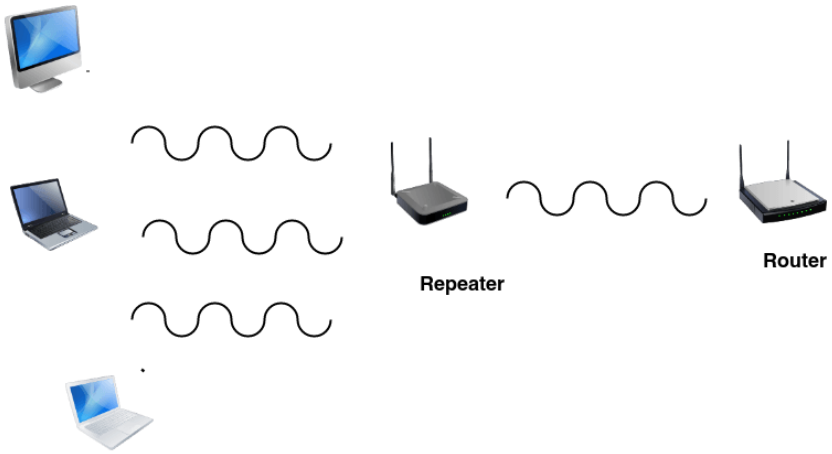


Figure 34 how to work the network repeater.

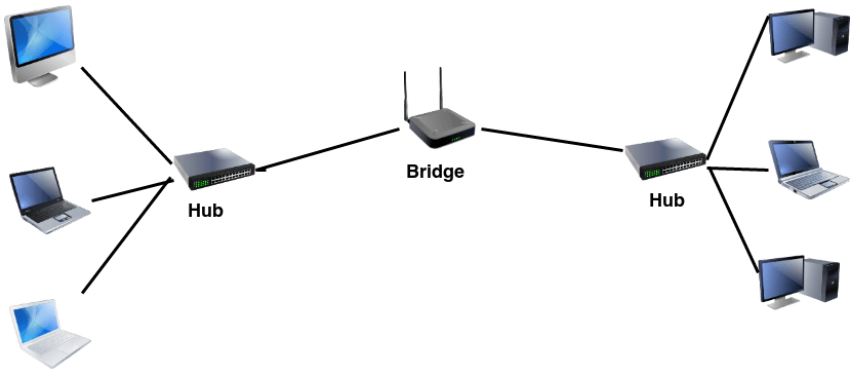


Figure 36 how to config the network by repeaters

7.1.5.1 Features of Repeater

1. Signal amplification: Repeaters amplify weak signals to improve their strength and extend the range of a network.

2. Signal regeneration: Repeaters regenerate network signals, ensuring that they maintain their integrity over long distances.

3. Compatibility: Repeaters are compatible with a wide range of network technologies, including Ethernet, Wi-Fi, and fiber optic.

4. Plug-and-play: Repeaters are easy to install and require minimal configuration, making them a simple and cost-effective solution for extending network coverage.

5. Transparency: Repeaters do not modify or alter network signals in any way, ensuring that data is transmitted accurately and without interference.

6. Reliability: Repeaters are highly reliable and require minimal maintenance, providing continuous network coverage and minimizing downtime.

7. Scalability: Repeaters can be used in combination with other networking devices, such as switches and routers, to create larger and more complex network environments

7.1.5.2 Advantages of Repeaters

1. Repeaters amplify and regenerate signals, extending the range of a network.
2. They are easy to install and require minimal configuration.
3. Repeaters are compatible with a wide range of network technologies.
4. They are transparent and do not modify network signals, ensuring accuracy and reliability.
5. Repeaters are highly reliable and require minimal maintenance.

7.1.5.3 Disadvantages of Repeaters

1. Repeaters can introduce signal delay or noise, degrading network performance.
2. They are not suitable for use in large or complex network environments.
3. Repeaters can be expensive, especially for high-end models.
4. They do not provide advanced network functionality, such as security or Quality of Service (QoS).
5. Compatibility issues may arise with certain devices or networks.

7.1.6 Access point

A network access point (NAP) is a device that allows multiple devices to connect to a network, such as the internet or a local area network (LAN). NAPs act as a bridge between different networks, enabling communication between devices that are connected to them.

NAPs can come in different forms, such as wired or wireless access points. Wired access points typically use Ethernet cables to connect devices to the network, while wireless access points use Wi-Fi technology to enable wireless connections. In both cases, the NAP acts as a central point that connects devices to the network and manages data traffic between them.

NAPs are commonly used in homes, offices, and public spaces to provide internet access to multiple devices, such as computers, smartphones, and tablets. They are also used in larger networks, such as corporate networks and data centers, to provide access to a large number of devices and ensure efficient data transfer.

Figure 37 access point image

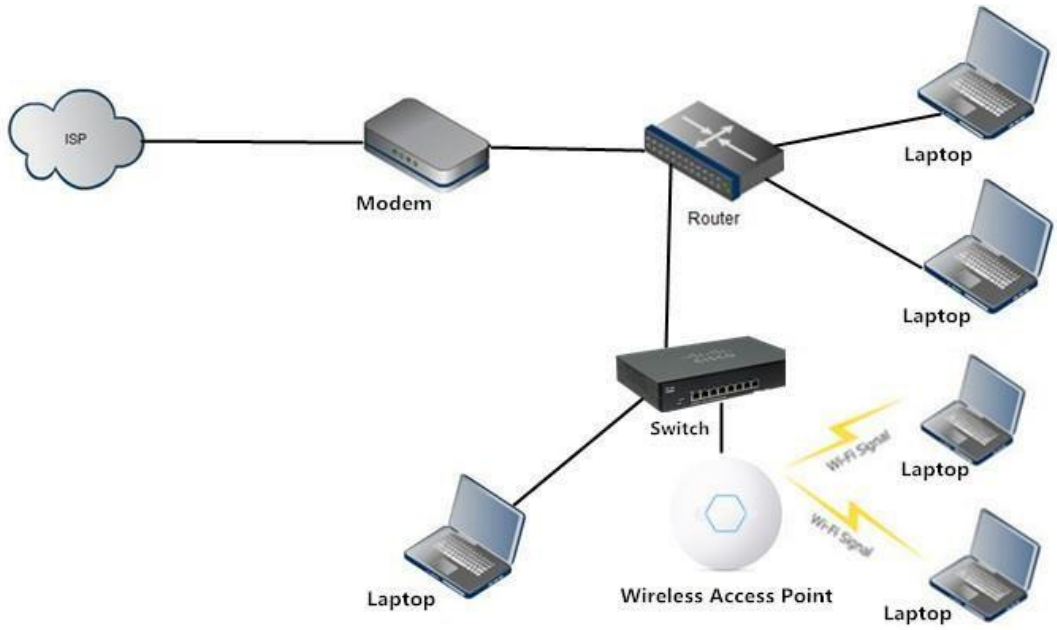


Figure 38 how to install the access point in network.

7.1.6.1 Features of Access point

1. Wireless connectivity: The primary function of an access point is to provide wireless connectivity to a network. It allows multiple wireless devices to connect to the network and access resources such as the internet or shared files.

2. Multiple connectivity options: An access point can connect to a wired network through Ethernet cables, or wirelessly using Wi-Fi technology.

3. Compatibility: An access point is usually compatible with various wireless standards such as 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac, making it possible to work with any wireless device that supports these standards.

Security: Access points support various security protocols such as WPA2, WPA3, and WEP, which provide secure wireless communication and protect against unauthorized access.

Management: Access points can be managed through a web-based interface, allowing administrators to configure and manage the network settings.

Scalability: An access point can be used to expand the coverage of a wireless network by adding more access points to the network.

Quality of Service (QoS): Access points can prioritize network traffic based on the type of data being transmitted, ensuring that critical applications such as voice and video are given priority over less important traffic.

Roaming: Access points can support seamless roaming, allowing wireless devices to switch from one access point to another without interruption, ensuring a continuous connection to the network

7.1.6.2 Advantages of Access Point

1. Provides wireless connectivity to a network, allowing multiple devices to connect and access network resources.
2. Increases mobility and flexibility by allowing users to connect from anywhere within the access point's range.
3. Easy to install and configure, with most offering a web-based interface for setup and management.
4. Increases range and coverage of a wireless network, allowing devices to connect from a greater distance.
5. Allows for scalability by adding more access points to the network as it grows.

7.1.6.3 Disadvantages of Access Point

1. Interference from other wireless networks or electronic devices can cause signal degradation and affect network performance.
2. Limited bandwidth shared among connected devices can result in reduced network performance as more devices connect.
3. Cost of access points, especially those that support the latest wireless standards and security protocols, can be expensive.
4. Network congestion can occur when too many devices connect to the network, resulting in slower data transfer rates and reduced network performance.
5. Security risks can arise if access points are not properly secured, potentially exposing sensitive data and allowing unauthorized access to the network.

7.1.7 Server Types

In computer networking, servers are computers or devices that provide resources or services to other computers or devices on a network. There are different types of servers that serve specific purposes in a network, including:

1. **File server:** A file server stores and manages files, allowing users to access and share files over a network.

2. **Web server:** A web server is a computer that stores and serves websites, allowing users to access them over the internet.

3. **Mail server:** A mail server is a computer that manages email messages, allowing users to send and receive emails over a network.

4. **Database server:** A database server stores and manages databases, allowing users to access and manipulate data over a network.

5. **Print server:** A print server manages and controls access to printers, allowing users to print documents over a network.

6. **Application server:** An application server is a computer that runs applications and provides services to other computers over a network.

7. **Game server:** A game server is a computer that hosts multiplayer games, allowing multiple players to connect and play together over a network.

8. **DHCP (Dynamic Host Configuration Protocol) Server**: That network server that automatically assigns IP addresses, subnet masks, default gateways, and other network parameters to devices on a network.

9. **DNS (Domain Name System) Server:** That network server that translates domain names into IP addresses, allowing users to access websites and resources on a network using easy-to-remember domain names instead of numerical IP addresses.

Each type of server has its own unique configuration and requirements, depending on the resources and services it provides. Understanding the different types of servers can help network administrators choose the right server for their network and optimize its performance.

7.1.7.1 DHCP (Dynamic Host Configuration Protocol) Server

A DHCP (Dynamic Host Configuration Protocol) server is a network server that automatically assigns IP addresses, subnet masks, default gateways, DNS servers, and other network parameters to devices on a network.

When a device connects to the network, it sends a DHCP request message to the server, requesting an IP address and other network parameters. The DHCP server responds with a DHCP offer message, offering the device an IP address and other network parameters. The device can then accept the offer by sending a DHCP request message to the server, and the server will respond with a DHCP acknowledgment message, assigning the device an IP address and other network parameters.

The use of DHCP simplifies network administration and reduces the likelihood of human error when configuring IP addresses manually. It also allows for efficient management of IP addresses, as IP addresses can be dynamically assigned to devices on an as-needed basis, reducing IP address conflicts and ensuring that all devices on the network have a unique IP address.

DHCP servers are commonly used in large enterprise networks, where manually configuring IP addresses for every device would be impractical and time-consuming. However, DHCP servers can also be used in small networks and home networks, where they can simplify network administration and reduce the likelihood of IP address conflicts

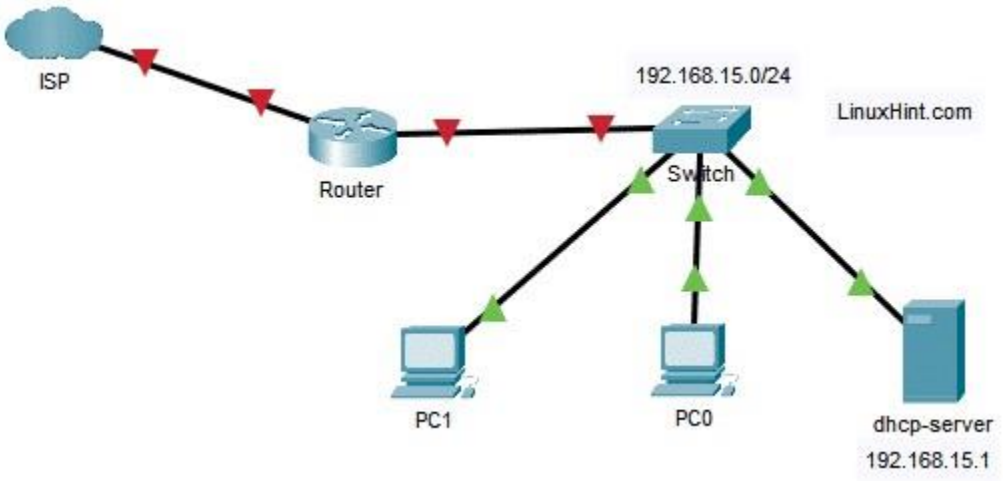


Figure 39 Example of DHCP

Deland-Han (n.d.). *Install and Configure a DHCP Server - Windows Server*.
[online] learn.microsoft.com

7.1.7.2 Mail Sever

A mail server is a network server that is responsible for sending, receiving, and storing email messages. A mail server is typically used to facilitate email communication within an organization or between organizations.

When an email message is sent from a sender's email client, the message is sent to the sender's outgoing mail server, also known as the SMTP (Simple Mail Transfer Protocol) server. The outgoing mail server then forwards the email message to the recipient's incoming mail server, also known as the POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) server. The recipient can then access the email message from their email client by connecting to the incoming mail server using their email address and password.

Mail servers can be used for both internal and external email communication, and they can support various email protocols such as SMTP, POP, IMAP, and MIME
(Multipurpose Internet Mail Extensions). Mail servers can also support various security measures such as encryption and authentication to ensure that email messages are transmitted and stored securely.

There are various types of mail servers, including on-premise mail servers, cloud-based mail servers, and hybrid mail servers. On-premise mail servers are typically installed and managed within an organization's own network infrastructure, while cloud-based mail servers are hosted and managed by a third-party service provider. Hybrid mail servers are a combination of on-premise and cloud-based mail servers, where some email services are hosted on-premise, and others are hosted in the cloud.

Mail servers are an essential component of modern communication, and they enable organizations to communicate efficiently and securely through email messages.

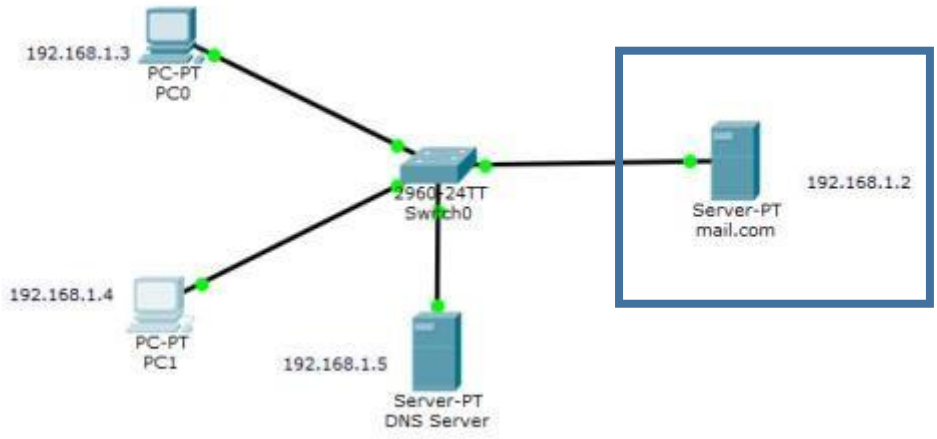


Figure 40 mail server r example.

7.1.7.3 Database server

A network database server is a type of database management system that is designed to provide centralized access to a database over a network.

A network database server typically consists of a software program that runs on a dedicated server computer and manages access to a database. The server software provides a set of tools and protocols that allow client computers to connect to the database and perform operations such as querying, updating, and managing data.

One of the primary benefits of a network database server is that it allows multiple users to access the same database simultaneously, which can improve efficiency and reduce data redundancy. The server can also provide advanced security features, such as user authentication and access control, to ensure that only authorized users can access the database.

Examples of network database servers include Oracle Database Server, Microsoft SQL Server, and PostgreSQL. These systems are widely used in enterprise applications, web applications, and other contexts where large volumes of data need to be managed and accessed over a network.

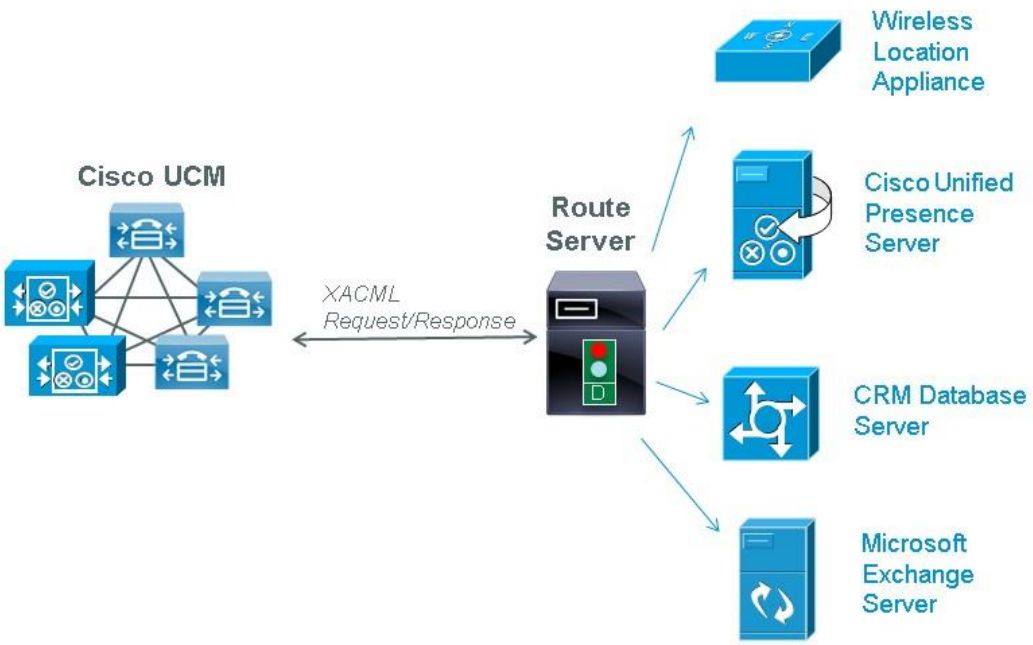


Figure 41 database server example.

DNS server

7.2 Recommendation network devices and operations

1. When designing and implementing a networked system, it is important to choose the appropriate network devices and operations as well as relevant networking software to ensure optimal performance and security. Here are some recommendations for network devices, operations, and software:

2. Network Devices: It is important to choose network devices that are reliable, scalable, and secure. Some examples of recommended network devices are switches, routers, firewalls, and access points. These devices should be able to handle the traffic and data transfer requirements of the network, provide redundancy and failover capabilities, and support the latest network protocols and standards.

3. Network Operations: To ensure smooth and efficient network operations, it is important to implement network management tools and protocols. For example, implementing Simple Network Management Protocol (SNMP) enables network

administrators to monitor and manage network devices, detect and diagnose network issues, and optimize network performance.

4. Networking Software: The choice of networking software is critical to the success of a networked system. The software should be reliable, secure, and scalable, and should support the latest network protocols and standards. Some recommended networking software includes:

Network operating systems (NOS): These are software platforms that provide the core functionality for a networked system. Examples of popular NOS include Windows Server, Linux, and macOS Server.

Network security software: To ensure the security of the network, it is important to implement security software such as antivirus, firewalls, intrusion detection/prevention systems (IDS/IPS), and virtual private network (VPN) software.

Network monitoring and analysis tools: These tools enable network administrators to monitor and analyze network traffic, detect and diagnose network issues, and optimize network performance. Examples of popular network monitoring and analysis tools include Wireshark, SolarWinds, and PRTG Network Monitor.

In summary, choosing the right network devices, operations, and software is critical to the success of a networked system. By implementing reliable and secure devices, optimizing network operations, and choosing the right software, network administrators can ensure optimal network performance, scalability, and security

7.2.1 The interdependence of workstation

The interdependence of workstation hardware and relevant networking software is a fundamental concept in the field of computer networking. Workstation hardware refers to the physical components of a computer, such as the processor, memory, storage devices, and input/output devices, that are used to perform specific tasks. Networking software, on the other hand, is the set of programs and protocols that enable communication and data exchange between computers on a network.

The interdependence between workstation hardware and networking software is critical because both are required to ensure the proper functioning of a networked system. The hardware must be designed to support the software, and the software must be designed to take advantage of the capabilities of the hardware. For example, if the

network software requires high-speed data transfer, the workstation hardware must be equipped with a fast network interface card (NIC) to support this requirement.

Furthermore, the performance of a network is heavily dependent on the capabilities of the individual workstations that make up the network. The speed and processing power of the workstation's CPU and the amount of RAM and storage it has available can affect the network's overall performance. In addition, the network software must be designed to take advantage of the capabilities of the hardware to ensure optimal performance.

In summary, the interdependence of workstation hardware and relevant networking software is a critical aspect of computer networking. Without the proper hardware and software, a network may not function correctly, and its performance may suffer. Therefore, it is essential to consider both hardware and software requirements when designing and implementing a networked system

Server	Cost	Scalability	Ease of Use	Security
Microsoft Exchange Server	High	High	Moderate	High
Zimbra Collaboration Server	Moderate	High	Moderate	High
Google Workspace	Moderate	High	High	Moderate
IBM Lotus Notes/Domino	High	High	Moderate	High
MDaemon Email Server	Low	Moderate	High	Moderate

Table 8Categorizing Mail Servers according to various Criteria.

Server	Cost	Scalability	Reliability	Security	Ease of Use
Microsoft SQL Server	High	High	High	High	Moderate
Oracle Database	High	High	High	High	Moderate
MySQL	Low	High	Moderate	Moderate	High
PostgreSQL	Low	High	High	High	Moderate
MongoDB	Moderate	High	High	Moderate	Low

8 Activity 3

8.1 Network Building

How to be Build a good network?

1. Define Your Requirements: Determine the specific requirements of your network, including the number of devices, the amount of data traffic, and the level of security needed.
2. Choose Your Hardware: Select the appropriate network hardware, such as routers, switches, and access points, that can meet your requirements. Make sure to choose reliable and high-quality hardware from reputable manufacturers.
3. Plan Your Network Topology: Design the network topology that will be used to connect devices to the network. This will involve deciding on the placement of routers, switches, and access points.
4. Configure Your Network: Set up the hardware and configure the network settings. This includes setting up IP addresses, security settings, and access control policies.
5. Test Your Network: Test the network to ensure that it is functioning correctly and meets your requirements. This can include testing the speed and reliability of the network, as well as the security settings.
6. Maintain Your Network: Regularly maintain and update your network to ensure that it continues to meet your requirements. This includes updating firmware, monitoring network performance, and addressing any issues that arise.
7. Provide Training: Provide training to users on how to properly use and maintain the network, including how to connect devices, troubleshoot issues, and follow security policies.
8. Review and Improve: Regularly review the network and look for opportunities to improve its performance, security, and usability. This can involve upgrading hardware or software, changing network configurations, or implementing new security measures.

(divition, the panel of lecturers HND;, 2022)
Esoft ELNS

8.2 Fundamental Design Goals

Network Fundamental Design Goals are a set of guiding principles that network designers and administrators should follow to ensure that the network functions optimally.

1. **Availability**: This goal refers to the ability of the network to remain operational and accessible to users. To achieve high availability, network designers must plan and implement redundancy and fault tolerance mechanisms in the network infrastructure. They must also monitor the network proactively to identify and resolve issues that could affect availability.

2. **Security**: Network security is crucial to prevent unauthorized access, data breaches, and other security threats. To achieve this goal, network designers and administrators must implement access control policies, encryption, firewalls, and other security measures to ensure the confidentiality, integrity, and availability of the network.

3. **Scalability:** A scalable network is designed to grow and adapt to changing requirements. This includes the ability to add new devices, users, and applications without compromising network performance. Network designers must plan the network architecture with scalability in mind, and use hardware and software components that can support growth and expansion.

4. **Manageability:** A manageable network is one that is easy to maintain and troubleshoot. This involves implementing tools and processes that simplify network administration, automate monitoring, and reporting, and provide centralized management capabilities. Network designers and administrators should strive to make the network easy to manage, with a low total cost of ownership.

8.3 Network Design Methodologies

Network design methodologies provide a structured approach to designing networks. The following are the basic steps involved in most network design methodologies:

Step 1: Identify the network requirements - This involves understanding the organization's business goals, technical requirements, and user needs. Network designers must identify the number of users, applications, devices, and data flows that the network must support.

Step 2: Characterize the existing network - This step involves analyzing the current network infrastructure and identifying any shortcomings, such as bottlenecks, security vulnerabilities, or scalability issues. Network designers must gather information on the network's architecture, protocols, hardware, software, and security policies.

Step 3: Design the network topology and solutions - Based on the requirements and existing network analysis, network designers must develop a network topology that meets the organization's needs. This involves selecting the appropriate hardware and software components, such as switches, routers, firewalls, and servers, and configuring them to work together. Network designers must also ensure that the network is secure, scalable, and easy to manage.

Once the network design is complete, network designers must test and validate the network's functionality, performance, and security. Ongoing monitoring and maintenance are also critical to ensure that the network remains operational and meets the organization's changing needs.

8.4 Quality of Service (QoS)

Quality of Service (QoS) is a set of technologies and techniques used in computer networking to ensure the reliable and efficient transmission of network traffic. QoS enables network administrators to prioritize certain types of traffic over others, ensuring that critical traffic, such as voice and video, receive the necessary bandwidth and are not affected by lower priority traffic, such as email or file transfers.

QoS operates by assigning traffic to different classes or levels of service based on their importance or sensitivity. Network

administrators can set policies that define the priority of each class of traffic, and the network devices use these policies to prioritize traffic accordingly. QoS also includes techniques such as traffic shaping, which regulates the flow of traffic to prevent congestion and ensure that each class of traffic receives its appropriate bandwidth.

The benefits of QoS in a network include improved application performance, reduced latency, and better user experience, particularly for real-time applications such as voice and video. QoS is especially critical in large, complex networks where traffic is competing for limited bandwidth.

Overall, QoS is an essential tool for network administrators to ensure that critical traffic is delivered with the necessary priority, bandwidth, and reliability, while also ensuring that other traffic does not negatively impact network performance.

8.4.1 QoS Characteristics

QoS (Quality of Service) is a set of techniques and technologies that ensures the reliable and efficient transmission of network traffic. QoS has four primary characteristics:

Reliability: QoS ensures that the network provides reliable delivery of data packets by minimizing packet loss and ensuring that packets are delivered in the correct order.

Delay: QoS aims to minimize delay, also known as latency, in network traffic. This is particularly important for real-time applications such as video conferencing and online gaming, where delays can negatively impact the user experience.

Jitter: Jitter is the variation in packet delay, and it can negatively impact the quality of real-time applications. QoS helps to minimize jitter by ensuring that packets are delivered at consistent intervals.

Bandwidth: QoS enables network administrators to prioritize certain types of traffic over others, ensuring that critical traffic receives the necessary bandwidth while also preventing less critical traffic from consuming too much bandwidth

Figure 42 Concepts of Quality Of Service

Mathur, V. (n.d.). *What is the Quality of Service (QoS)? | Analytics Steps*.

9 Network Verification - Ping Command

Network verification is the process of checking whether the network is functioning correctly and meeting the design requirements. One tool commonly used for network verification is the Ping command, which is available in most operating systems. Here are some key points about Ping and how it can be used for network verification:

Ping sends Internet Control Message Protocol (ICMP) packets to a specified network device or host and measures the time it takes for the device to respond.

Ping can be used to test connectivity, packet loss, and round-trip time (RTT) for network devices.

Ping can help identify network performance issues, such as high latency or packet loss, that may affect the user experience.

Ping can be used to verify network reachability between two devices or hosts, and to troubleshoot connectivity problems.

Ping can also be used to verify the correct configuration of network devices, such as routers, switches, and firewalls.

Overall, Ping is a simple yet powerful tool for network verification that can help identify network issues and verify the correct functioning of network devices.

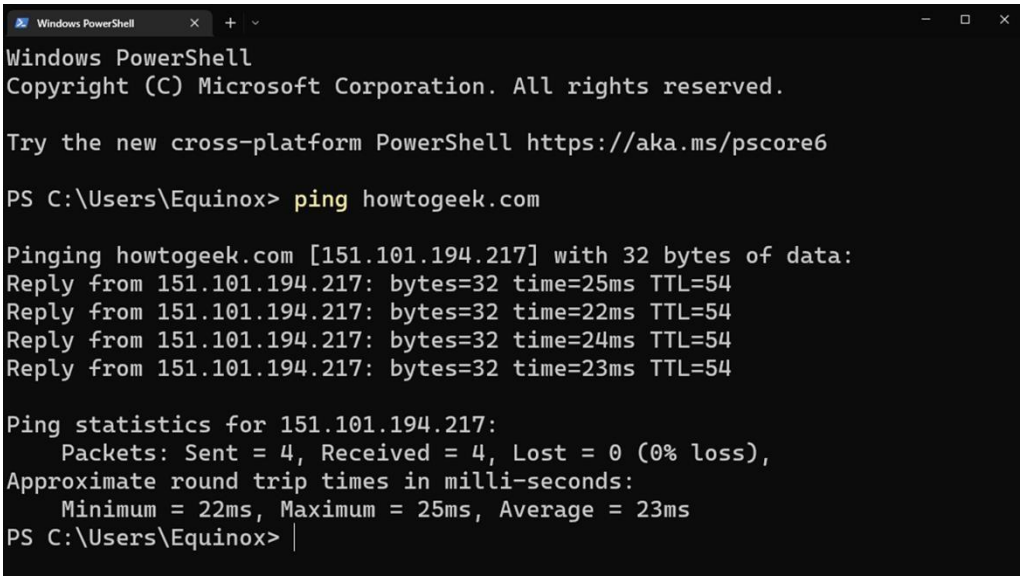


Figure 43 Network Verification - Ping Command testing

10 the Network Verification – Traceroute Command

Another tool commonly used for network verification is the Traceroute command, which is available in most operating systems. Here are some key points about Traceroute and how it can be used for network verification:

Traceroute is a command-line utility that helps to identify the path that network packets take from one network device to another, and the latency of each hop along the way.

Traceroute sends packets with gradually increasing TTL (Time To Live) values, and each network device along the path decrements the TTL and sends an ICMP Time Exceeded message back to the source when the TTL reaches 0. This allows Traceroute to build a map of the networks path and measure the latency of each hop.

Traceroute can be used to identify network performance issues, such as high latency or packet loss, that may affect the user experience.

Traceroute can help identify network topology issues, such as routing loops or misconfigured devices, that may cause connectivity problems.

Traceroute can be used to verify the correct functioning of network devices, such as routers, switches, and firewalls.

Overall, Traceroute is a powerful tool for network verification that can help identify network issues and verify the correct functioning of network devices.

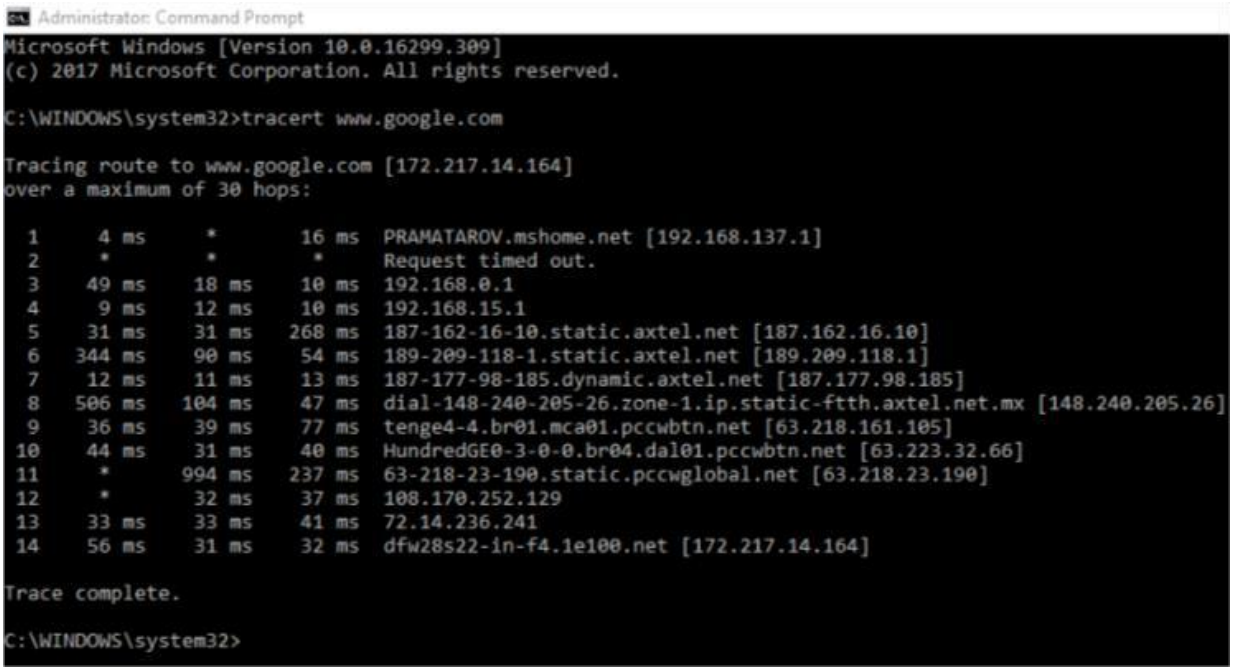


Figure 44 the Network Verification – Traceroute Command testing.

11 Network Monitoring

Network monitoring is the process of constantly monitoring a network to detect and diagnose problems, as well as to ensure that the network is functioning optimally. Network monitoring can be performed using a variety of tools and techniques, including:

Network monitoring software: This type of software monitors network traffic in realtime, detecting anomalies and providing alerts when network performance deviates from normal parameters.

SNMP (Simple Network Management Protocol): This protocol allows network devices to be monitored and managed from a central location. SNMP provides a standardized way for network administrators to collect data from network devices, such as routers, switches, and servers.

Packet capture: This technique involves capturing and analyzing network traffic to identify network performance issues and diagnose problems.

Performance metrics: Network performance metrics, such as latency, packet loss, and bandwidth utilization, can be monitored and analyzed

to identify trends and patterns that may indicate network performance problems.

Network monitoring can provide a range of benefits, including:

Early detection of network problems: Network monitoring tools can alert network administrators to potential issues before they become serious problems, allowing them to take proactive measures to resolve issues.

Improved network performance: By constantly monitoring network traffic and performance metrics, network administrators can identify bottlenecks and other performance issues and take steps to optimize the network.

Better security: Network monitoring tools can detect security threats, such as malware and suspicious network traffic, allowing network administrators to take action to mitigate security risks.

Overall, network monitoring is an essential part of network management and can help ensure that the network is functioning optimally and securely.

Types of network monitoring protocols

1. SNMP
2. ICMP
3. Cisco Discovery Protocol
4. ThousandEyes Synthetics

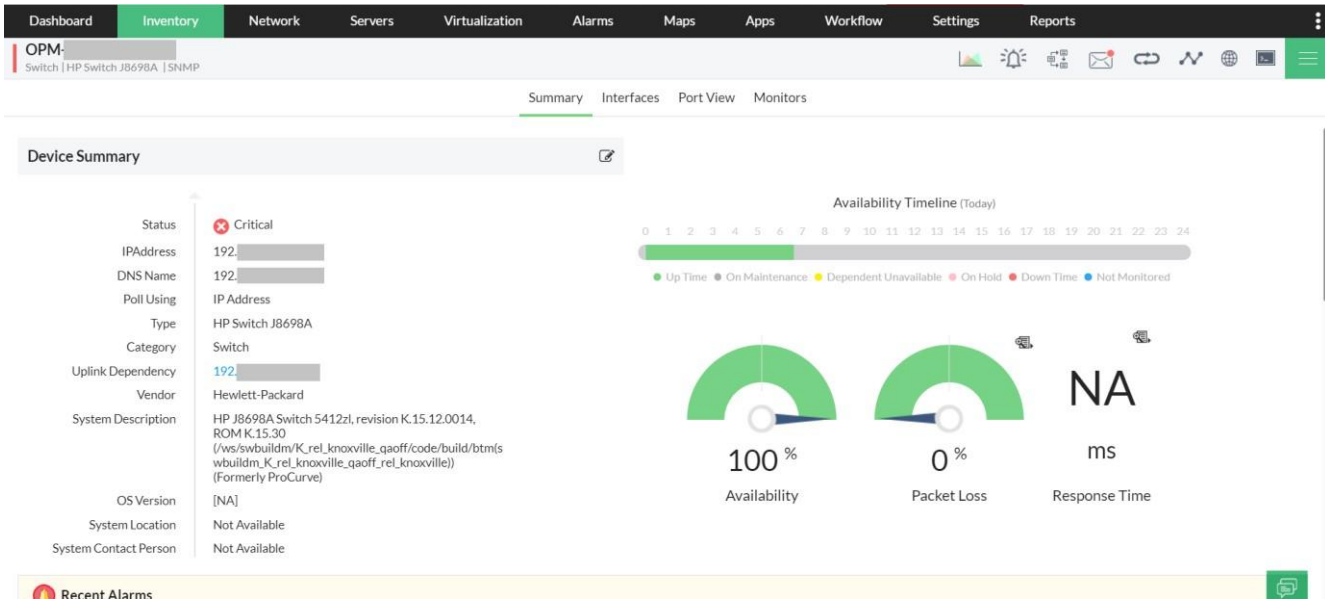


Figure 45 example the network monitoring software

VMware. (2021). *What Is Network Monitoring?*

Cisco. (n.d.). *What Is Network Monitoring?*

11.1 Designing a Maintenance Schedule

In a network system, branch maintenance refers to the process of maintaining and updating the networking equipment and infrastructure at various branch locations of an organization. A branch maintenance schedule is a plan that outlines the maintenance activities and tasks that need to be performed on a regular basis to ensure the smooth functioning of the network.

Here are some of the key aspects of a branch maintenance schedule in a network system:

1. Regular Maintenance: Regular maintenance is essential to keep the network infrastructure up to date and ensure optimal performance. This includes activities such as updating firmware and software, checking network device configurations, and replacing hardware components that are no longer functioning properly.

2. Schedule Frequency: The frequency of maintenance activities depends on the specific needs of the organization and the nature of the network. For example, some networks may require daily or weekly maintenance, while others may only need monthly or quarterly maintenance.

3. Prioritization of Tasks: It is important to prioritize maintenance tasks based on their criticality to the network's functioning. This involves identifying the most critical components of the network infrastructure and scheduling maintenance activities accordingly.

4. Coordination with Stakeholders: The branch maintenance schedule should be communicated to all stakeholders involved in the network system, including network administrators, branch managers, and other relevant personnel. This ensures that everyone is aware of the maintenance activities and their impact on the network's functioning.

5. Contingency Planning: It is important to have contingency plans in place in case of unexpected issues or downtime during maintenance activities. This involves having backup systems and procedures in place to minimize the impact of any disruptions on the network and the business operations.

In summary, a branch maintenance schedule is an essential part of maintaining a network system. By scheduling regular maintenance activities, prioritizing tasks, coordinating with stakeholders, and having contingency plans in place, network administrators can ensure that the network infrastructure remains reliable, secure, and optimized for performance

Table 10Maintenance Schedule for Colombo Branch

System	Maintenance Times	Notice
Sever Maintenance	Monday to Saturday At 9.00am to 1.00pm	Since this is routine maintenance, no more warning is required.
WIFI Router Maintenance	8 am - 1 pm, Monday and Wednesday , only as needed	give user a 24-hour heads-up.
Main Switch Maintenance	9.30am – 5.00 pm ,at Sundays, only as needed	Will provide 24-48 hour notice when taking down Main Switch
Secondary Switches (Third Floor Switches) Maintenance	9.00am to – 6.00 pm, Sundays, only as needed	Will provide 24-48 hour notice when taking down Secondary Switches

Ip range table

With the recommendations on the architecture and topology of the network and its requirements based on the given scenario, the next phase involves having a sketch on the implementation before simulating the plan.

Illustrated below is the design of the network prior to implementation, along with its details on its relevant characteristics given in the table further below.

Floor	Department	VLAN ID	IP Range	No of Computers	subnet mask
1	Reception	101	192.168.10.209-192.168.10.216	8	255.255.255.248
	Sales and Marketing	102	192.168.10.161-192.168.10.176	16	255.255.255.240
	Customer Services	103	192.168.10.217-192.168.10.224	8	255.255.255.248
2	Admin	201	192.168.10.65-192.168.10.96	32	255.255.255.224
	HR	202	192.168.10.97-192.168.10.128	32	255.255.255.224
	Accounting	203	192.168.10.129-192.168.10.160	32	255.255.255.224
	Audit	204	192.168.10.177-192.168.10.192	16	255.255.255.240
	BDD	205	192.168.10.193-192.168.10.208	16	255.255.255.240
3	Conferencing	301	192.168.10.225-192.168.10.232	8	255.255.255.248
	IT	302	192.168.10.1-192.168.10.64	64	255.255.255.192
Matara Branch					
1	Reception	101	198.12.52.116-198.12.52.132	16	255.255.255.240
	Customer	102	198.12.52.133-198.12.52.149	16	255.255.255.240

2	IT	201	198.12.52.1-198.12.52.64	64	255.255.255.192
	Administrator	202	198.12.52.65-198.12.52.81	16	255.255.255.240
	Account	203	198.12.52.82-198.12.52.98	16	255.255.255.240
	HR	204	198.12.52.99-198.12.52.115	16	255.255.255.240

Activity Four

Implementing a networked system based on the prepared design with valid evidences

A networked system for the Alliance Health Colombo and Matara branches has been developed in Cisco Packet Tracer software. Let us see the final networked systems and evidence.

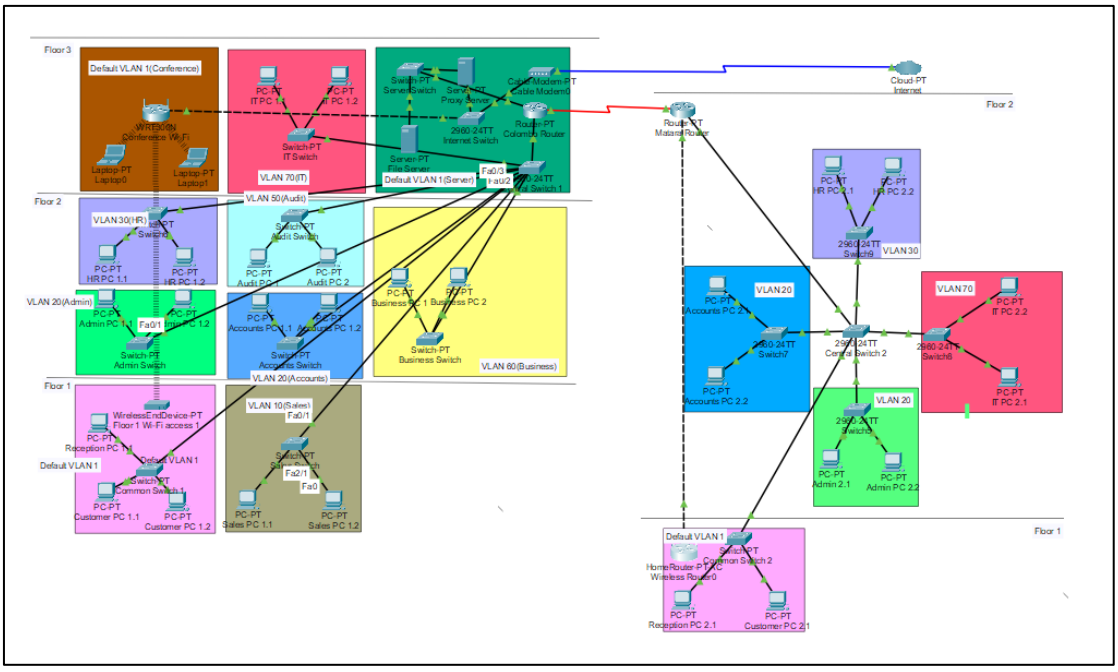


Figure 61 : Full Network Design

From the first look, you will see that this system uses VLAN systems in the branches to connect the departments with each other. Both branches have various departments such as Administrative department, HR department, Accounting & Finance department and much more.

VLAN configurations are achieved by single switches connected to all the PCs. Then I utilized routers-on-stick to give inter VLAN connectivity for the various departments.

Providing WIFI facilities to Customer service areas was a Customer request. So, I utilized WIFI routers, Cable modems, PT-Clouds and DHCP Servers to create functional WIFI networks. Customers can access internet through these facilities. Also, the Sales and

Marketing department of Colombo branch requested access to the internet facilities. I used separate PCs with wireless network modules (WMP300N) to provide internet facilities to the Sales & Marketing department.

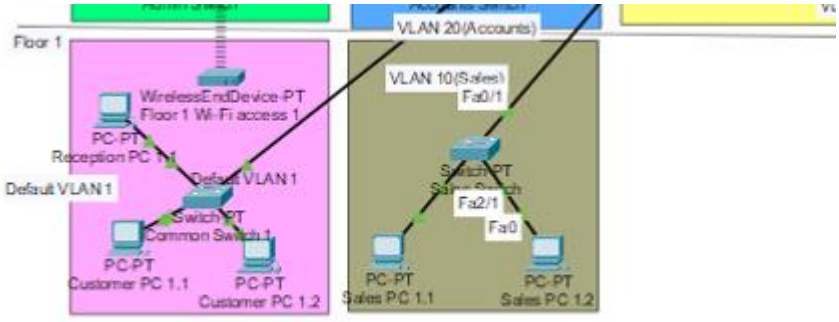


Figure 62 : First Floor - Colombo Branch

Other than that, all the other PCs in Sales & Marketing department & Reception are connected to the Main Switch at the second floor. All the departments at the second floor are also connected to the same switch.

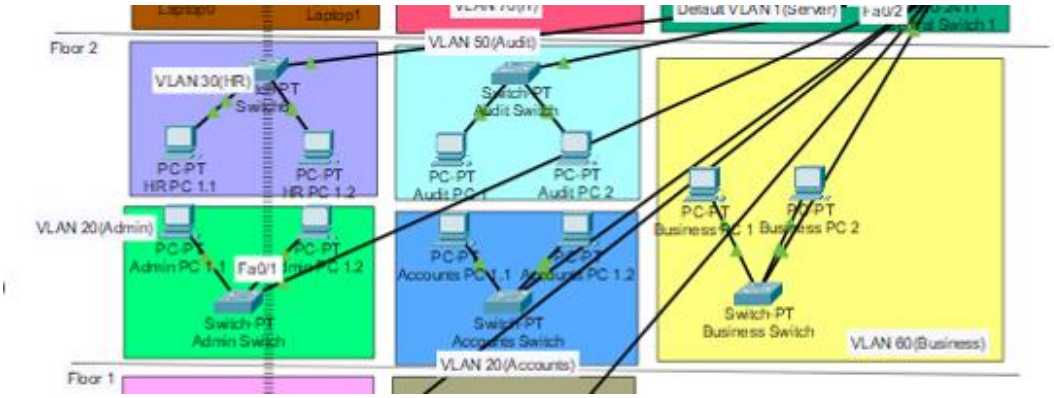


Figure 63 : Second Floor - Colombo Branch

You can also see the Router-on-stick here that enables inter VLAN connectivity.

Now let us see the third floor of Colombo branch.

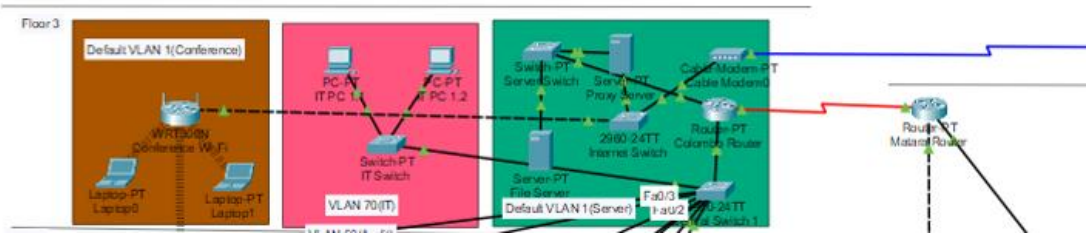


Figure 64 : Third Floor - Colombo Branch

The IT department utilize a separate switch. They also utilize a Printer connected to the same switch.

The Server room has four servers. Print Server, Database Server, DHCP Server & Mail Server. For the connectivity of this room, another switch is being utilized. A separate PC named ‘Server Manager’ is also connected to this switch for Managing the connected Servers. A printer is also available here connected to the same switch.

Video Conference room requested Connection to Internet facilities. So, I utilized a PC with a wireless module (WMP300N) to connect to the WIFI router at the first floor. This provides internet facilities easily without any cabling hassles.

✞ Now let us take a look at the **Matara branch**.

Figure 65 : First Floor - Matara Branch

The first floor of the Matara branch contains both the Reception Area and the Customer Service Area. The reception area PC is connected to the Main Switch at the second floor. Customer Service Area is equipped with Internet facilities. I utilized a WIFI router, a Cable Modem, a PT-Cloud and a DHCP Server just like I did with the Colombo branch.

Now let us take a look at the second floor.

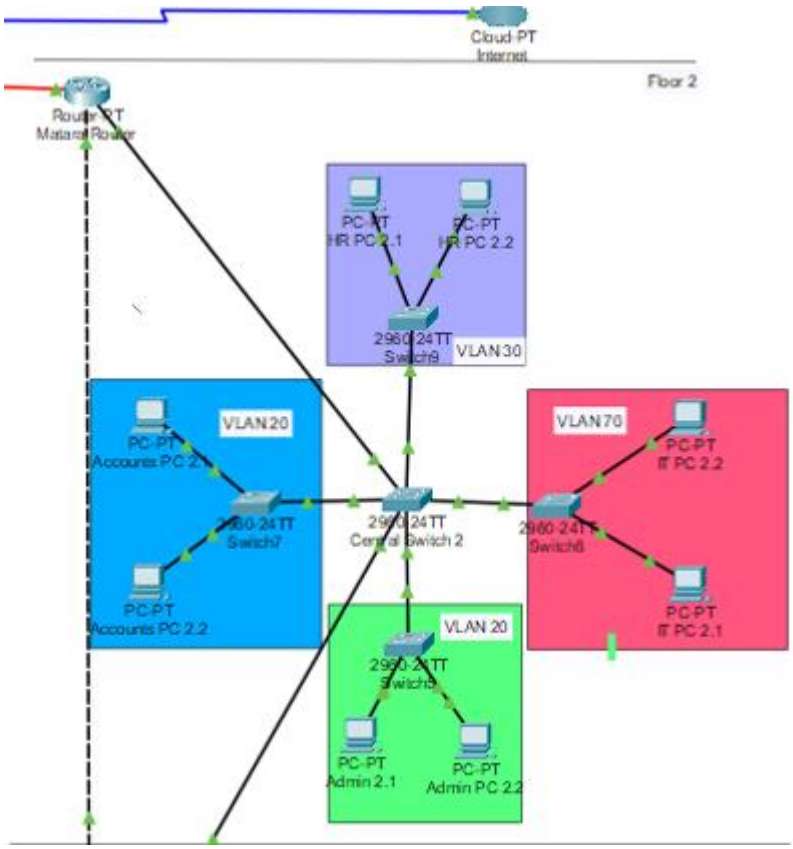


Figure 66 : Second Floor - Matara Branch

This floor contains all the departments. All of them are connected to the same switch enabling VLAN facilities. A Router-on-stick configuration is utilized same as before for inter VLAN connectivity. There are a lot of room for improvement in Matara branch.

WIFI & Internet Ping Test Results

Colombo Branch

Figure 67 : IP & DNS Details - Internet PC ~ Sales & Marketing Department.

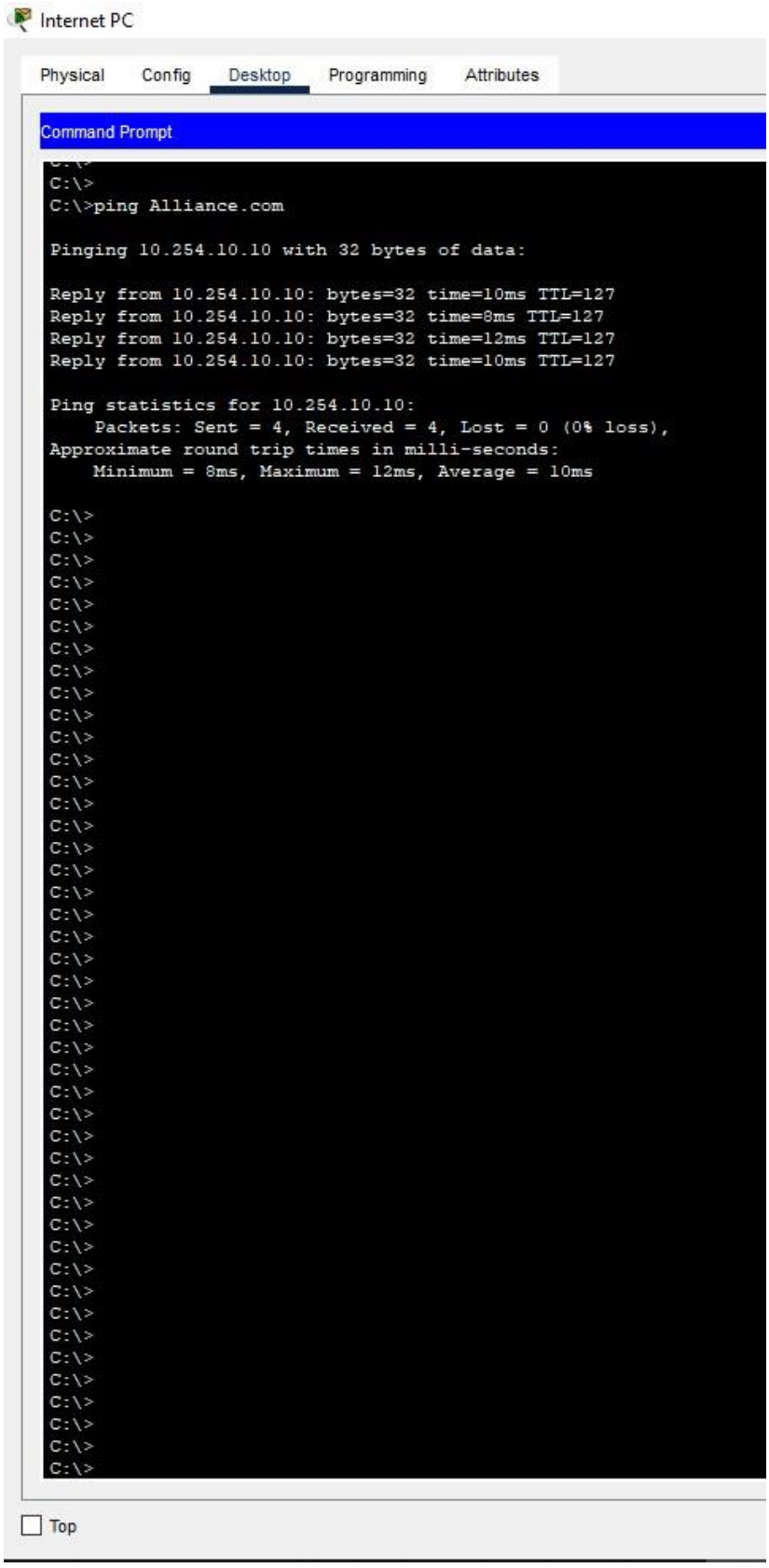


Figure 68 : Ping Test - Internet PC ~ Sales & Marketing Department.

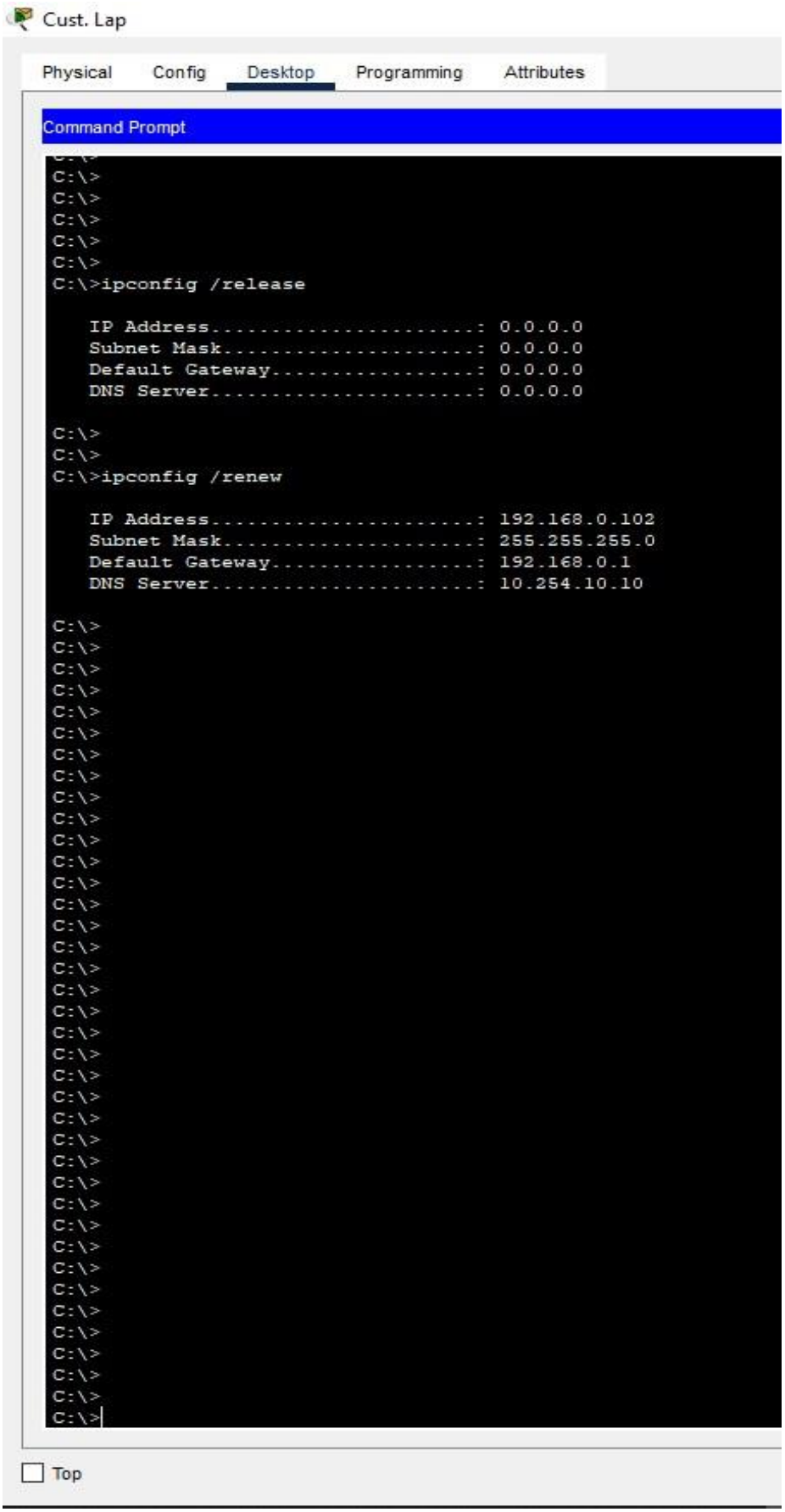


Figure 69 : Customer Laptop - IP Configuration ~ Customer Service Area.

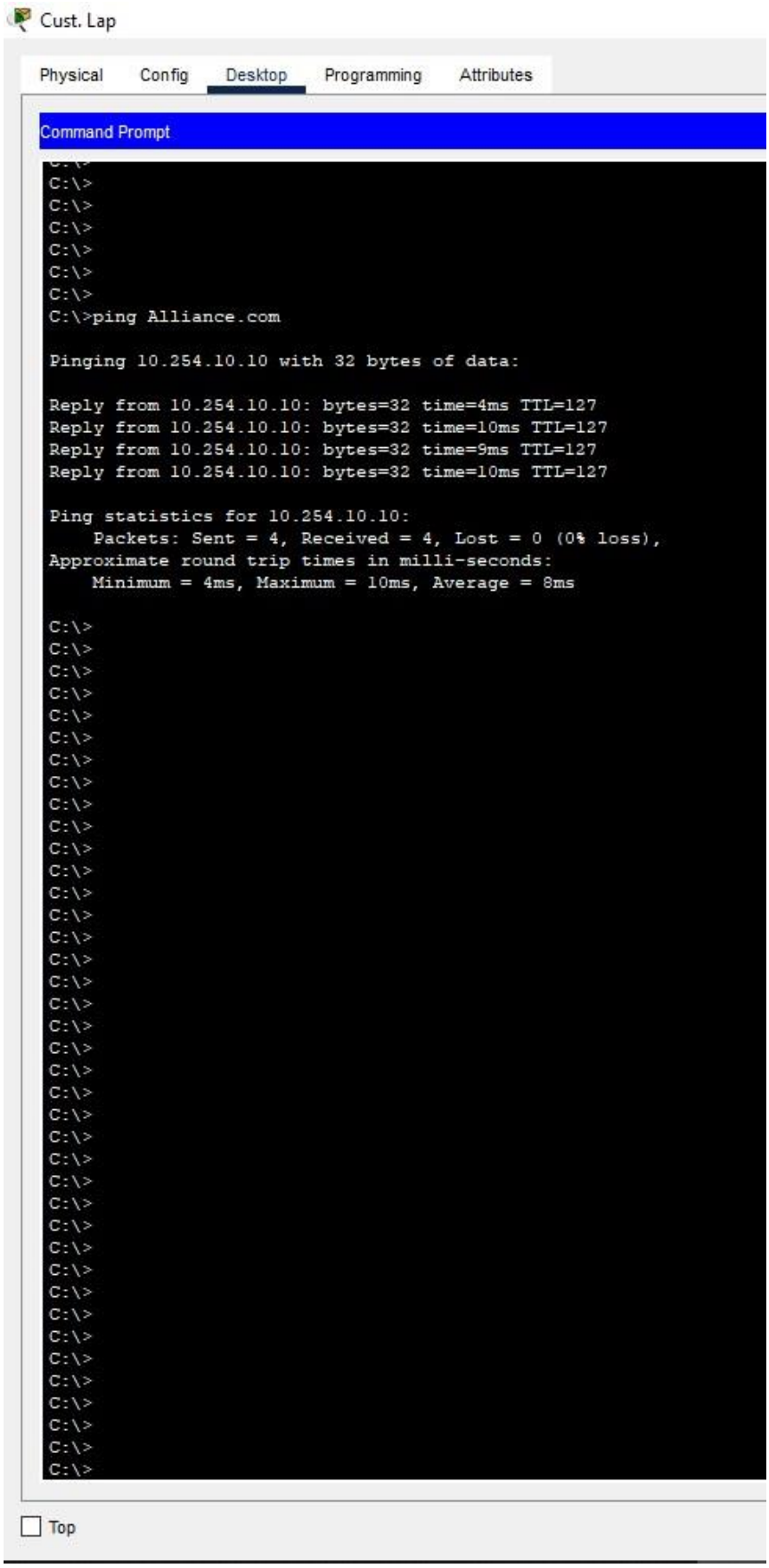


Figure 70 : Customer Laptop - Ping Test ~ Customer Service Area.

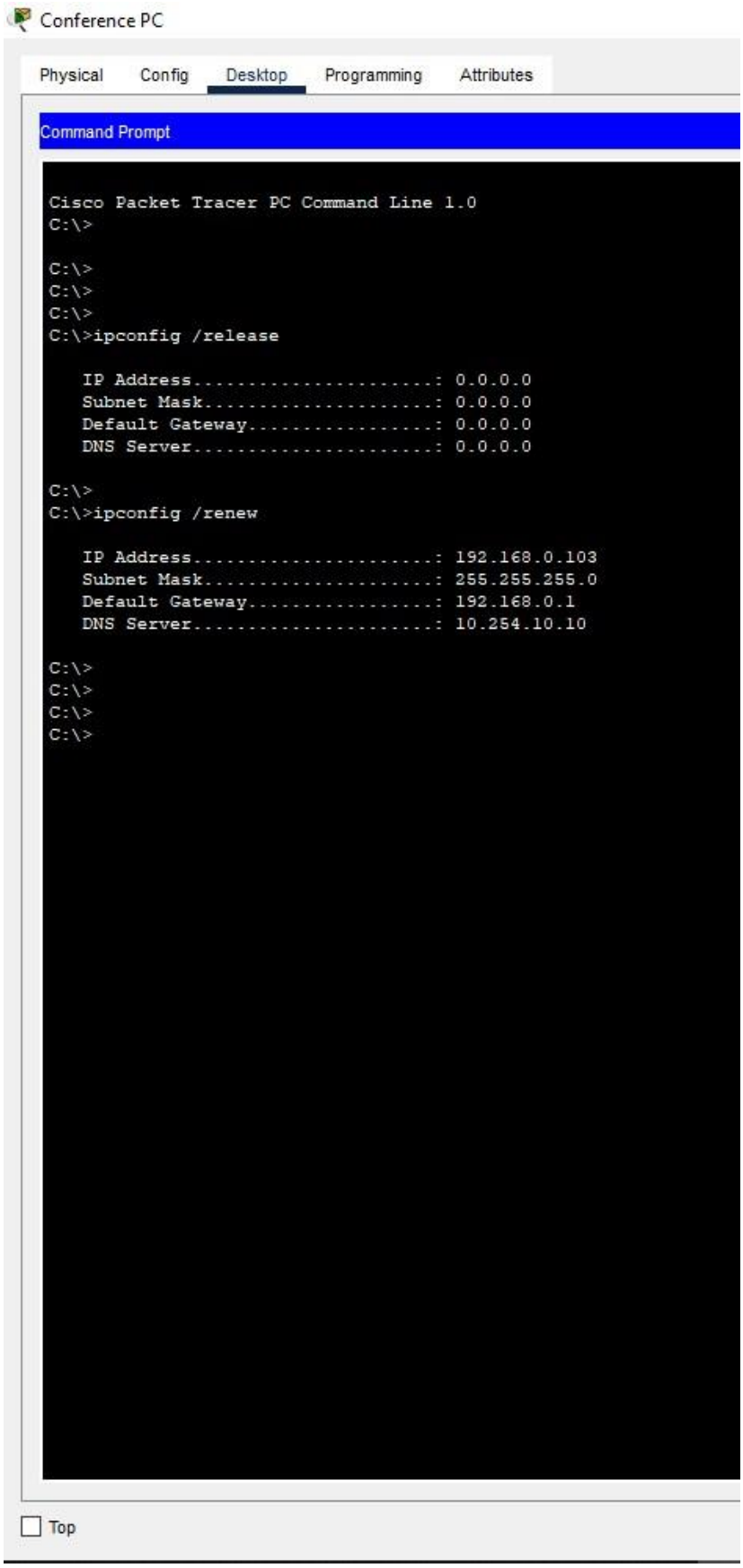


Figure 71 : Conference Room PC - IP Configuration

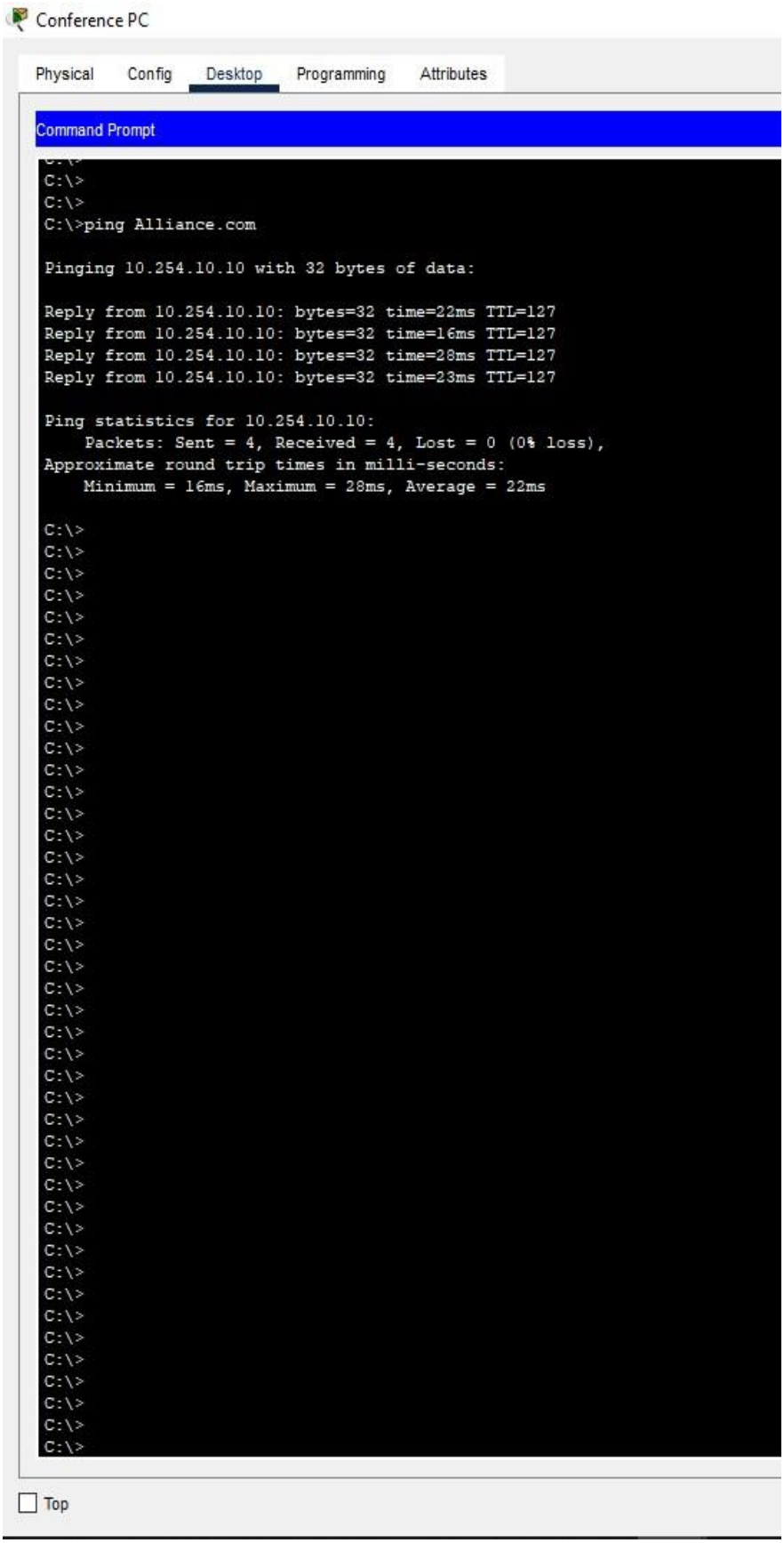


Figure 72 : Conference Room PC - Ping Test.

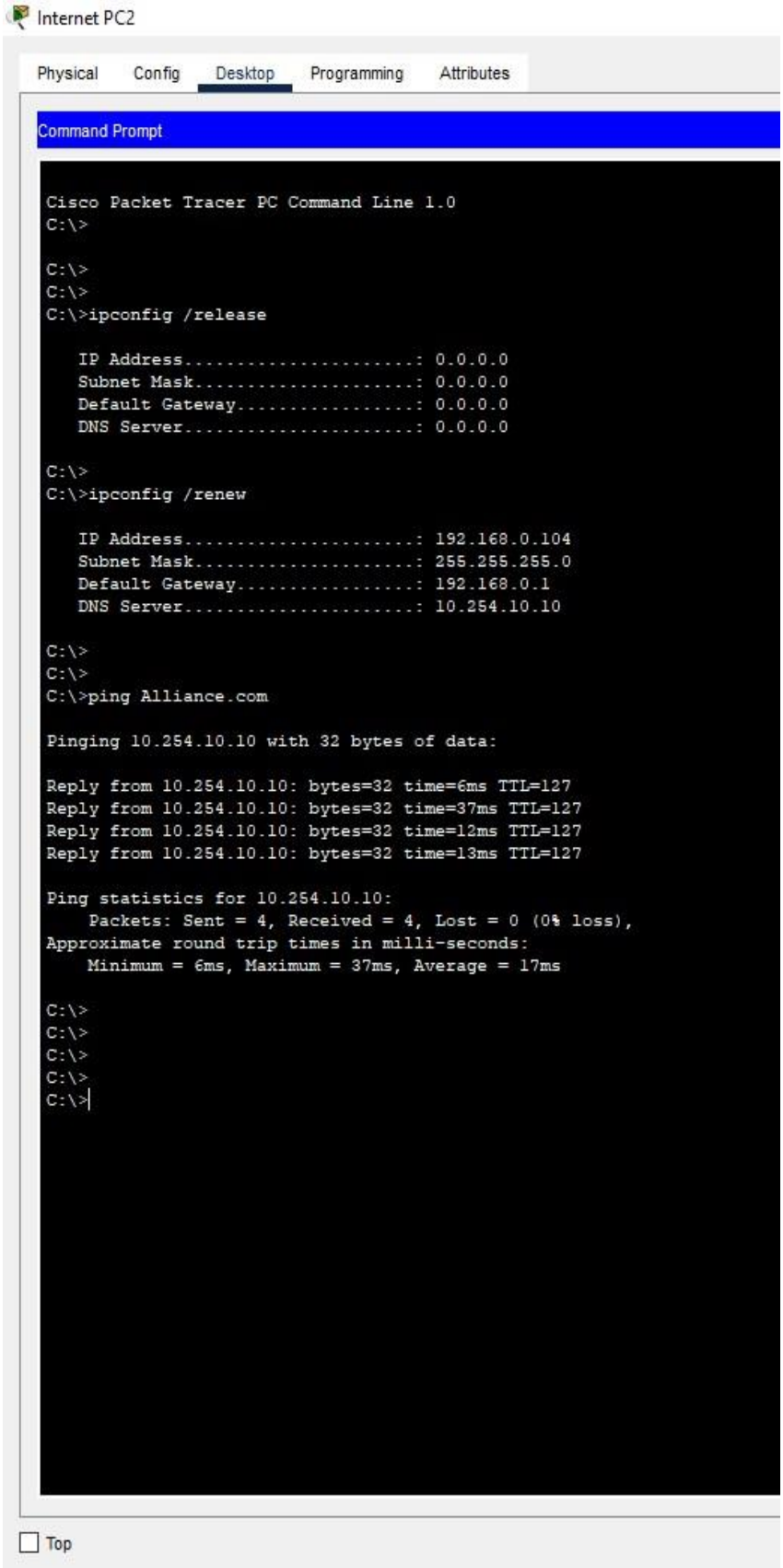


Figure 73 : Internet PC2 - IP Config & Ping Test ~ Sales & Marketing Department.

Matara Branch

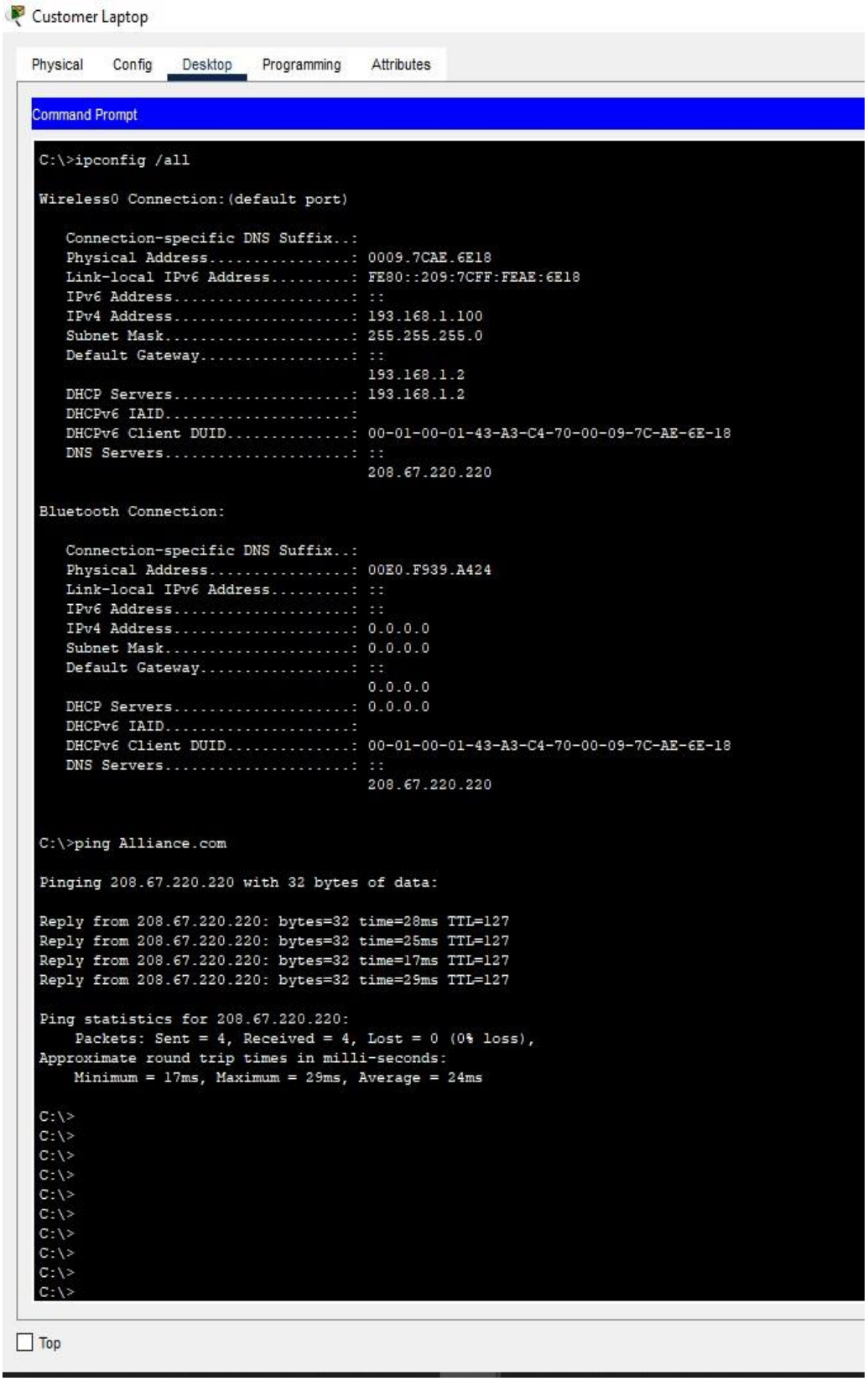


Figure 74 : Customer Laptop - IP Configurations & Ping Test ~ Customer Service Area.

Traceroute Tests

These tests were conducted by utilizing the Routers-on-stick in both branches.

Colombo Branch

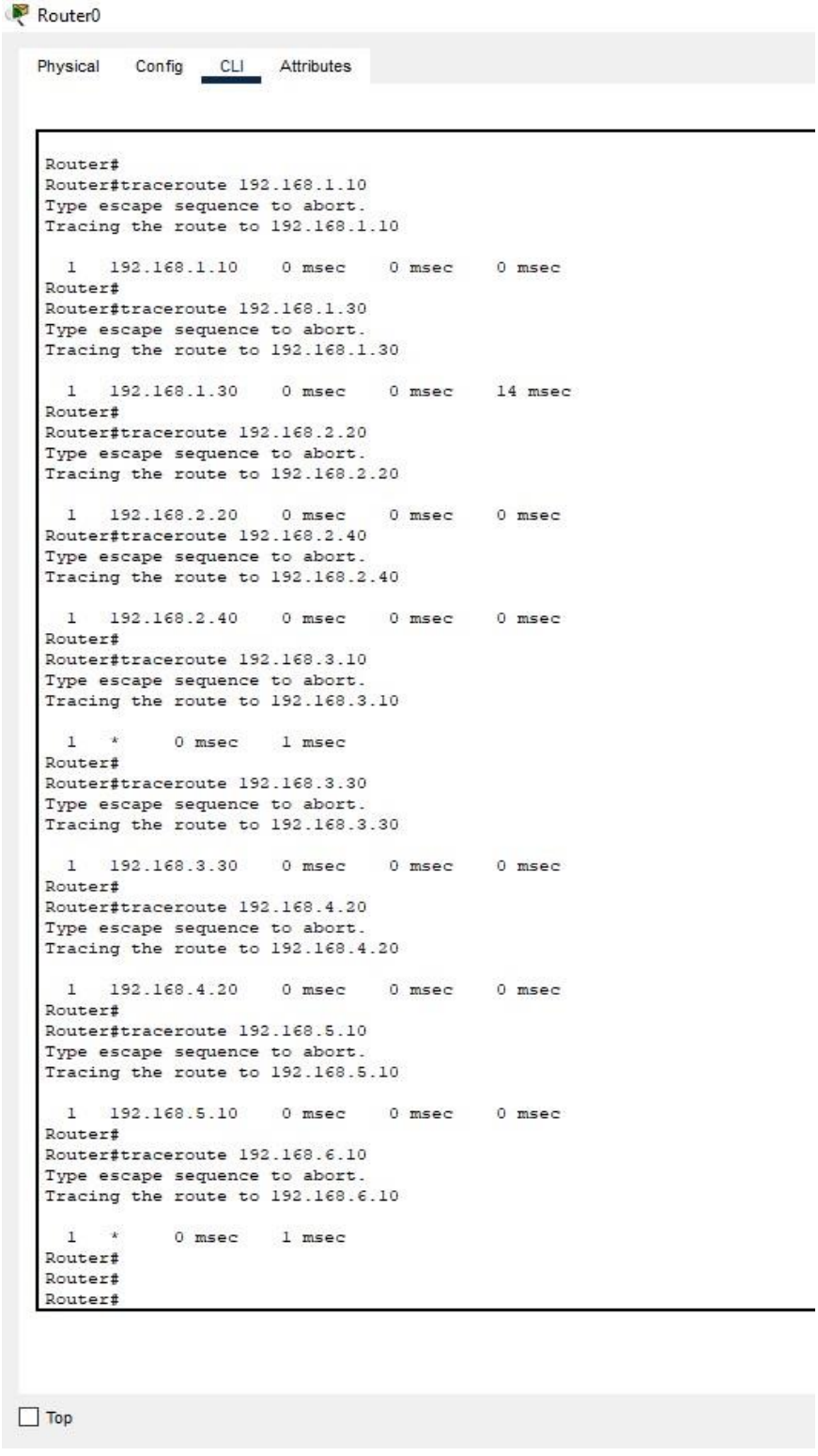


Figure 75 : Traceroute Verifications - Colombo Branch.

Matara Branch

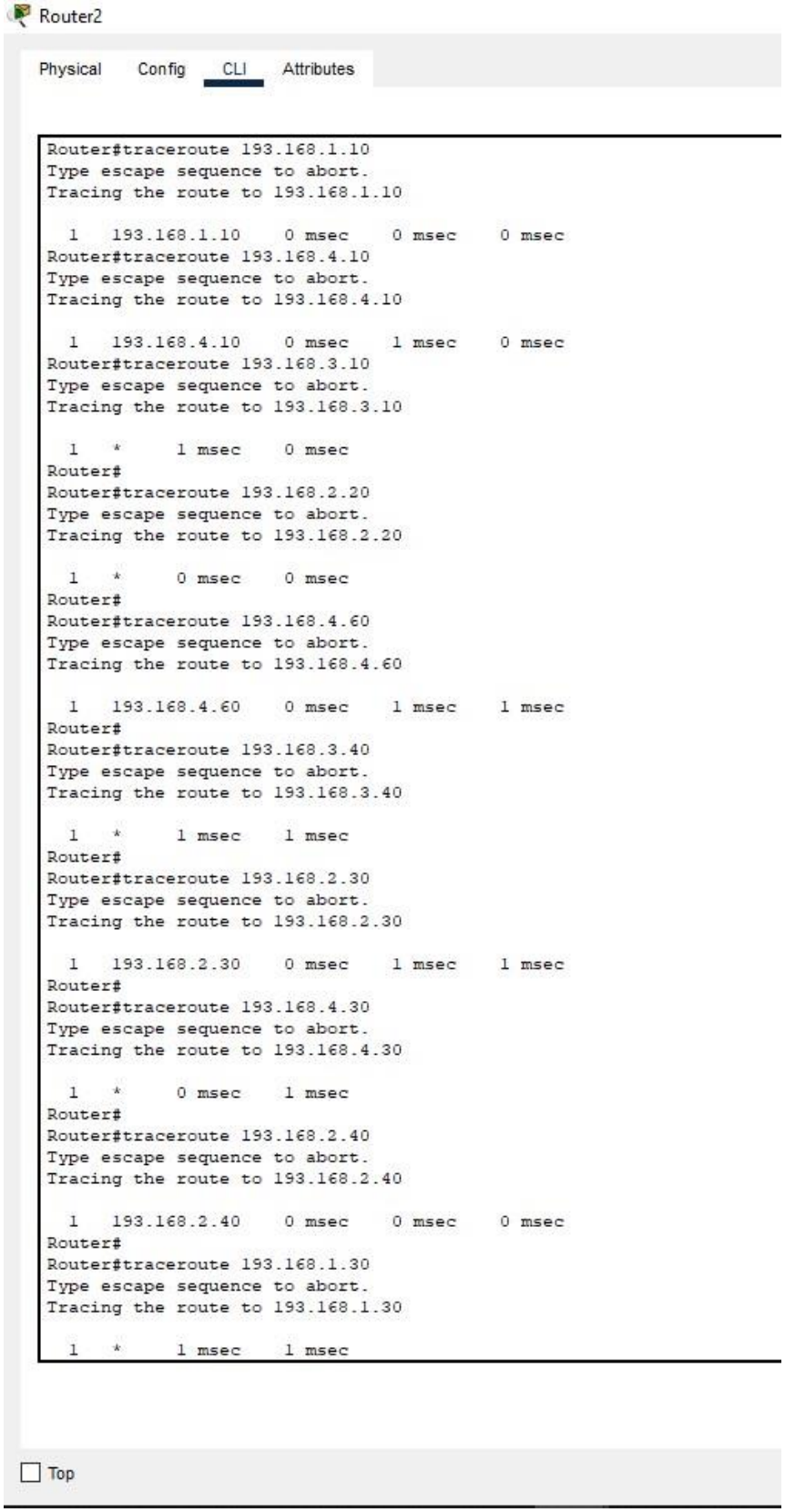


Figure 76 : Traceroute Verifications - Matara Branch.

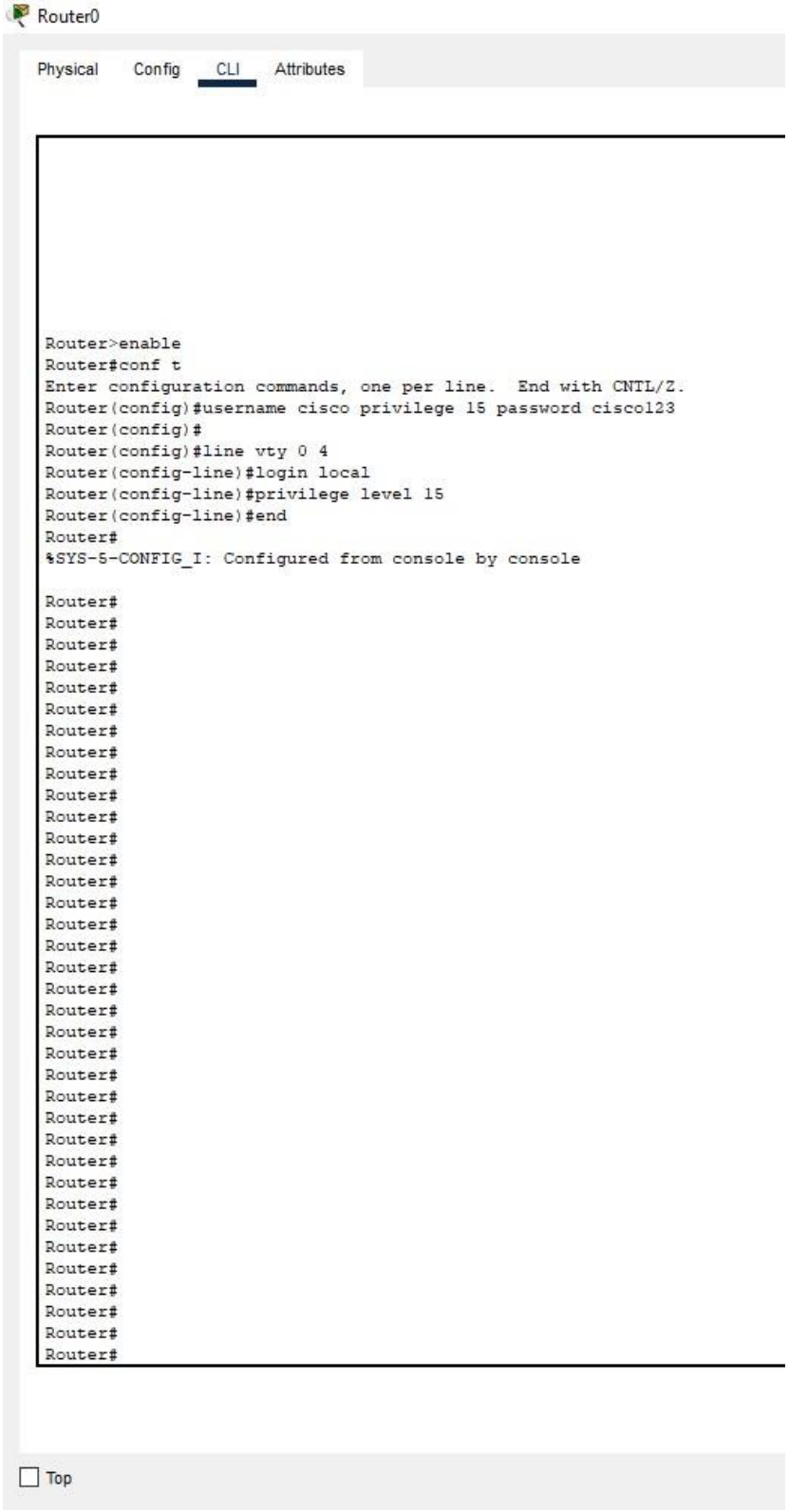


Figure 77 : Telnet Configuration - Router.

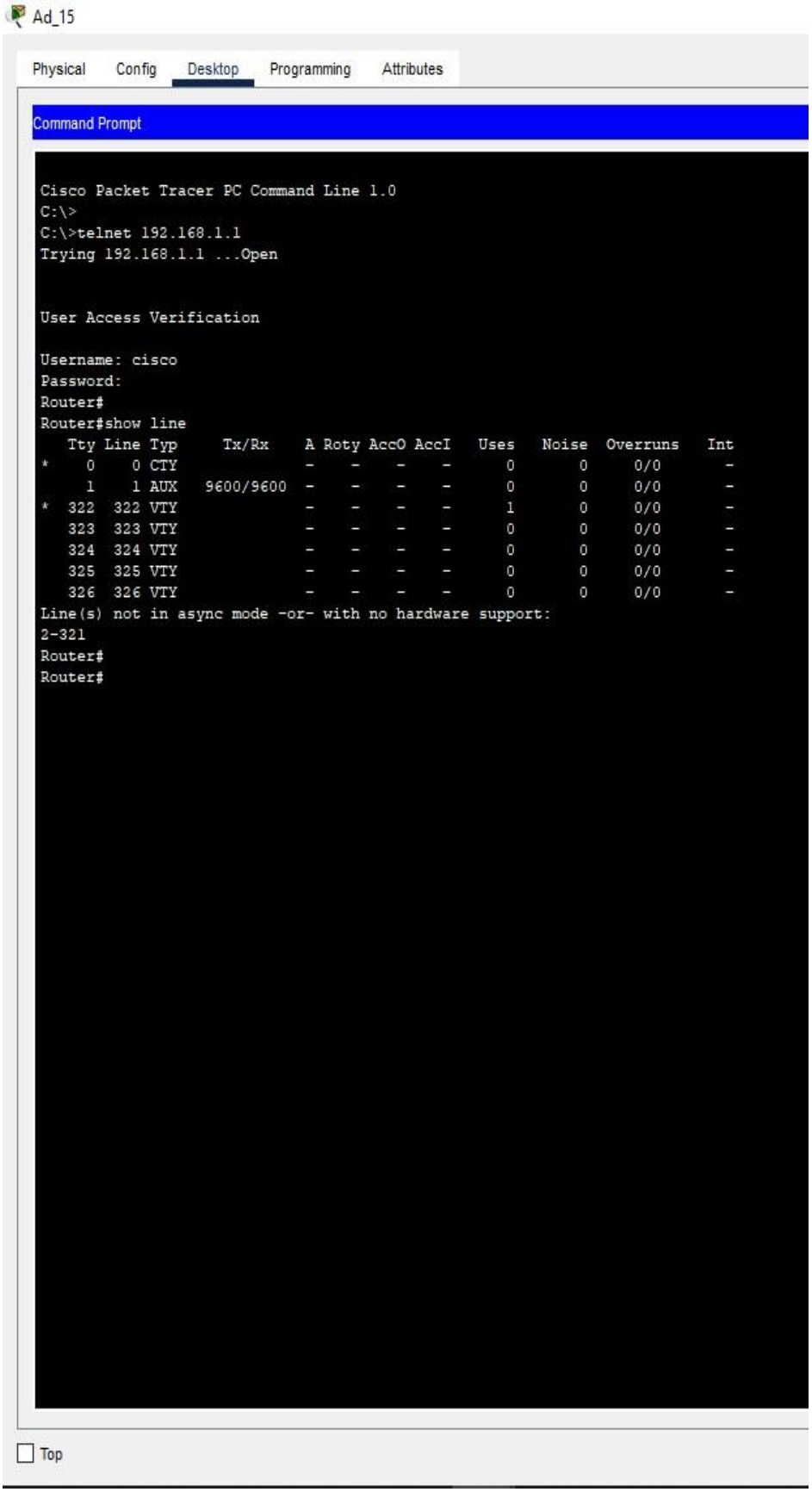


Figure 78 : Telnet Configuration - Ad_15 (PC).

Matara Branch

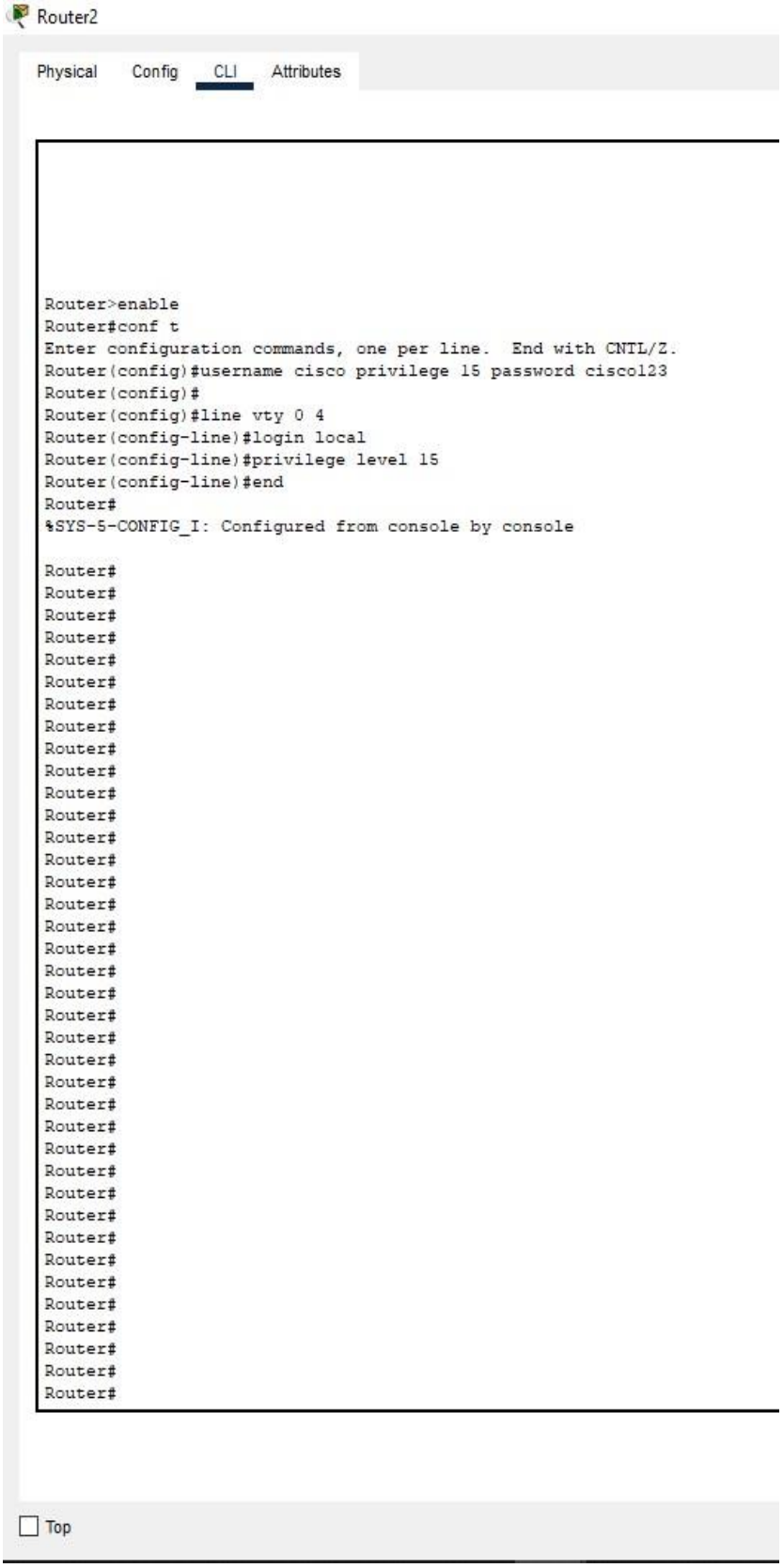


Figure 79 : Telnet Configuration - Router.

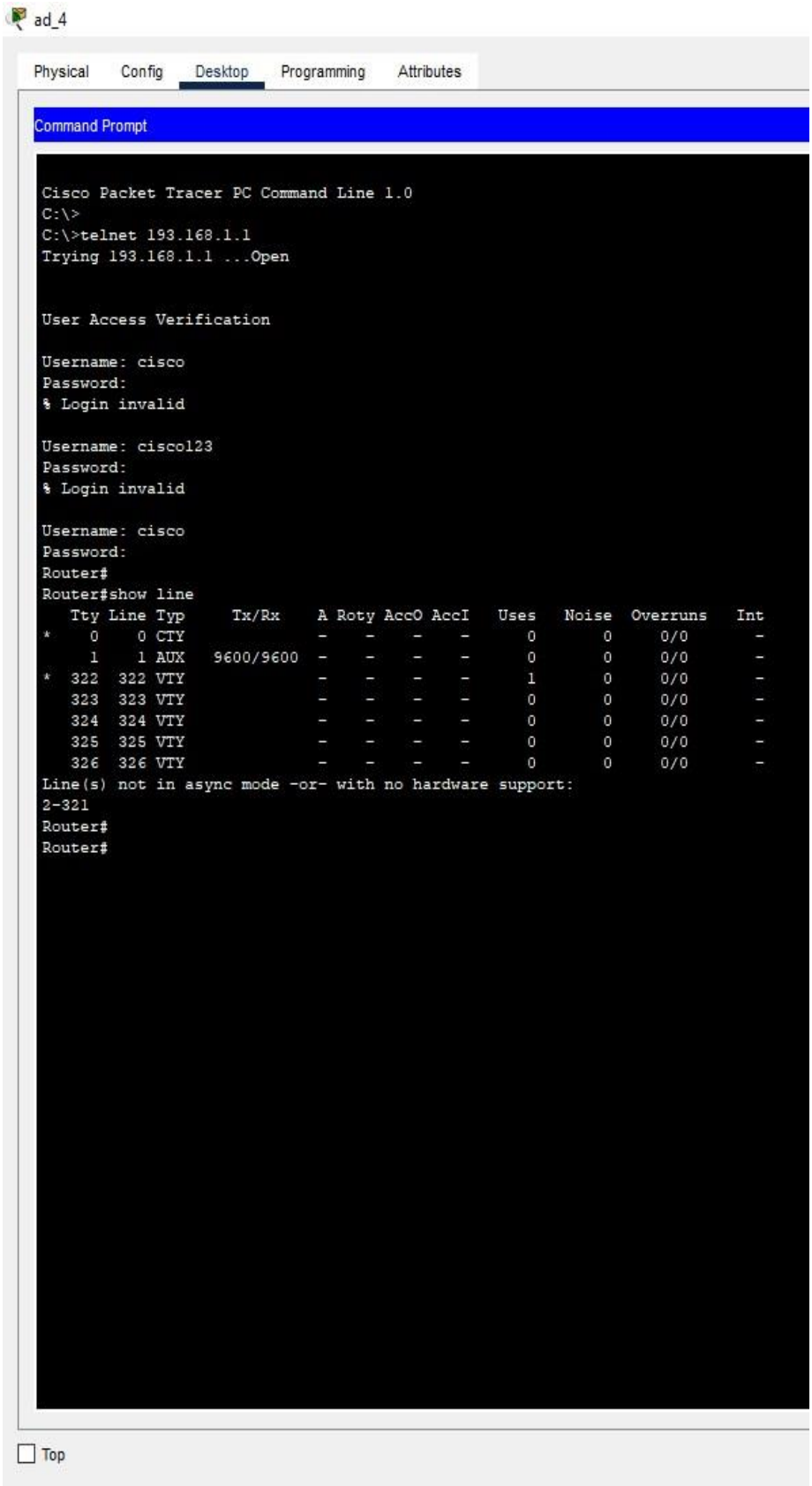


Figure 80 : Telnet Configuration - ad_4 (PC).

Analyzing the Test results against the Expected results

I have conducted three test cases so far. The results are shown in the above section.

1. Ping Test
2. Traceroute Test
3. Telnet Verification

Ping Test

I conducted this test in both branches by utilizing the WIFI connectivity in Devices. So, in Colombo branch I conducted this test with Internet PC, Internet PC2 (Sales & Marketing department), Customer Laptop (Customer Service Area), & Conference room PC. This test can be conducted by using the 'ping' command in the selected device. All these devices were pinged to 'Alliance.com' which was the DNS service name of the DHCP Server.

(I configured the DHCP Server as a DNS Server to provide DNS services)

The same practice was used in Matara branch. It has a Customer Service Area, which has a Customer Laptop connected to the WIFI service. The DHCP server in Matara is also configured as a DNS server providing DNS facilities. This server also has the DNS name

'Alliance.com', so pinging to that DNS was possible.

Now let us analyze the test results against the expected results.

Table 23 : Ping Test Analyzing - Colombo Branch.

No.	Test Description	Received Results	Expected Results
1	Ping 'Internet PC' to 'Alliance.com'	All packets were sent successfully, none were lost.	All packets being sent successfully without being lost.
2	Ping 'Internet PC2' to 'Alliance.com'	All packets were sent successfully, none were lost.	All packets being sent successfully without being lost.
3	Ping 'Customer Laptop' to 'Alliance.com'	All packets were sent successfully, none were lost.	All packets being sent successfully without being lost.
4	Ping 'Conference PC' to 'Alliance.com'	All packets were sent successfully, none were lost.	All packets being sent successfully without being lost.

Table 24 : Ping Test Analyzing - Matara Branch.

No.	Test Description	Received Results	Expected Results
1	Ping ‘Customer Laptop’ to ‘Alliance.com’	All packets were sent successfully, none were lost.	All packets being sent successfully without being lost.

All the ping tests were successful in both branches.

Traceroute Test

Traceroute tests are conducted using routers. So, I utilized the Router-on-stick configurations that I designed in both branches in order to conduct the tests. To conduct these tests, all I had to do was to access the router and type the command ‘traceroute’ followed by the IP address of the selected device. I conducted this test in random PCs of all the departments in both branches. The results are shown in the previous section of this document.

Now let us analyze the test results against the expected results.

Table 25 : Traceroute Test - Colombo Branch.

No.	Test Description	Received Results	Expected Results
1	Traceroute to ‘192.168.1.10’	Trace Success (0msec 0msec 0msec)	Trace Success
2	Traceroute to ‘192.168.1.30’	Trace Success (0msec 0msec 14msec)	Trace Success
3	Traceroute to ‘192.168.2.20’	Trace Success	Trace Success
		(0msec 0msec 0msec)	
4	Traceroute to ‘192.168.2.40’	Trace Success (0msec 0msec 0msec)	Trace Success
5	Traceroute to ‘192.168.3.10’	Probe timed out (0msec 1msec)	Trace Success

6	Traceroute to ‘192.168.3.30’	Trace Success (0msec 0msec 0msec)	Trace Success
7	Traceroute to ‘192.168.4.20’	Trace Success (0msec 0msec 0msec)	Trace Success
8	Traceroute to ‘192.168.5.10’	Trace Success (0msec 0msec 0msec)	Trace Success
9	Traceroute to ‘192.168.6.10’	Probe timed out (0msec 1msec)	Trace Success

Most of the results were **successful**, even though there were two timeouts.

Table 26 : Traceroute Tests - Matara Branch.

No.	Test Description	Received Results	Expected Results
1	Traceroute to ‘193.168.1.10’	Trace Success (0msec 0msec 0msec)	Trace Success
2	Traceroute to ‘193.168.4.10’	Trace Success (0msec 1msec 0msec)	Trace Success
3	Traceroute to ‘193.168.3.10’	Probe timed out (1msec 0msec)	Trace Success
4	Traceroute to ‘193.168.2.20’	Probe timed out (0msec 0msec)	Trace Success

5	Traceroute to ‘193.168.4.60’	Trace Success (0msec 1msec 1msec)	Trace Success
6	Traceroute to ‘193.168.3.40’	Probe timed out (1msec 1msec)	Trace Success
7	Traceroute to ‘193.168.2.30’	Trace Success (0msec 1msec 1msec)	Trace Success
8	Traceroute to ‘193.168.4.30’	Probe timed out (0msec 1msec)	Trace Success
9	Traceroute to ‘193.168.2.40’	Trace Success (0msec 0msec 0msec)	Trace Success
10	Traceroute to ‘193.168.1.30’	Probe timed out (1msec 1msec)	Trace Success

These tests done in Matara branch have a considerable amount of **timeouts**.

Recommending Potential Future enhancements for the Networked system with valid Justifications

The developed system is functional, although has some shortcomings. Future enhancements may be the answer to these issues.

Table 27 : Potential Future Enhancements & Justifications.

No.	Future Enhancement	Justification
1	Adding printers to all the departments of Matara Branch.	Currently do not have any.
2	Adding more printers to Colombo Branch departments.	Currently only available in IT department and the Server room.

3	Fixing errors in the connection between the IT department switch & the Server room switch (Colombo Branch)	Currently packets are not transferring.
4	Fixing errors in the connection between the IT department switch & the Second floor switch (Colombo Branch)	Currently packets are not transferring.
5	Adding Telephones to the Reception areas of both branches	Currently do not have any telephones.
6	Adding more PCs to the Reception areas of both branches	Currently only have one each.
7	Adding a large screen to the Video Conference room of the Colombo branch and connecting to the Conference Room PC	Currently only has the PC and its own monitor.

Critically reflecting on the implemented Network

The Plan

Originally, the plan of the Project was to build a new networked system for connecting the new Alliance Health branch in Matara with the Head Office in Colombo. Both these branches had various departments which had number of devices needed to interconnect.

Then, the branches themselves needed to be connected.

The Design

The final design of the network was a functional product with some shortcomings. But we discussed ways to enhance the system in the prior section.

Currently, this design has Routers-On-Stick for inter VLAN communication. But we could have used a Multilayer switch method for creating a more efficient inter VLAN connection. This would be perfect if the users intend to upscale the network model. Although, this would have made the designing more complex. The Configurations

I have utilized various configurations in this networked system.

VLAN setup

Configured with router-on-a-stick VLAN system. Simple design for connecting departments within the same switch. Multilayer switch setup would have been much suitable for the configuration. Server Configurations

- DHCP Server
- Mail Server
- Database Server
- Print Server

In the Colombo server room, above servers are connected to each other using a single switch setup. More efficient connection to the IT department would have been more suitable.

WIFI Configuration

WIFI provided with a simple setup including a WIFI router, a PT Cloud and a DHCP Server in both branches. Even though an access point would have been more suitable for providing WIFI services.

The Tests

I conducted Ping tests, Traceroute and Telnet tests. They were able to point out the functionality scope of the developed system. But more tests should be conducted for getting a complete evaluation. An **SSH** test would be able to test the security capabilities of the Network.

The Decisions

The decision to provide the IT department and Server room with separate switches was suitable in terms of giving simplicity to the multi floor setup of the Colombo branch. Although, it would have been much better to include the IT department with the same switch as the Main switch at the second floor in terms of inter department connectivity.

The decision to include the Reception area PCs with the Administrative VLAN in Colombo and IT VLAN in Matara was reasonable even though in the future enhancements it would be better to provide Reception area with their own VLAN.

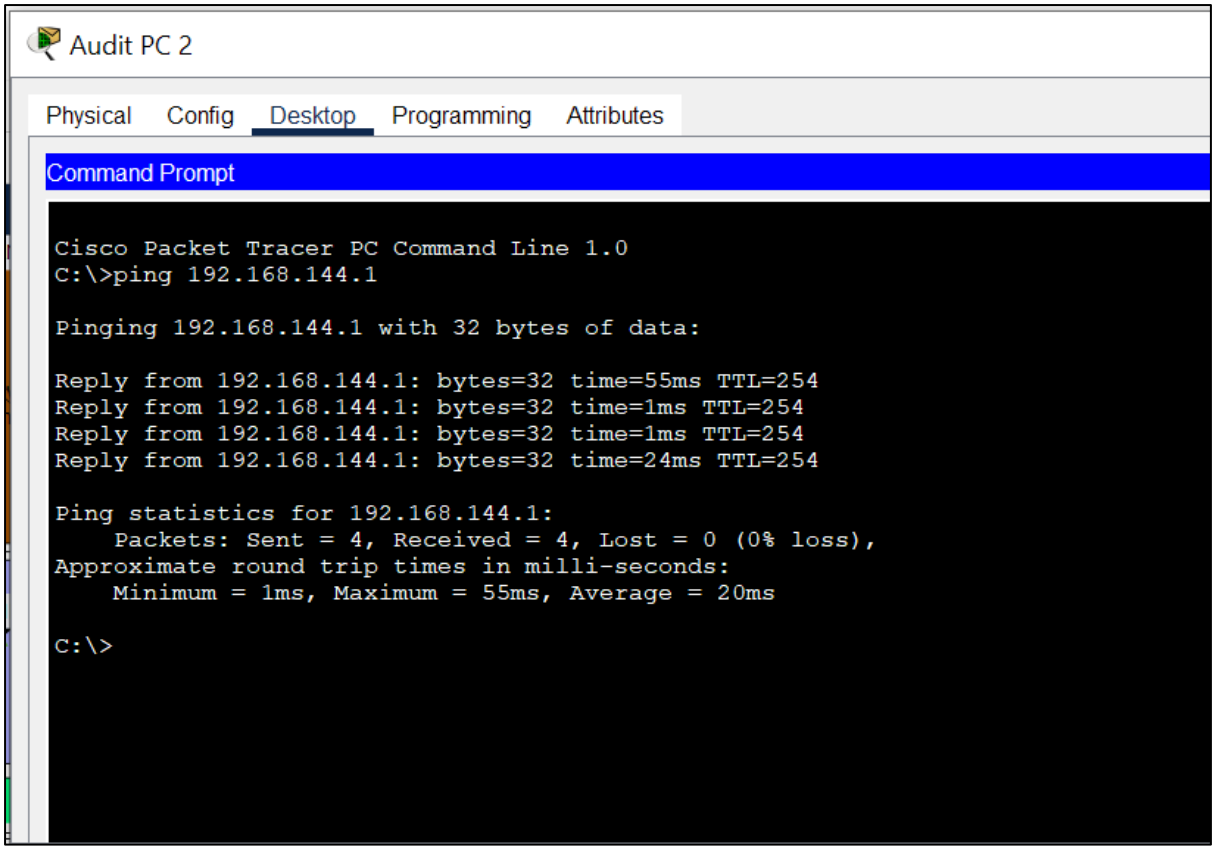


Figure 3 Test Case 05

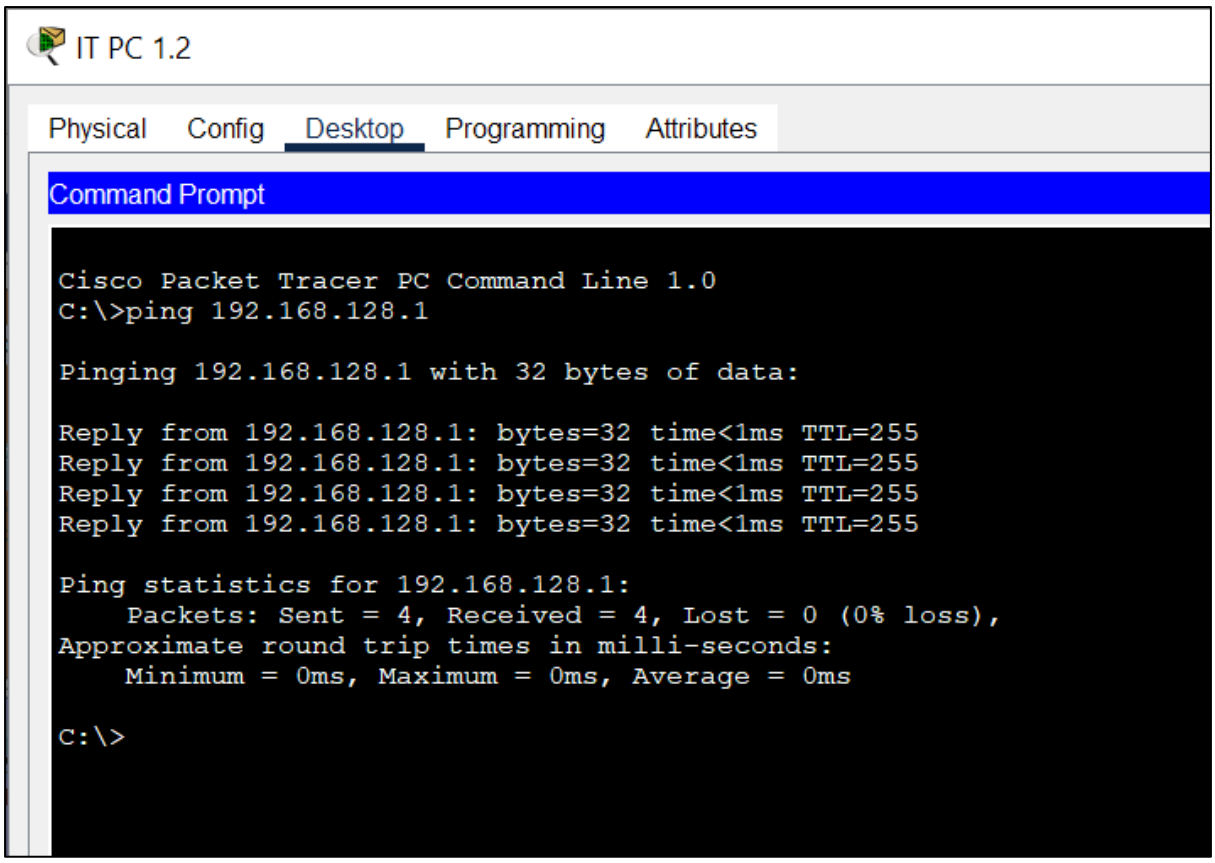


Figure 4 Test Case 06 a

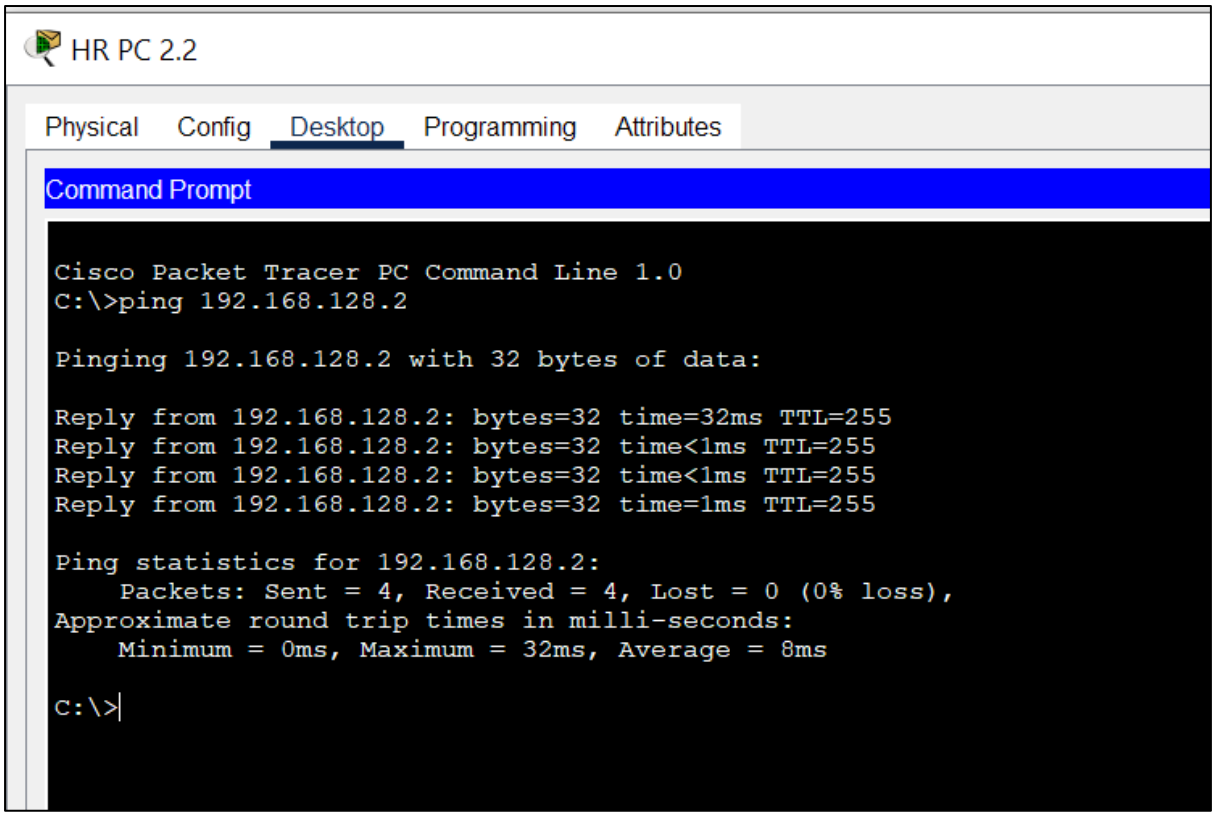


Figure 5 Test Case 06 b

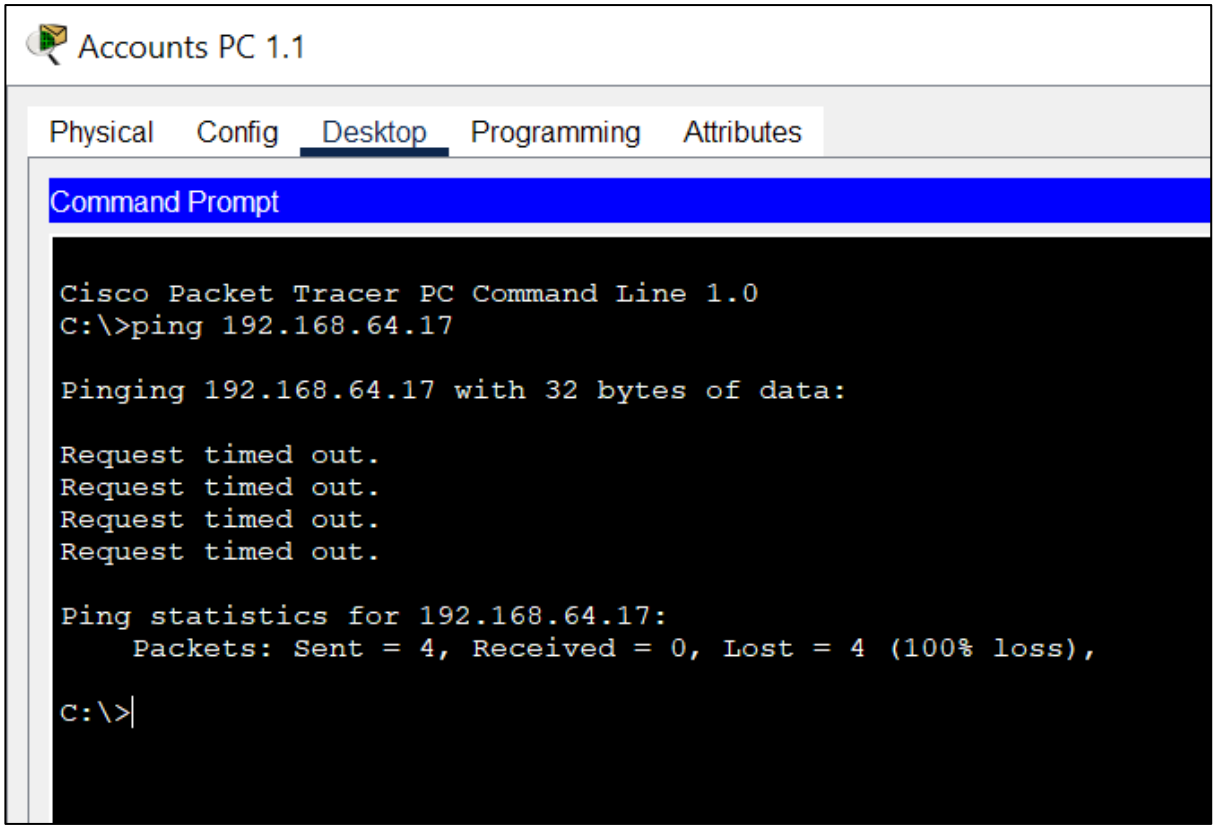
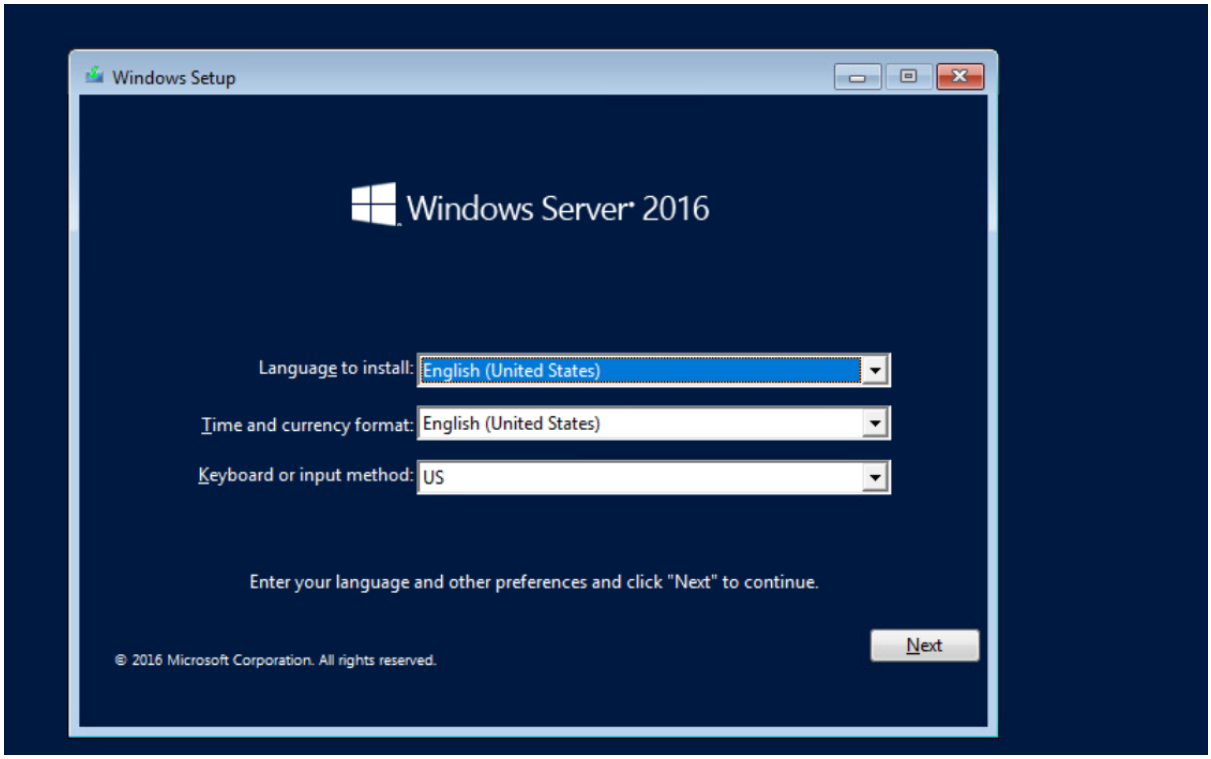


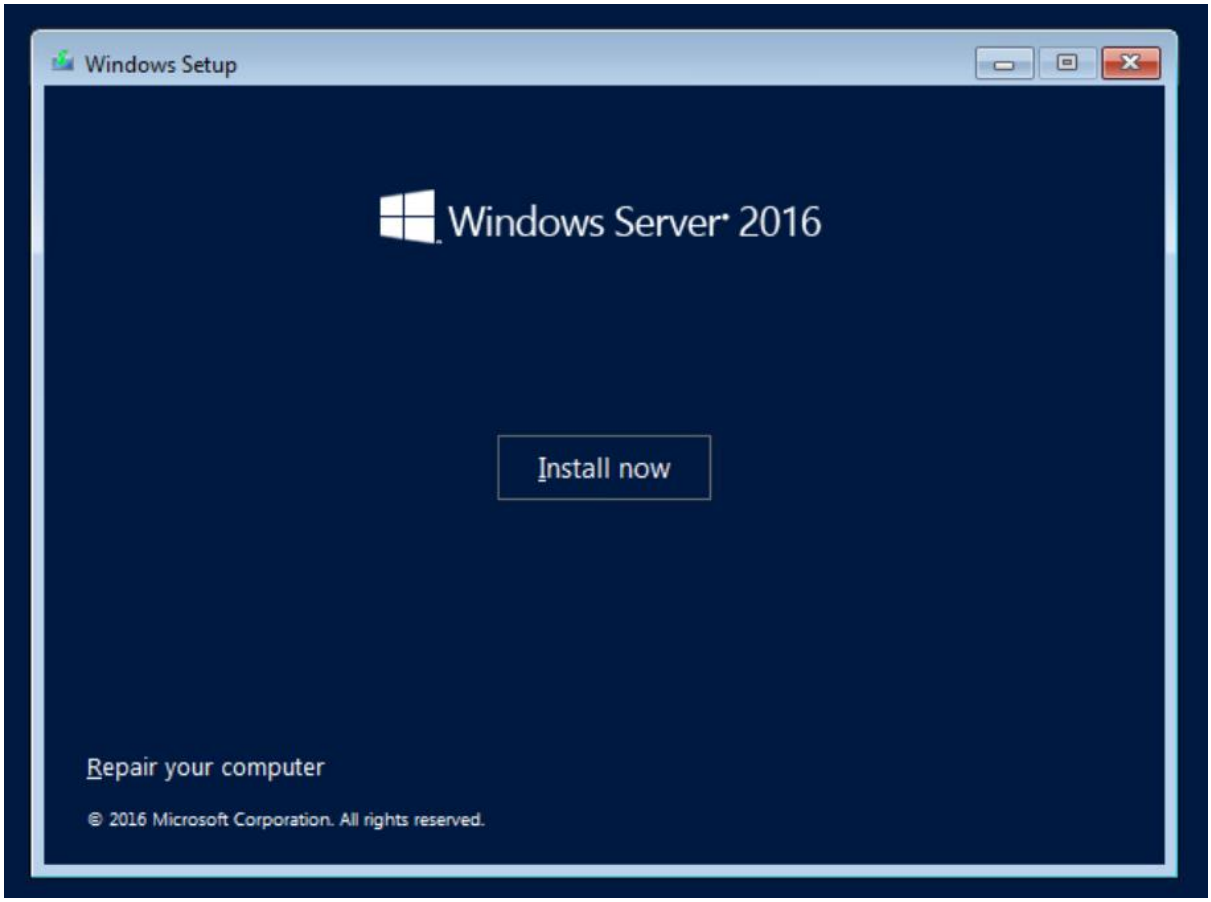
Figure 6 Test Case 07

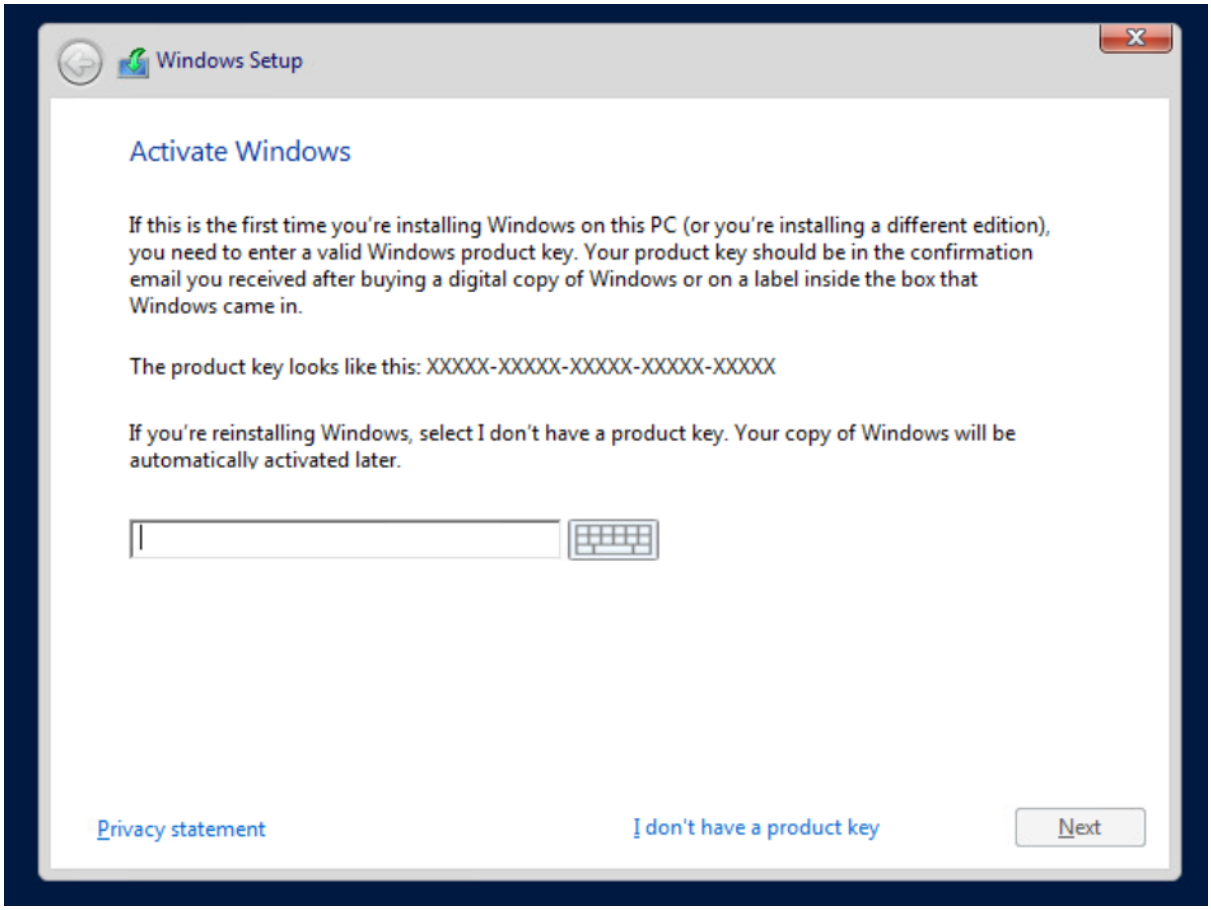
The communication between buildings of each department has failed, and the designer assumes that it is due to serial interfaces not responding to the sub interfaces of the routers fast ethernet interfaces. But the designer shall investigate further.

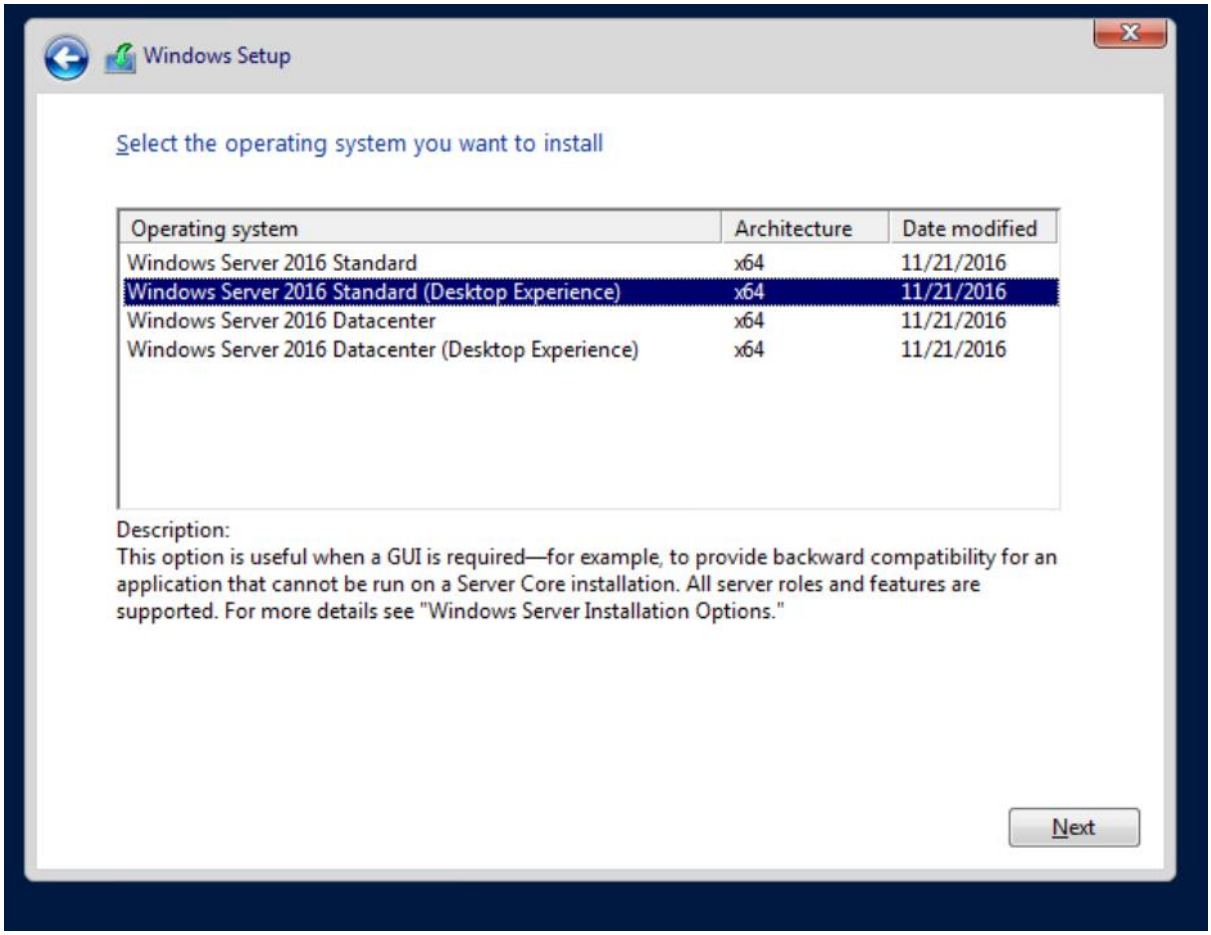
With the concerns raised by the user in domain management, control and security the domain was configured with the use of Windows Server 2016. The evidence is provided below.

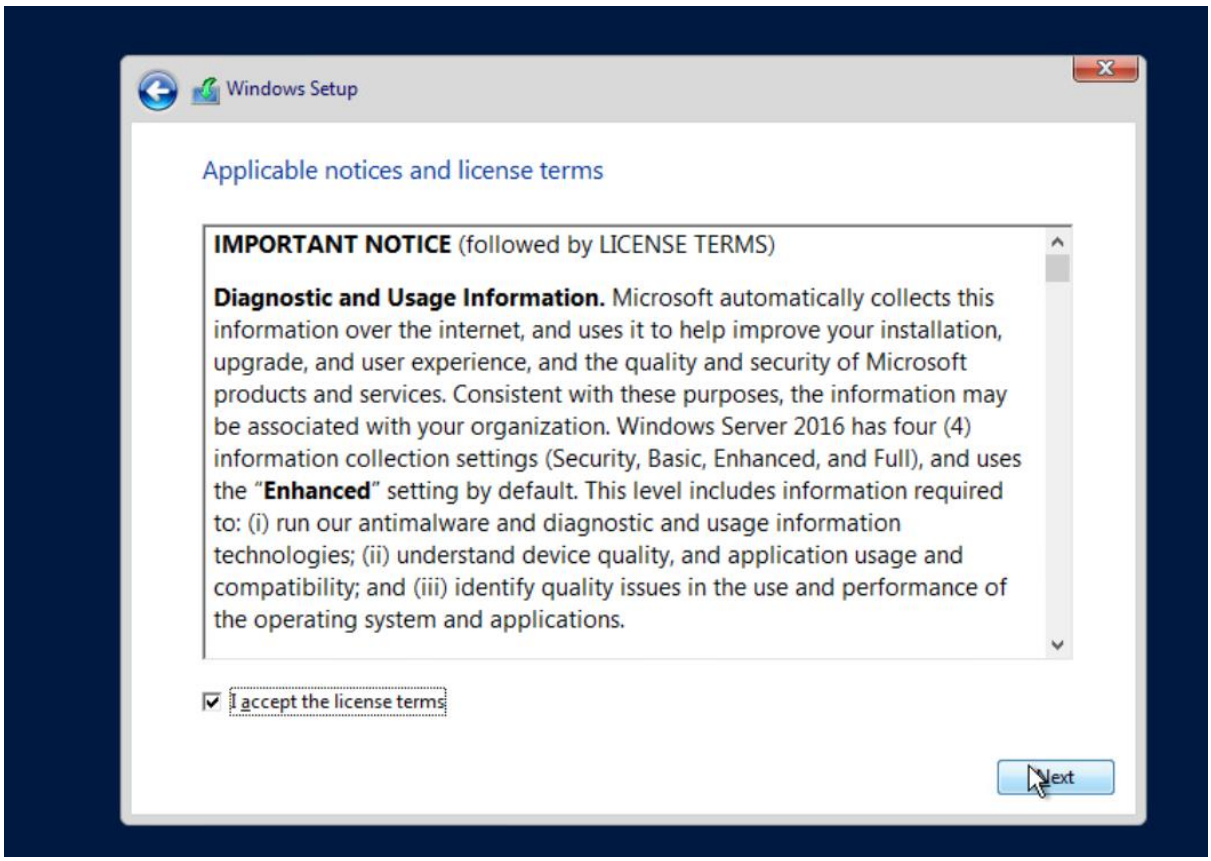
Domain Configuration

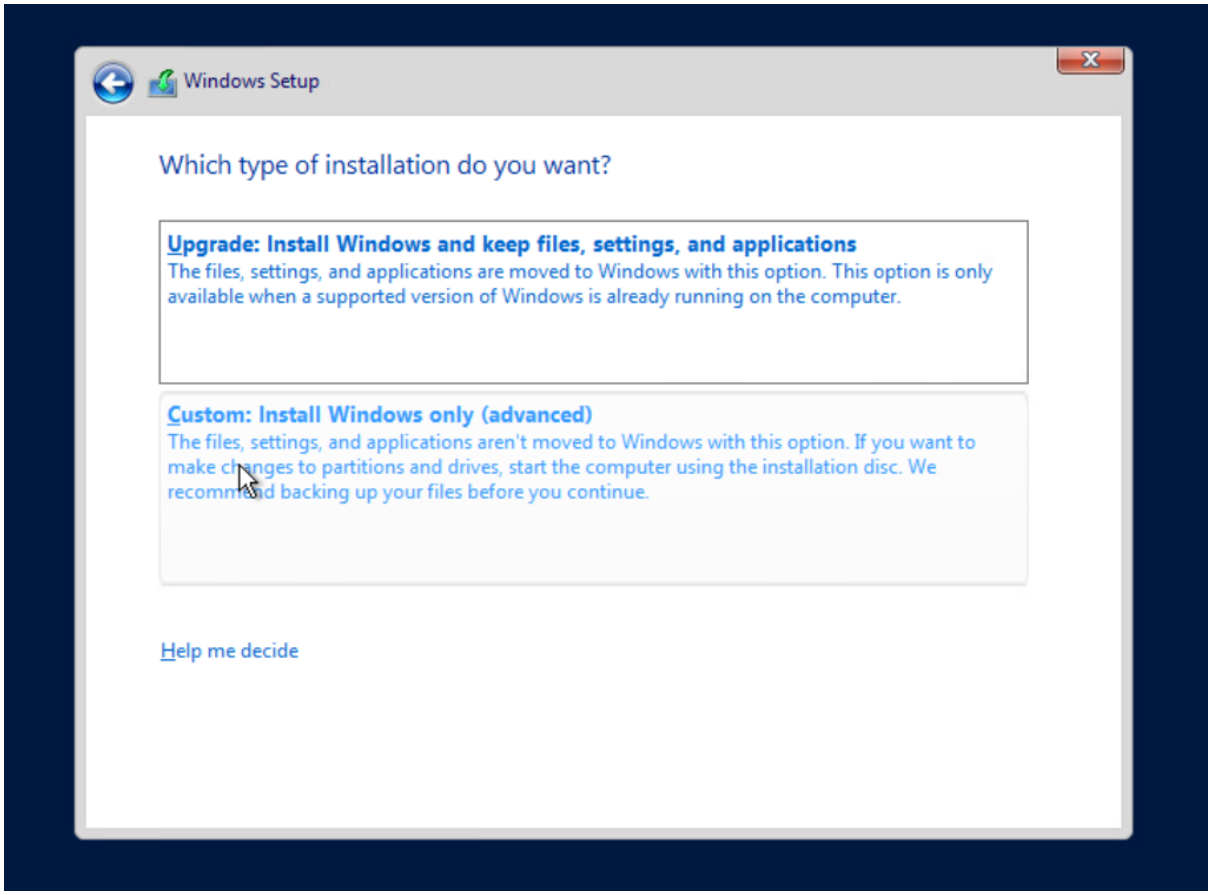


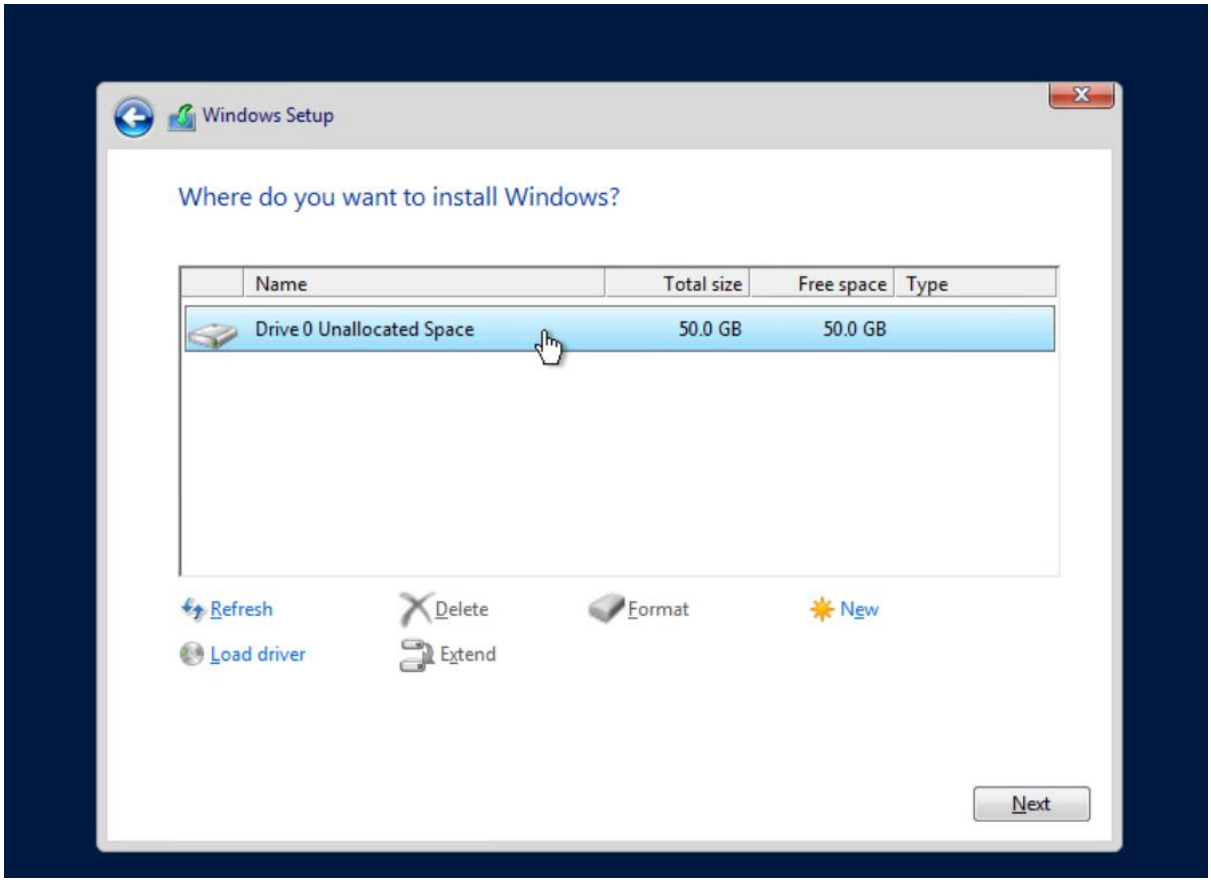


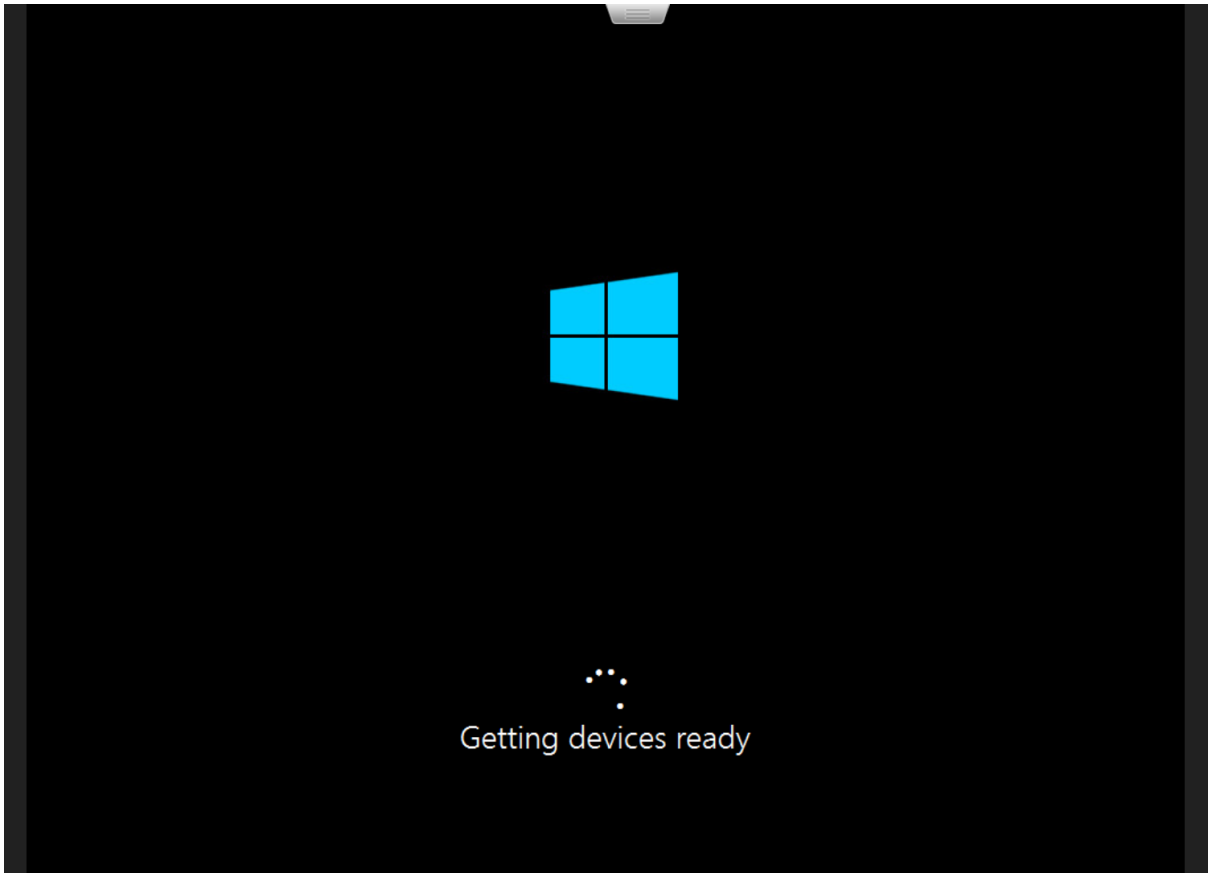

Windows Setup
Activate Windows
If this is the first time you're installing Windows on this PC (or you're installing a different edition), you need to enter a valid Windows product key. Your product key should be in the confirmation email you received after buying a digital copy of Windows or on a label inside the box that Windows came in.
The product key looks like this: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
If you're reinstalling Windows, select I don't have a product key. Your copy of Windows will be automatically activated later.
Privacy statement
I don't have a product key
Next

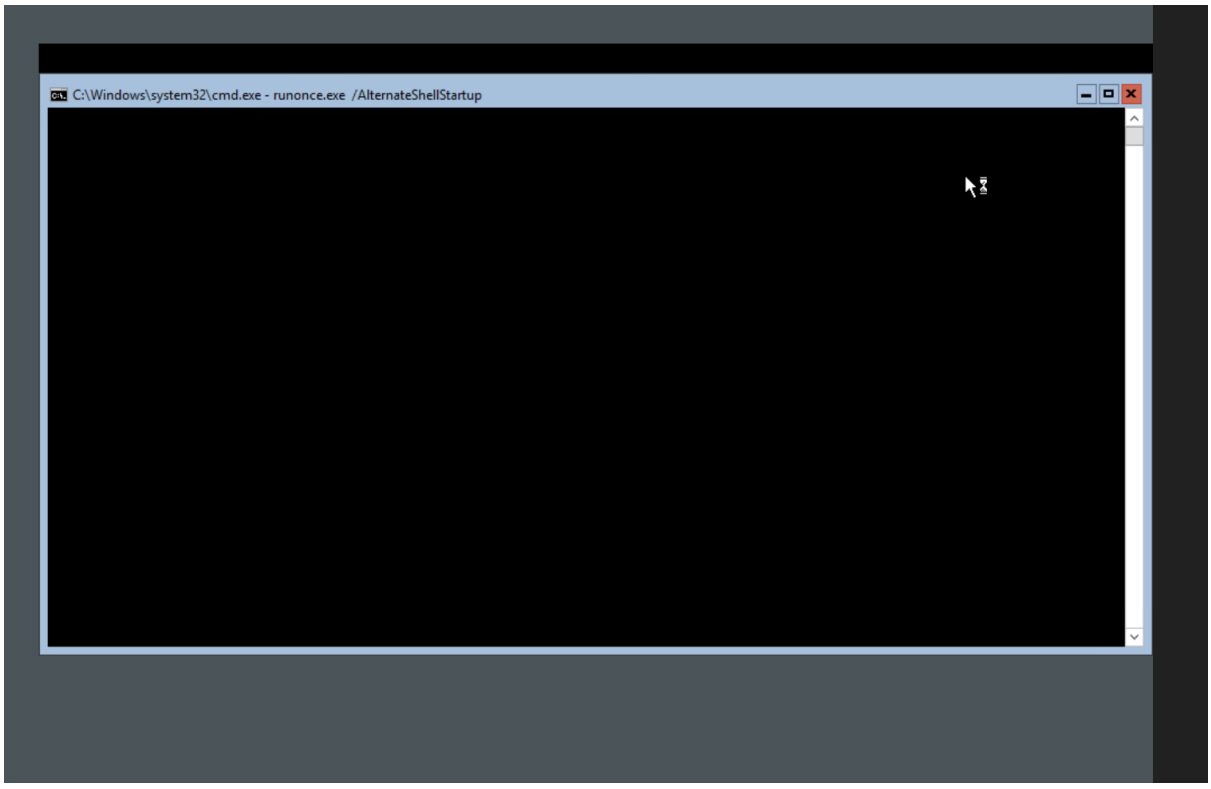

Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2016 Standard
x64
11/21/2016
Windows Server 2016 Standard (Desktop Experience)
x64
11/21/2016
Windows Server 2016 Datacenter
x64
11/21/2016
Windows Server 2016 Datacenter (Desktop Experience)
x64
11/21/2016
Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."
Next


Windows Setup
Applicable notices and license terms
IMPORTANT NOTICE (followed by LICENSE TERMS)
Diagnostic and Usage Information. Microsoft automatically collects this information over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Consistent with these purposes, the information may be associated with your organization. Windows Server 2016 has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "Enhanced" setting by default. This level includes information required to: (i) run our antimalware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.
I accept the license terms
Next

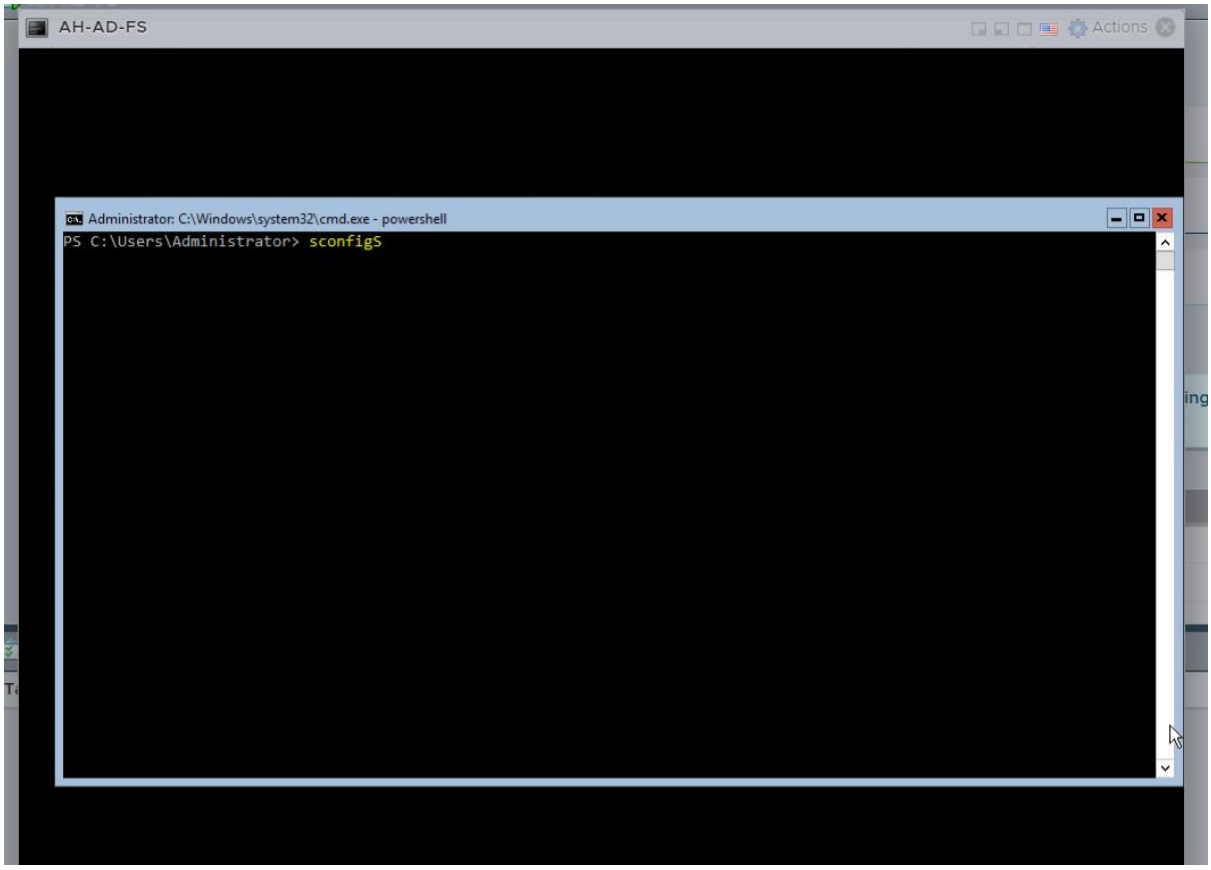

Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.
Help me decide


Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
50.0 GB
50.0 GB
Refresh
Delete
Format
New
Load driver
Extend
Next

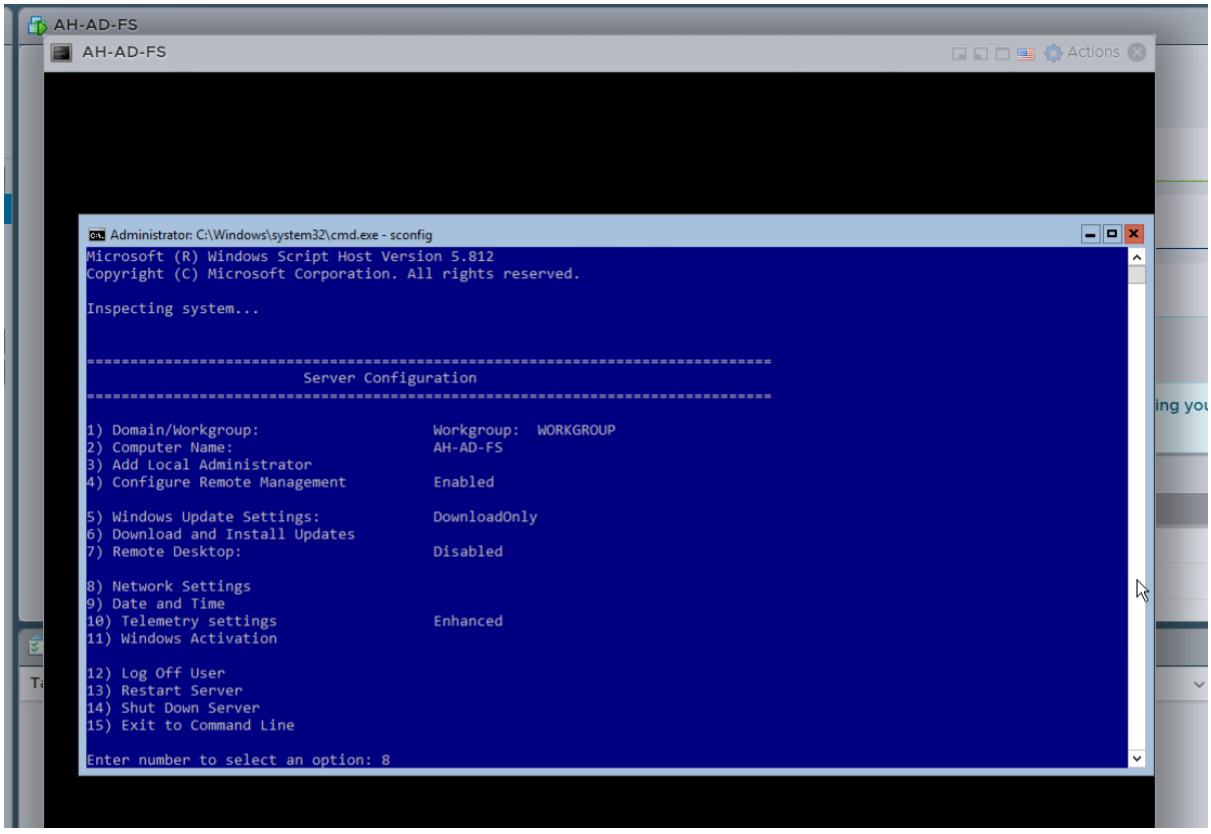




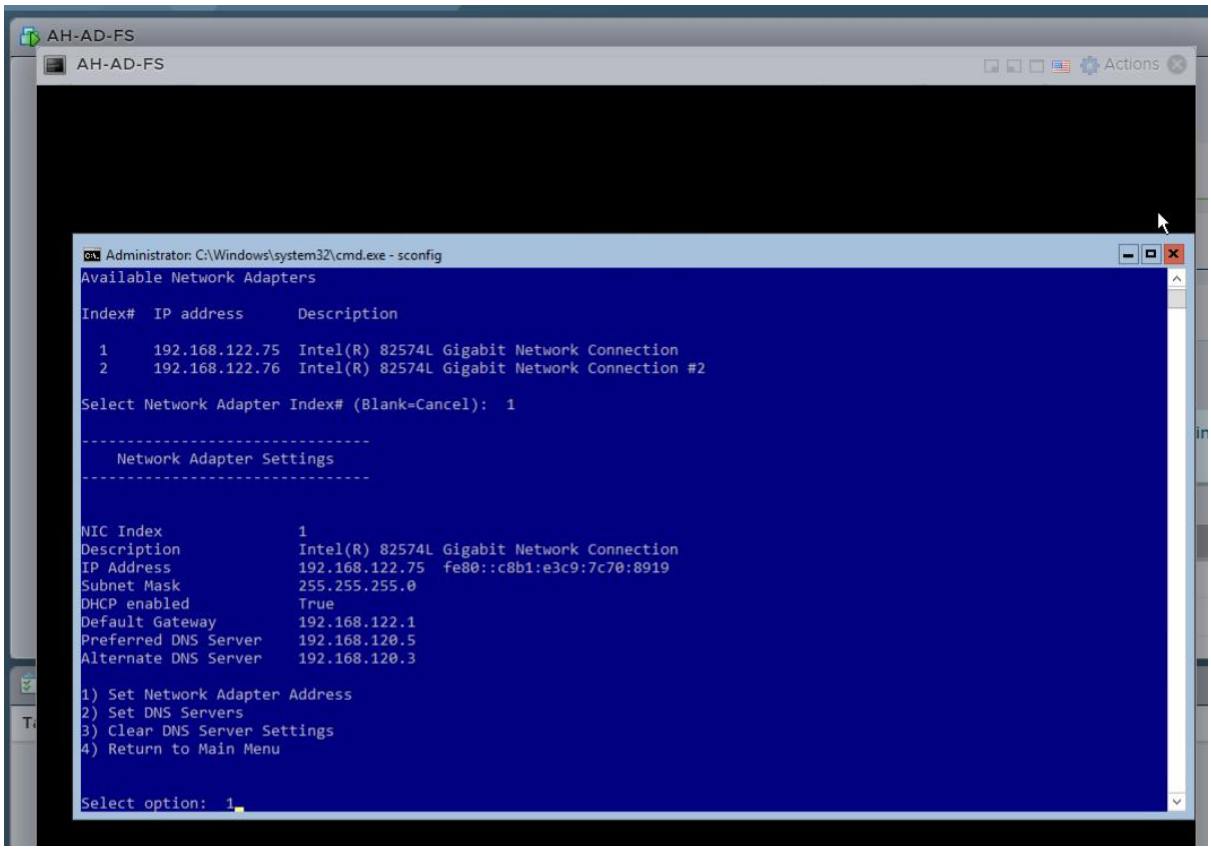
Screen starts and request for password change for Administrator account



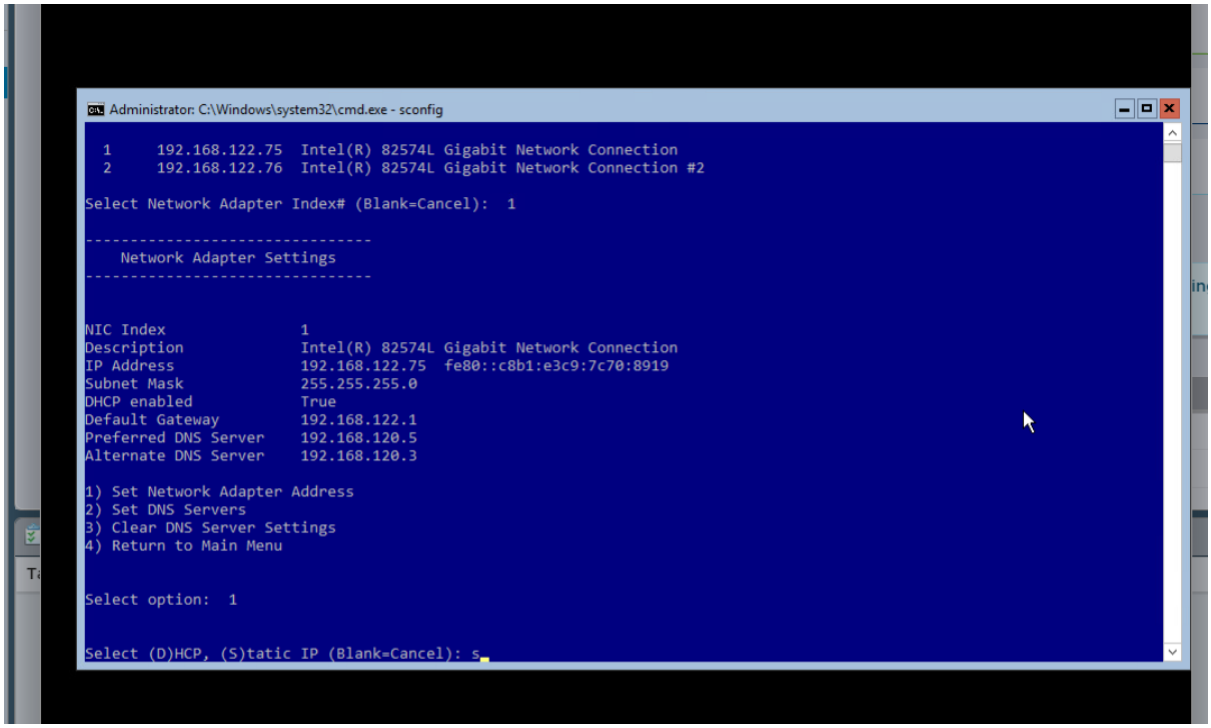
"sconfig" is typed to start server configuration



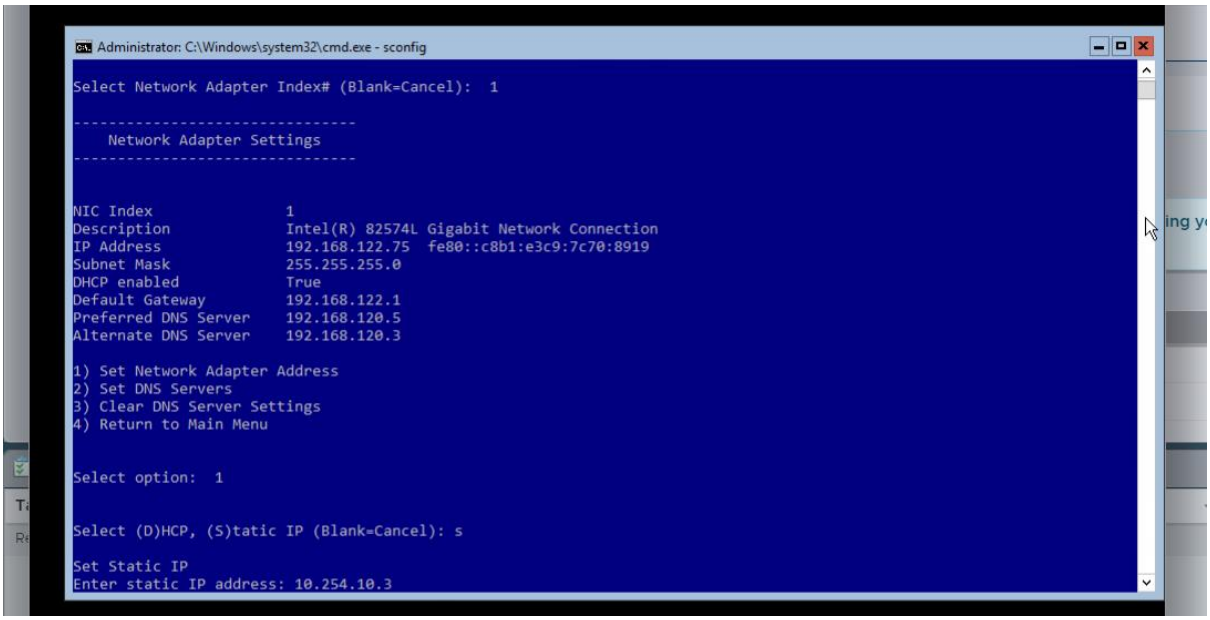
"Network configuration" is selected (option 8)



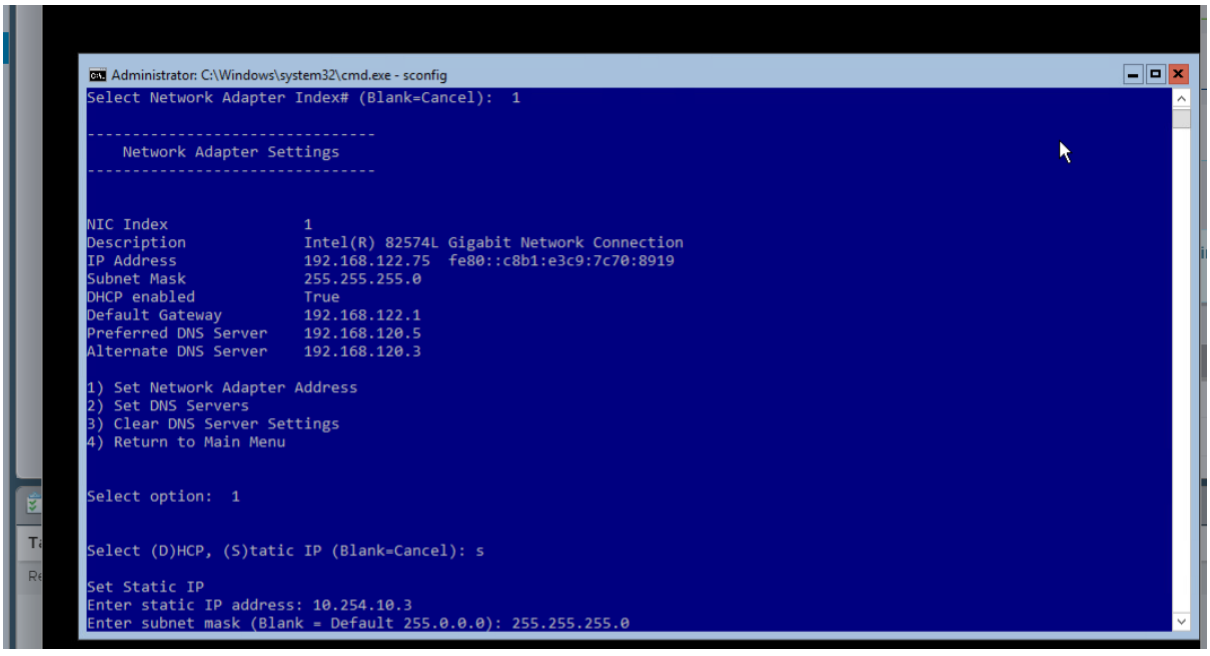
Select option 1



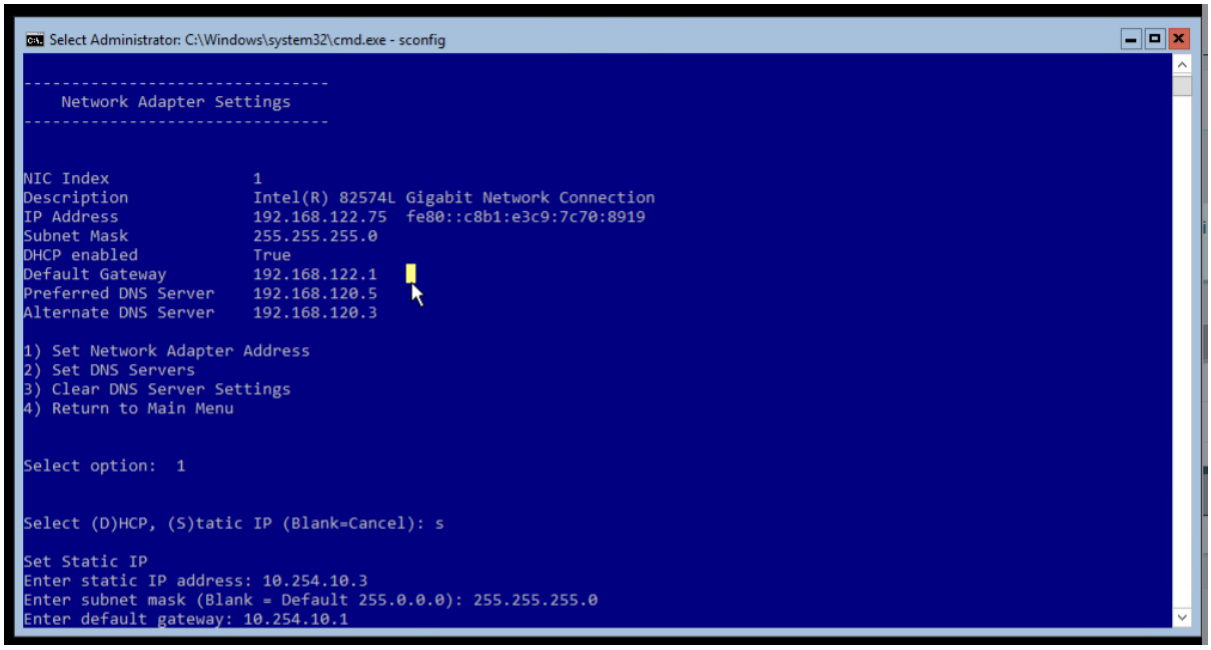
Go to the static IP option



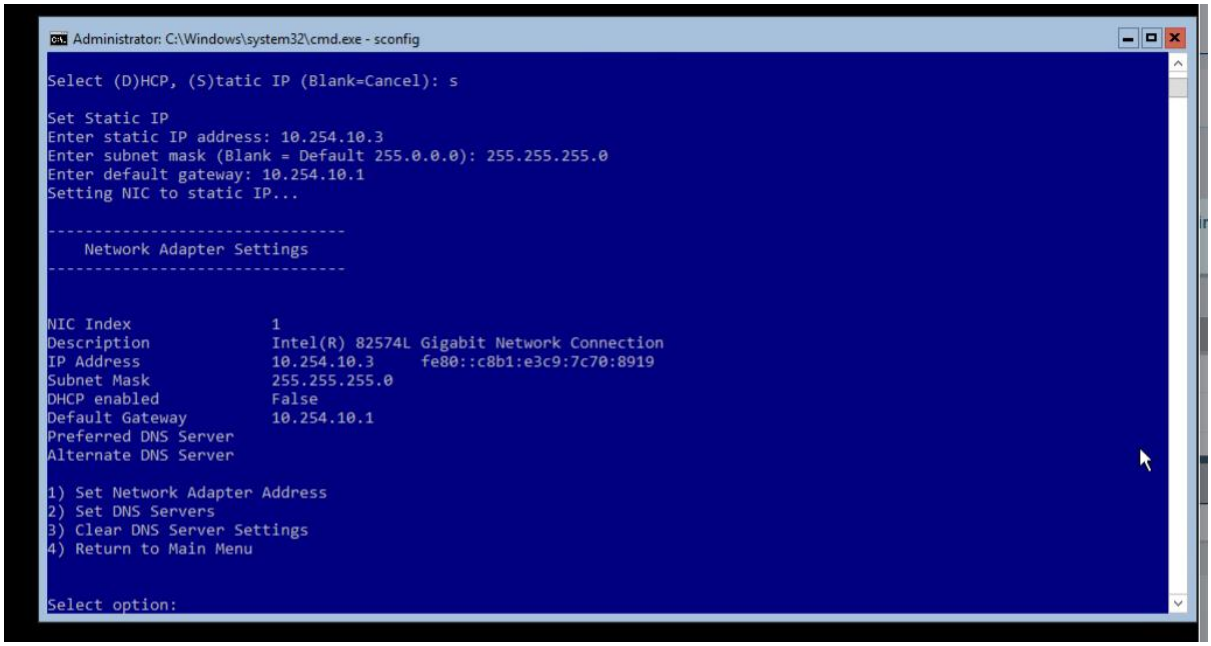
Set server IP



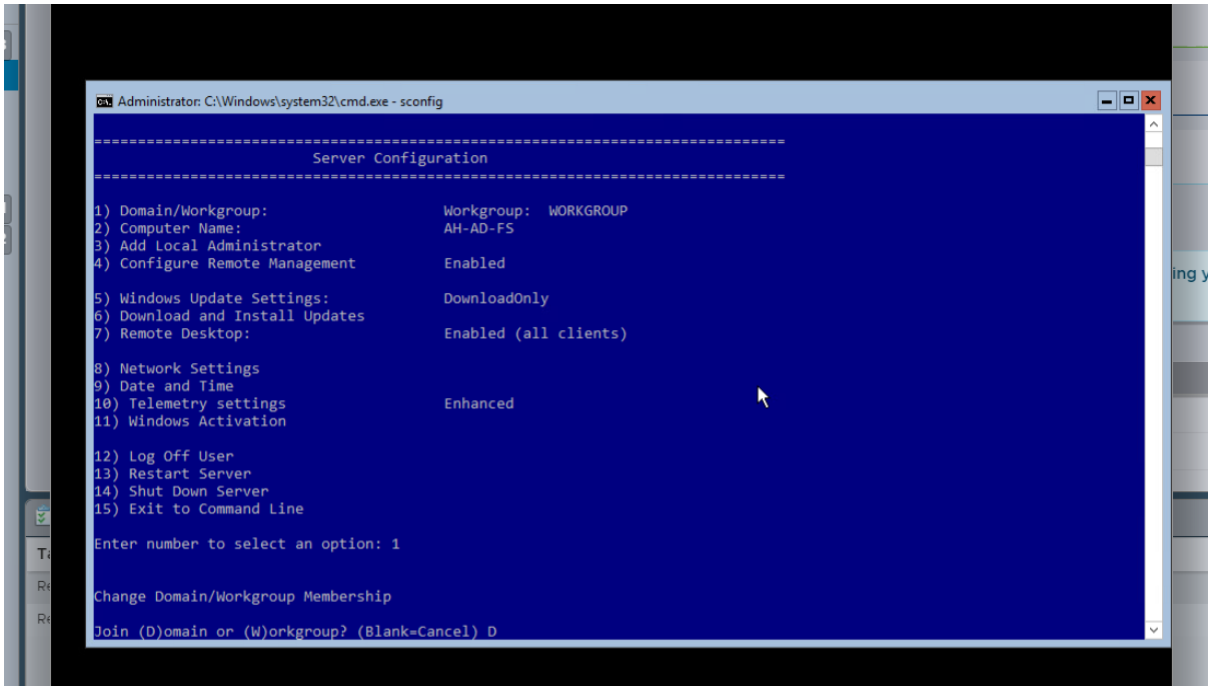
Along with subnet mask



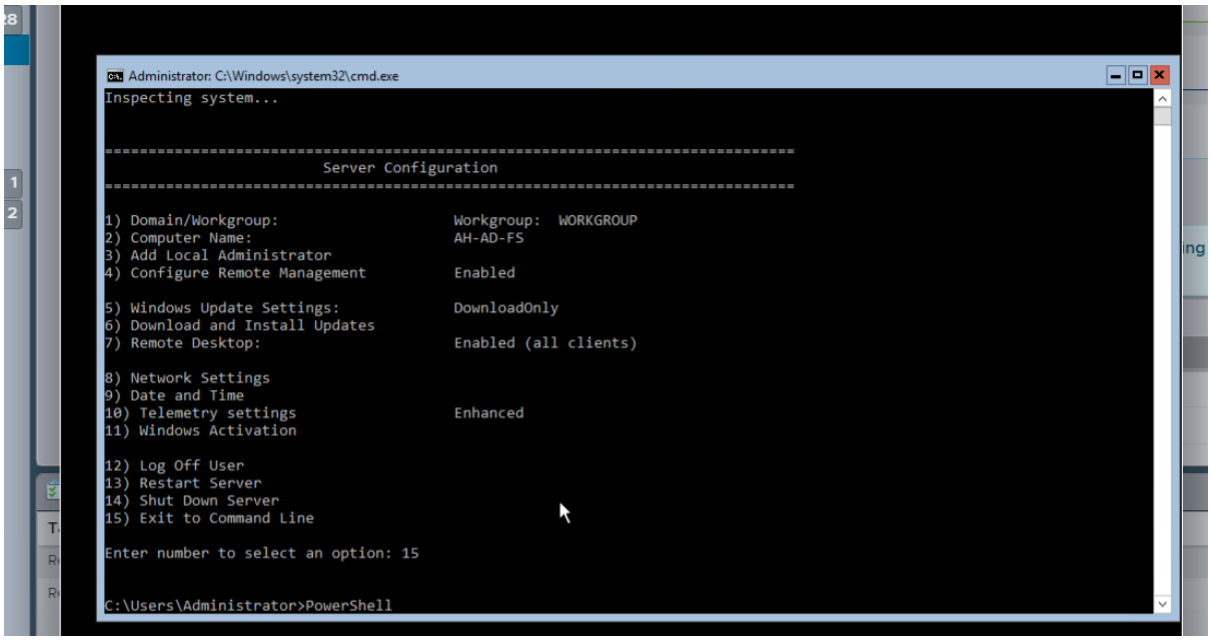
Set its default gateway as per the network



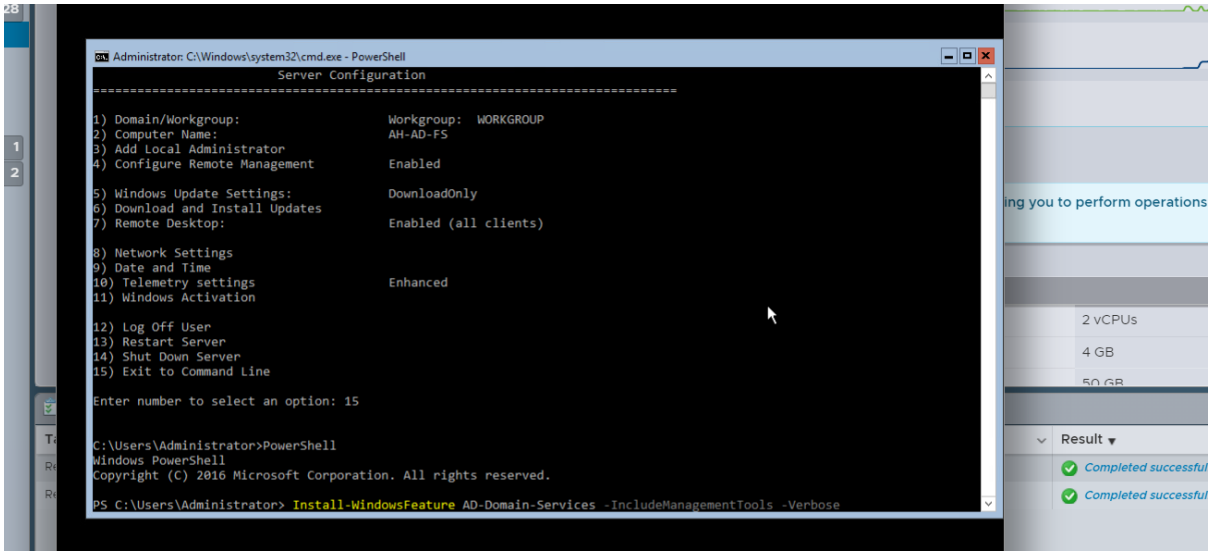
Select option 1



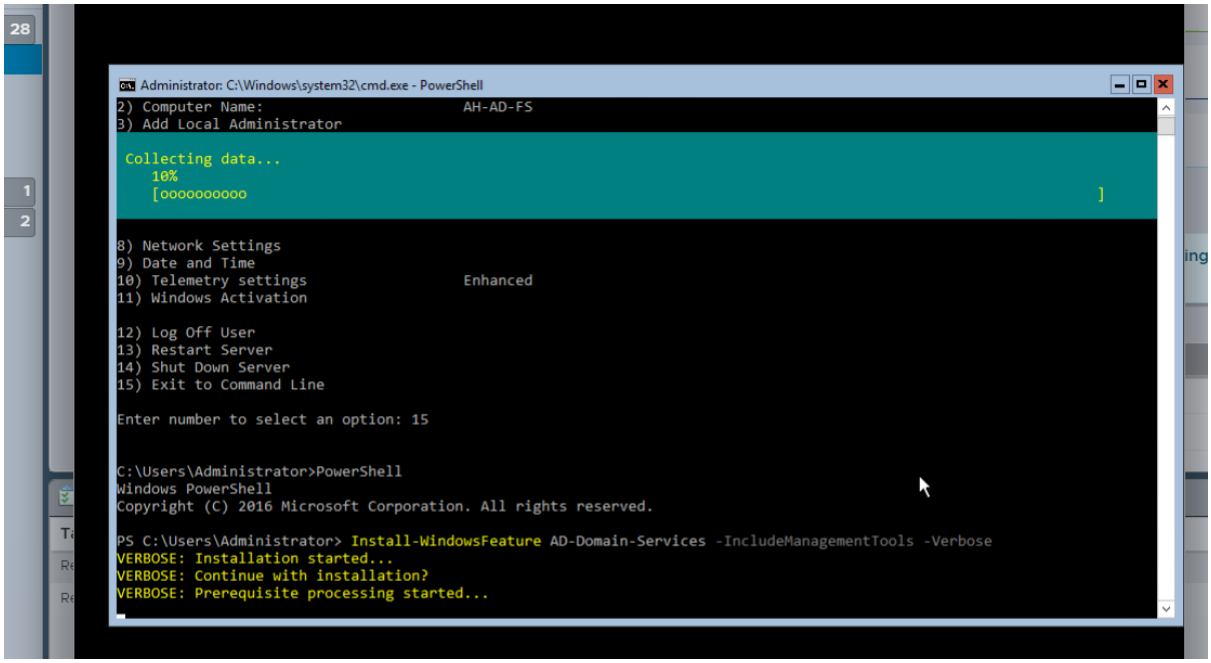
And enter the Domain option

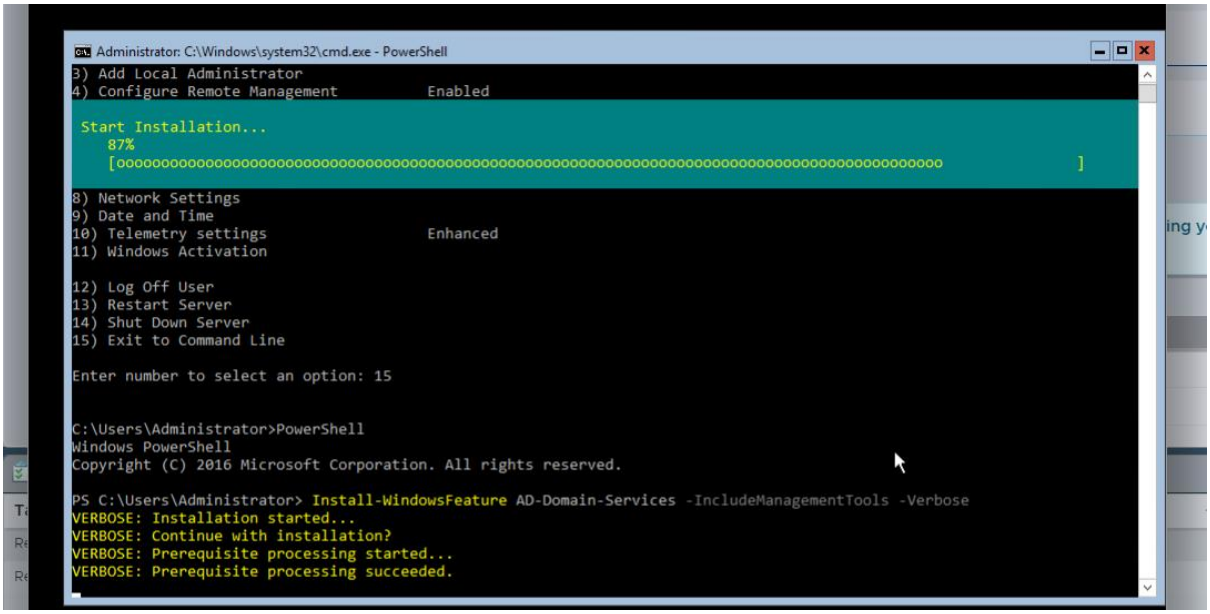


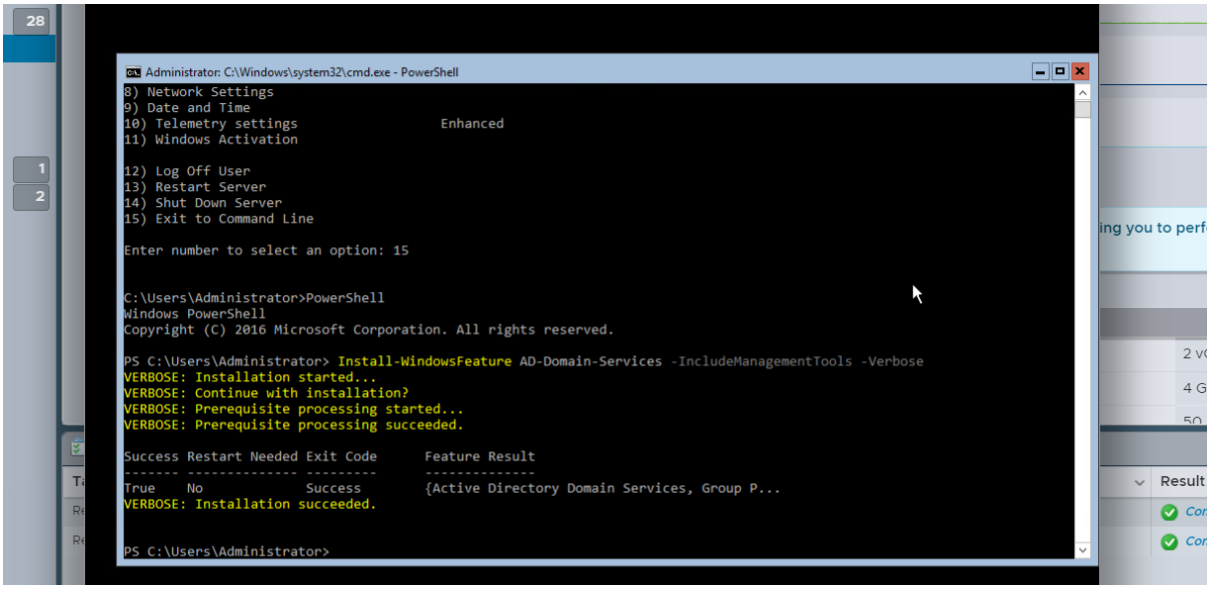
After setting up the Domain's details, enter option 15 to redirect to the command line

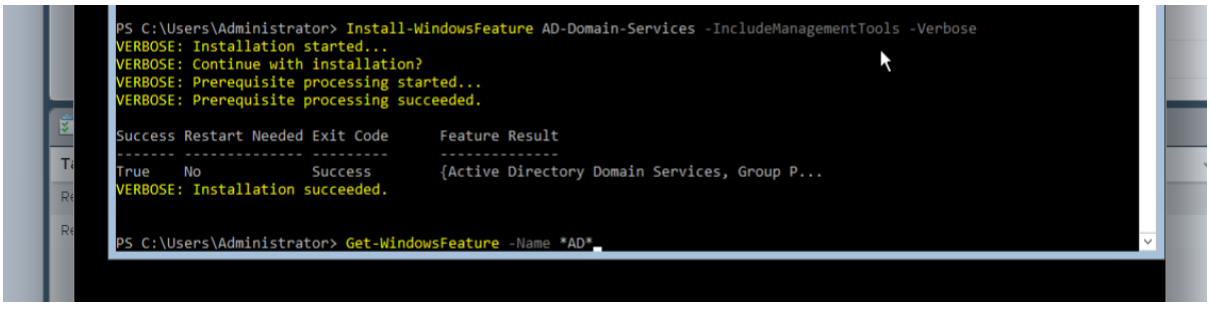


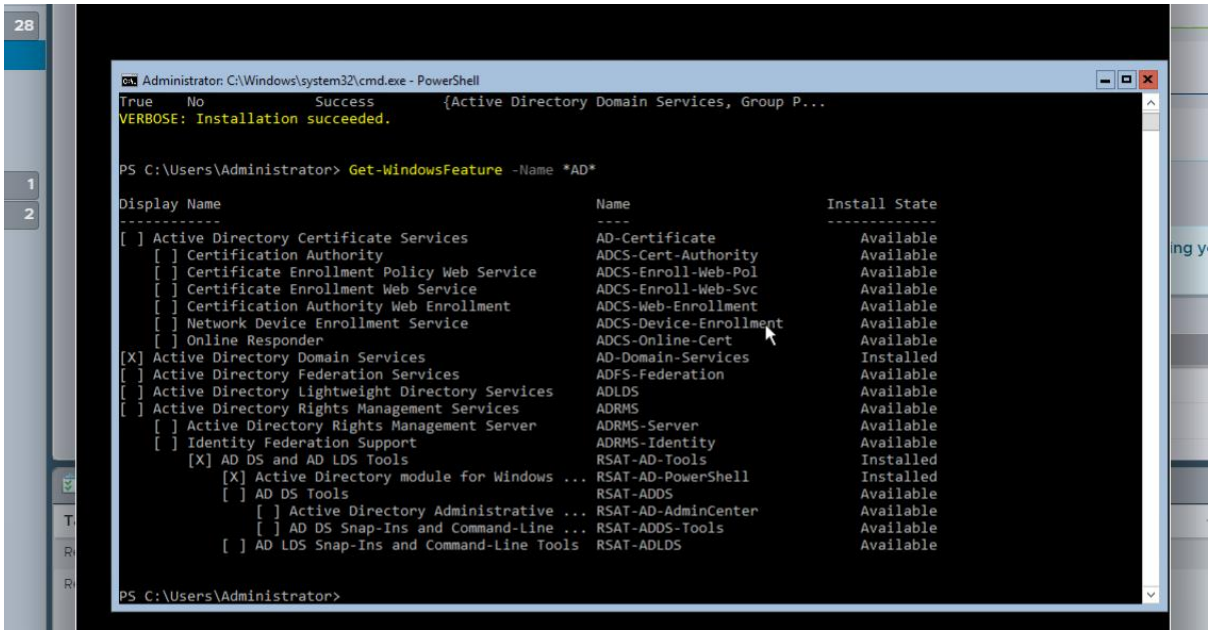
And initiate the installation of the domain in the server



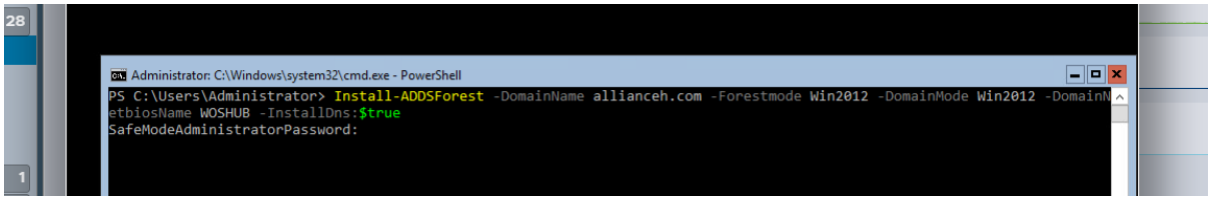

Administrator: C:\Windows\system32\cmd.exe - PowerShell
3) Add Local Administrator
4) Configure Remote Management Enabled
Start Installation...
87%
8) Network Settings
9) Date and Time
10) Telemetry settings Enhanced
11) Windows Activation
12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line
Enter number to select an option: 15
C:\Users\Administrator>PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools -Verbose
VERBOSE: Installation started...
VERBOSE: Continue with installation?
VERBOSE: Prerequisite processing started...
VERBOSE: Prerequisite processing succeeded.


Administrator: C:\Windows\system32\cmd.exe - PowerShell
8) Network Settings
9) Date and Time
10) Telemetry settings Enhanced
11) Windows Activation
12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line
Enter number to select an option: 15
C:\Users\Administrator>PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools -Verbose
VERBOSE: Installation started...
VERBOSE: Continue with installation?
VERBOSE: Prerequisite processing started...
VERBOSE: Prerequisite processing succeeded.
Success Restart Needed Exit Code Feature Result
True No Success {Active Directory Domain Services, Group P...
VERBOSE: Installation succeeded.
PS C:\Users\Administrator>

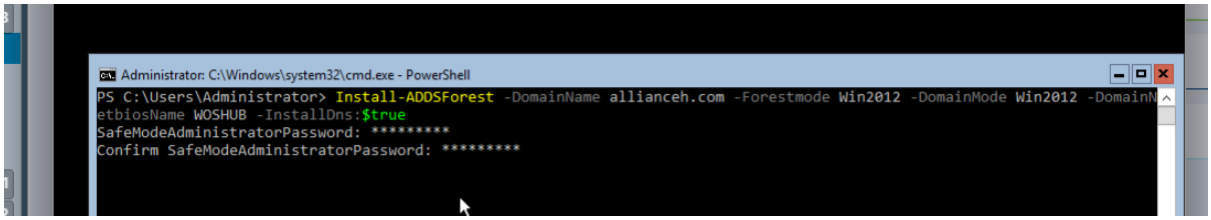

PS C:\Users\Administrator> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools -Verbose
VERBOSE: Installation started...
VERBOSE: Continue with installation?
VERBOSE: Prerequisite processing started...
VERBOSE: Prerequisite processing succeeded.
Success Restart Needed Exit Code Feature Result
True No Success {Active Directory Domain Services, Group P...
VERBOSE: Installation succeeded.
PS C:\Users\Administrator> Get-WindowsFeature -Name *AD*



Once the installation has succeded, configure the domain controller

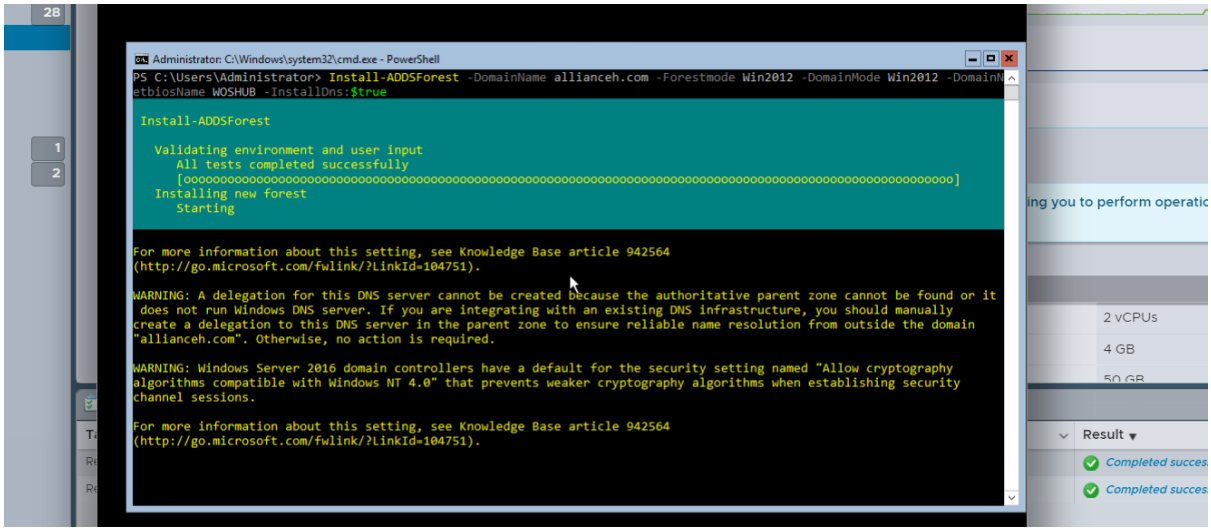


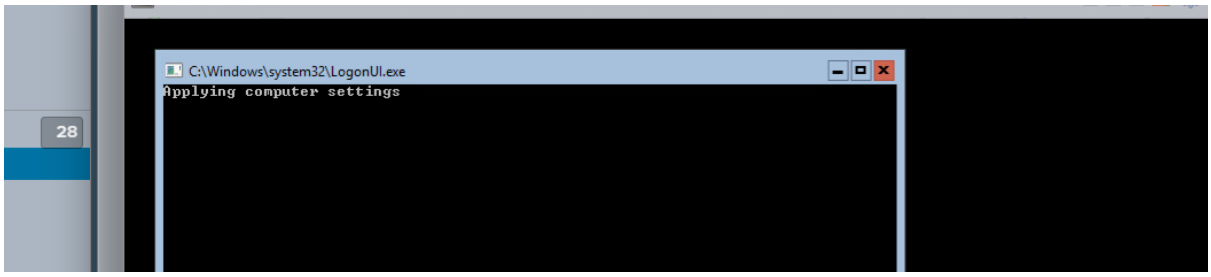
With the domain name set, set the dns to be installed

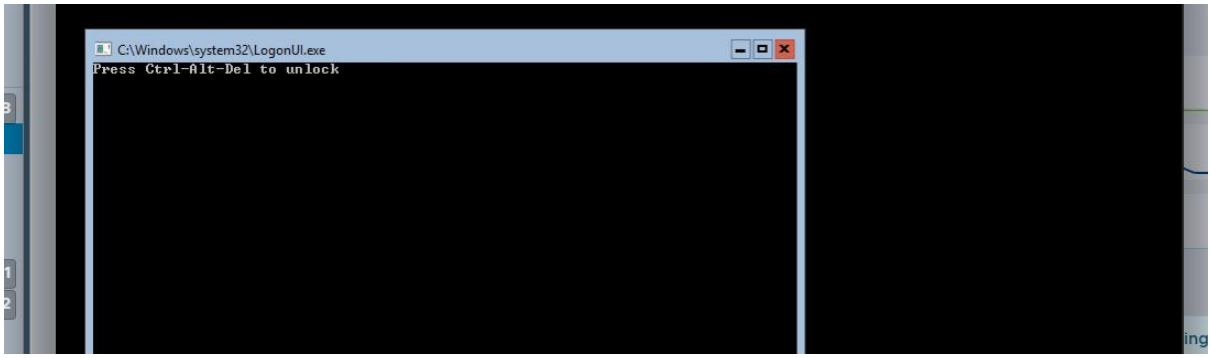


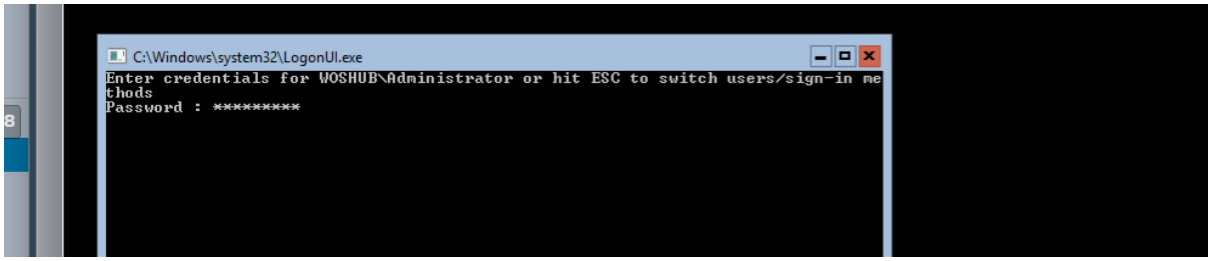
Enter set credentials

Select “Yes”

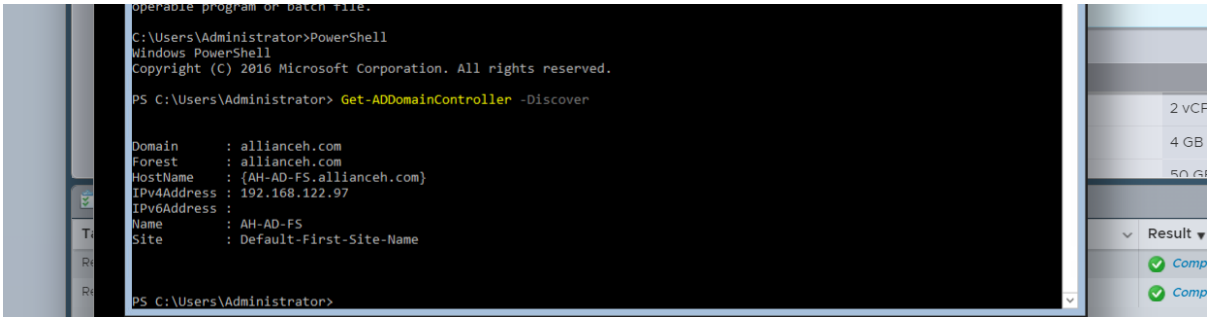


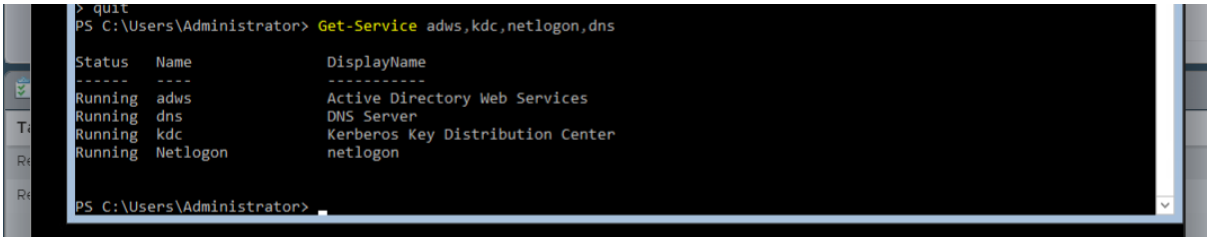


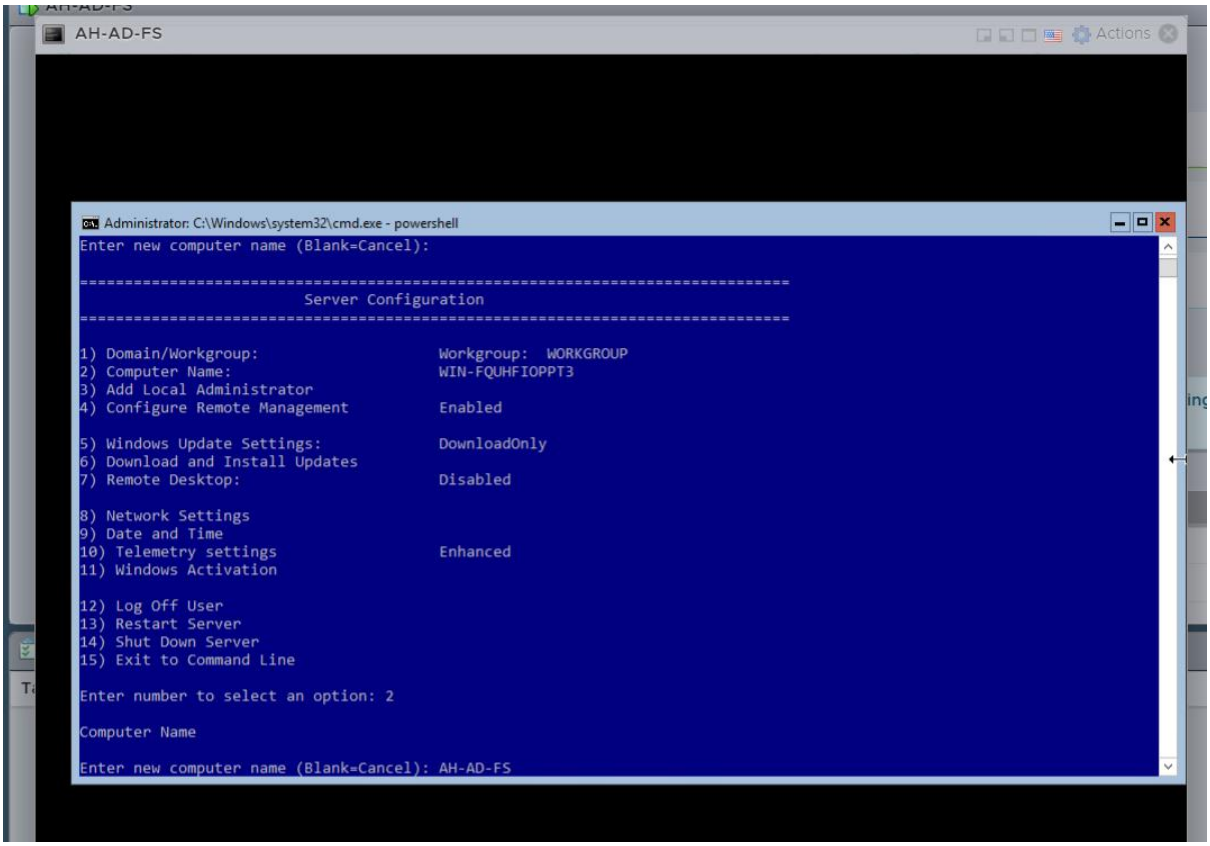


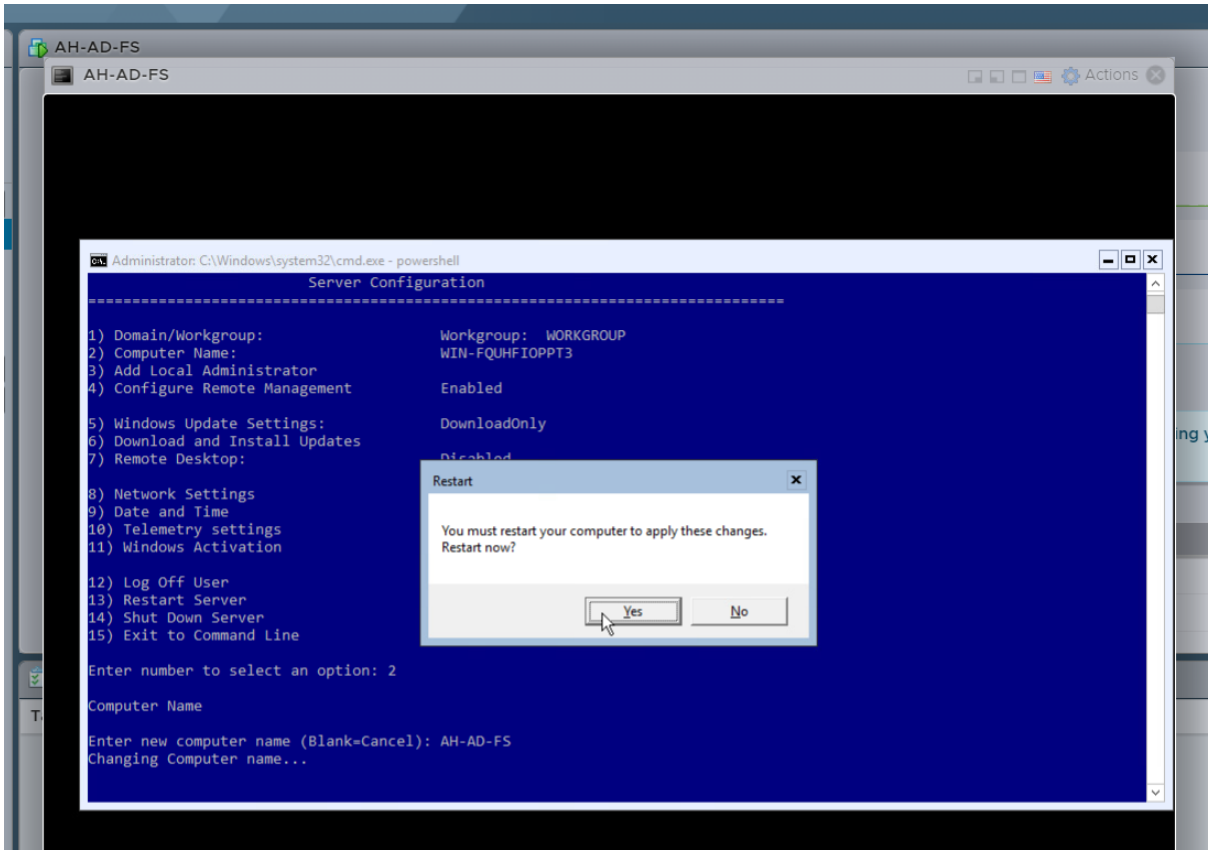


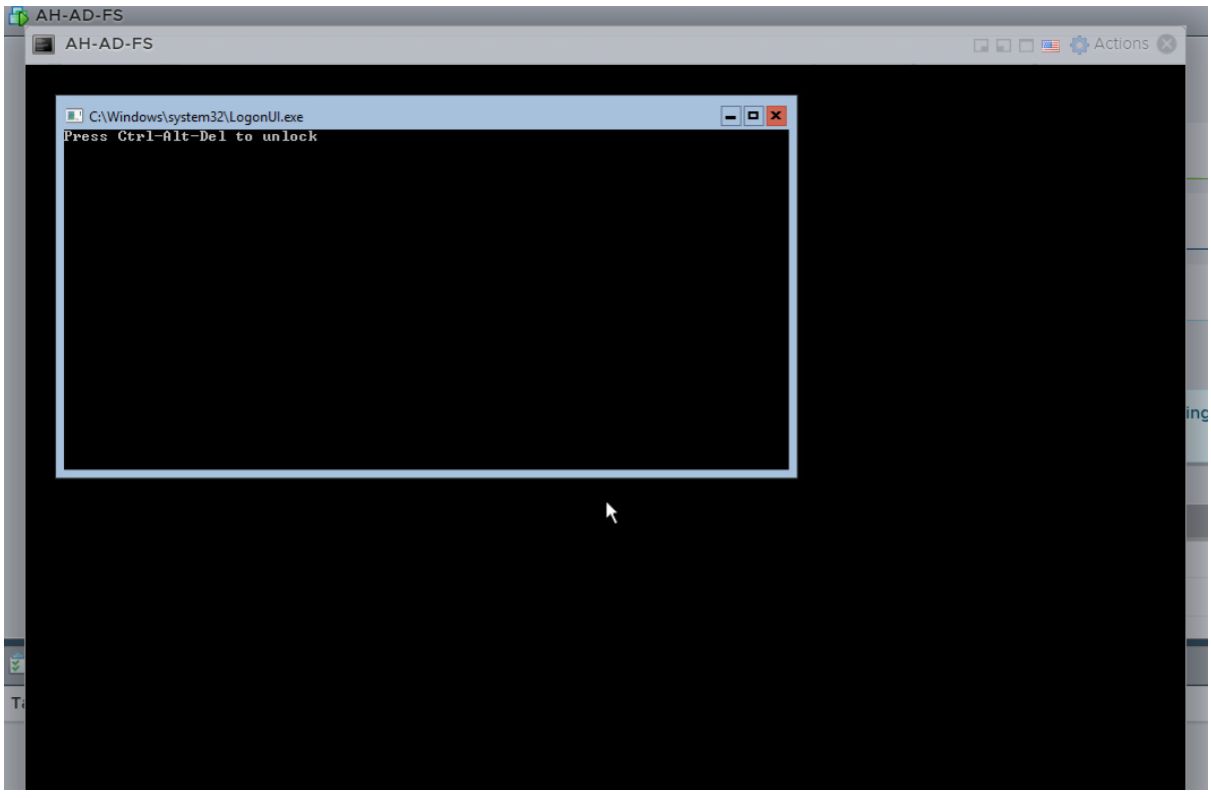
Enter credentials again after restarting

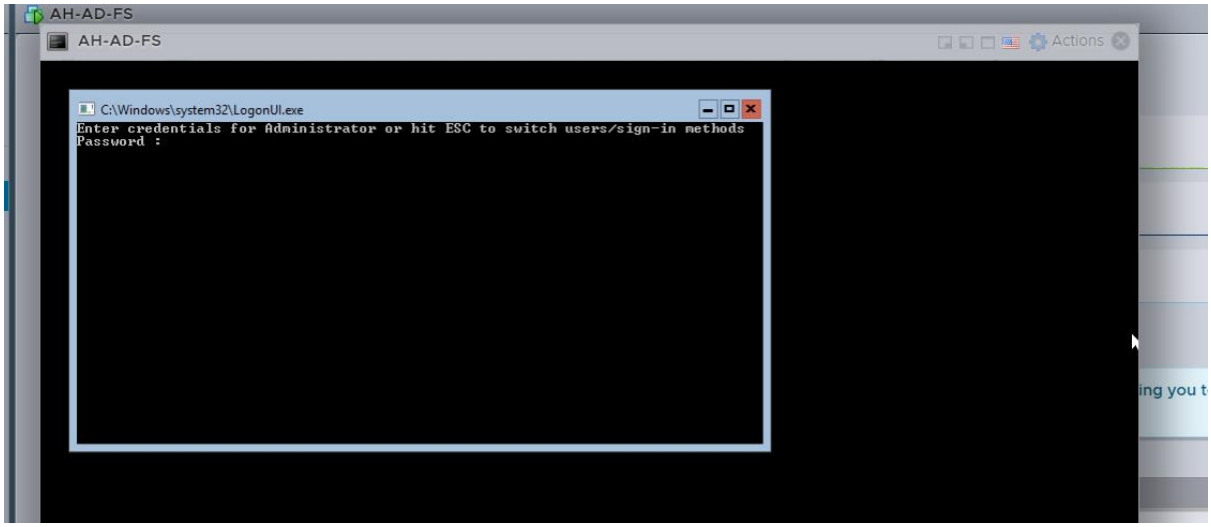

C:\Users\Administrator>PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Get-ADDomainController -Discover
Domain : allianceh.com
Forest : allianceh.com
HostName : {AH-AD-FS.allianceh.com}
IPv4Address : 192.168.122.97
IPv6Address :
Name : AH-AD-FS
Site : Default-First-Site-Name
PS C:\Users\Administrator>


PS C:\Users\Administrator> Get-Service adws,kdc,netlogon,dns
Status Name DisplayName
Running adws Active Directory Web Services
Running dns DNS Server
Running kdc Kerberos Key Distribution Center
Running Netlogon netlogon
PS C:\Users\Administrator>


AH-AD-FS
Actions
Administrator: C:\Windows\system32\cmd.exe - powershell
Enter new computer name (Blank=Cancel):
Server Configuration
1) Domain/Workgroup: Workgroup: WORKGROUP
2) Computer Name: WIN-FQUHFIOPPT3
3) Add Local Administrator
4) Configure Remote Management Enabled
5) Windows Update Settings: DownloadOnly
6) Download and Install Updates
7) Remote Desktop: Disabled
8) Network Settings
9) Date and Time
10) Telemetry settings Enhanced
11) Windows Activation
12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line
Enter number to select an option: 2
Computer Name
Enter new computer name (Blank=Cancel): AH-AD-FS


AH-AD-FS
AH-AD-FS
Actions
Administrator: C:\Windows\system32\cmd.exe - powershell
Server Configuration
1) Domain/Workgroup: Workgroup: WORKGROUP
2) Computer Name: WIN-FQUHFIOPPT3
3) Add Local Administrator
4) Configure Remote Management Enabled
5) Windows Update Settings: DownloadOnly
6) Download and Install Updates
7) Remote Desktop:
8) Network Settings
9) Date and Time
10) Telemetry settings
11) Windows Activation
12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line
Enter number to select an option: 2
Computer Name
Enter new computer name (Blank=Cancel): AH-AD-FS
Changing Computer name...
Restart
You must restart your computer to apply these changes.
Restart now?
Yes
No


AH-AD-FS
AH-AD-FS
Actions
C:\Windows\system32\LogonUI.exe
Press Ctrl-Alt-Del to unlock



The domain has been set and configured

The user was satisfied with the design and believed that its performance would exceed the expectations of the simulation due to the obstacles that the designer faced when using the packet tracer software.

The domains were also configured as per the user's requirement and was fully manageable now, through a Network Administrator.

Bibliography

Kapoor, A. (2022). *Importance of Types of Networks: LAN, MAN, and WAN | Simplilearn*. [online] Simplilearn.com. Available at: https://www.simplilearn.com/tutorials/networking-tutorial/importance-oftypes-of-networks-lan-man-wan.

Bourgeois, S. (2016). *Network-types*. [online] belden.com. Available at: https://www.belden.com/blogs/network-types.

javaTpoint (2011). *Types of Computer Network - JavaTpoint*. [online] www.javatpoint.com. Available at: https://www.javatpoint.com/types-ofcomputer-network.

www.javatpoint.com. (n.d.). *Advantages and Disadvantages of WAN - Javatpoint*. [online] Available at: https://www.javatpoint.com/advantagesand-disadvantages-of-wan.

Cisco. (n.d.). *Cisco IP VSAT Satellite WAN Network Module for Cisco Integrated Services Routers*. [online] Available at: https://www.cisco.com/c/en/us/products/collateral/interfacesmodules/ip-vsat-satellite-wanmodule/product_data_sheet0900aecd804bbf6f.html.

Anon, (2022). *What is Peer to Peer Network, and How does it work?* -. [online] Available at: https://www.blockchain-council.org/blockchain/peerto-peer-network/.

Computer Science GCSE GURU. (n.d.). *Client-Server Networks*. [online] Available at: https://www.computerscience.gcse.guru/theory/client-servernetworks.

Code Institute Global. (2022). *What is a Client-Server Network?* [online] Available at: https://codeinstitute.net/global/blog/what-is-a-client-servernetwork/.

Frankenfield, J. (2022). *Cloud Computing*. [online] Investopedia. Available at: https://www.investopedia.com/terms/c/cloud-computing.asp.

Google (n.d.). *What is Cloud Computing?* [online] Google Cloud. Available at: https://cloud.google.com/learn/what-is-cloud-computing.

Virtana. (n.d.). *What are computer clusters?* [online] Available at: https://www.virtana.com/glossary/what-is-a-cluster/.

Capital One. (n.d.). *What is a Cluster? An Introduction to Clustering in the Cloud*. [online] Available at: https://www.capitalone.com/tech/cloud/whatis-a-cluster/.

REDMOND\\markl (n.d.). *Network Load Balancing Provider*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/enus/previous-versions/windows/desktop/wlbsprov/network-load-balancingprovider-portal [Accessed 27 Mar. 2023].

REDMOND\\markl (n.d.). *Failover Cluster APIs*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/enus/previous-versions/windows/desktop/mscs/failover-cluster-apis-portal [Accessed 27 Mar. 2023].

N-Able (2018). *The Difference Between Centralized and Decentralized Networks*. [online] N-able. Available at: https://www.nable.com/blog/centralized-vs-decentralized-network.

EasyTechJunkie. (n.d.). *What Is Centralized Network Management? (with pictures)*. [online] Available at: https://www.easytechjunkie.com/what-iscentralized-network-management.htm.

www.redhat.com. (n.d.). *What is network virtualization*. [online] Available at: https://www.redhat.com/en/topics/virtualization/what-is-networkvirtualization.

www.sciencedirect.com. (n.d.). *Network Virtualization - an overview | ScienceDirect Topics*. [online] Available at: https://www.sciencedirect.com/topics/computer-science/networkvirtualization.

www.javatpoint.com. (n.d.). *Intranet - javatpoint*. [online] Available at: https://www.javatpoint.com/intranet.

GeeksforGeeks. (2021). *What is Extranet? Definition, Implementation, Features*. [online] Available at:

https://www.geeksforgeeks.org/what-isextranet-definition-implementation-features/.

ISO (2022). *About us*. [online] ISO. Available at: https://www.iso.org/about-us.html.

www.creativesafetysupply.com. (n.d.). *International Standards Organizations (ISO)*. [online] Available at: https://www.creativesafetysupply.com/glossary/international-standardsorganizations-iso/ [Accessed 27 Mar. 2023].

American National Standards Institute - ANSI. (n.d.). *ANSI Introduction*. [online] Available at: https://www.ansi.org/about/introduction.

Available at: https://www.ansi.org/about/introduction.

irtf.org. (n.d.). *Internet Research Task Force*. [online] Available at: https://irtf.org/.

W3C (2008). *World Wide Web Consortium (W3C)*. [online] W3.org. Available at: https://www.w3.org/.

Anon, (n.d.). *4.6. Network Standards and Standardization Bodies – Wachemo University e-Learning Platform*. [online] Available at: https://wachemo-elearning.net/courses/31781/lessons/chapter-fourcommunications-networks-architectures/topic/4-6-network-standardsand-standardization-bodies/.

Gaurav, S. (2022). *What is the OSI Model? Layers of OSI Model*. [online] Scaler Topics. Available at: https://www.scaler.com/topics/computernetwork/osi-model/.

GeeksforGeeks (2019). *TCP/IP Model - GeeksforGeeks*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/tcp-ipmodel/.

communications @manageengine.com, M. (n.d.). *Network Monitoring Software by ManageEngine OpManager*. [online] ManageEngine OpManager. Available at: https://www.manageengine.com/networkmonitoring/network-protocols.html.

Default. (n.d.). *Network Protocol Definition | Computer Protocol | Computer Networks | CompTIA*. [online] Available at: https://www.comptia.org/content/guides/what-is-a-networkprotocol#:~:text=A%20network%20protocol%20is%20an.

Mitchell, C. (n.d.). *File Transfer Protocol (FTP) Definition*. [online] Investopedia. Available at: https://www.investopedia.com/terms/f/ftp-filetransfer-protocol.asp#:~:text=File%20transfer%20protocol%20(FTP)%20is.

www.ssh.com. (n.d.). *SSH Secure Shell home page, maintained by SSH protocol inventor Tatu Ylonen. SSH clients, servers, tutorials, howtos.* [online] Available at: https://www.ssh.com/academy/ssh.

www.javatpoint.com. (n.d.). *POP Protocol | Post Office Protocol - javatpoint*. [online] Available at: https://www.javatpoint.com/popprotocol.

Kaspersky (2021). *What is an IP Address – Definition and Explanation*.
[online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-an-ipaddress.

Contributor, S. (2019). *What is network topology? Best guide to types & diagrams - dnsstuff*. [online] DNSstuff. Available at: https://www.dnsstuff.com/what-is-network-topology.

GeeksforGeeks (2020). *Advantages and Disadvantages of Bus Topology*.
[online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-bustopology/.

GeeksForGeeks (2020). *Advantage and Disadvantage of Mesh Topology*.
[online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/advantage-and-disadvantage-of-meshtopology/.

Computer Hope (2017). *What is a Tree Topology?* [online] Computerhope.com. Available at: https://www.computerhope.com/jargon/t/treetopo.htm.

www.javatpoint.com. (n.d.). *What is Tree Topology - javatpoint*. [online] Available at: https://www.javatpoint.com/what-is-tree-topology.

www.javatpoint.com. (n.d.). *What is Tree Topology - javatpoint*. [online] Available at: https://www.javatpoint.com/what-is-tree-topology.

GeeksforGeeks (2018). *Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter) - GeeksforGeeks*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/network-devices-hubrepeater-bridge-switch-router-gateways/.

Cloudflare (n.d.). What is a network switch? | Switch vs. router | Cloudflare. *Cloudflare*. [online] Available at: https://www.cloudflare.com/learning/network-layer/what-is-a-networkswitch/.

Diffen.com. (2019). *Hub vs Switch - Difference and Comparison | Diffen*.
[online] Available at: https://www.diffen.com/difference/Hub_vs_Switch.

www.javatpoint.com. (n.d.). *What is Router - javatpoint*.
[online] Available at: https://www.javatpoint.com/router.

Mathur, V. (n.d.). *What is the Quality of Service (QoS)? | Analytics Steps*.
[online] www.analyticssteps.com. Available at: https://analyticssteps.com/blogs/what-quality-service-qos.

VMware. (2021). *What Is Network Monitoring? | VMware Glossary*. [online] Available at: https://www.vmware.com/topics/glossary/content/network monitoring.html.

Cisco. (n.d.). *What Is Network Monitoring?* [online] Available at: https://www.cisco.com/c/en/us/solutions/automation/what-is-networkmonitoring.html#~ben [Accessed 5 Apr. 2023].

Deland-Han (n.d.). *Install and Configure a DHCP Server - Windows Server*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/enus/troubleshoot/windows-server/networking/install-configure-dhcpserver-workgroup.