## Higher Nationals

### Internal verification of assessment decisions – BTEC (RQF)

| INTERNAL VERIFICATION – ASSESSMENT DECISIONS | | | | | |
|---|---|---|---|---|---|
| **Programme title** | BTEC Higher National Diploma in Computing | | | | |
| **Assessor** | | **Internal Verifier** | | | |
| **Unit(s)** | **Unit 02: Networking** | | | | |
| **Assignment title** | LAN Design & Implementation for SYNTAX SOLUTIONS | | | | |
| **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:**<br>Give details:<br>• Constructive?<br>• Linked to relevant assessment criteria?<br>• Identifying opportunities for improved performance?<br>• Agreeing actions? | Y/N<br>Y/N<br>Y/N<br>Y/N | | | | |
| **Does the assessment decision need amending?** | Y/N | | | | |
| **Assessor signature** | | **Date** | | | |
| **Internal Verifier signature** | | **Date** | | | |
| **Programme Leader signature** (if required) | | **Date** | | | |

| Confirm action completed | | | |
|---|---|---|---|
| **Remedial action taken**<br>Give details: | | | |
| **Assessor signature** | | **Date** | |
| **Internal Verifier signature** | | **Date** | |
| **Programme Leader signature** (if required) | | **Date** | |

# Higher Nationals - Summative Assignment Feedback Form

| | | | |
|---|---|---|---|
| **Student Name/ID** | | | |
| **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 Descripts** **P1** ☐ **P2** ☐ M1 ☐

**LO2 Explain networking devices and operations.**

**Pass, Merit & Distinction Descripts** **P3** ☐ **P4** ☐ **M2** ☐ **D1** ☐

**LO3 Design efficient networked systems.**

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

**LO4 Implement and diagnose networked systems.**

**Pass, Merit & Distinction Descripts** **P7** ☐ **P8** ☐ **M4** ☐ **D3** ☐

| | | |
|---|---|---|
| **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.

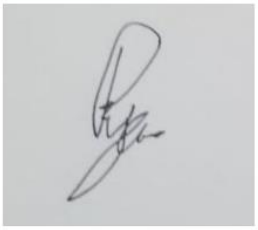
**Important Points:**

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.



ryandilthusha@gmail.com

19/11/2021

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

**Date:**
**(*Provide Submission Date*)**

## Higher National Diploma in Computing

## Assignment Brief

| | |
|---|---|
| Student Name /ID Number | Ryan Wickramaratne (COL 00081762) |
| **Unit Number and Title** | **Unit 2: Networking** |
| Academic Year | 2021/22 |
| Unit Tutor | Mr. Ilham |
| **Assignment Title** | **LAN Design & Implementation for SYNTAX SOLUTIONS** |
| 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.<br><br>**LO2** Explain networking devices and operations.<br><br>**LO3** Design efficient networked systems.<br><br>**LO4** Implement and diagnose networked systems. |
| | **Assignment Brief and Guidance:** |

## Scenario

**SYNTAX SOLUTIONS** is a privately owned, well-known Software company located in Colombo. The Management of **SYNTAX SOLUTIONS** has purchased a 3-story building in the heart of **Matara**. They are planning to make it one of the state-of-the-art companies in Matara with the latest facilities.

It is expected to have nearly **150 employees** in Matara branch.

| **Department** | **Number of Users** |
|---|---|
| Customer Care | 10 |
| Sales and Marketing | 20 |
| Finance | 25 |
| Legal | 5 |
| HR | 10 |
| Developers | 25 |
| Network Team | 5 |
| Server Room | Servers +ISP connections |

**Following requirements are given by the Management.**

- All the departments **must be separated** with **unique subnet** and should not communicate with each other **unless there is a special requirement**.
- **192.168.10.0/24** is given and should be used for all the departments except the server room. IPs should assign **using DHCP**.
- **ERP and CRM Systems** need to be implemented in Matara branch in local servers.
- **Number of servers required for the Server room** need to be decided by the Network designer and should be assigned with **10.254.1.0/24** subnet. (Uses **static IPs**)
- **High level of redundancy** is expected in network design to eliminate single point

of failures and traffic bottle necks.

- **Sales and Marketing** Team need to access Network resources **using WIFI** connectivity.
- **Proper methods** for **networking monitoring** and **troubleshooting** need to be established.
- All possible **network security** mechanisms should be implemented.

Assume you have been appointed as the new network consultant of **SYNTAX SOLUTIONS**. Prepare a network architectural design and implement it with your suggestions and recommendations to meet the company requirements.

***(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 network protocol suites while comparing the main network topologies and network protocol suites that are used in network design using examples. Recommend suitable network topologies and network protocol suites for above scenario and justify your answer with valid points.

**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 with 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).

  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.

- Test and evaluate the proposed design to meet the requirements and analyse user feedback by using a User feedback form.

- Install and configure Network services, devices and applications (Ex: VLAN,DHCP, 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 and recommend potential future enhancements for the networked system with valid justifications to your recommendations. Use critical reflection to critically evaluate the design, plan, configuration, and testing of your network while justifying with valid conclusions.

- 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.

**Grading Rubric**

| Grading Criteria | Achieved | Feedback |
|---|---|---|
| **LO1 : Examine networking principles and their protocols.** | | |
| **P1** Discuss the benefits and constraints of different network types and standards. | | |
| **P2** Explain the impact of network topology, communication and bandwidth requirements. | | |
| **M1** Compare 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 inter-dependence of workstation hardware with relevant networking software. | | |
| **M2** Explore a range of server types and justify the selection of a server, considering a given scenario regarding cost and performance optimization. | | |
| **LO 1 & LO2** | | |
| **D1** Critically evaluate the topology protocol selected for a given scenario to demonstrate the efficient utilisation of a networking system. | | |

| LO3 : Design efficient networked systems | | |
|---|---|---|
| **P5**<br>Design a networked system to meet a given specification. | | |
| **P6**<br>Test and evaluate the design to meet the requirements and analyze user feedback. | | |
| **M3**<br>Install and configure network services and applications on your choice. | | |
| **D2**<br>Design a maintenance schedule to support the networked system. | | |
| **LO4 : Implement and diagnose networked systems** | | |
| **P7**<br>Implement a networked system based on a prepared design. | | |
| **P8**<br>Document and analyze test results against expected results. | | |
| **M4**<br>Recommend potential enhancements for the networked systems. | | |
| **D3**<br>Use critical reflection to evaluate own work and justify valid conclusions. | | |

## Acknowledgement

I would like to express my special thanks of gratitude to my networking lecturer Mr. Ilham for providing invaluable guidance and giving immense amount of knowledge to work on this assignment perfectly. I specially thanks him because he helped us in doing a lot of research and I came to know about so many new things about the computer networking.

Secondly, I would like to thank my parents and friends who helped me a lot in finalizing this project within the limited time frame.

## Executive Summery

This entire assignment is based on an implementation of a network architectural design for selected company (SYNTAX Solutions Matara branch). The purpose of this assignment is to improve networking skills.

This report includes basic networking principles and protocols, topologies being used, LAN designing, virtual LAN implementing, and test cases and many more things related to implementation of a network architectural design for SYNTAX Solutions Matara branch.

# Abbreviations

MAN - Metropolitan Area Network

CAN - Campus Area Network

CAN - Controlled Local Area Network

WLAN - Wireless Local Area Network

LAN - Local Area Network

PAN - Personal Area Network

NFC -Near Field Communication

USB - Universal Serial Bus

WAN - Wide Area Network

SAN - Storage Area Network

SAN - System Area Network

POLAN - Passive Optical Local Area Network

EPN - Enterprise Private Network

VPN - Virtual Private Network

SQL - Structured Query Language

SaaS - Software as a service (SaaS)

PasS - Platform as a service (PaaS)

IaaS - Infrastructure as a service (IaaS)

XaaS Anything as a service (XaaS)

IEEE - Institute of Electrical and Electronics Engineers

WPAN - Wireless Personal Area Networks

CSMA/CD - Carrier-sense multiple access with collision detection

UTP - Unshielded Twisted Pair

NAT - Network Address Translation

OSI Model - Open Systems Interconnection Model

RU - Rack Unit

DL - Density Line

CPU - Central Processing Unit

RAM - Random Access Memory

SMB - Server Message Protocol

NFS - Network File System

DNS - Domain Name System

OS - Operating System

SMTP - Simple Mail Transfer Protocol

IMAP - Internet Message Access Protocol

POP3 - Post Office Protocol version 3

HTTP - Hypertext Transfer Protocol

DHCP - Dynamic Host Communication Protocol

PC - Personal Computer

SDN - Software Define Networks

FTP - File Transfer Protocol

OS - Operating System

IPV4 - Internet Protocol version 4

OEM - Original Equipment Manufacturer

VM - Virtual Machine

ISO - International Organization for Standardization

ISP - Internet Service Providers

NIC - Network Interface Card

SSL - Secure Socket Layer

API - Application Programming Interface

NETBIOS - Network Basic Input/Output System

ARR - Automatic Repeat Request

ARPANET - Advanced Research Project Agency Network

SSH - Secure Shell

TELNET - Teletype Network

TFTP - Trivial File Transmission Protocol

SFTP - Secure File Transfer Protocol

FTP - File Transfer Protocol

SMTP - Simple Mail Transfer Protocol.

POP 3 - Post Office Protocol 3.

IMAP - Internet  Message Access Protocol.

HTTP - Hyper Text Transfer Protocol

SSL - Secure Sockets Layer

TLS - Transport Layer Security

HTTPS - Secure Hyper Text Transfer Protocol.

ARP - Address Resolution Protocol.

ICMP - Internet Control Message Protocol.

SNMP - Simple Network Management Protocol.

DHCP - Dynamic Host Configuration Protocol.

ARP -Address Resolution Protocol.

# List of figures

# List of Tables

# TABLE OF CONTENTS

# Task 1

## 1.1 Computer networks

A Network is a group of interconnected people or things so. Hence, Computer network is a group of devices or computers that are interconnected to exchange information to communicate. In generally computer network would consist of desktop computers, mobile phones, printers etc. But the world has changed. Still, computer networks have desktop computers, mobile phones and printers. But now computer networks now have many smart devices such a security camera, smart lights, smart robots and many more devices connected to our networks as well.

Below figure is shown a basic computer network of a common home setup which consist of a switch , router, wireless access point, desktop computer, and a phone. All these devices connected to the same network as shown. But in most home networks the switch and the wireless access point will be built into the router.

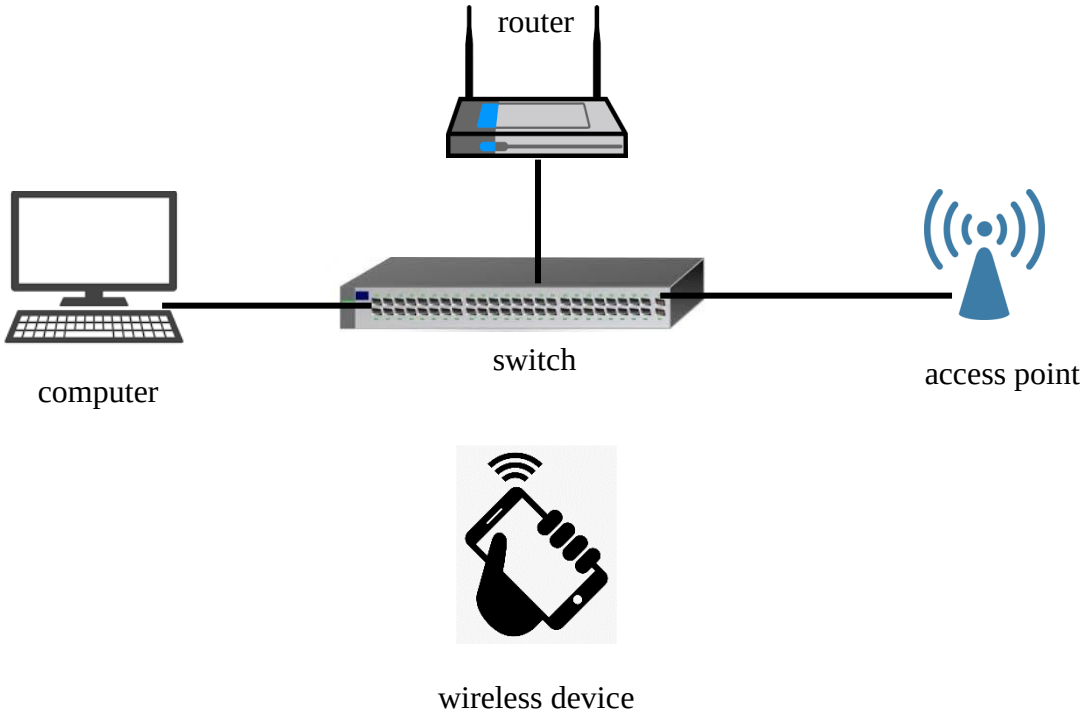



*Figure 1. 1 Common home computer network*

### 1.1.1 Benefits and risks computer networks

Benefits of computer network

- Enhances the communication.
- Allows to access vast amount of information.
- Allows share devices such as printers, smart home devices and many more.
- Share computer resources such as hardware and software.
- Share files anywhere and anytime easily with saving more time and effort.
- Giving flexibility to users to explore about essential things.
- Networking system or a software doesn't cost too much.
- Cost efficiency is increased since lot of software products can be shared through network system.

Risks of computer networks

- Since lot of people using computer networks the files and resources shared through network could be vulnerable to hackers.
- Since most people deepened on main file server, users having lack of independence.
- If the main servers break down, the whole computer network become useless. (Ex:- Recent incident on 4th October 2021 of Facebook servers' failure for 6 hours cost 6 billion US dollars revenue loss.)
- Files and data could be vulnerable of being attack by viruses and malwares.
- The internet connectivity has fostered of promoting negative acts and behaviors.
- To handle and work optimally using computer networks require high technical skills.
- Some networks require expensive devices such as routers, switches.

## 1.2 Types of computer networks

1. Area Networks
2. Client-Server Networks
3. Peer-to-peer Networks
4. Cloud computing Networks
5. Cluster Networks
6. Intranet and Extranet

### 1.2.1 (1) Area Networks

This is a type of computer network that can be more divided according to physical locations of the shared devices.

**Personal Area Network (PAN) :**

This is the most basic type of computer network which is being used. This type of network is used on personal level. The communication through wireless technology such as Bluetooth, Infrared, NFC(Near Field Communication) or wires like USB. This type of network mostly uses to transfer small files such as music, photos, and videos.

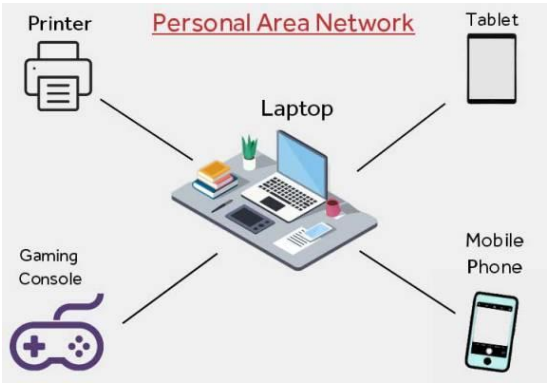



*Figure 1. 2 Personal Area Network diagram*

**Local Area Network (LAN) :**

Most frequently used type network is LAN. This is a computer network that connects devices and computers together in one physical location, such as a building, office, or home. Technologies like Ethernet and Wi-fi are involved to build LAN network. Most commonly used type of LAN is Ethernet LAN.

LAN networking can be applied in a home, school, library, office, etc.

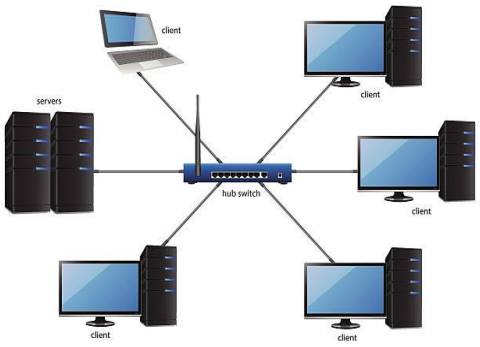



*Figure 1. 3 Local Area Network diagram*

**Wireless Local Area Network (WLAN) :**

WLAN is a type of computer network that use of wireless network technology like Wi-Fi to connect computers and devices in a LAN. This type of network doesn't use physical cables such as ethernet, twisted pair cable or fiber optics to connect computer and devices. Basically, this type of network has Wi-Fi router to connect devices wirelessly.


*Figure 1. 4 Wireless Local Area Network diagram*

**Campus Area Network (CAN) :**

When compared to LAN the CAN network is bigger than a LAN. But CAN network is smaller than MAN network. CAN is basically used for joining 2 or more LAN within a limited area. CAN is generally used for interconnect different departments of a particular organization.

CAN networking can be applied in campuses, schools, buildings, etc.

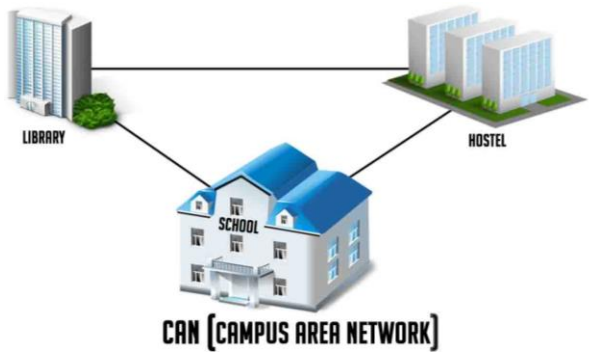



*Figure 1. 5 Campus Area Network diagram*

**Metropolitan Area Network (MAN) :**

When compared to CAN the MAN network is bigger than a CAN and LAN. But MAN is smaller than WAN network. MAN is used for connecting computers and devices over a distant geographical area. This spans over a city, town, or metropolitan area. Generally, for MAN networks high-speed connection such as fiber optics is being used.

CAN networking can be applied in towns, cities, large area within multiple buildings, etc.

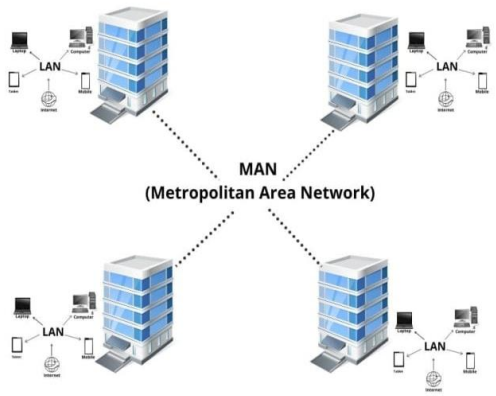



*Figure 1. 6 Metropolitan Area Network diagram*

**Wide Area Network (WAN) :**

WAN is the biggest type of area network. WAN connects computers over a large geographical area through multiple types of communication paths. WAN is extending over many geographical locations. WAN includes LAN, CAN and MAN which MAN gives ability to span over the whole world

The best example for WAN network is the Internet.

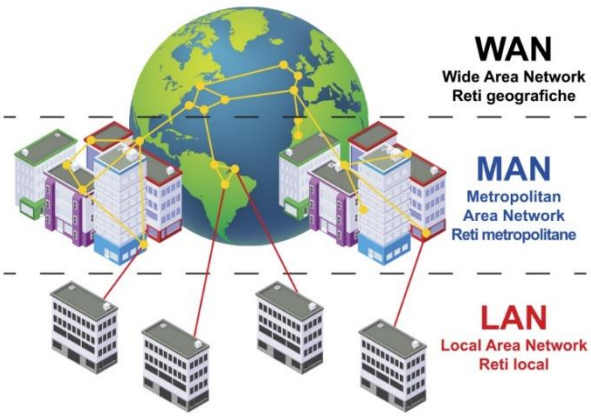



*Figure 1. 7 Wide Area Network diagram*

**Storage Area Network (SAN) :**

SAN is a type of computer network that has special high-speed network to store data by using storage devices to several servers. This network does not depend on LAN, CAN, MAN or WAN. SAN uses storage resources such as Multiple Disk Arrays, Switches, and Servers with a high-speed network to give high speed access to large amount of data.

An example for SAN is network of disks accessed by a network of servers.

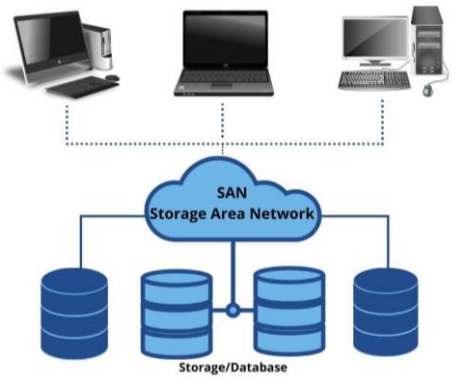



*Figure 1. 8 Storage Area Network diagram*

**System Area Network (SAN) :**

This is a type of computer network that connects a cluster of high-performance computers with a high bandwidth network. This network is very similar to LAN, but SAN handles high amounts of information in large requests. SAN is used for processing applications that require high network performance.

An example for SAN is Microsoft SQL Server 2005 uses SAN through virtual interface adapter.

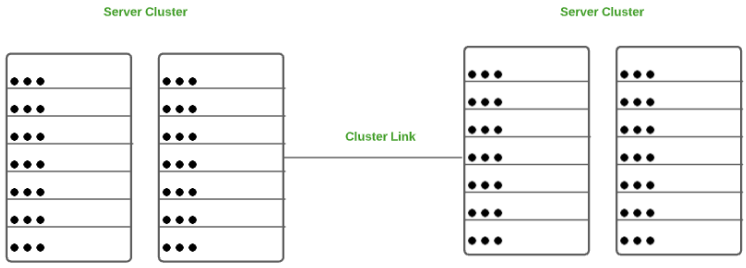



*Figure 1. 9 System Area Network diagram*

**Passive Optical Local Area Network (POLAN) :**

This type of network is an alternative to a LAN network, but this uses a point to multipoint LAN architecture. POLAN generally uses optical splitter to split optical signals. Optical splitter splits single strand of single mode optical fiber to multiple signals to distribute users and devices.

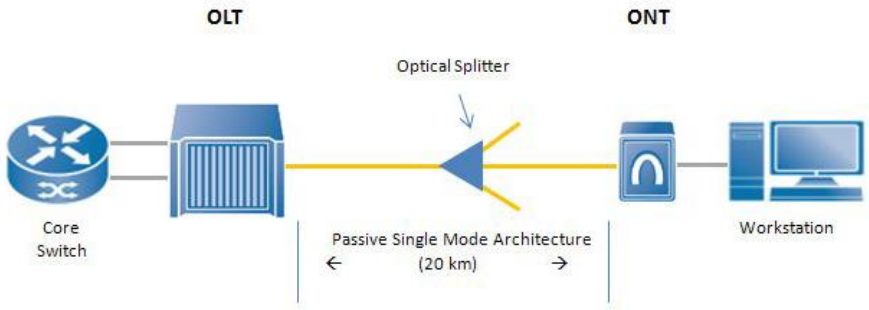



*Figure 1. 10 Passive Optical Local Area Network diagram*

**Enterprise Private Network (EPN) :**

EPN is a type of computer network which is used by businesses as a connection over various locations to share computer resources. And also, this provides high speed internet connection within the organization. EPN uses routers, switches, fiber optics and modems to build private network within the organization. EPN can be made by several network technologies such as LAN, WAN, VPN (Virtual Private Network) or Cloud based network.

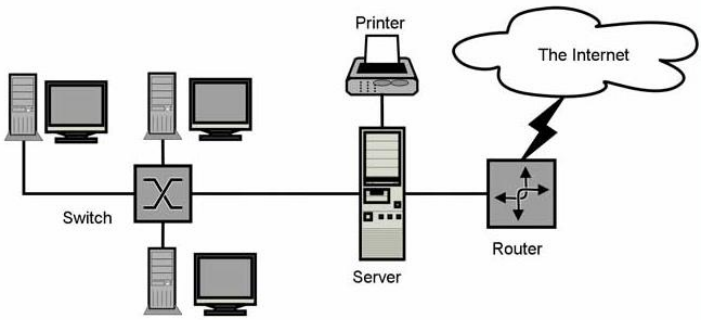



*Figure 1. 11 Enterprise Private Network diagram*

**Virtual Private Network (VPN) :**

VPN is very similar to LAN. But the major difference between VPN and LAN is the devices that are part of a VPN could be anywhere. VPN network extends a private network across the internet. VPN network allows users to send and receive data as if they were connected to a private network. Users can connect to the private network remotely even they are stay at very distant locations.

Since VPN uses technologies, such as tunneling and encryptions for security purpose, this network protects users and organizations from hackers. With a VPN an employee can securely access his own private corporate network while sitting at home or in a hotel. Physically employee is outside his corporate private network, but virtually he/she is inside.

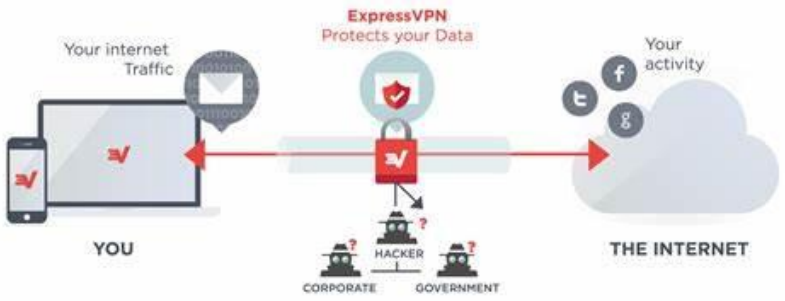



*Figure 1. 12 Virtual Private Network diagram*

**Controlled Local Area Network (CAN) :**

This type of network is helping to communicate with multiple electronics such as sensors, processors, etc. CAN is generally used in industries such as automobiles, robotics, hospital robotics. CAN is using a peer-to-peer network to connect all devices like a web. Because of that we can easily add other devices to this network. In this type of network all electronics can transmit signal with among them.

CAN is work like a smart device. For example, each electronic receive signal will decide if the message relevant to it or not. If 2 electronic devices decide to send message at the very same time the “Priority ID System” comes in. Each transmitted message carries with a priority ID which means how important is the message. When 2 messages clash Priority ID System will allow to relay highest priority message. For example, car fire alarm system has major priority than the light system.

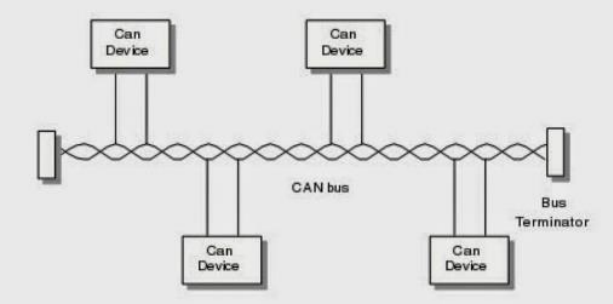



*Figure 1. 13 Controlled Local Area Network typical diagram*

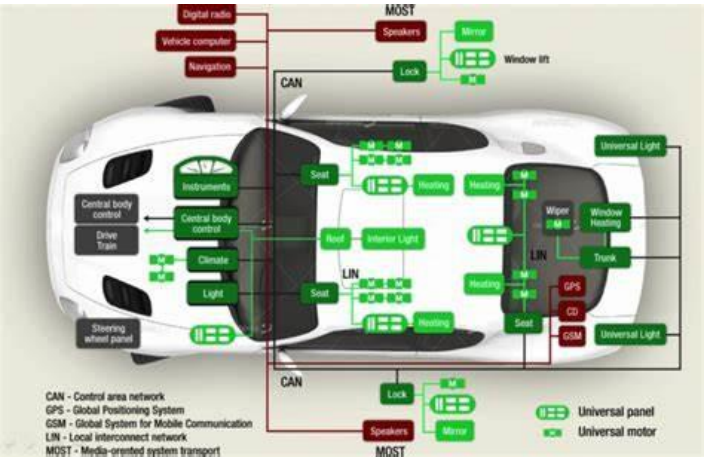



*Figure 1. 14 Controlled Local Area Network used in a car*

### 1.2.2 (2) Client-Server Networks

This type of network is known as Server Based network or Domain Network. In this model centralized server is used to store the data to respond the requests of the clients. Hence, the management is centralized in Client-Server Network.

### 1.2.3 (3) Peer-to-Peer Networks

In Peer-to-Peer Network every node is work as a client and server. Hence, every node can do both request and respond activities. Hence, the management is decentralized in Client-Server Network.

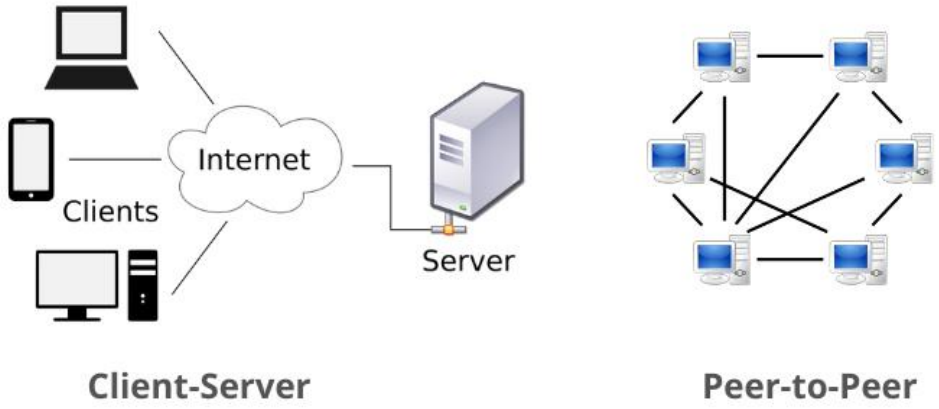



*Figure 1. 15 Client-Server network vs Peer-to-Peer network*

**Difference between Client-Server and Peer-to-Peer Network**

| Differences | |
|---|---|
| **Client -Server Network** | **Peer-to-Peer Network** |
| Clients and Server are differentiated. | Clients and Server are not differentiated. |
| Focus on information sharing. | Focus on connectivity. |
| Centralized server is used to store data. | Each peer has its own data. |
| Server responds to Client's requests. | Every node can do both request and respond. |
| Expensive. | Inexpensive. |
| More stable. | Less stable. |
| Used for both small and large networks. | Suited for smaller networks. |

*Table 1. 1 Client-Server network vs Peer-to-Peer network*

### 1.2.4 (4) Cloud computing Networks

Cloud computing refers accessing and storing data and software through remote servers that are hosted on internet. Unlike using traditional computer hard drive or a local server, cloud computing is an internet based computing network.

Since the reduction in hardware cost cloud computing saves money. Instead of purchasing lot of space and expensive hardware equipment, cloud computing networks offers inexpensive network system that can access quick and easy from anywhere and anytime. And this saves money from spending money for hardware replacements, upgrades and repairing equipment.

**Types of cloud networking services :**

Most cloud computing services fall into three broad categories:

1. Software as a service (SaaS)

SaaS is a type of cloud networking of delivering services and applications over internet.

2. Platform as a service (PaaS)

PaaS is a type of cloud networking provides a platform and environment for developers to build applications and services over the internet.

3. Infrastructure as a service (IaaS)

IaaS is a type of cloud networking service model which delivers computer infrastructure on an outsourced basis to support for various types of operations.

4. Anything as a service (XaaS)

XaaS is a type of cloud networking service model which provides anything as a service. This includes above all services including some additional services.

### 1.2.5 (5) Cluster computer Network

In cluster computing, tasks are distributed among several computers. Individual nodes of a cluster are connected over fast network to increase the computing capacity and availability. There are several types of cluster computing networks such as Load Balancing clusters, High Availability clusters (HA) and High-Performance clusters (HP). Cluster computer Network has many advantages such as task managing and delegating tasks for available nodes. For example, if one node (computer or a server) in the cluster fails the work can be switched to a different computer in the cluster.

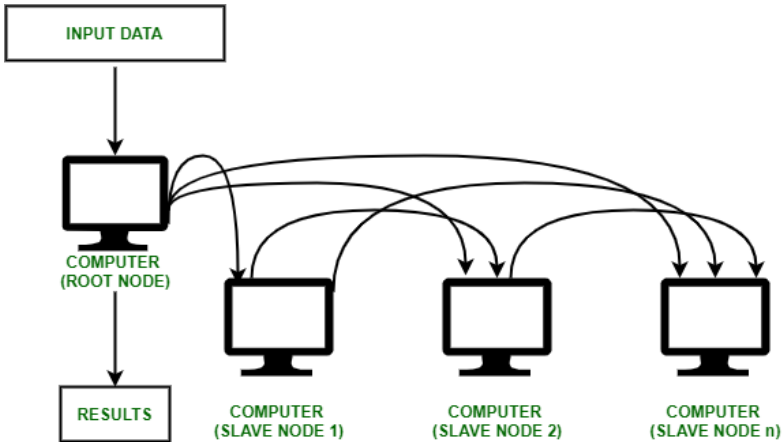



*Figure 1. 16 How Cluster computer Network works*

### 1.2.6 (6) Intranet and Extranet Network

Intranet is a network system that is used for sharing data and information throughout the organization only. This is a type of private network consists with limited number of connecting devices. Because of the Intranet should have a smaller number of visitors. Hence, Intranet is restricted area up to an organization.

On the other hand, Extranet is a network system used by single or many organizations for sharing data and information between internal and external members to the organization. Hence extranet is accessible for internal members of the organization as well as external members. Which means Extranet is restricted area up to organization and its stakeholders.

### 1.2.7 Choosing Computer Network standards for Matara Branch

As a Networking consultant I prefer LAN network which belongs to Area Network for Matara branch of SYNTAX Solutions company. As explained before LAN is a group of devices that are connected in a single physical place, such as a building, business, or home. Since SYNTAX Solutions Matara branch is a single 4 story building, the LAN network is the best network type for it. And there are few other reasons to choose LAN network for SYNTAX Solutions Matara branch as follows.

- In a Local Area Network, sharing resources like as hard disk drives, DVD drives, and printers is simple. For example, all of the resources may be networked to a single computer so that when resources are needed, they can be shared among the connected computers.
- Software sharing is another sort of sharing that is made simple here. Other users on the network can share a single computer with the licensed software. There is no need to acquire a separate license for each machine on the network. All of this can be done under a single license.
- LAN allows users to send and receive messages and data in a convenient manner. Because the data is stored on the server, LAN users can access it at any time. This is something that each LAN user can do with others on the network. As a result, not only does this save time, but it also assures that communications reach the intended recipients.
- As previously stated, the data of the users is stored on a centralized server. This information can be accessed from any computer in a given network. Furthermore, by logging into their accounts, users can view their own set of data.
- Data can be assured to be secure because it is stored on a local server. When the data on the server is updated, all LAN users have access to it. Furthermore, the host has the power to restrict or accept users in a specific network, allowing for extra security measures to be implemented.
- A LAN can share an internet connection among all users on the network. All connected computers share an internet connection from a single computer with an internet connection. Offices and Net cafés both have this type of infrastructure.

(Roomi, 7 Advantages and Disadvantages of LAN | Limitations & Benefits of LAN 2021)

## 1.3 Communication within computer networks

### 1.3.1 Components of Data Communication System

Data communication is described as the transfer of data between two devices using a transmission medium such as a cable, wire, or air or vacuum. Communicating devices must be a part of a communication system that consists of a combination of hardware and software devices and programs in order for data communication to occur.

**Data Communication System Components :**

A data transmission system is made up with following five key components.

**1.** Message

**2.** Sender

**3.** Receiver

**4.** Transmission Medium

**5.** Set of rules (Protocol)

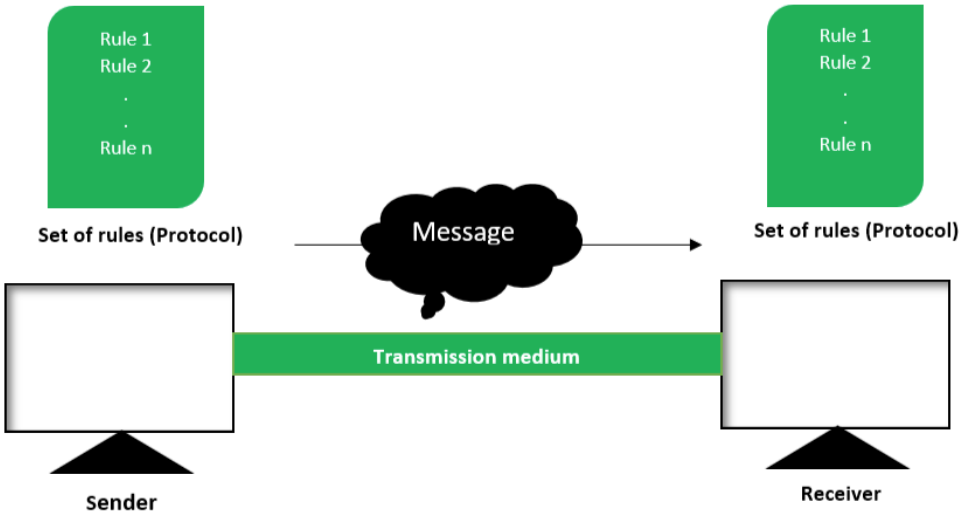



*Figure 1. 17 Components of data communication system*

- Message → In a data communication system, this is the most valuable asset. The message simply refers to the data or information that has to be shared. A message could be in the form of a text file, an audio file, a video file, or anything else.
- Sender → Someone who will perform the role of a source must be present to transfer messages from source to destination. In a data transmission system, the sender acts as a source. Simply put, it is a device that transmits data. The device could be in form of a computer, mobile, telephone, laptop, video camera, or a workstation etc.
- Receiver → It is the destination where the message sent by the source has finally arrived. Simply put it's a message-receiving device.
- Transmission Medium → The transmission medium serves as a bridge between the sender and the receiver in the entire data communication process. It's the physical path that data or messages take to get from sender to receiver. Twisted pair cable, fiber optic cable, radio waves, and microwaves are examples of transmission mediums that can be guided (with wires) or unguided (without wires).
- Set of rules (Protocols) → Various sets of rules had already been designed by the designers of the communication systems to govern data communications, which represent a kind of agreement between communicating devices. This is referred to as protocol. The protocol, in plain terms, is a set of rules that regulate data transfer. There will be no communication between two different devices if they are linked but do not share a protocol. As a result, the protocol is required for data communication.

Sending an e-mail is a good example of a data transmission system. The sender is the person who sends the email, the message is the data that the user wants to send, and the receiver is the person to whom the user wants to send the message. There are several protocols involved in this process, one of which being the Simple Mail Transfer Protocol (SMTP). To send and receive email, both the sender and the receiver must have an internet connection that uses a wireless channel.

(Components of Data Communication System – Geeks-for-Geeks 2021)

## 1.3.2 Transmission Modes in Networks (Simplex, Half-Duplex and Full-Duplex)

Transferring data between two devices knows as Transmission Mode. It's also known as a mode of communication. Networks are built to allow communication between related devices.

There are three types of transmission mode:-

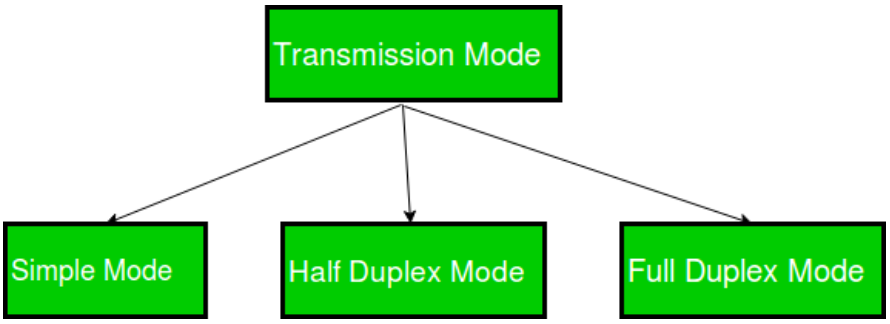



*Figure 1. 18 Transmission mode 3 types*

**Simplex Mode :**

The communication between the sender and the receiver occurs in only one direction in simplex transmission mode. The data can only be sent by the sender, and the data can only be received by the receiver. The receiver is unable to respond to the sender. Simplex transmission can be compared to a one-way street where traffic only flows in one direction and no vehicles from the opposing direction are permitted to pass.

In the case of a keyboard/monitor pairing, the keyboard can only send data to the monitor, while the monitor can only receive data and show it on the screen. The monitor is unable to respond or provide feedback to the keyboard.

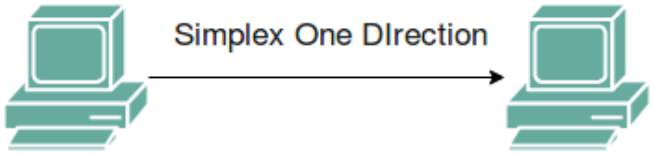



*Figure 1. 19 How simplex mode works*

**Half Duplex Mode :**

Half-duplex transmission allows communication between the sender and receiver in both directions, but only one at a time. Both the sender and the receiver can send and receive data, but only one of them can send at any one time. A half-duplex is still considered a one-way street, which means that a vehicle moving in the opposite direction of traffic must wait until the road is clear before passing.

In walkie-talkies, for example, the speakers on both ends can speak, but they must do so one at a time. They are unable to converse at the same time.

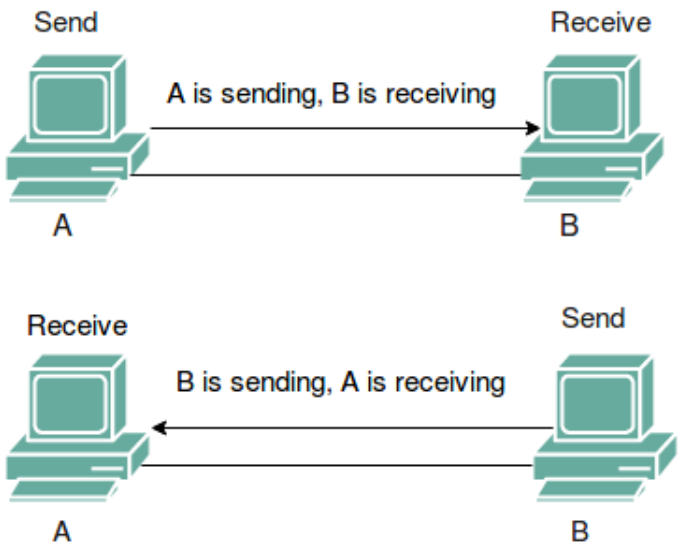



*Figure 1. 20 How half duplex mode works*

**Full Duplex Mode :**

In full duplex transmission mode, the sender and receiver can communicate at the same time. Both the sender and the receiver can send and receive data at the same time. Full duplex transmission mode is similar to a two-way street, with traffic flowing in both directions at the same time.

For example, in a telephone conversation between two people , both are free to speak and listen at the same time.

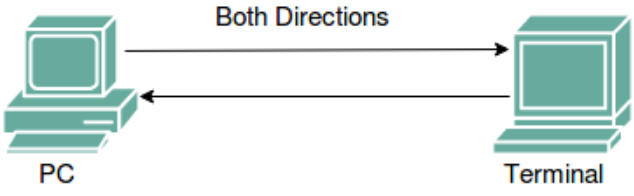



*Figure 1. 21 How full simplex mode works*

| Basis for comparison | Differences | | |
|---|---|---|---|
| | **Simplex Mode** | **Half Duplex Mode** | **Full Duplex Mode** |
| Direction of communication | Unidirectional. | Two-directional, one at a time. | Two-directional, simultaneously. |
| Send/Receive | Sender can only send data. | Sender can send and receive data, but one a time. | Sender can send and receive data simultaneously. |
| Performance | Worst performing mode of transmission. | Better than simplex. | Best performing mode of transmission. |
| Example | Keyboard and monitor. | Walkie-talkie. | Telephone. |

*Table 1. 2 Differences between Simplex Mode, Half Duplex Mode and Full Duplex Mode*

(Simplex, Half Duplex, Full Duplex | Definition, Comparison & Information 2021)

## 1.3.3 Line Configuration in Networks (Point-to-Point and Multipoint Connections)

A network is made up of two or more devices that are connected through a link. A link is a communication path that allows data to be sent from one device to another. A computer, printer, or any other device capable of sending and receiving data can be used as a device. Imagine any link as a line formed between two spots for the sake of visualization. Two devices must be linked to the same link in some way at the same moment for communication to occur.

There are two possible types of communication:

1. Point-to-Point Communication
2. Multipoint Communication

**Point-to-Point Communication :**

A dedicated link between two devices is provided by a point-to-point communication . Transmission between those two devices takes up the full bandwidth of the link. The majority of point-to-point connections employ a physical wire or cable to connect the two ends, however alternative solutions such as microwave or satellite links are also available. The point-to-point network topology is one of the most common and straightforward network topologies. It's also the simplest to set up and comprehend. For example, to change the channels, a point-to-point link between the remote control and the television is used.

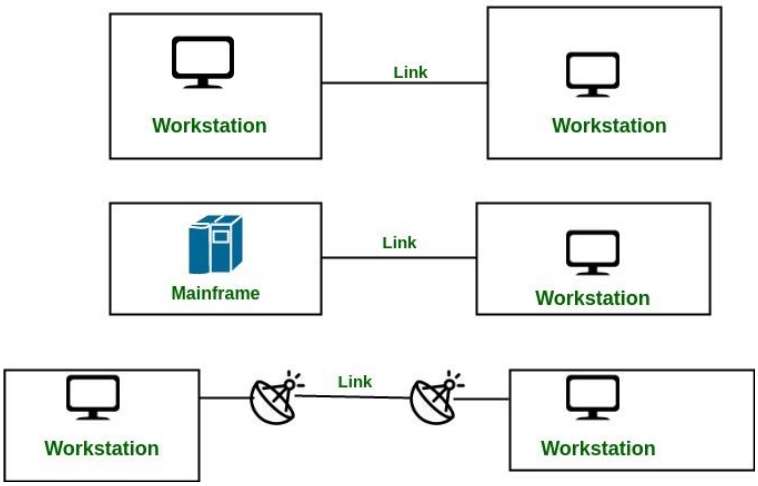



*Figure 1. 22 How Point-to-Point communication works*

**Multipoint Communication :**

Multidrop configuration is another name for it. Two or more devices share a single link in this connection. The capacity of the channel is now shared by more than two devices using the link.

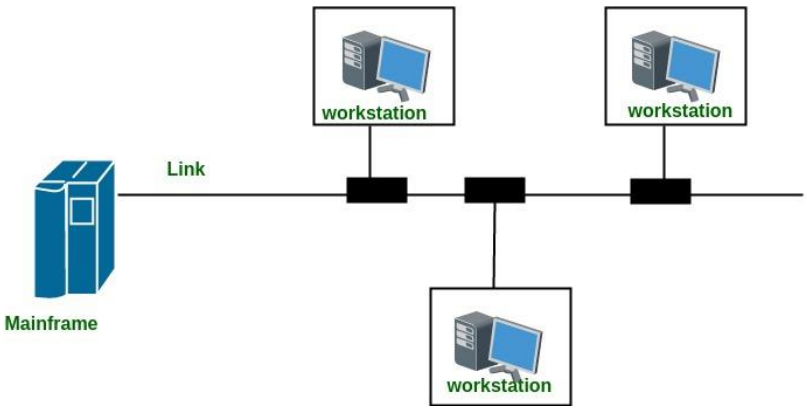



*Figure 1. 23 How Multipoint Communication works*

In a Multipoint Line setup with shared capacity, there are two options:

- Spatial Sharing → Spatially shared line configuration refers to when multiple devices can share a link at the same time.
- Temporal (Time) Sharing → Temporally shared or Time-Shared Line arrangement means that users must take turns utilizing the link.

(Line Configuration in Computer Networks – Geeks-for-Geeks 2021)

| Differences | |
|---|---|
| **Point-to-Point Communication** | **Multipoint Communication** |
| Channel is shared between two nodes. | Channel is shared among multiple nodes. |
| There is a dedicated link between two nodes. | Link is provided all times for share the connection among nodes. |
| The entire capacity is reserved between these connected two devices. | The entire capacity is dependent on quick sharing. |
| There is one transmitter and one receiver. | There is one transmitter and many receivers. |
| The smallest distance is most important to reach the receiver. | The smallest distance is not important to reach the receiver. |
| Provides security and privacy because communication channel is not shared. | Doesn't provide security and privacy because communication channel is shared. |

*Table 1. 3 Differences between Point-to-Point communication and Multipoint communication*

(Differences between Point-to-Point and Multi-point Communication – Geeks-for-Geeks 2021)

## 1.4 Network Bandwidth

**What is bandwidth :**

The maximum capacity of a wired or wireless communications link to send data via a network connection in a given amount of time is known as network bandwidth. The number of bits, kilobits, megabits, or gigabits that can be transmitted in one second is commonly used to describe bandwidth. Bandwidth is a term used interchangeably with capacity to indicate the rate at which data is transferred. A popular misperception is that bandwidth is a measure of network speed.

A data connection's bandwidth determines how much data it can send and receive at once. The volume of water that can flow through a tube can be likened to bandwidth. The larger the diameter of the tube, the more water can flow through it at once. The same idea applies to bandwidth. The higher the communication link's capacity, the more data it can handle per second.

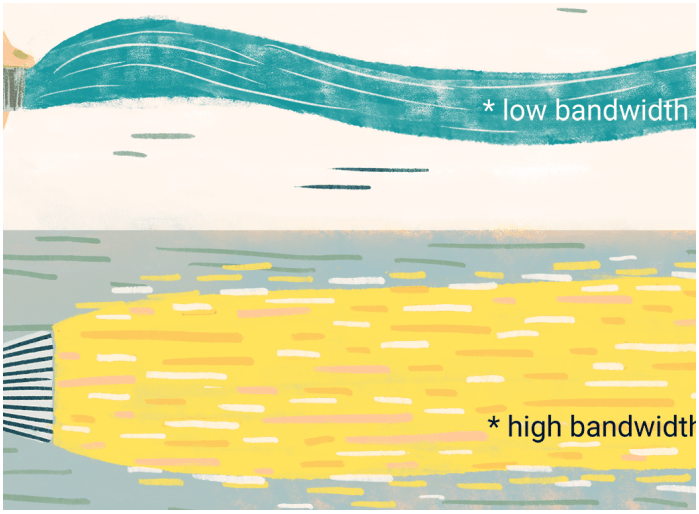



*Figure 1. 24 How low bandwidth and high bandwidth looks like*

**Measuring the bandwidth :**

While bandwidth was once measured in bits per second (bps), modern network links now have far greater capacity, so bandwidth is now measured in megabits per second (Mbps) or gigabits per second (Gbps). As bandwidth expands, so does the cost of a network connection. As a result, a Gigabit per second (Gbps) connection will cost more than one capable of a Megabits per second (Mbps) connection.

Measuring Bandwidth

| Unit of Bandwidth | Abbreviation | Equivalence |
|---|---|---|
| Bits per second | b/s | 1 b/s = fundamental unit of bandwidth |
| Thousands of bits per second | kb/s | 1 kb/s = 1,000 b/s = 10^3 b/s |
| Millions of bits per second | Mb/s | 1 Mb/s = 1,000,000 b/s = 10^6 b/s |
| Billions of bits per second | Gb/s | 1 Gb/s = 1,000,000,000 b/s = 10^9 b/s |
| Trillions of bits per second | Tb/s | 1 Tb/s = 1,000,000,000,000 b/s = 10^12 b/s |

*Figure 1. 25 Scalability of units of bandwidth*

Bandwidth connections can be symmetrical, meaning the data capacity is the same in both directions (upload and download), or asymmetrical, meaning the data capacity is not equal in both directions (upload and download). Upload capacity is often lower than download capacity in asymmetrical connections, which is common in consumer-grade internet broadband connections.

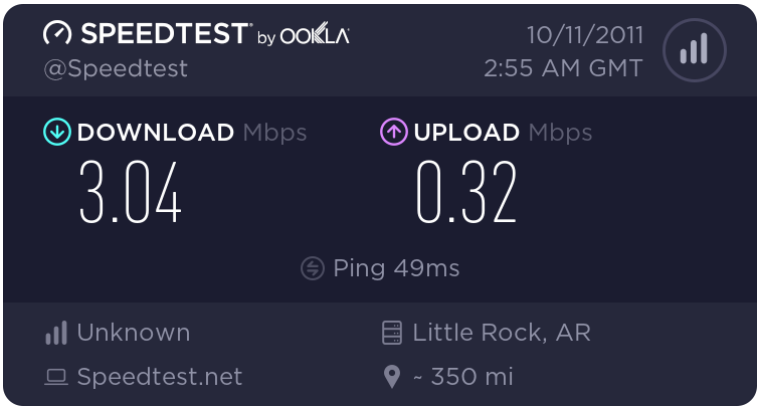



*Figure 1. 26 Asymmetrical bandwidth connection measured by speed-test*

**Bandwidth vs Speed :**

The terms bandwidth and speed are frequently and incorrectly used interchangeably. The root of the misunderstanding could be partly attributable to ads by internet service providers (ISPs) that mix the two by alluding to faster speeds when they really imply bandwidth.

In essence, speed relates to the rate at which data can be communicated, whereas bandwidth refers to the amount of data that can be delivered at that rate. To return to the water metaphor, speed refers to the rate at which water can be pushed through a pipe, whereas bandwidth refers to the amount of water that can be carried through the pipe in a given amount of time.

**The amount of bandwidth we need :**

The amount of bandwidth we require is determined by what we want to perform with our internet connection. More is, for the most part better, but we are bound by our money. In general, if all we intend to do is use Facebook and watch the occasional video, a low-end high-speed plan will suffice.

Depending on how we use the internet, we might be able to acquire an official bandwidth recommendation so that we know precisely how much bandwidth we'll need to get the most out of that service. For example, if our internet is currently working fine but we want to add a movie streaming service to the mix, we'll need to check out our ISP's website to see what minimum bandwidth they recommend for uninterrupted streaming.

Streaming, gaming, and other high-bandwidth activities demand a certain amount of bandwidth speed to avoid buffering and latency. The faster our machines perform, the more bandwidth our network can provide.

**Controlling the bandwidth :**

Some software allows the user to set a restriction on how much bandwidth a program can take, which is useful if user still want the application to work but don't need it to operate at full speed. The term "bandwidth control" is used to describe this type of purposeful bandwidth restriction. Many online backup services such as cloud storage services, torrenting tools, and routers enable bandwidth control. These are all services and programs that deal with a lot of data, so having alternatives to limit their access makes reasonable.

As an example, let's say we intend to download a 10 GB file. Rather than having it download for hours, consuming all available bandwidth, we could use a download manager and configure it to limit the download to only 10% of the available bandwidth. Of course, this would add a significant amount of time to the overall download time, but it would also free up a significant amount of bandwidth for other time-sensitive activities such as live video streaming.

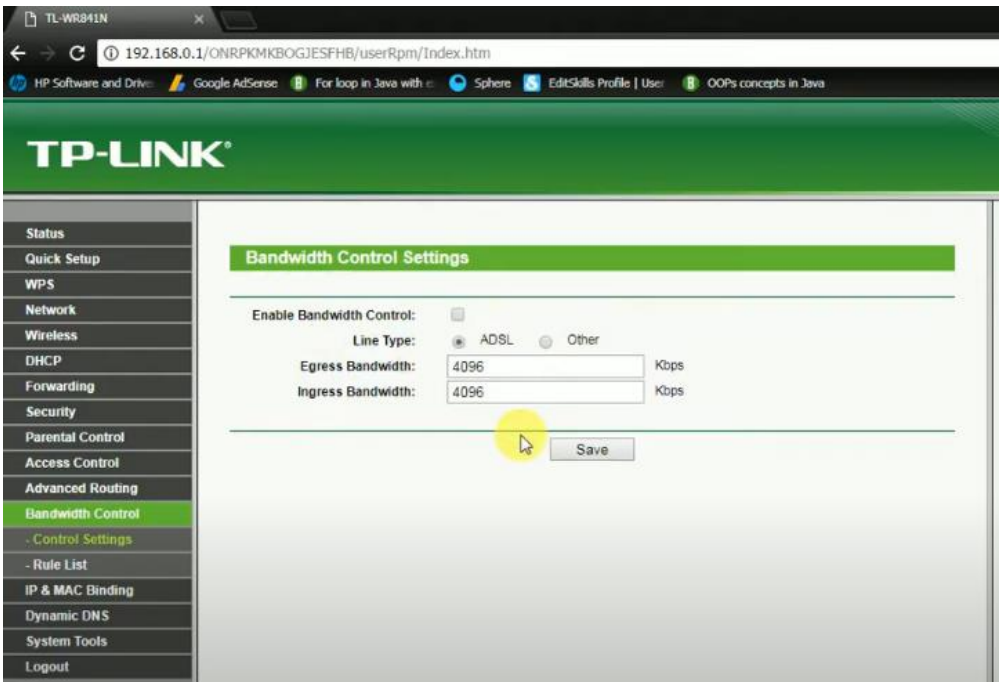



*Figure 1. 27 Limit Bandwidth In TP-Link Routers*

## 1.5 Common networking principles

### 1.5.1 OSI Model

The ISO launched a program in the late 1970s to establish generic networking standards and procedures. Then, in 1973, an Experimental Packet Switched System in the United Kingdom identified the need for higher-level protocols to be defined. The OSI model was created in 1983 with the intention of being a thorough specification of actual interfaces. Finally, in 1984, ISO formally accepted the OSI architecture as an international standard.

The Open System Interconnection Model (OSI Model) is a model for connecting systems. In a computer network, the OSI Model is used to understand how data is transmitted from one computer to the next. Two computers are connected with LAN cables and connectors and share data with the help of Network Interface Cards (NICs). The OSI Model was created in 1984 by ISO (International Organization for Standardization) in order to achieve successful communication between computer networks. Layers begin with number 7 and progress upwards.

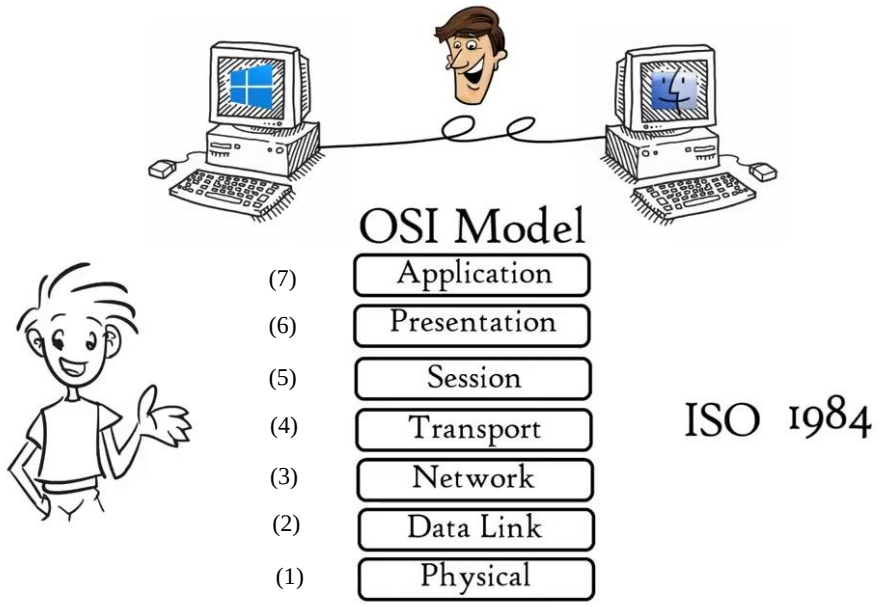



*Figure 1. 28 OSI model 7 layers*

**(7) Application Layer :**

Application layer is used to connect to a network. In addition, provide user interfaces and support services such as emails, phone calls, and other sorts of information services. As a result, network applications are used by Application Layer. A network application is a computer program that makes use of the internet.

Ex:- Chrome, Firefox, Outlook, Skype

There are numerous Application Layer protocols that enable diverse functions at this layer. These protocols serve as the foundation for a wide range of network services such as file transfer, web browsing, emails, and virtual terminals.

**(6) Presentation Layer :**

This layer gets information from the application layer. This information is presented in the form of characters and numbers. The presentation layer is utilized to translate these letters and numbers to machine-readable binary code, then bit reduction, and finally credibility maintenance.

The presentation layer serves three primary roles.

1) Translation
2) Compression
3) Encryption or Decryption

Translation :-

The process of converting letters and integers to binary representation is known as translation.

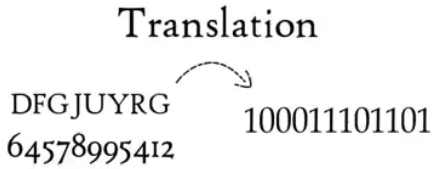



*Figure 1. 29 What translation simply do*

This layer lowered the number of bits necessary to represent the original data prior to data transmission. This bit reduction method is known as data compression. The amount of space required to hold the original file was lowered using data compression. Because the size is shrunk, it can reach at its destination in much less time. As a result, data compression is extremely beneficial in activities such as real-time video audio streaming.

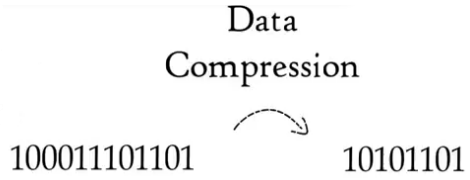



*Figure 1. 30 What data compression simply do*

To ensure data security, data is encrypted before to transmission. Encryption contributes to the security of data. Data is encrypted on the sender side and decoded on the receiver side. To ensure the safety of data The presentation layer uses SSL (secure socket layer) for encryption and decryption. SSH uses robust encryption to ensure the security and confidentiality of communications.

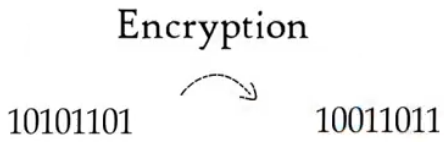



*Figure 1. 31 What encryption simply do*

**(5) Session Layer :**

The Session Layer manages connections, or sessions, to enable data transmission and receiving, as well as authentication and authorization. To carry out these operations, the Session Layer employs its own tools known as API (Application Programming Interface).

Example for API :- NETBIOS(Network Basic Input/Output System), NETBIOS is a system that allows applications on separate computers to connect with one another.

API performs a function called authentication just before establishing a session with the server. The process of identifying a device is known as authentication. When computer try to establish a connection with a Server, it uses a “username” and “password” before the connection. When the username and password are identical, a session is formed between the computer and the server.

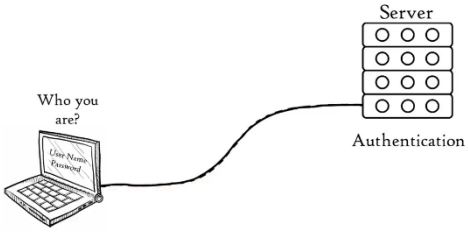



*Figure 1. 32 PC trying to establish a session with server*

The authorization is checked after authentication. Authorization is the procedure where a server determines who has authority to access a file. Otherwise, the user will be unable to access the file.

Hence, the session layer serves two primary roles.

1) Authentication
2) Authorization

The session layer maintains track of which files are being downloaded. For example, a web page including text and images is stored on the web server as separate files. When a user requests a website in his web browser, a separate session to the web server is opened to receive each of these text and image files independently. These files are transmitted as data packets. The session layer keeps track of data packets that belong to text or images and where they flow. This facilitates session management. The Web browser handles all Application Layer, Presentation Layer, and Session Layer activities.

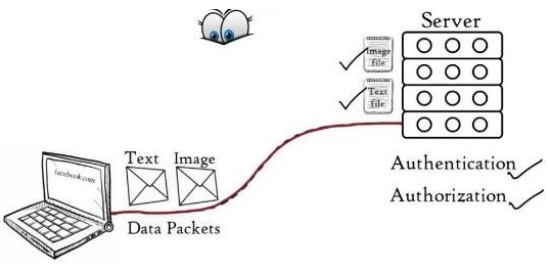



*Figure 1. 33 Keeps track of data packets that belong to text or images*

**(4) Transport Layer :**

The Transport Layer contributes to the regulation of communication reliability.

The Transport Layer serves three primary roles.

1) Segmentation
2) Flow Control
3) Error Control

Segmentation :-

Data at the session layer is separated into small data units known as segments. Each segment includes a destination port number as well as a sequence number. While the destination port number assists in directing each segment to the appropriate application, the sequence number assists in reassembling smaller units in the proper order.

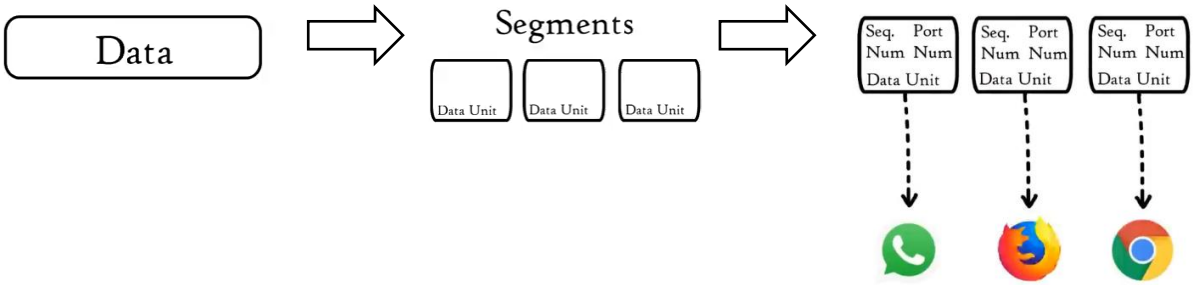



*Figure 1. 34 What segmentation simply do*

Flow Control :-

Flow control helps in controlling the amount of data transferred. Consider a server that can transfer data at a maximum rate of 100Mbps connected to a mobile device that can only process at a maximum rate of 10Mbps. If a server sends data at a rate of 50Mbps, which is faster than the rate at which a mobile device can handle it, the Transport Layer instructs the server to reduce the data transmission rate to 10Mbps so that data is not lost due to overflowing.

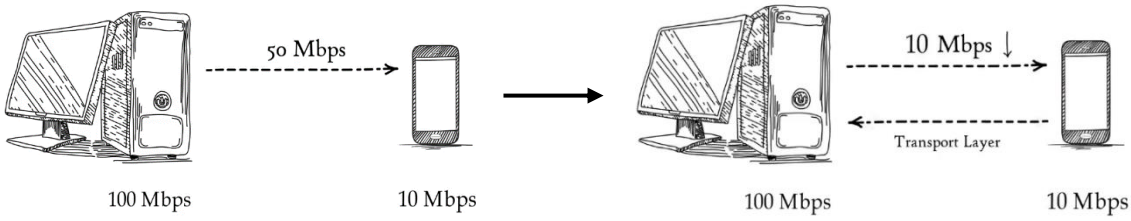



*Figure 1. 35 What flow control simply do*

Error Control :-

In error control when some data units fail to arrive at their destination, the transport layer employs ARR (Automatic Repeat Request) techniques to retransmit the lost or corrupted data.

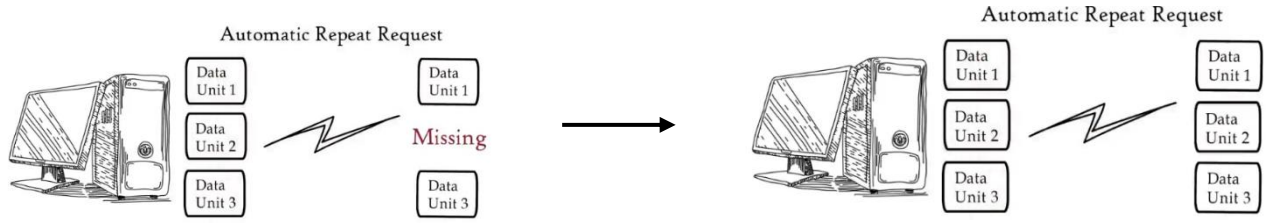



*Figure 1. 36 What error control simply do*

There are another two types of significant protocols and two types of major services utilized in the Transport Layer.

Services → 1.Connection Oriented Transmission
2.Connectionless Transmission

Protocols → 1.Transmission Control Protocol (TCP)
2.User Datagram Protocol (UDP)

TCP is used for connection-oriented transmission.
UDP is used for connectionless transmission.

Hence, it does not provide any feedback, UDP is faster than TCP. As a result, UDP is utilized where it doesn't matter if data is received or not. For example, UDP can be used for Online streaming Movies, songs, Voice over IP.

TCP, on the other hand, provides feedback, allowing for the retransmission of lost data. As a result, TCP is used when complete data delivery is required. For example, web surfing , Email, FTP.

**(2) Data Link Layer :**

More header information on IP packets, such as Source and Destination MAC addresses, can be added using the Data Link Layer. Data units in this layer called Frames. The source and destination IP addresses should be included in data packets. In this layer Source and Destination MAC addresses are assigned to each data packet to form Frame.

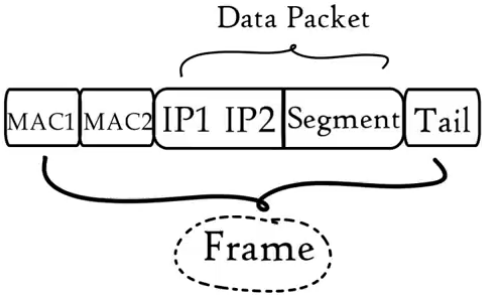



*Figure 1. 37 Components of a frame*

The MAC Address is a 12-digit alpha-numeric number embedded in the computer's NIC (Network Interface Card). In NIC, the data link layer is implemented as software. Furthermore, Data Link Layer provide mechanisms for data transfer from one computer to another via local media such as copper wire and optical fiber.

The Data Link Layer provides two key functions:

1) It allows the upper layers of the OSI Model to access media via techniques such as framing.
2) Using techniques such as Media Access Control and Error Detection, users can control how data is placed from the media.

Media Access Control is the technique used to get the frame on and off the media. A common media may be shared by a number of devices. If two devices connected to the same media send data at the same time, there is a chance that the two messages will contact, resulting in a useless message. To avoid a crash, Data Link Layer monitors shared media to ensure that it is free. Carrier Sense Multiple Access (CSMA) is what it's called (CSMA). As a result, the Data Link Layer has the capability to regulate data transmission.

**(1) Physical Layer :**

Until now, data sent from Session Layer has been segmented in the Transport Layer, placed into packets in the Network Layer, and then framed in a sequence of binary and zeros by the Data Link Layer. The physical layer assists in the conversion of binary sequenced data to a signal, which is then transmitted through a medium. Depending on the media, this signal can be light, electrical, or radio (copper, fiber, air).

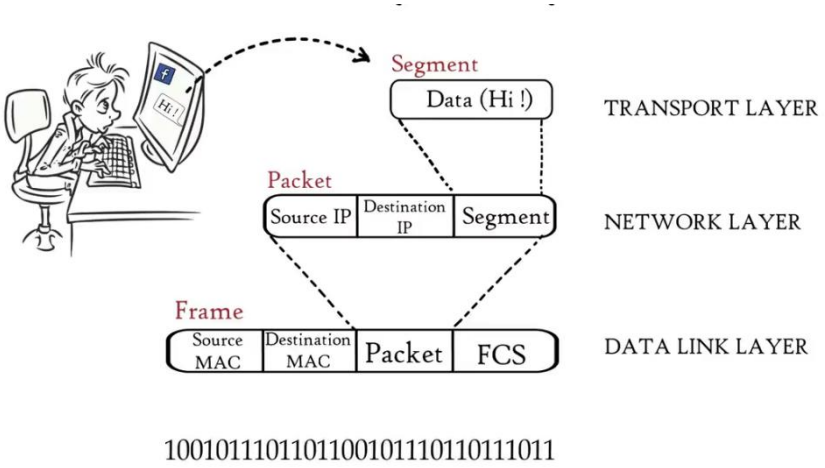



*Figure 1. 38 Data transformation in each layer*

## 1.5.2 TCP / IP Model

The Transmission Control Protocol/Internet Protocol paradigm is also known as TCP/IP. The OSI model is a conceptual model that isn't used in modern networking. However, the TCP/IP model employs a variety of protocols to enable Internet connection. These protocols are grouped together under a name TCP IP model.

However, we no longer hear the name very often; instead, we hear IPV4 or IPV6, although it is still valid. The TCP IP model has four layers as opposed to the OSI model's seven. It is presented to have a precise fit on the OSI model, however it does not.

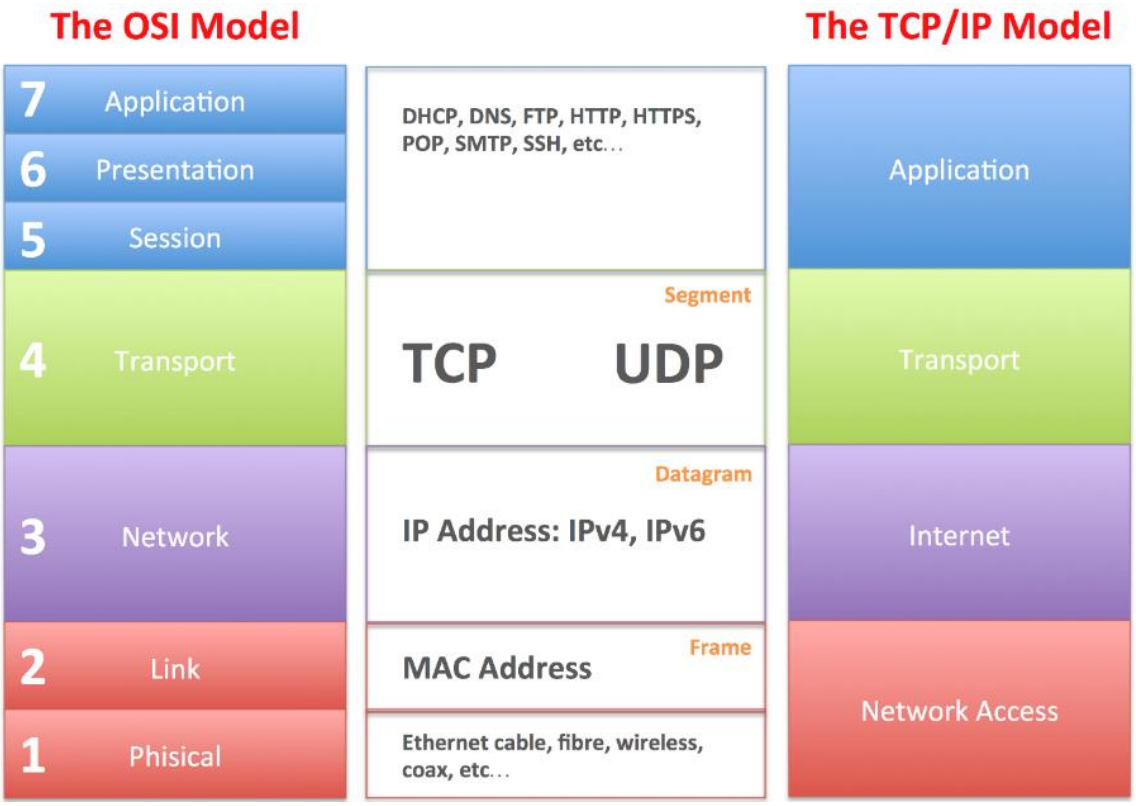



*Figure 1. 39 OSI model layers vs TCP/IP model*

| Differences | |
|---|---|
| **OSI Model** | **TCP / IP Model** |
| This model has 7 layers | This model has 4 layers |
| This is a conceptual model that defines network communication used by systems open to interconnection and communication with other systems. | This assists in determining how a particular computer should connect to the internet and how information can be sent between them. |
| This assists in determining how a particular computer should connect to the internet and how information can be sent between them. | This supports in the establishment of a connection between various sorts of computers. |
| ISO (International Standard Organization) created this in 1978. | ARPANET (Advanced Research Project Agency Network) created this in 1970. |
| Interfaces, services, and protocols are all clearly separated in this approach. | There are no apparent distinctions between services, interfaces, and protocols in this approach. |
| The OSI model includes the session and presentation layers. | The TCP model includes the session and presentation layers. |
| The Data Link Layer and the Physical Layer are two different layers in this model. | The Data Link Layer and Physical Layer are integrated into a single host-to-network layer in this model. |
| This model simplifies interfaces and standardizes them. | This model is complicated to set up and manage |

*Table 1. 4 OSI model layers vs TCP/IP model*

## 1.6 Types of Protocols

### 1.6.1 File Transfer Protocol (FTP)

FTP is an acronym for "File Transfer Protocol." FTP allows files or data to be transferred between two computers via the internet. FTP is a TCP-based network transport protocol. TCP ensures the reliability of FTP. This ensures that your data is sent to its intended location. For example, if someone anywhere in the world wanted to make their files available for others to download, all they had to do was upload them to an FTP server. Others can then connect to the FTP server and download the files via the FTP protocol.


*Figure 1. 40 FTP client sends and receive files from FTP client*

We can set up our own PC to operate as an FTP server as well. This can be done, on Microsoft Windows using Internet Information Service Manager.

There are 2 of ways to transfer files using FTP :

(1) By using standard internet browser

(2) By using FTP Client → There are a variety of FTP clients available, however "FileZilla" is the most popular free FTP client. When compared to utilizing a web browser, FTP clients offer a more graphical interface and overall experience.

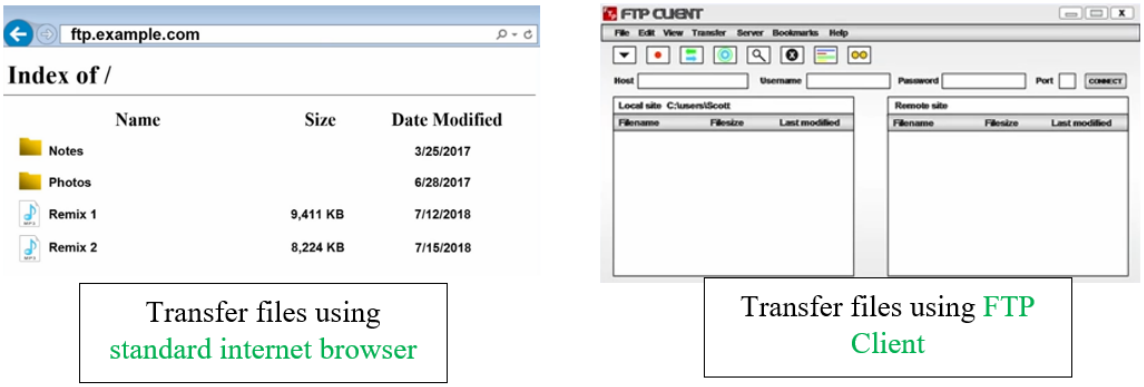



*Figure 1. 41 Two ways of transfer files using FTP*

**Uses of FTP :-**

- FTP is used by some businesses for important processes such as file exchange on a regular basis.
- FTP is ideal for uploading large files and transferring large numbers of files.
- FTP is the quickest and most straightforward method of transferring data and images.
- When sharing files with employees, clients, and consumers all around the world, FTP comes in handy.
- FTP also helps in the coordination of accountants, bookkeepers, and a variety of business owners.

### 1.6.2 Secure File Transfer Protocol (SFTP)

People can utilize the SFTP protocol to communicate sensitive data. SFTP is an acronym for “Secure File Transfer Protocol.” This is similar to FTP, but data is transmitted with encryption. SFTP, on the other hand, uses port 22 while FTP uses port 21.

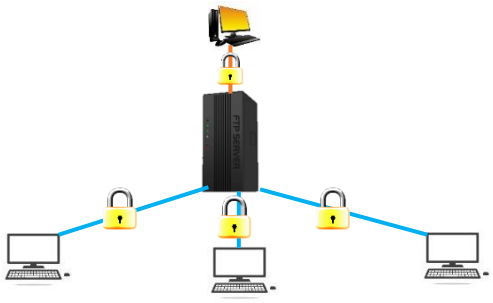


*Figure 1. 42 How SFTP simply looks like*

### 1.6.3 Trivial File Transmission Protocol (TFTP)

TFTP is an acronym for "Trivial File Transmission Protocol." Unlike FTP, this protocol does not use the internet, however SFTP does. This is used to transmit files between computers on a LAN. This is accomplished through the use of UDP. And this is not providing security like SFTP does.

### 1.6.4 Teletype Network (TELNET)

TELNET is an acronym for “Teletype Network.” TELNET is a network protocol that allows users to connect to a computer or a server remotely. TELNET is a basic command-line utility that may be launched on a computer to transmit commands to a server remotely. So, when a user connects remotely to a server through TELNET, all he has to do is type commands to tell the server what to do.

So, a user may use commands to launch programs, create folders, remove files, create files, transfer data, browse directories, start or stop services, and do everything from afar. TELNET can also be used to manage and configure other network devices such as switches and routers. TELNET can also be used to check if a server's ports are open or closed.

TELNET is compatible with different types of operating systems, including Windows and Mac OS. It is, however, mostly utilized on Linux and Unix systems. TELNET, as previously indicated, is a command-line utility with no graphical user interface. It's a simple text-oriented program that runs on a computer. In fact, even if the user does not have access to a computer, TELNET may be launched using a simple dumb terminal and all commands can be sent using a keyboard.

TELNET was created in 1969, before the internet, and thus has no encryption. As a result, security was not a problem because all commands were sent in clear text. As a result, TELNET has become outdated. However, some people use it on a LAN rather than via the internet. Furthermore, some people must use it when working with older devices.

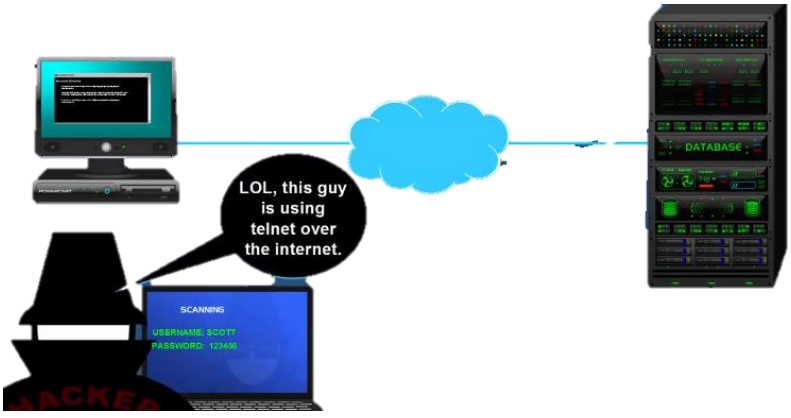



*Figure 1. 43 Hacker spectating the TELNET communication between server and PC*

### 1.6.5 Secure Shell (SSH)

SSH is the acronym for “Secure Shell.” This is a superior option to TELNET. SSH is used to connect to distant servers, such as TELNET, and it encrypts data sent over a network. SSH additionally uses password and public key authentication in addition to encryption. SSH performs the same functions as TELNET, but it is a more secure protocol, which is why it is now preferred over TELNET.

### 1.6.6 Simple Mail Transfer Protocol (SMTP)

SMTP is an acronym for “Simple Mail Transfer Protocol.” Emails are retrieved using the POP and IMAP protocols. SMTP, on the other hand, is used to send emails. This is done through the TCP protocol. When a user sends an email using an email client like Outlook, Mail-bird, or Thunderbird, it is sent directly to his email server. This server is also referred to as an SMTP server. The email will then be sent to the recipient's email server via the SMTP server. The email will be downloaded using the POP/IMAP protocol when the receiver logs into his email account. Alternatively, the recipient can simply view the email on the server without having to download it.

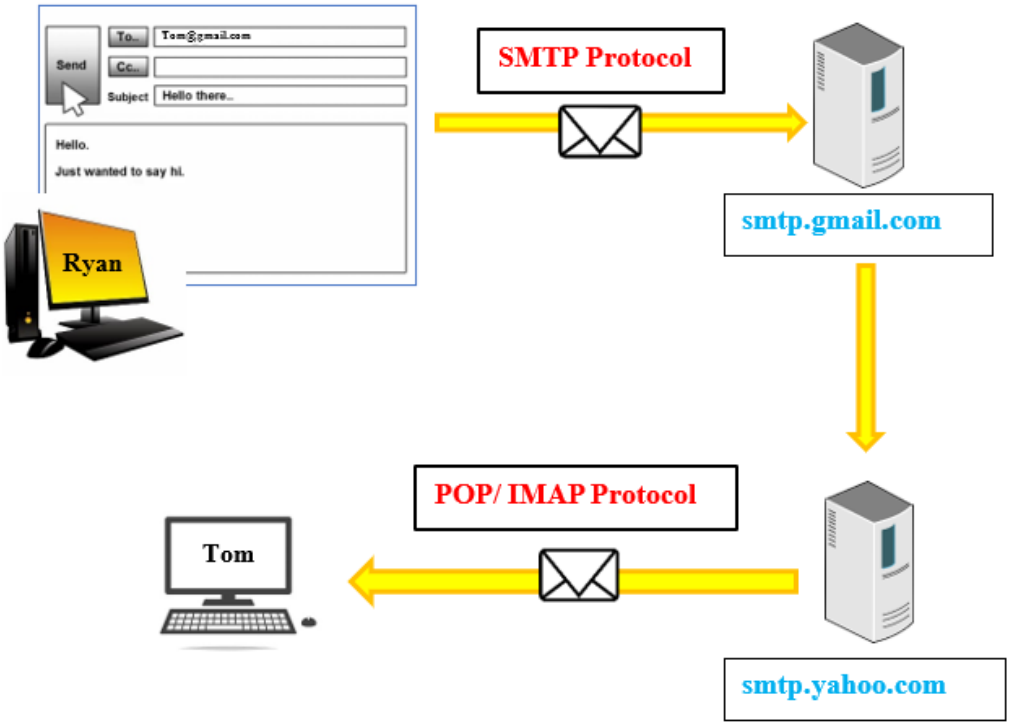



*Figure 1. 44 How SMTP simply works*

## 1.6.7 Post Office Protocol 3 (POP3)

POP 3 is an acronym for “Post Office Protocol 3.” This is more straightforward simpler than IMAP. POP3 is a protocol that allows to download emails from a server to a single device. Only the inbox folder is downloaded. As a result, no further folder is downloaded. Because there is no synchronization with this.

As shown in the figure below, two computers are configured to fetch the same email account. On these two machines, however, the folder arrangement is different. Because the folders in POP3 are not synchronized.

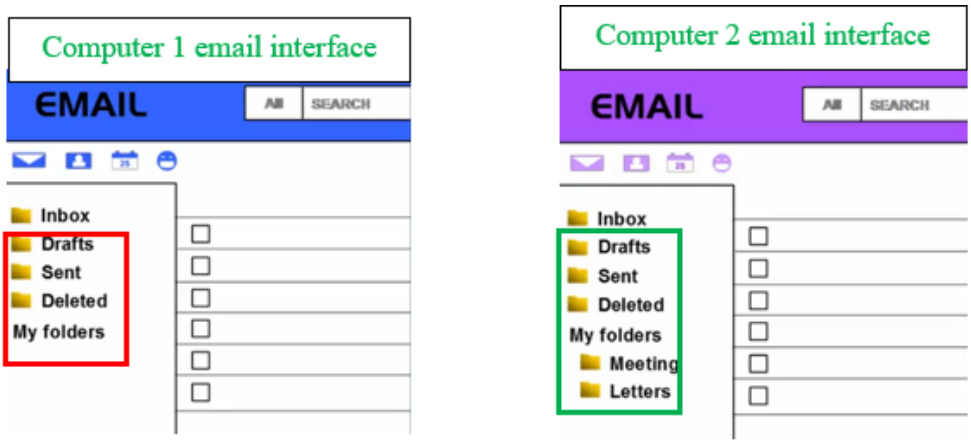



*Figure 1. 45 File arrangement difference between 2 PC which using POP 3*

Emails on the server will be erased once it downloads emails to the device. For instance, consider a user log into his email account using a mobile phone and downloads the emails. After that, that person won't be able to read the emails downloaded on his phone if he logs them on his PC. Because when emails are sent to a mobile phone, they are automatically erased. As a result, no email copies are stored on the server. However, the user can set it up to keep a copy on the server.

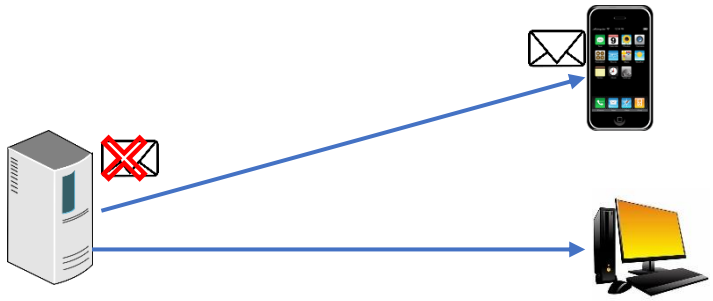


*Figure 1. 46 How emails on the server erased once it downloaded from a mobile phone*

### 1.6.8 Internet Message Access Protocol (IMAP)

IMAP is an acronym for “Internet Message Access Protocol.” IMAP is a protocol for receiving and sending email from a server to many devices. IMAP stores local copies of emails on the device rather than downloading them. To put it another way, emails are cached. As a result, users who do not have access to the internet will be unable to view their emails. (However, instead of caching the emails, the user can setup it to download them.)

IMAP also synchronizes all folders and the contents within them. Two PCs are configured to fetch the same email account, as indicated in the figure below. The folder layout on these two PCs is identical. Because IMAP's folders aren't synchronized. If a user deletes any folder of email account on one computer, the folder is also destroyed on the mail server and then on other computers too.

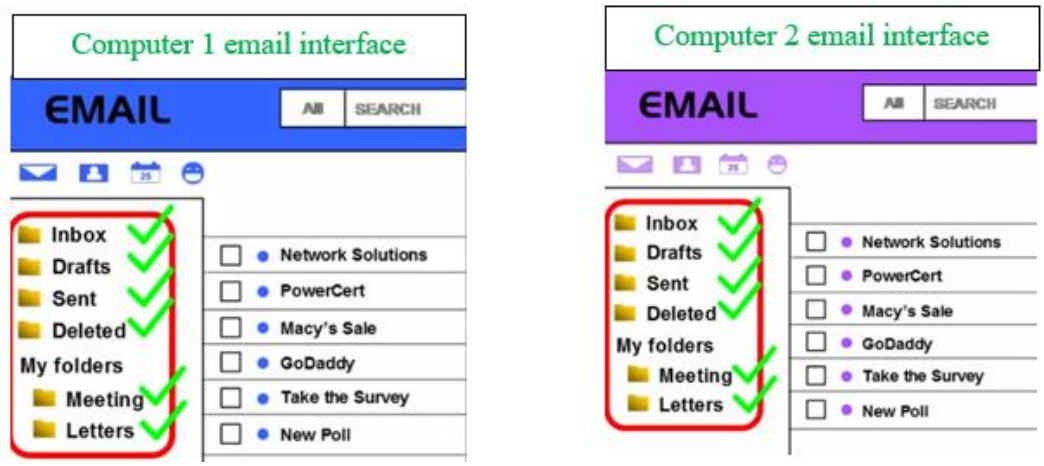



*Figure 1. 47 File arrangement difference between 2 PC which using IMAP*

### 1.6.9 Domain Name System (DNS) Protocol

Computers not using names in the same way that humans do. They employ IP addresses, which are numbers. As a result, network experts created DNS protocol to bridge the communication gap between computers and humans. DNS is an acronym for “Domain Name System.” This is a service that converts domain names into IP addresses. In other words, DNS allows people to find websites by utilizing human-readable hostnames rather than numeric IP addresses.

For example, the IP address 142.250.191.142 belongs to the "google.com" domain. As a result, people will not have to type this IP address into the address bar. Simply input google.com, and the DNS Server will look for the IP address for that domain name in its database. In a sense, DNS works like a phonebook. Millions of IP addresses do not need to be remembered. They only need to memorize the domain name.

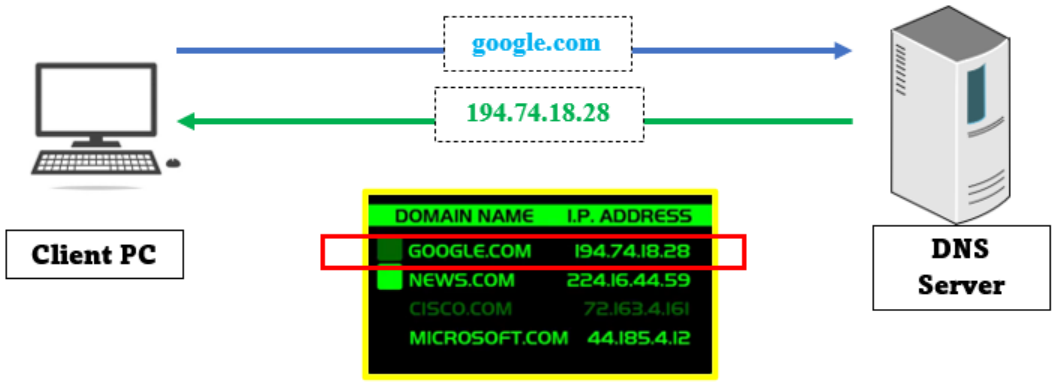



*Figure 1. 48 How DNS simply works*

### 1.6.10 Hyper Text Transfer Protocol (HTTP)

The HTTP stands for “Hyper Text Transfer Protocol.” This protocol is widely used in the world. On the Internet, the HTTP protocol is used to access web pages. HTTP is automatically placed to the beginning of a web URL when typing anything into a web browser. This means that the web browser is currently retrieving this page over the HTTP protocol.


*Figure 1. 49 How http is being used when web surfing*

HTTP sends all data in plain text. As a result, there isn't any encryption. If sensitive data, such as passwords or credit card numbers, were to be inserted, this would be a significant problem. This is when HTTPS comes into play.

### 1.6.11 Secure Hyper Text Transfer Protocol (HTTPS)

The HTTPS stands for Secure “Hyper Text Transfer Protocol.” The HTTPS protocol is used to browse web pages on the Internet while ensuring that they are encrypted. Because of this protocol, if a hacker tries to steal data, he will get nonsensical data.

For this HTTPS using one of these 2 protocols.

1) SSL (Secure Sockets Layer)

2) TLS (Transport Layer Security)

SSL (Secure Sockets Layer) :-

The SSL protocol is used to assure internet security. To protect data, Public Key Encryption is used. When a computer connects to a website via SSL, it will request that the website identify itself. The web server will then deliver a copy of its SSL certificate to the computer. This certificate is a digital certificate that is used to verify a website's legitimacy. In simple words SSL is used to inform computers that the website they are visiting is secure.


*Figure 1. 50 How SSL being used simply when visiting a web page*

TLS (Transport Layer Security) :-

This is SSL's successor, and it is based on the same specification. This protocol, like SSL, encrypts the data. Many websites now use HTTPS as their default protocol. Because websites that aren't secure are now flagged by Google.

### 1.6.12 Dynamic Host Configuration Protocol (DHCP)

DHCP is an acronym for "Dynamic Host Configuration Protocol." A DHCP server assigns unique IP addresses and configures other network settings automatically.

And there are two ways that a computer can be assigned an IP address.

1) Static IP

2) Dynamic IP

Static IP :-

In static IP, the user must manually assign an IP address to the device. This was the first approach used in the early days of networking. As a result, network administrator had to manually write an IP address for each computer network on the computer network configuration page. Network administrators had to type a subnet mask, default gateway, and DNS server in addition to an IP address.

If a new computer was added to the network, the network administrator had to repeat the procedure of assigning IP addresses. Also, while working with a large number of machines, network administrators need ensure that all IP addresses are unique. As a result, assigning a static IP address is quite challenging.

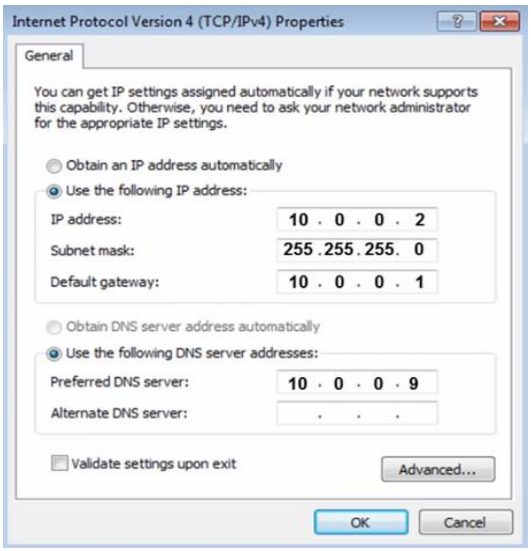



*Figure 1. 51 How Static IP is looked like in IPV4 properties*

Dynamic IP: -

In Dynamic IP, the machine receives an IP address from the DHCP server automatically. The DHCP server assigns a subnet mask, default gateway, and DNS server in addition to an IP address. So, dynamic IP addressing is the ideal option because it is automatic and makes network management much easier.

Another main aspect is that the DHCP server leases IP addresses for a specified period of time. As a result, the IP address does not belong to the computer. The purpose of the lease is to ensure that the DHCP server's scope does not run out of IP addresses. If one computer is withdrawn from the network, it will not take its IP address with it. When the IP address expires, it will be sent back to the DHCP server.

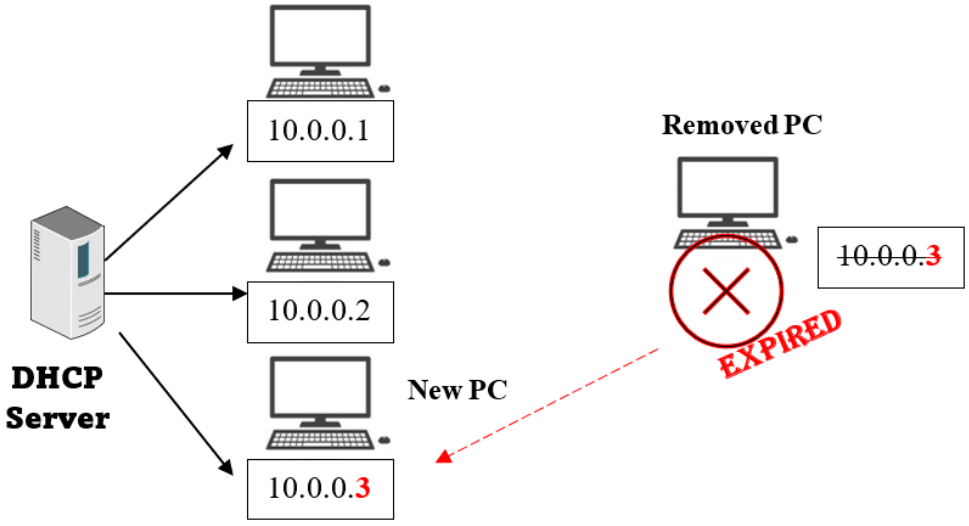



*Figure 1. 52 How Dynamic IP replace a used IP address*

If someone wants to provide a machine a specific IP address, they can make a reservation on the DHCP server. When a machine requests an IP address from the DHCP server's IP pool, reservation assures that the computer identified by its Mac address will always acquire the same IP address.

Special computers, such as network printers, servers, and routers, are given reservations. Because machines like this should always be assigned the same IP address. The DHCP service is often hosted on a server. It might be either a Microsoft or a Linux server. However, this can also be done using routers. If the router is a small office or home office router, it will have a built-in DHCP server.

## 1.6.13 Simple Network Management Protocol (SNMP)

SNMP is an acronym for “Simple Network Management Protocol.” SNMP is a protocol that can be used to monitor a network, detect network problems, and even configure remote devices. SNMP is an application layer protocol uses UDP port 161/162 to communicate. We can monitor network bandwidth and CPU consumption using SNMP.

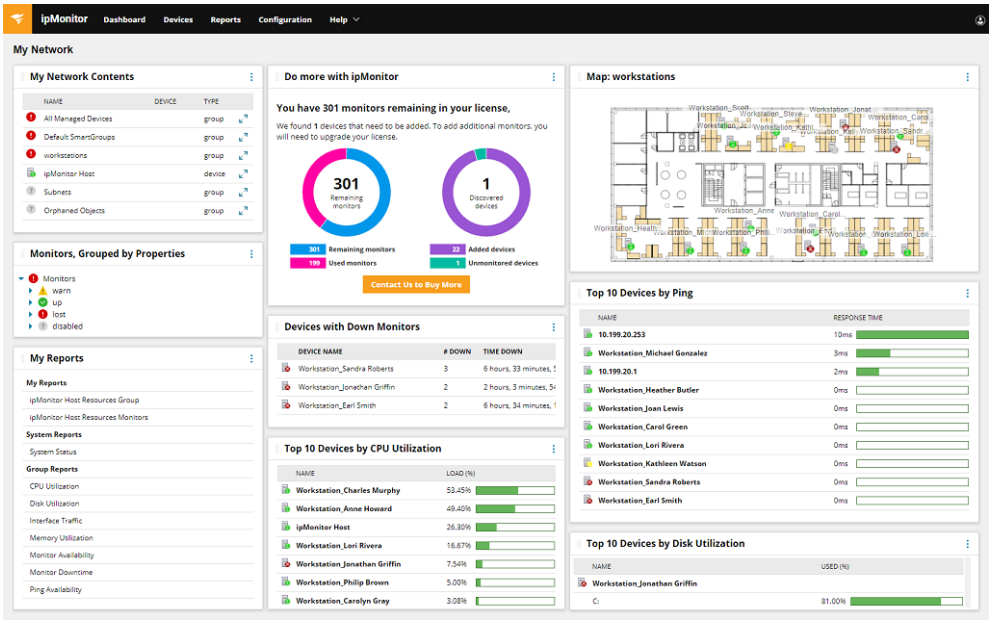



*Figure 1. 53 Network monitoring tool interface*

There are 3 parts of SNMP.

1) SNMP Manager → This is a centralized network monitoring system. Network Management Station is another name for it (NMS)
2) SNMP Agent → On a managed device, it is a software management software module. Network equipment such as PCs, routers, switches, and servers are examples of managed devices.
3) Management Information Base (MIB) → MIB is a database that contains information about the resources that need to be controlled. This data is arranged in a hierarchical order. It is made up of instances of objects, which are effectively variables.

There are 3 versions of SNMP.

SNMP v1 → Original Version of SNMP

SNMP v2c → Revised version of SNMP v1. Introduced with enhancements with community strings. Think community strings like password.

SNMP v3 → Improved SNMP with authentication and encryption. This version is more secure than previous one.

### 1.6.14 Internet Control Message Protocol (ICMP)

The ICMP is an acronym for "Internet Control Message Protocol." The basic purpose of ICMP is to see if data is getting to its intended destination. When network difficulties prevent IP packets from getting through, ICMP generates error messages. The ICMP protocol is commonly used on network devices like routers. ICMP is one of the most important system that allows the internet to function.

Ping is another name for ICMP. As a result, anyone can use the ping command to see if they're connected to a LAN or the Internet. Also, we can use ICMP to test DNS issues like name resolution.


*Figure 1. 54 Properties of data when pinging google.com*

## 1.6.15 Address Resolution Protocol (ARP)

ARP is an acronym for “Address Resolution Protocol.” ARP is a protocol for retrieving a device's hardware (MAC) address from its IP address. A MAC address is a physical address that is unique to each device that is issued to a Network Interface Card (NIC). When a device needs to communicate with another device over LAN, it requires that device's MAC address.

As below figure computer A wants to communicate with computer B. computer A knows IP address of B, but in order to communicate A still needs MAC address of B. Computer A will issue a broadcast message to the network, asking for the MAC address of any device with computer B's IP address. When computer B receives a message, it responds with its MAC address.

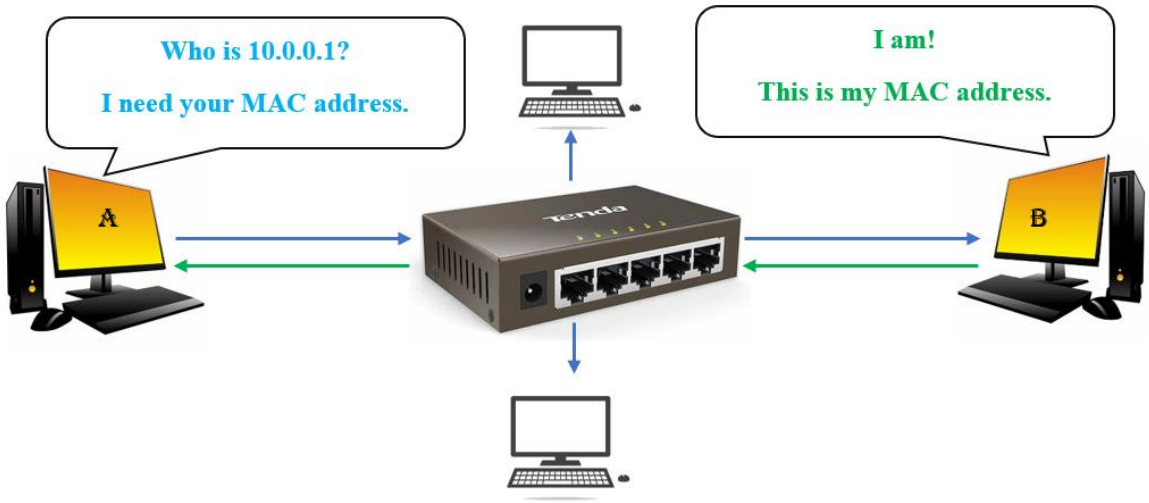



*Figure 1. 55 How ARP simply works*

Computers A and B can now communicate with one another. The information will then be saved in machine A's ARP cache. As a result, the next time A needs to know machine B's MAC address, it won't have to send a broadcast message to the network.

### 1.6.16 Reverse Address Resolution Protocol (RARP)

RARP is an acronym for “Reverse Address Resolution Protocol.” RARP is a protocol for determining a device's IP address based on its MAC address.

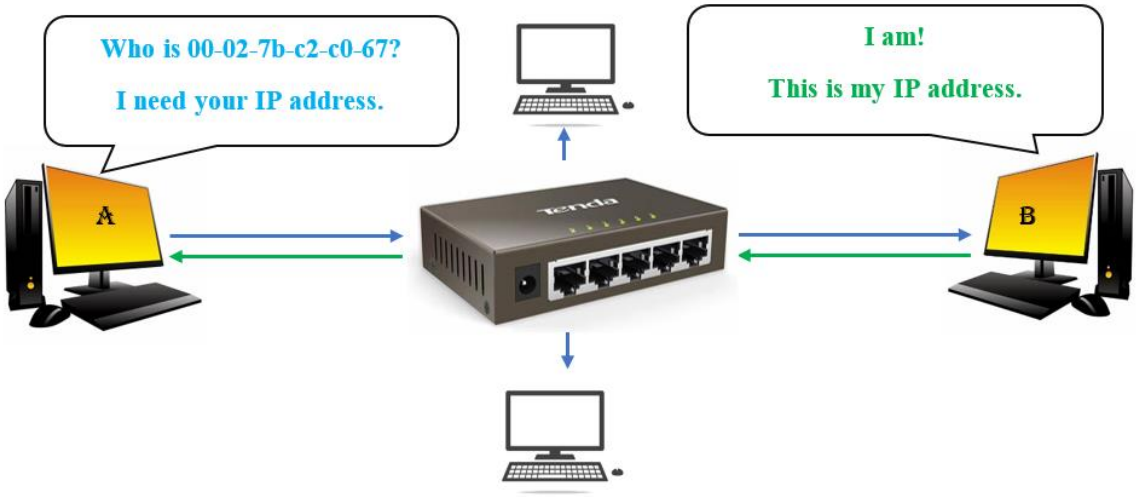



*Figure 1. 56 How RARP simply works*

| Differences | |
|---|---|
| **ARP** | **RARP** |
| ARP is an acronym for Address Resolution Protocol. | RARP is an acronym for Reverse Address Resolution Protocol. |
| ARP is using to find MAC address by using IP address. | RARP is using to find IP address by using MAC address. |
| Through ARP, 32-bit IP address mapped into 48-bit MAC address. | Through RARP, 48-bit MAC address mapped into 32-bit IP address. |
| ARP table is managed by local host. | RARP table is managed by RARP Server. |

*Table 1. 5 Differences between ARP and RARP*

## 1.7 Evaluate Principles and Protocols for SYNTAX Solutions Matara branch

As a logical and conceptual model, the OSI model developed. It was originally documented, with each layer's functionalities outlined. The protocols for each tier are then identified. The TCP/IP model, on the other hand, is implemented first with the predefined protocols and then described. As a result, the OSI model became a theoretical model, whereas TCP/IP became a practical model. Since, if I just wants to practically implement the model, I prefer to go with the TCP/IP model.

Another reason to choose TCP/IP model is because the OSI model's purpose is to create a generic standard for describing connection methods, layered architecture, services, interfaces, and protocols. But the TCP/IP model, on the other hand, strives to provide a secure and end-to-end transmission model. I chose the TCP/IP model since I only need to develop a model that is reliable and secure over the network.

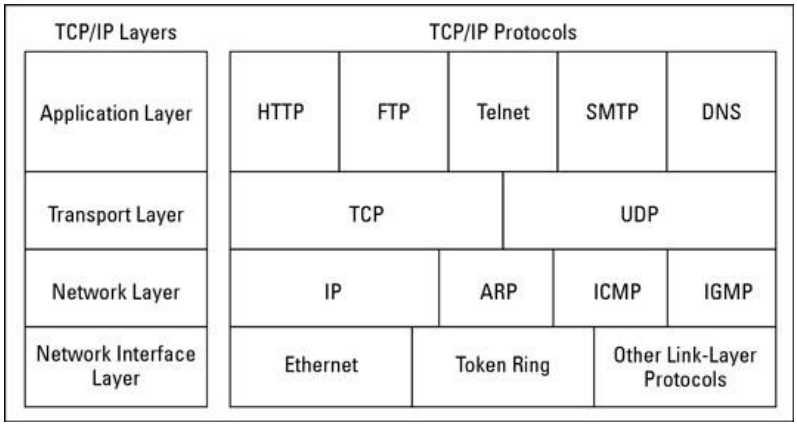



*Figure 1. 57 Protocols that are being used in each layer of TCP/IP model*

As above figure indicates I choose following protocols for each layer since they work fine with TCP / IP model. Since the Application Layer of the TCP/IP model corresponds to the Session, Presentation, and Application layers of the OSI Reference Model the HTTP, FTP, TELNET, SMTP and DNS protocols can be used. Since Transport Layer is where sessions are established, and data packets are exchanged between hosts the TCP and UDP protocols can be used in this layer. And the Network layer is where data is addressed, packaged, and routed among networks. Because of that ARP and ICMP protocols can be used in this layer.

## 1.8 IEEE standards

IEEE (Institute of Electrical and Electronics Engineers) is a nonprofit organization with it headquarter in New York in USA. The IEEE 802 networking standards have coordination with other international standards such as ISO (International Organization for Standardization). IEEE standards mainly helps to maintain international standards. IEEE 802 standards are defined for Ethernet LAN, MAN and WLAN. IEEE 802 networking standard standards cover the physical and data-link layer specifications for technologies such as Ethernet and WLAN.

The IEEE 802 standards assure the internet services follow a standard way to work smoothly. Otherwise, manufacturers could make network hardware that only compatible with certain computers. Hence, organizations and networking engineers would face difficulties to connect computers and other devices since networking equipment not using same set of rules. Because of IEEE standards connect multiple types of devices to multiple types of networks is possible. These standards making the networking management easy.

| Standard | Overview | Basic Concept |
|---|---|---|
| 802.1 | Bridging | This is the standard for LAN/MAN bridging and management.<br>Helps to routing, bridging and network to network communication. |
| 802.2 | Logical Link Control | Disbanded.<br>This is the standard for Logical Link Layer (LLC) connectivity.<br>Helps to error control and flow control over data frames. |
| 802.3 | Ethernet LAN | Helps to manage all forms of Ethernet media. |
| 802.4 | Token Bus LAN | Disbanded.<br>Helps to manage all forms of Token Bus media. |

| | | |
|---|---|---|
| 802.5 | Token Ring LAN | Disbanded.<br>Helps to manage all forms of Token Bus media. |
| 802.6 | Distributed Queue Dual Bus | Suppressed by 802.1D- 20004 standard.<br>Helps to exchange information between systems. |
| 802.7 | Broadband LAN practices | Disbanded.<br>Helps to manage broadband network media and other equipment. |
| 802.8 | Fiber Optics Practices | Disbanded.<br>Helps to manage fiber optic media used in token passing networks. |
| 802.9 | Integrated Services LAN | Disbanded.<br>Helps to manage integration of voice and data traffic over single network medium. |
| 802.10 | Interoperable LAN security | Disbanded.<br>Helps to manage network access control, encryption, certification, and other security topics. |
| 802.11 | Wi-Fi | This is the standard for wireless networking for many different broadcast frequencies. |
| 802.12 | High speed networking | Helps to manage variety of 100Mbps or plus technologies. |
| 802.13 | Not used | Not used |
| 802.14 | Cable broadband LAN and MAN | Disbanded.<br>This is the standard for designing network over coaxial cable based broadband connections. |
| 802.15 | Wireless Personal Area Networks | Helps to coexistence of WPAN with other wireless devices in unlicensed frequency bands. |
| 802.16 | Broadband Wireless Access | Helps to manage fixed and mobile broadband wireless access methods that used to create Wireless MAN. |

*Table 1. 6 IEEE standards*

### 1.8.1 IEEE 802.3 standard for LAN

Ethernet is a multi-access network in which set of nodes share a common link. Ethernet was created and developed in early 1970s at Xerox PARC. In 1983, IEEE ratified Ethernet as LAN standard which specification of IEEE 802.3. IEEE 802.3 standard is for a 1 persistent CSMA/CD (Carrier-Sense Multiple Access with Collision Detection) LAN. Whenever a station wants to transmit, it senses the carrier to determine the channel is idle or busy.

The topologies of Ethernet are Linear Bus and Star Bus. The signaling is mainly baseband signals which is digital signals. The transfer speed of Ethernet is 10Mbps, 100Mbps or above with using of Coaxial cables or UTP (Unshielded Twisted Pair) cables.

| Ethernet Type | Speed | IEEE Standard specification |
|---|---|---|
| Standard Ethernet | 10Mbps | IEEE 802.3 |
| Fast Ethernet | 100Mbps | IEEE 802.3u |
| Gigabit Ethernet | 1 Gbps | IEEE 802.3z |
| Ten Gigabit Ethernet | 10 Gbps | IEEE 802.3ae |

*Table 1. 7 IEEE 802.3 standard for LAN*

**Standard Ethernet :**

Originally, this was intended to be a 2.95Mbps system for connecting 100 computers over a 1km Ethernet connection. Later, Xerox, Intel, and DEC developed a 10Mbps Ethernet standard. As a result, standard Ethernet has a longer latency than Gigabit or Fast Ethernet. The 802.3 specification was developed by IEEE to produce a Standard Ethernet.

| Standard Ethernet Type | Cable Type | Using Topology | Advantage |
|---|---|---|---|
| 10Base5 | Thick Coax | Bus | Good for back bones |
| 10Base2 | Thin Coax | Bus | Cheapest system |
| 10Base-T | Twisted Pair | Star | Easy maintenance |
| 10Base-T | Fiber Optics | Star | Best between buildings |

*Table 1. 8 Standard Ethernet types and their properties*

**Fast Ethernet :**

IEEE created Fast Ethernet under the 802.3u specification. This is a version of Ethernet with 100Mbps data rate. Fast Ethernet was designed to compete with LAN protocols such as Fiber channel. The access mode method for fast Ethernet also same as standard Ethernet. Which is CSMA/CD for half duplex operation. For full duplex Fast Ethernet, there is no need of CSMA/CD. Since configuration and installment of Fast Ethernet is easy, it is more popular than Gigabit Ethernet.

**Gigabit Ethernet :**

IEEE created Gigabit Ethernet under the name 802.3z. Gigabit Ethernet provides the data rate of 1Gbps which is 1000Mbps. This is compatible with Standard or Fast Ethernet. The frame format is also similar to Standard Ethernet. Gigabit Ethernet operates in both half and full duplex mode like Fast Ethernet.

| Basis | Fast Ethernet | Gigabit Ethernet |
|---|---|---|
| Speed | 100Mbps | 1Gbps (1000Mbps) |
| Configuration | Simple | Complicated |
| Delay | Generate more delay | Less delay |
| Round trip delay | 100-to-500-bit times | 4000-bit times |
| Coverage limit | Up to 10km | Up to 70km |
| Successor of | 10Base-T Ethernet | Fast Ethernet |

*Table 1. 9 Gigabit Ethernet characteristics*

**Ten Gigabit Ethernet :**

IEEE created Ten Gigabit Ethernet under 802.3ae specification. This provides data rate of 10Gbps. Ten Gigabit Ethernet is compatible with Standard Ethernet, Fast Ethernet, and Gigabit Ethernet. The frame format of Ten Gigabit Ethernet is similar to Standard Ethernet. This allows to interconnection of existing LANS into MAN or WAN.

### 1.8.2 Choosing IEEE 802.3 LAN standards for Matara Branch

The latest Ethernet standard which is Ten Gigabit Ethernet (IEEE 802.3ae) won't be necessary since the SYNTAX solutions company is a 3-story building. Since this company works on software, 100Mbps Fast Ethernet connection is sufficient. Fast Ethernet installment for the company cost lesser than Gigabit and 10 Gigabit Ethernet and it is easy to configure compared to them. So as a Network Consultant I prefer to follow IEEE 802.3u standard, which involves Fast Ethernet networking system.

Fast Ethernet networks have a number of advantages over Standard Ethernet networks. Fast Ethernet can transmit data at speeds of up to 100 million bits per second. It's ten times quicker than older 10BaseT networks, making it ideal for high-speed applications like streaming video, streaming music, and data-intensive apps. This also has a better error detection and correction system. Fast Ethernet hardware is only slightly more expensive than 10BaseT hardware. Fast Ethernet is similarly simple to set up. Only a few 100Mbps network cards, a hub, and Category 5 twisted-pair cabling are required. It's simply that simple.

But to connect different departments' switches I recommend IEEE 802.3z Gigabit Ethernet standard. to transmit multiple clients' data and information to different departments and to server rooms,

Gigabit Ethernet system is sufficient since it has 1Gbps data frame rate. It will be challenging to store and transport data quickly when we have numerous machines sharing bandwidth in a server cluster. Gigabit Ethernet can transform the game and help the entire team avoid data bottlenecks. As a result, Gigabit Ethernet is often used as a backbone that businesses can rely on. This improves connection speeds and allows department PCs to share a single server.

### 1.8.3 Evolution of IEEE 802.11 standard for WLAN

IEEE 802.11, also known as Wi-Fi, has expanded from 2 Mbps to over gigabit speeds in the last 20 years, a 1000-fold increase in throughput. The standard has evolved over time, with additional protocols such as 802.11n, 802.11ac, and 802.11ax (Wi-Fi 6) being introduced . The world began to change as Wi-Fi (802.11) standards were released and implemented, as markets expanded, and new technology arose. Each new standard builds on the preceding one, improving speed and reliability.

Wireless LAN base version was released in 1997 with IEEE 802.11 specification. Unfortunately, the 802.11 specification only supported a maximum network bandwidth of 2Mbps which is too slow for most applications. Because of that, 802.11 wireless products are no longer manufactured. There have been 5 main different versions of WLAN. These 5 versions are referred below table.

| Standard | Year | Maximum data rate | Frequency |
|---|---|---|---|
| 802.11 | 1997 | 2Mbps | 2.4GHz |
| 802.11b | 1999 | 11Mbps | 2.4GHz |
| 802.11a | 1999 | 54Mbps | 5GHz |
| 802.11g | 2003 | 54Mbps | 2.4GHz |
| 802.11n (Wi-Fi 4) | 2009 | 600Mbps | 2.4GHz and 5GHz |
| 802.11ac (Wi-Fi 5) | 2014 | 1.3Gbps | 2.4GHz and 5GHz |
| 802.11ax (Wi-Fi 6) | 2019 | 10-12Gbps | 2.4GHz and 5GHz |

*Table 1. 10 Evolution of IEEE 802.11 standard for WLAN*

According to above table there are too many options and terminologies while trying to purchase new wireless networking equipment or a mobile device. Since Wi-Fi was initially introduced to the public in 1997, its standards have been growing at a rapid pace, resulting in faster speeds and improved network efficiency.

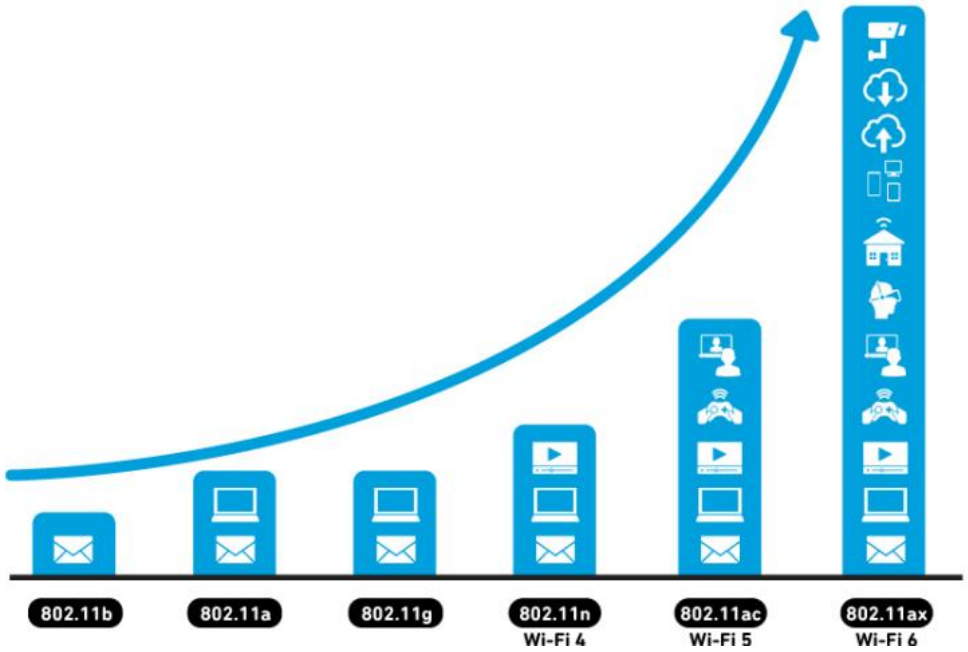



*Figure 1. 58 The evolution of Wi-Fi*

**Wi-Fi standards with their Characteristics :**

| Standard | Characteristics |
|---|---|
| 802.11 | * Base Version |
| 802.11b | * Least expensive version.<br>* Signal range is good.<br>* Slow maximum speed |
| 802.11a | * Fast maximum speed<br>* Higher cost.<br>* Because of the higher frequency, signal have more difficulty for penetration walls.<br>* Because of the higher frequency shortens the range of the network.<br>* Rarely used. |
| 802.11g | * Compatible with 802.11b networks.<br>* Attempts to combine the best of both 802.11a and 802.11b.<br>* Cost more than 802.11b. |
| 802.11n<br>(Wi-Fi 4) | * Fast maximum speed.<br>* This uses multiple antennas to hit high speed.<br>* Best signal range over earlier Wi-Fi standards.<br>* Resistant to outside signal interferences.<br>* Cost more than earlier standards. |
| 802.11ac<br>(Wi-Fi 5) | * 802.11ac standard supported devices are costly<br>* Useful for cloud storage services and streaming platforms. |
| 802.11ax<br>(Wi-Fi 6) | * Improves the coordination of transmitting data between router and several wireless devices. |

*Table 1. 11 Wi-Fi standards with their Characteristics*

### 1.8.4 Choosing IEEE 802.11 WLAN standards for Matara Branch

Single band routers use only 2.4GHz frequency for wireless signal. But dual band routers transmit both 2.4Ghz and 5GHz frequencies of wireless signals simultaneously. Hence dual band routers provide a better performance compared to a single band router. And also, dual band routers are easier to set up.

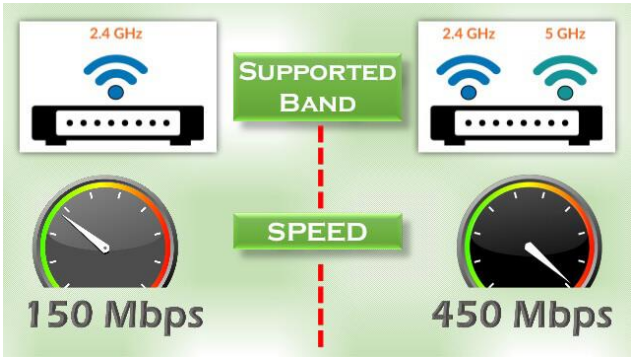



*Figure 1. 59 Speed difference between single band router and double band router*

Since IEEE 802.11n standard supports both frequencies of 2.4Ghz and 5GHz and the maximum data rate 600Mbps is more than enough for a software company. The 2.4GHz band is used to communicate with older pre-n devices, whereas the 5GHz band is used to communicate with other n devices. And since this networking standard can communicate with other all standards, this standard would be beneficial to use.

The 802.11n standard allows users to broadcast and receive several data streams at the same time. This is referred to as MIMO (Multiple-Input Multiple-Output). Wi-Fi 4 devices use two or more antennae because of this. Because the wireless link quality is improved on 802.11n, less retries are required due to failed transmissions. But 802.11n standard cost higher than earlier standards. Despite to that, this provides best signal range over earlier Wi-Fi standards and resistant to outside signal interferences.

The security of products that use the 802.11n standard is excellent. Intruders should find it difficult to gain unauthorized access due to the recent security features. Our wireless LAN can have the finest protection possible when combined with the latest wireless intrusion detection tools.

(Mareco, Benefits of Using 802.11n Wifi Access Points 2021)

## 1.9 Network Topologies

Network topology is the arrangement of linkages linking pairs of nodes in a network. In other words, network topology describes how computers in a computer network are connected or related to one another. A node can have one or more links to other nodes, and the linkages can have a number of shapes. Only the configuration of links between nodes determines network topology.

There are 2 types of Topologies,

1) Physical Topology
2) Logical Topology

**Physical Topology:-**

The method by which computers communicate with one another via cables. In simple words the way computers connected physically.

Ex:- Bus, Ring, Star, Mesh, Hybrid

**Logical Topology :-**

The way data flows from one computer to the next within a computer network is known as logical topology.

For example, a network can be physically different type, but logically could work as the same. Or in contrast physically may same, but logically can be different.

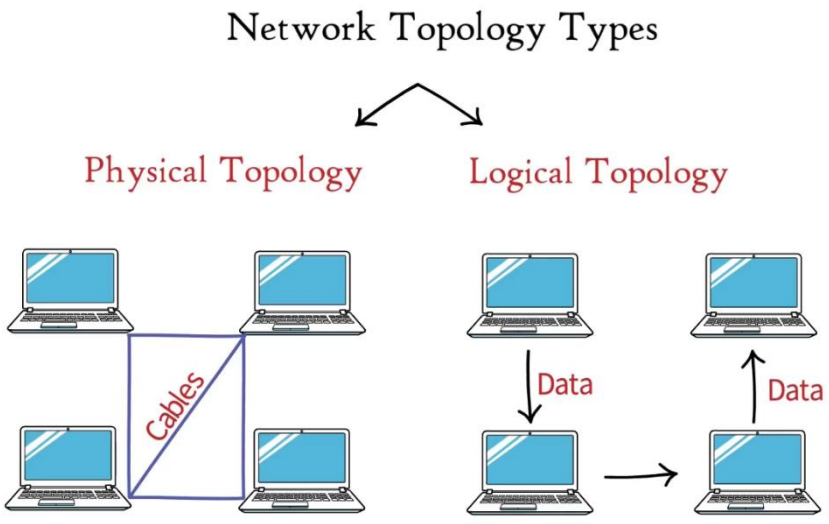



*Figure 1. 60 Two types of network topology*

## 1.10 Physical Topologies

The data in Network Layer is in the form of IP packets. In the Data Link Layer, IP packets are bundled into frames. The frames are subsequently transmitted into the transmission media via the Physical Layer. As a result, data is transferred in frames from one computer to another.

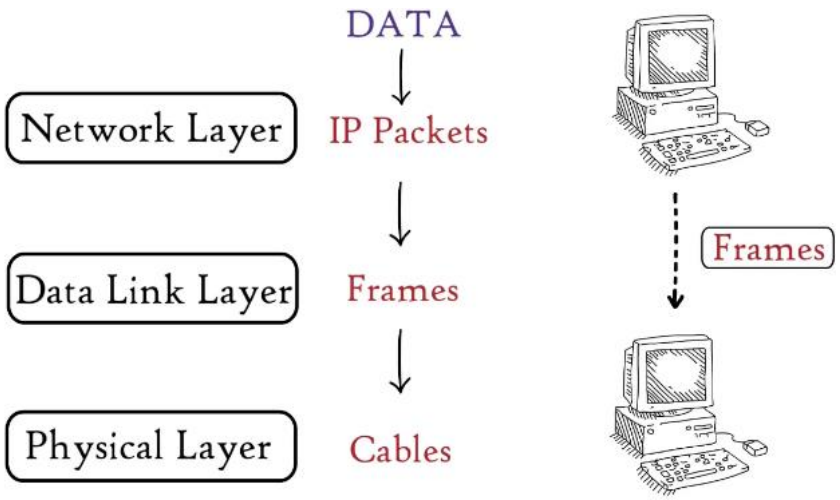



*Figure 1. 61 How data is being sent in each layer*

### 1.10.1 Bus Topology

All devices in a Bus Topology are connected to a central cable called Bus. Taps and Drop Lines link the gadgets to the bus. The connectors are known as taps or T-connectors. The wires that connect the computers to the bus are known as drop lines. The Terminator signifies the beginning and ending of the network.

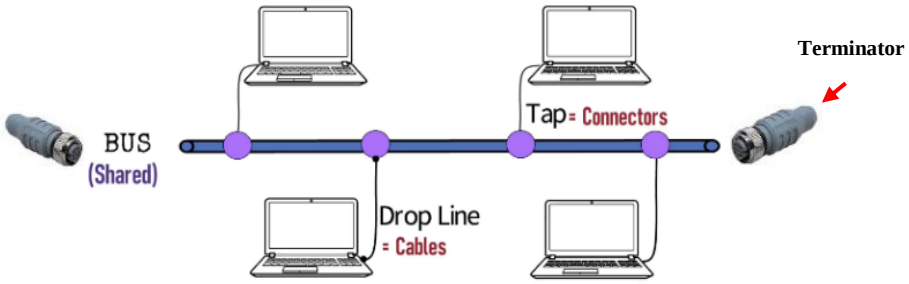



*Figure 1. 62 Simple diagram of Bus Topology*

If a computer delivers data frames to another computer in this architecture, the frame is received by all other computers connected to the same central cable. That means, the message is broadcasted. Other computers can hear what the first computer is saying, in other words. Only the targeted machine, however, accepts the data frame. The destination MAC address in the received frame is checked by other computers, and they reject the frame.

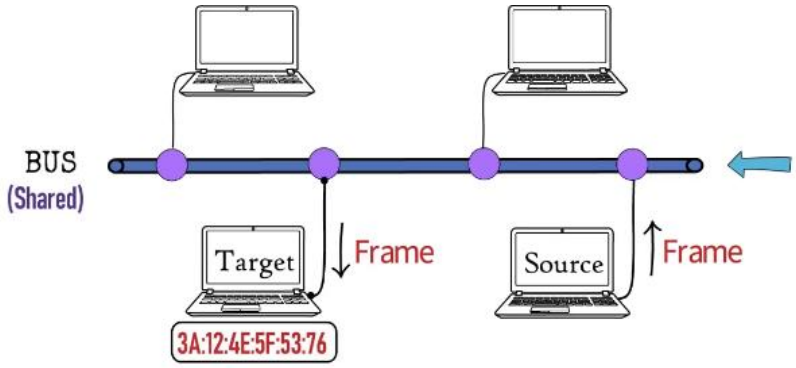



*Figure 1. 63 How frame is sent from source PC to Target PC*

Example of bus topology is Ethernet LANs.

**Advantages :**

- Less cabling:- So it's easy to install, less expensive

**Disadvantages :**

- Limited Computers :- The intensity of the signal drops as the length of the central cable and the number of taps increase. As a result, in a bus topology, only a limited number of computers can be connected.
- Little fault tolerance:- All computers in this design rely on the central connection for data delivery. As a result, if the central cable fails, the entire network is brought to an end.

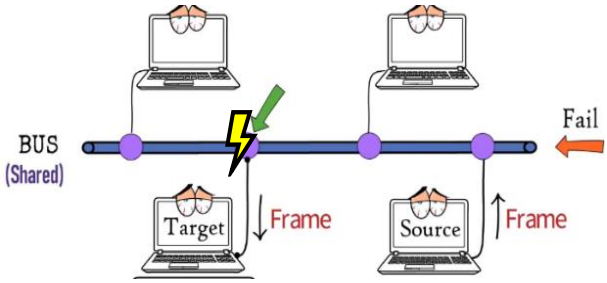



*Figure 1. 64 Bus Topology little fault tolerance example*

- Security risks:- On shared media, all machines can listen what the other machines are communicating.
- Difficult Installation:- We must break the connection and insert a new Tap to connect it with the new computer if we want to add a new machine to the network.
- Data Collision:- Only one computer can transfer data at a time in a bus topology. As a result, other computers must wait while one computer sends a file to another computer. If multiple computers communicate data at the same time, the data will collide and get corrupted. Data should be retransmitted in this scenario. When there are a lot of machines on a network, it slows down the network and increases the likelihood of data collisions. One of the reasons why bus topology is seldom used in modern computer networks is because of this. The use of an Access Control Protocol can prevent clashes. CSMA/CD is an example (Carrier Sense Multiple Access with Collision Detection)Ex:- CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

## 1.10.2 Ring Topology

Each computer in the Ring Topology forms a ring by connecting to other computers. As a result, there is neither a beginning nor an end. Data sent from one computer travels in a circular path until it reaches its final destination. Data only goes in one direction in this topology. It lowers the likelihood of data packet collisions.

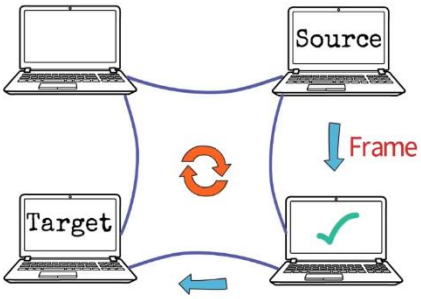



*Figure 1. 65 Simple diagram of Ring Topology*

Example of ring topology is Token Ring.

**Advantages :**

- Easy Installation with less Cabling.
- Less chance of frame collisions.
- East to Troubleshoot.:- All we have to do is find the machine that has stopped receiving data from its upstream neighbor.

**Disadvantages :**

- Less Security:- Between the source and destination, frames must flow through all computers.
- Slower Transmission:- Because frames must flow through all computers between the source and destination, it makes data transfer slower than the Star Topology.
- Little fault tolerance:- Because all computers are connected in a closed loop, if one computer goes down, the entire network goes down.
- Difficult to Reconfigure:- To add or remove computers, we must break the ring. Physical ring topology is rarely used as a result of this. However, logical ring topology is utilized in some manner.

### 1.10.3 Token Ring Topology

IBM created Token Ring for LAN in the 1980s. Physical ring topology is not used in token rings. Physical Star Topology and logical Ring Topology are utilized. Even though the network has a Star Topology from the outside, the frames travel in a circular pattern.

A Token Ring network is known for its determinism. This means that each linked computer has access to transmit data at predetermined periods. As a result, a network might have one physical topology and another logical topology at the same time.

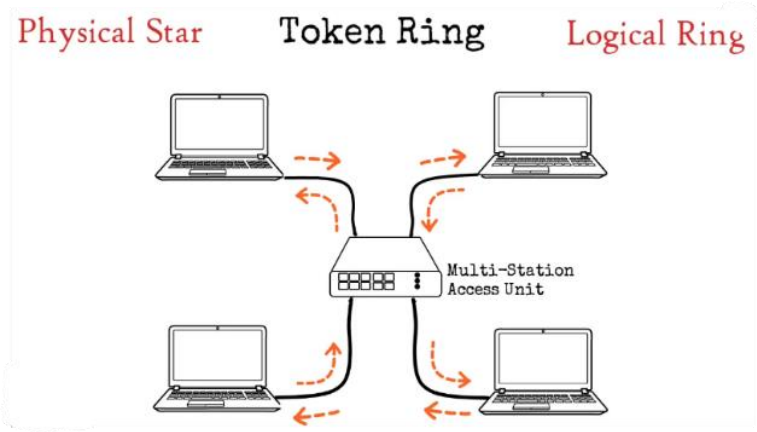



*Figure 1. 66 Simple diagram of Token Ring Topology*

Token Ring utilizes a token passing mechanism, in which the frame is referred to as Token. This Token keeps the ring in circulation. If a computer needs to send data frames, it keeps the token and sends the data frame. The token is released onto the network once the transmission is completed.

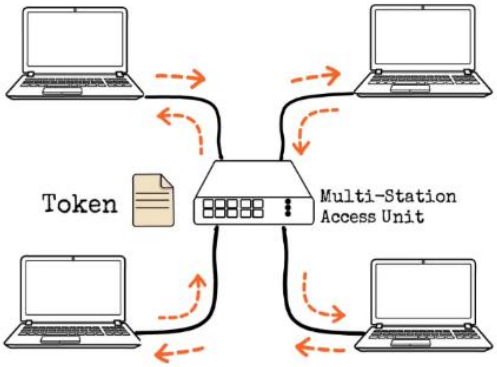



*Figure 1. 67 Token circulation in Token Ring Topology*

**Advantages**

- As opposed to Ethernet (CSMA/CD), the token passing access technique does not generate collisions.
- Token ring allows for larger frame size than Ethernet.
- When the token ring was first launched, it was quicker than Ethernet.

### 1.10.4 Star Topology

Computers connected to a central device, a switch, or a hub in a Star topology. Point-to-point communication links connect them to a switch or hub. A dedicated link or a cable connects the two devices in a point-to-point connection. It is inaccessible to other devices.

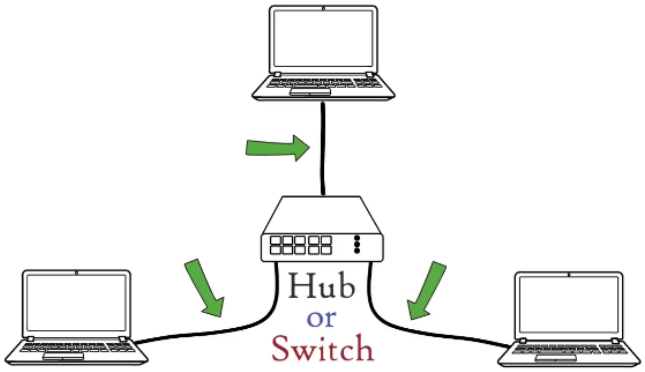



*Figure 1. 68 Simple diagram of Star Topology*

If a computer wants to send a data frame to another computer in this topology, it must first go through the central device. Depending on the type of central device utilized, the received data frame is subsequently broadcast or unicast towards the target computer. The term "broadcast" refers to the distribution of data to all linked devices. The term "unicast" refers to data delivery to only the target device.

The receive frame is broadcast to all linked computers if the central device is a hub. As a result, hub operates as a multiport repeater. As a result, Hub broadcasted the frame. In addition, Hub only permits one device to communicate at a time.

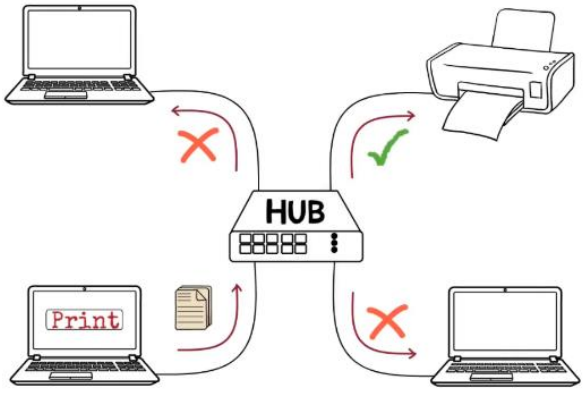



*Figure 1. 69 Limitation when frame is sent through a Hub*

The frame has a destination MAC address which is unique to every computer present in the network. As a result, only the target computer accepts the frame, while the other computers reject it. As a consequence, the hub broadcasts the received data, and increases unnecessary data traffic in the network.


*Figure 1. 70 How destination MAC is being a component of a frame*

A switch is utilized to get over this limitation. The MAC addresses of all devices connected to the switch's ports are saved. It's known as a switch table. Because the frame's date contains the destination MAC address, the switch can use the switch table to guide the frame to its intended destination without broadcasting it. As a result, unicast the frame.

Furthermore, while the computer is transferring a file to the printer, computers A and B can communicate with one another without interfering with the computer-printer link. Hence, Switch Unicast the frame. Simultaneous communication is possible because to the Switch connection.

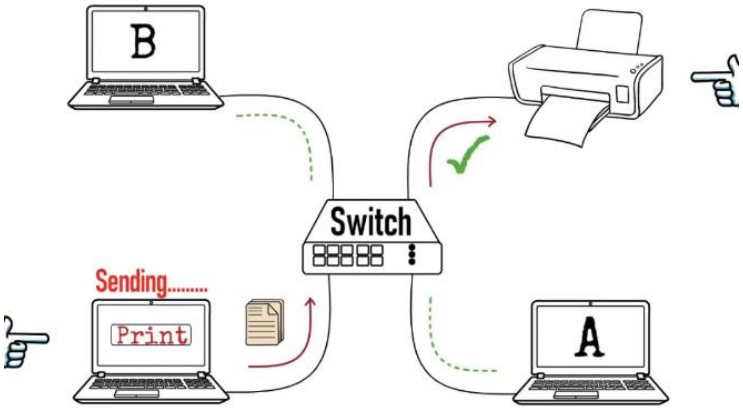



*Figure 1. 71 Advantage when frame is sent through a Hub*

Example of star topology is High Speed LANs.

**Advantages :**

- Less Expensive:- In Star Topology, only 1 input/output cable and port are needed to connect each device to the central device. (Less expensive than the mesh topology.)
- Easy to Reconfigure:- We can add or remove devices simply by connecting/disconnecting 1 cable.
- Good Fault Tolerance:- If one cable connecting to the central device fails, only one communication link goes down. Not the entire network.
- Easy Fault Detection:- We only need to locate the computer. Which not receiving the frames.

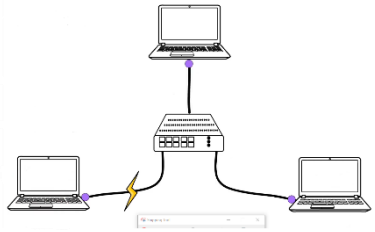


*Figure 1. 72 Star Topology little fault tolerance example*

**Disadvantages :**

- Central Device dependency:- In this topology all computers depend on the central device for data transmission. So, if central device fails it paralyzes the whole network.
- Limited computers count:- Numbers of computers in the network is limited by the number of input/output ports in the central device.

### 1.10.5 Mesh Topology

In a fully connected Mesh Topology, each device has a point-to-point link to every device in the network.

There 2 types of Mesh Networks.

1) Fully connected Mesh:- Every computer will be dedicatedly connected to each other.
2) Partially connected Mesh:- Some computers will be partially connected to each other.

*Figure 1. 73 Simple diagram of Mesh Topology*

The following formula can be used to calculate the number of cables required for each device. Data can only move in one direction in Simplex Links. As a result, one link is utilized to send data while the other is used to receive data from the computer next to it.

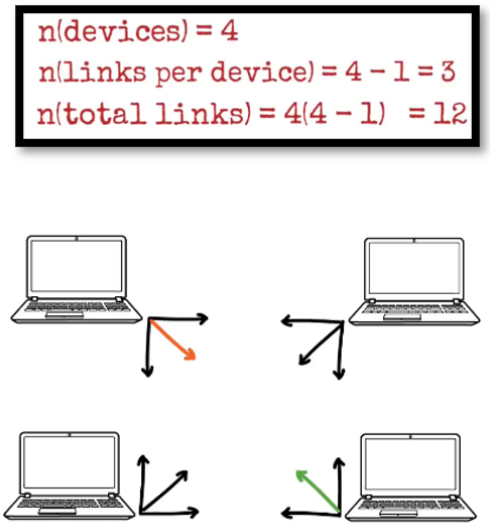
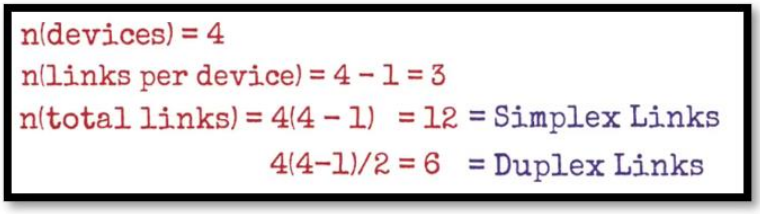



*Figure 1. 74 Adding 4 PCs for formula and physically how it is looks like*

The term "duplex" refers to a link that allows data to flow in both directions. As a result, we can use one Duplex Link instead of two Simplex Links. As a result, the total number of Duplex Links can be calculated using the formula below.



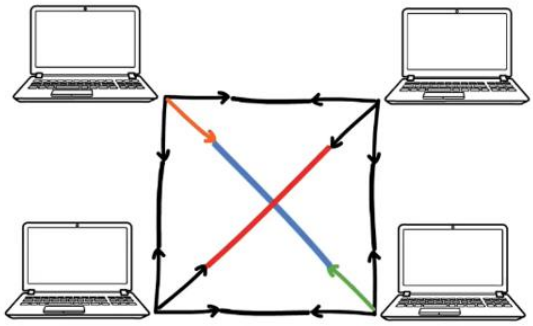



*Figure 1. 75 Adding 4 PCs for formula and physically how it is looks like*

Example of mesh topology is regional telephone offices.

**Advantages :**

- No Traffic problems:- The dedicated point-to-point link prevents traffic congestion that might occur when a link is shared by multiple devices.
- Privacy and Security:- Since other computers cannot guarantee the privacy and security of the messages sent between two devices, the dedicated point to point link ensures that the communications shared between the two devices remain private and secure.
- Good Fault Tolerance:- If one link fails it doesn't affect the whole network.

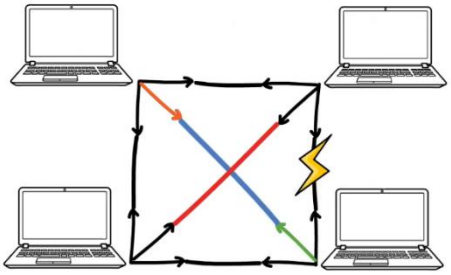


*Figure 1. 76 Mesh Topology little fault tolerance example*

**Disadvantages :**

- Limited computers count:- If there are 10 computers to link, the total number of Duplex Links required is 45, and each device must have nine input/output ports, making management harder and increasing costs.


*Figure 1. 77 Adding 10 PCs for formula*


*Figure 1. 78 How physically looks like when adding 5, 6 and 9 PCs as a Mesh Topology*

- Difficult Installation:- Since each device is connected to every device, the installation is difficult.
- Expensive:- Multiple input output ports and large number of cables increase the cost and make it expensive.
- Large Space:- More cables in Mesh Topology consume large space too.

## 1.10.6 Hybrid Topology

A Hybrid Topology is made up of multiple topologies that are linked together. Every topology has advantages and disadvantages. As a result, we should consider the cost, convenience of installation, ease of maintenance, and cable fault tolerance while choosing a physical topology for a network.

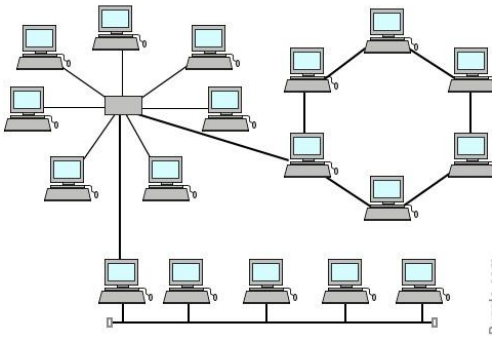


*Figure 1. 79 Start Topology, Ring Topology and Bus Topology interconnected as Hybrid Topology*

For example, if one office department has a Ring topology and another has a Bus topology, connecting the two will result in Hybrid Topology. Hybrid networks are most commonly seen as Star - Ring and Star - Bus networks.

Hybrid Star -Bus Topology :- In large networks, the Star-Bus Topology is paired with the linear Bus. The linear Bus acts as a backbone in these situations, connecting several Stars.

Hybrid Star - Ring Topology :- This is a hybrid of the Ring and Star Topologies. The primary hub in a Star - Ring connects the hubs in a Star design.

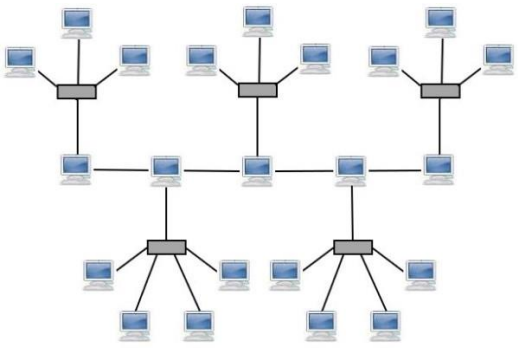


*Figure 1. 80 Hybrid Star -Bus Topology physically looks like*

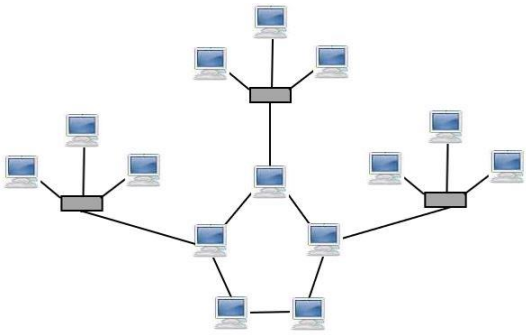


*Figure 1. 81 Hybrid Star -Ring Topology physically looks like*

**Advantages :**

- Reliability :- Unlike other networks, its structure makes fault identification and troubleshooting simple.
- Scalability :- By adding new components, it is simple to expand the network's size without disrupting the present architecture.
- Flexibility :- Hybrid networks can be developed to meet the needs of the company while also maximizing the use of existing resources.

**Disadvantages :**

- Complexity of the design :- The design of Hybrid Topology is one of its biggest drawbacks. This style of architecture is difficult to create, and designers have a tough challenge to create it. And also, the process of configuration and installation is not easy in this type of architecture.
- Costly Hubs :- Hubs, which are used to connect two separate networks, are quite expensive. These hubs differ from traditional hubs in that they must be sophisticated enough to deal with a variety of architectures and must continue to function even if a portion of the network is down.
- Costly infrastructure :- Hybrid architectures require a lot of wires, cooling systems, and sophisticated network devices because they are usually larger in scale.

## 1.11 Hierarchical Topologies

A Hierarchical Network design involves dividing the network into discrete layers (Basically 3-layer architecture or 2-layer architecture). Each layer provides specific functions.

### 1.11.1 Three−Tier (3 Layer) Hierarchical Network Model

When we take a switch, it has multiple works to do the same time. So, we can divide the workload by hierarchical model. This helps the network designer to optimize network hardware and software easily going through layers.

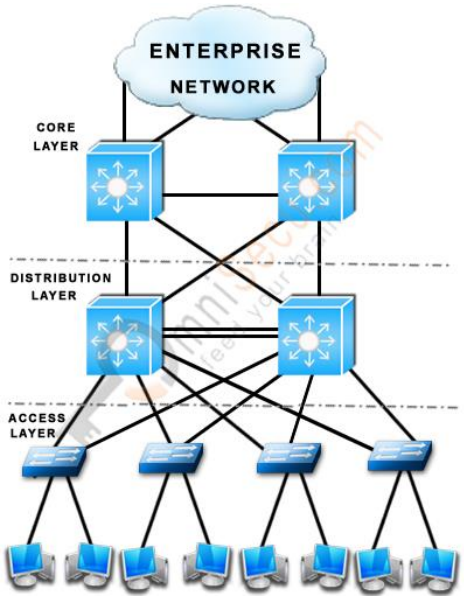



*Figure 1. 82 Three−Tier (3 Layer) Hierarchical Network Model*

There are 2 routers for each Distribution and Core Layer to keep redundancy if 1 router goes down

**Access Layer :**

Access layer includes access switches which are connected to the end devices (Computers, Printers, Servers, etc.). But these switches don't do high amount of workload as it was used to do in separate. That means this is lack of processing in this layer. Access layer switches ensures that packets are delivered to the end devices.

**Distribution Layer :**

The Distribution Layer is located between the access and core layers. This is also contained with switches with routing ability. The distribution layer is the smart layer in the three-layer model. Routing, ACL (Access Control List), filtering, and QoS policies are managed at the distribution layer.

Routing - Routing is the process of selecting a path for traffic in a network or between or across multiple networks in correct direction. It can determine the path of the traffic.

Ex:- If 1 computer go for internet, from this layer can be define the rules for it.

Access Control List (ACL) - Refers to a specific set of rules used for filtering network traffic.

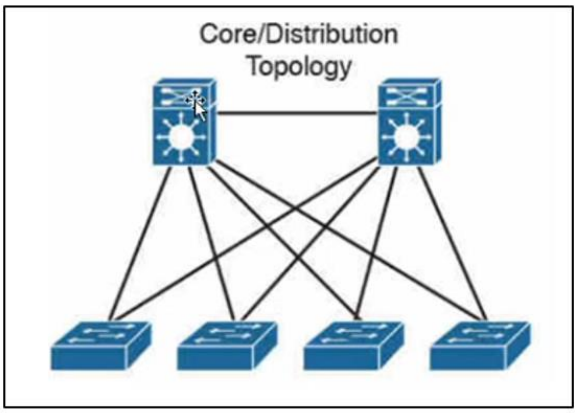
**Core Layer :**

Most of processing is done by Core Layer. Core Layer consists of biggest, fastest, and most expensive routers with the highest model numbers and Core Layer is considered as the backbone of networks.

Core Layer routers are used to merge geographically separated networks. The Core Layer routers move information on the network as fast as possible. Major job of this layer is sending the packets to the internet in fast. Core network devices manage the highest-speed connections, such as 10 Gigabit Ethernet or 100 Gigabit Ethernet. We can put ACL on this layer too. But we don’t do that because we focus on the high speed here.

## 1.11.2 Two−Tier (2 Layer) Hierarchical Network Model

This is known as Collapsed Network Model, The three-tier hierarchical design maximizes performance, network availability, and the ability to scale the network design. However, many small enterprise networks do not grow significantly larger over time. Therefore, a two-tier hierarchical design where the core and distribution layers are A "collapsed core" is when the distribution layer and core layer functions are implemented by a single device. That's why this topology is called Collapsed Core. The core and the distribution layers both run on the same physical switches. The primary motivation for the collapsed core design is reducing network cost, while maintaining most of the benefits of the three-tier hierarchical model.



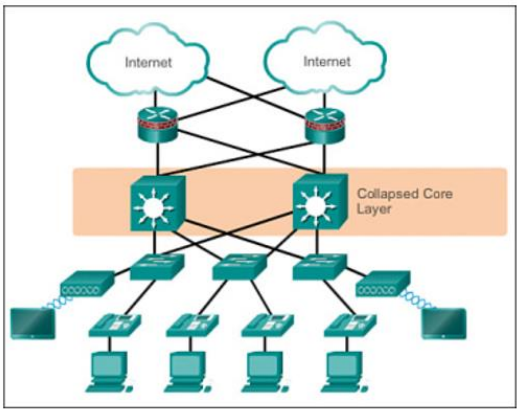




*Figure 1. 83 Two−Tier (2 Layer) Hierarchical Network Model*

### 1.11.3 Choosing Network Topology for Matara Branch

The Bus and Ring topologies are difficult to reconfigure after installation. And there are lot of security risks in these networks. Because of that, for software company those both network topologies useless. But as described before there are lot of unique advantages of each topology as well as disadvantages.

Since SYNTAX Solutions company has many employees, the Mesh Topology isn't fulfilling the network requirement of the company. Because as described this topology is difficult to manage with many numbers of computers.

I Choose Hybrid Topology to use as the network topology for this company. There are several reasons to choose this topology as follows.

- Reliability :- Unlike other networks, its structure makes fault identification and troubleshooting simple. The part of the network where the issue is detected can be isolated from the remainder of the network, allowing necessary corrective actions to be done without disrupting the rest of the network's operation.
- Scalability :- By adding new components, it is simple to expand the network's size without disrupting the present architecture.
- Flexibility :- Hybrid networks can be developed to meet the needs of the company while also maximizing the use of existing resources. Special attention can be given to nodes with a large volume of traffic as well as a high risk of failure.
- Effectiveness :- Because a hybrid topology combines two or more topologies, we can build it so that the constituent topologies' strengths are maximized while their weaknesses are minimized. For example, we saw that Ring Topology has good data reliability (due to the use of tokens) and Star Topology has high tolerance capability (due to the fact that each node is not directly connected to the others but rather through a central device), so these two can be combined to form a hybrid Star-Ring topology.

Below figure illustrate a part of LAN network design for SYNTAX Solution's Matara branch which I created. As in the figure I implemented Bus Topology network for each department and also for Server room. And I used Start Topology to interconnect every department and the Server room. Hence, I used Star- Bus Hybrid Topology effectively for SYNTAX Solutions Matara branch LAN network.

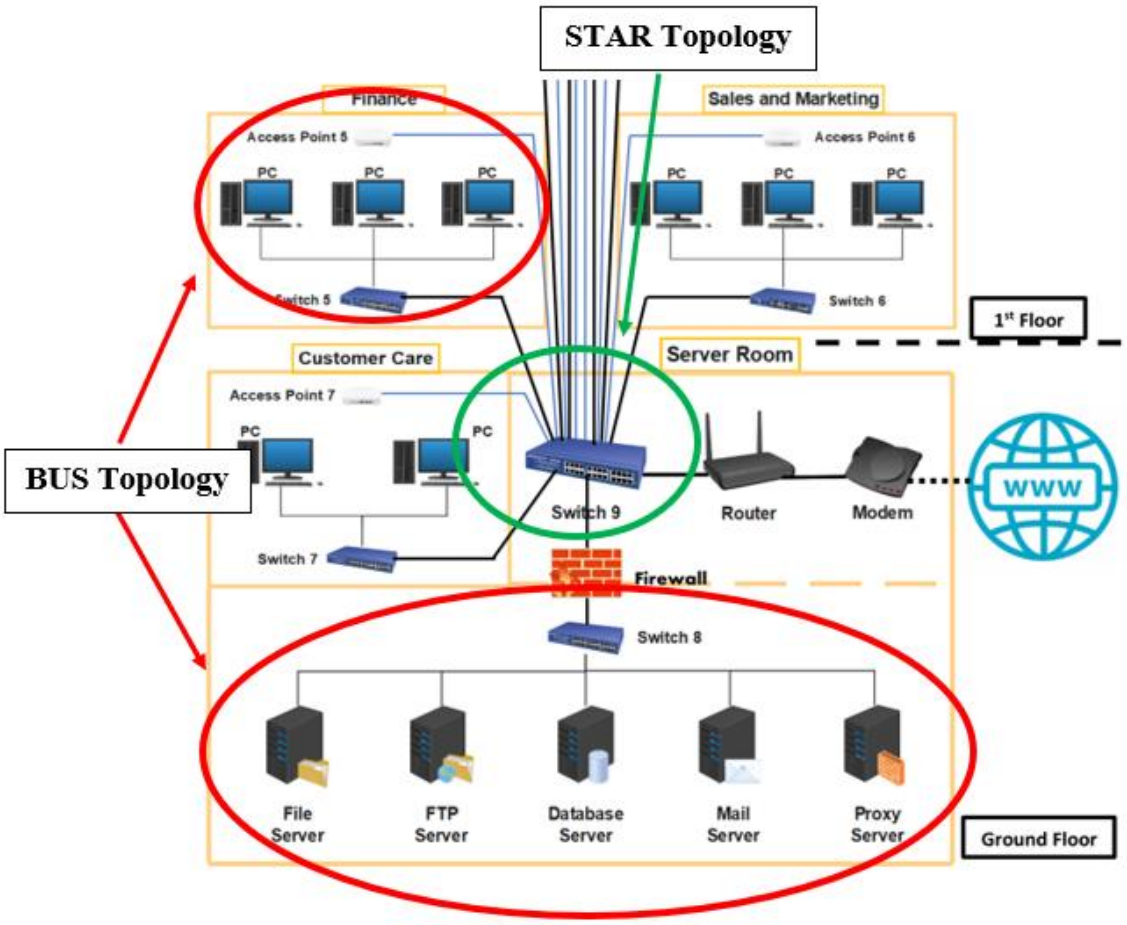



*Figure 1. 84 Diagram of Matara branch Hybrid Star - Bus network topology*

# Task 2

## 2.1 Network Devices

### 2.1.1 Repeater

The Physical Layer is where Repeaters operate. As a result, it's a Layer 1 device. When electrical signals travel over a network medium, their strength deteriorates as the distance between them grows. This attenuation is determined by the channel's or technology's characteristics.

Ex:- Using very long cables to connect computer to a switch.

The Repeater's job is to reproduce the digital signal on the same network before it deteriorates or becomes corrupted. A repeater can increase the length of a signal that can be sent over the same network. Repeaters, on the other hand, do not increase the digital signal. The repeater's job is to restore the weak signal to its original power.

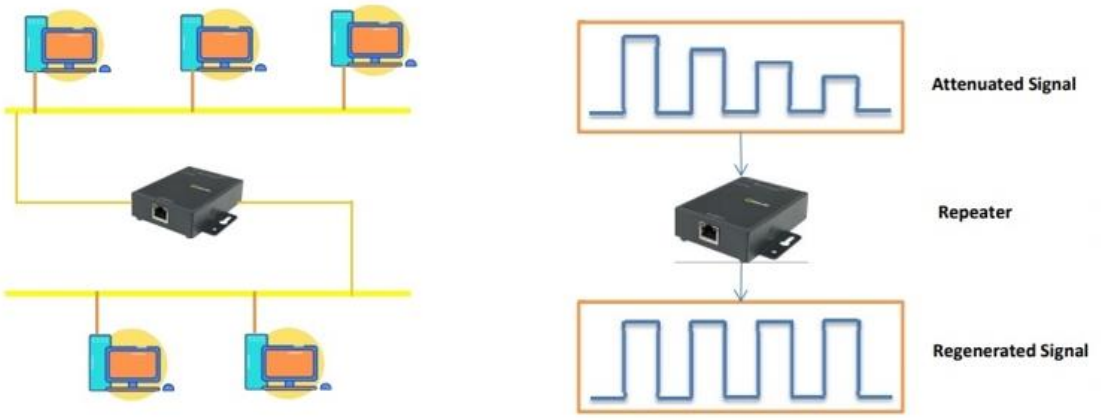



*Figure 2. 1 Reproduce the digital signal by Repeater*

The repeaters do not have intelligence. Repeaters are rarely utilized in industry since they simply regenerate even faults. Also, when the twisted pair wires are 100 meters or longer, repeaters are utilized. Companies, on the other hand, do not utilize such extensive connections for networking. However, if extensive lines are required, corporations can simply utilize fiber optics, which can transmit data over kilometers.

### 2.1.2 Hub (Multi-port Repeater)

A Hub is a device that works at the Physical Layer. As a result, it's a Layer 1 device. Hubs allow several devices in a network to communicate with one another. They're typically used to connect computers in a Local Area Network (LAN). Hub, on the other hand, can be considered of as a Multiport Repeater. As a result of Hub's ability to link several wires from various branches. Hub, for example, can be used as a connecter to connect different stations in a Star Topology.

Hubs are using a broadcast system. As a result, Hub is devoid of intelligence. Because the Hub lacks intelligence, it has trouble determining the best way for routing data packets. Furthermore, since Hub is unable to filter data, data packets are broadcast to all connected devices.

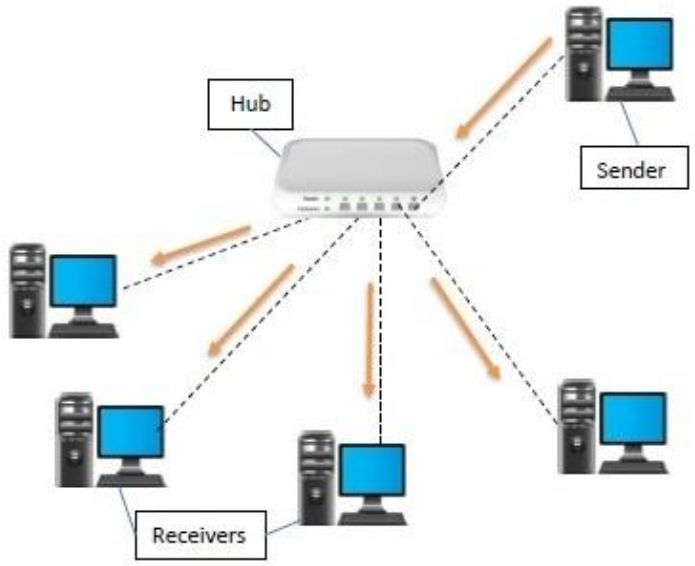



*Figure 2. 2 Connect Hub into network*

When it comes to networks, switches have mostly supplanted Hubs. Hubs, on the other hand, can be used to temporarily replace faulty network switches when network performance is not a vital consideration.

## Types of Hubs:

### Active Hub:-

Active Hubs are used to regenerate the electric signal of incoming packets before broadcasting them out of the network. This behavior similar as a repeater. Hence, some people used to refer Active Hub as a "Multiport Repeater."

These hubs have their own power supply. And also, they can clean, boost, and relay the signal within the network. Hence, Active Hub serves as both repeater as well as a wiring center. So, Active Hubs can be used to extend the maximum distance between nodes.

### Passive Hub :-

Unlike Active Hubs, the Passive Hubs do not used to regenerate the electric signal of incoming packets before broadcasting them out of the network. Hence, the broadcasting signal can become weak and corrupted before reach the final destination. So, some people used to refer Passive Hub as a "Concentrator."

Passive Hubs collecting wires from the nodes and the power supply from Active Hub. And Passive Hubs relay signals onto the network without cleaning and boosting like Active Hubs do. And also, they and cannot be used to extend the distance between nodes.

### Intelligent Hub :-

Intelligent Hub works like Active Hubs, and it includes remote management capabilities via SNMP and VLAN support. Intelligent Hub is enabled for remote monitoring and management. This is done through Simple Network Management Protocol (SNMP). They also provide flexible data rates to network devices.

Intelligent Hub enables an administrator to monitor the traffic passing through the hub. And it enables to configure each port of the hub. Hence, this is very similar to switch because of given intelligence.

### 2.1.3 Switches

Since switches came, hubs are not in use today. Switch operates at the Data Link Layer of the OSI model. Hence, it is a Layer 2 device. A Switch is a buffered multiport bridge. Since switch has many ports to plugged in it can boost efficiency and performance.

Switches has intelligence. Because of that when data frames arrive to any port of the switch, it reads the destination address and sends the frame to the corresponding device or destination.

Switches can perform checking errors before sends data to the destination. This makes the switch very efficient because it does not forward packets that have any errors. And they forward valid packets to the correct port/destination only. And also, switch supports unicast, multicast as and broadcast communications.

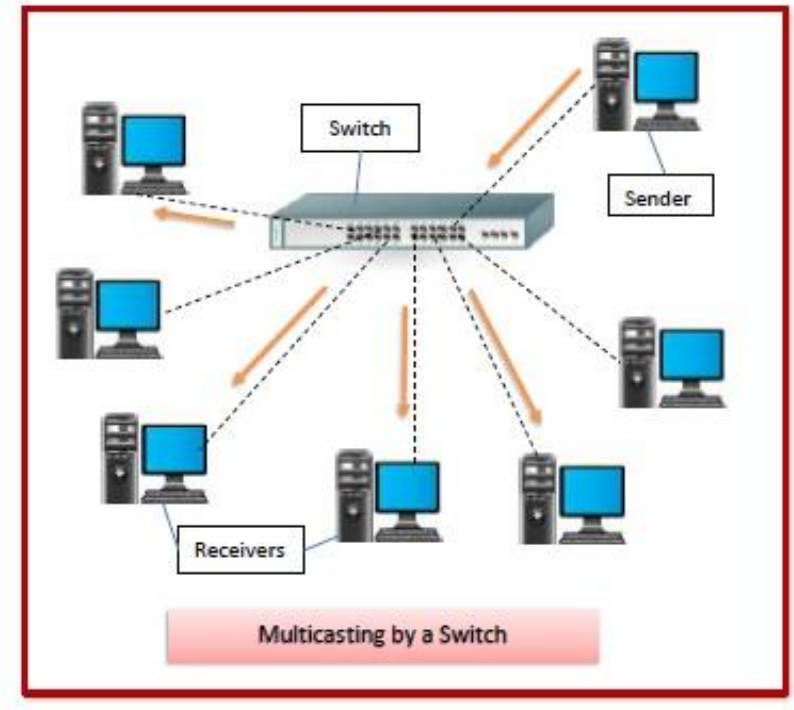



*Figure 2. 3 Connect Switch into network*

## Types of Switches:

**Unmanaged Switch :-**

These switches can't be configured.

Ex:- D-Link, Prolink switches.

These switches commonly used in home networks and small businesses since they are inexpensive. They can be simply set up by plugging in to the network. And then they can be use instantly and start operating. We can apply this simple plug and play method if more devices need to be added. These switches are referred as "Unmanaged Switches" since they don't need to be configured.

**Managed Switch :-**

These switches can be configured.

Ex:- Cisco, Juniper switches.

These switches are expensive switches. These types of switches are used in organizations with large and complex networks. Since these switches can be customized to enhance the functionalities of a standard switch, they referred as "Managed Switches." Despite their cost, organizations preferred to have these switches due to their scalability and flexibility. To configure these switches Simple Network Management Protocol (SNMP) is used.

**Layer 3 Switch :-**

Above switches works at Data Link Layer of the OSI model. Which means they are Layer 2 devices. But Layer 3 Switches work at Network Layer. Because these switches combine the functionality of both switch and router. They can perform some functions of router but cannot do all the functions of it. Separating VLANs and routing are some performable functions of it. But Layer 3 switches don't support NAT (Network Address Translation). Hence, they cannot connect to the internet.

**Multilayer Switch :-**

Multilayer Switch is a network device which enables to operate at multiple layers of the OSI model. This switch performs functions up to almost application Layer (Layer 7). For example, Multilayer Switch can do the context-based access control, which is a feature of layer 7.

Unlike other traditional switches, Multilayer Switch can do the functions of routers at incredible speed. In addition, the Layer 3 switch is one type of Multilayer Switch which is commonly used. Multilayer switch has multiple number of switches to connect lot of nodes.

*Figure 2. 4 Multilayer Switch*

### 2.1.3 Bridge

The Bridge operates at the Data Link Layer. Hence, it is a Layer 2 device. Bridge is used to connect similar networks together. But not to connect individual computers. This means Bridge can interconnect 2 LANs which working on the same protocol to form a bigger LAN. This function is very similar to Router.

A Bridge is a Repeater, with having additional functionalities such as filtering content by reading the MAC addresses of source and destination. And Bridge is a 2-port device since it has a single input and single output port.

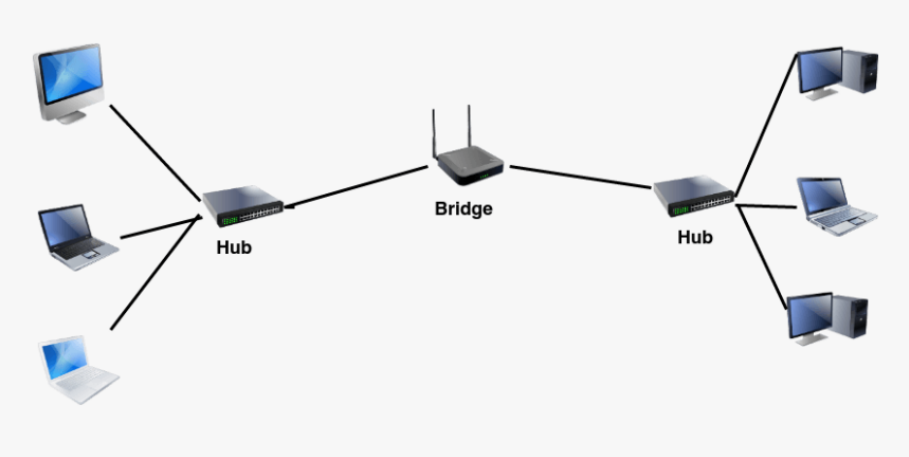



*Figure 2. 5 How Bridge interconnecting 2 networks*

### 2.1.4 Router

Bridges are not in use today since the arrival of the Router. Router operates at the Network Layer of the OSI model. Hence, it is a Layer 3 device. Router is being used to connect different networks together. But not individual computers. This function is very similar to Bridges. That's why the Bridges aren't use in today world.

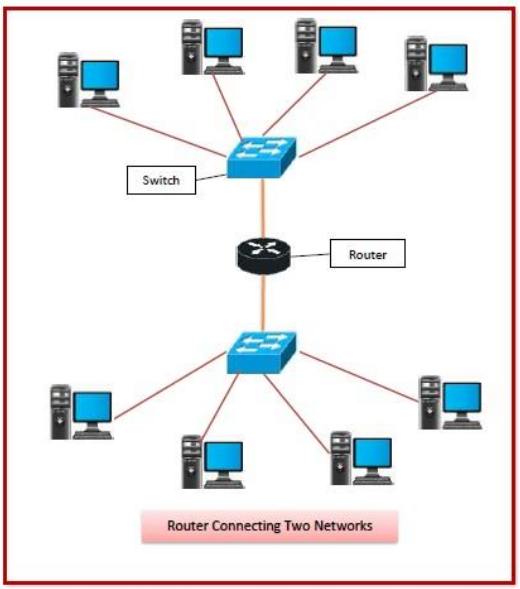



*Figure 2. 6 How Router interconnecting 2 networks*

A Router can be used in both LANs (Local Area Networks) and WANs (Wide Area Networks). A router is a device like a switch which can routes data packets based on their IP addresses. Which means routers have ability to understand IP addresses.

Routers can receive, analyze, and forward data packets among the connected computer networks. One of main task of Router is routing. Which means selecting the best route to the destination. When a data packet arrives, the Router inspects the destination address and then decide the optimal route to transfers the data packet. As described before Layer 3 switches can't use NAT. But Routers can use NAT protocol. Hence, Router can connect to the internet by using the NAT protocol.

There are ADSL routers for 3500/= LKR. It can be varied to 500 000/= LKR or more. The price is dependent on the capabilities. Such capabilities are dividing VLANs, ACL and HSRP configuration.

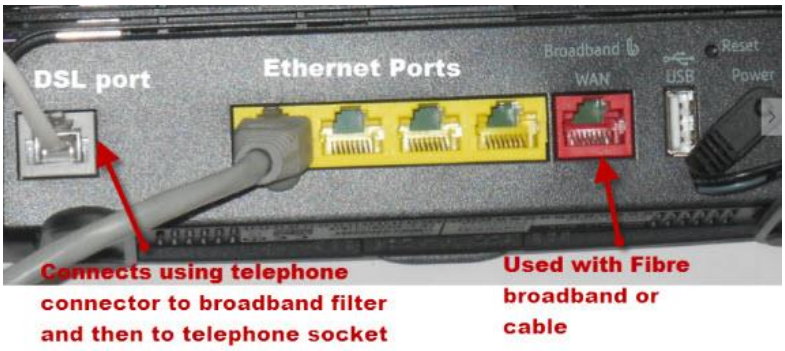



*Figure 2. 7 Ports of a Router*

## 2.1.5 Gateway

Gateway is not a device like Switch or Router. It is a concept. Gateway will show the exit/entrance to the LAN and show the way to the internet. Gateway could be a Router or Firewall or a Server that will show the exit of the network and entrance of another network.

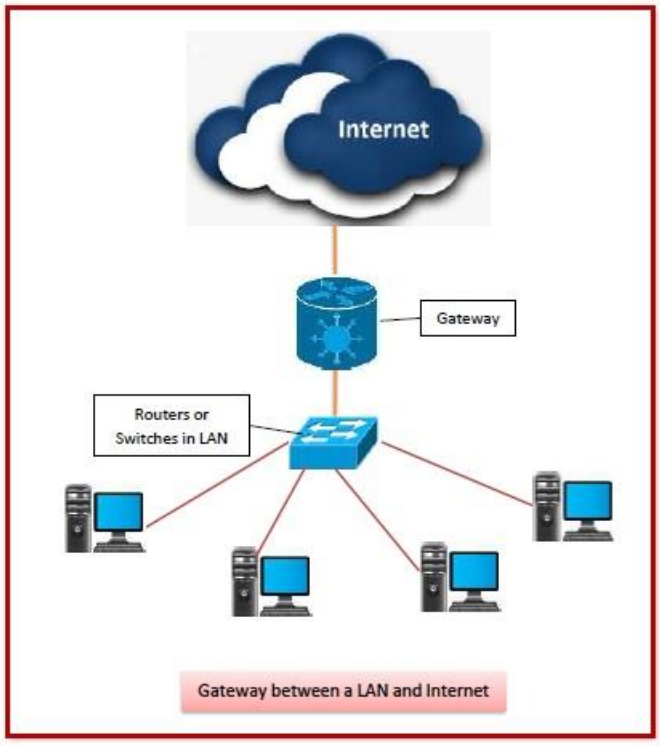



*Figure 2. 8 Router act as a Gateway*

## 2.2 Servers

Server could be a software or hardware that accept requests from multiple clients to provide immediate responses. In simple terms, Server is a device or a software which provide services to client. This is a centralized machine where multiple clients can connect through LAN or from the internet.

Client is a device which make requests or client is a device which accept responses from a server. For example, students as a client request a video from YouTube server. We can set up even our own Desktop PC or mobile phone as a server. Because as told before, server is not just a physical computer. We can set up them as servers with right software's. For example, Desktop PC can be used as a File Server to share files to other networks.

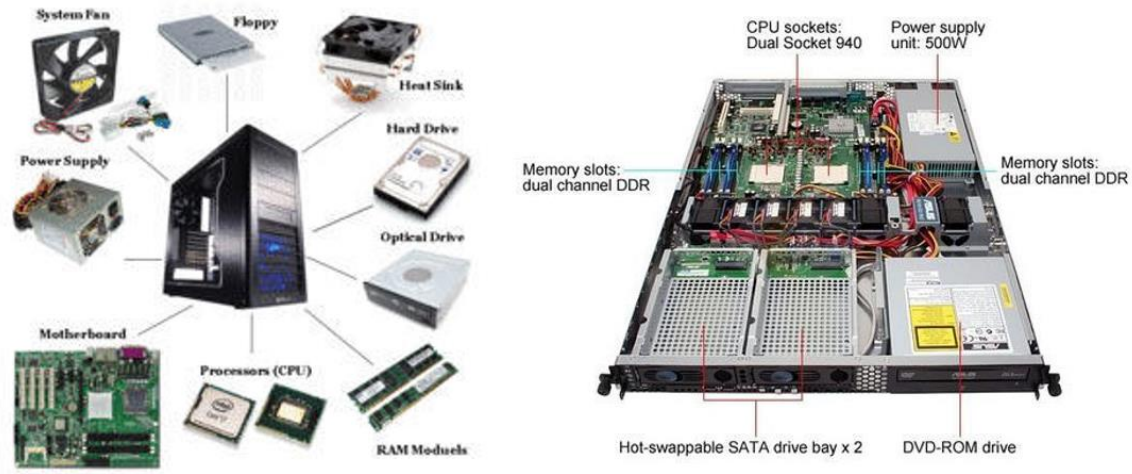



*Figure 2. 9 Parts of a Server*

### 2.2.1 Types of Servers

Some servers are committed to do specific tasks. For example, some servers can be dedicated to website, some can be dedicated to store files likewise. Big organizations tend to have multiple servers to handle these tasks. But in small organizations they set up 1 server to handle all types of work.

There are mainly 3 types of servers.

1. Physical Servers (Dedicated Server) – Dedicated servers which use traditional CPU and RAM components. This is a type of server which buyer purchase hardware and store inside home or business area. Hence the buyer has physical access to its resources.

2. Virtual Server – This is a part of physical server. Virtual server is representing physical server and buyer doesn't have to purchase hardware. Most servers which are available online are Virtual Servers. This is a web server which shares computer resources such as CPU,RAM and storage space with operating system (OS). Hence the buyer doesn't have physical access to its resources.

3. Hybrid Server – Hybrid server is more like a dedicated server, but vendor provides a slice of dedicated server. But it has flexibility of cloud, but with the power of dedicated. Buyer have to share the hardware with other customers of the vendor. Buyer have to share the hardware (CPU, RAM's, processor) but hard drives aren't shared with others. Hence the buyer's data will always be safe and secured. The data is kept separately, and everybody got their own credentials.

There are types of servers which can perform different kind of functions. Below down here are the common server types which are specialized for different functions.

**1.Application Servers**

Application Server handles all application operations between end users and an organization's backend business applications data. They occupy large computing territory between database servers and the end user. There are many Application Server platforms such as JBoss, WebLogic, J2EE, Glassfish, Tomcat.

**2.FTP Server**

FTP (File Transfer Protocol) Servers are built to handle data transfer between computers. These servers allow users to browse, upload and download files as they wish. This can be done by authentication through FTP client. Some of the FTP clients are FileZilla Client, FTP Voyager and Core FTP.

**3.File Servers**

This is different from FTP Server. This is a common server being used by lot of companies. This is specifically made for storing files and folders. Hence, companies tend to save business data and documents on file servers. Commonly File Servers use protocols such as SMB (Server Message Protocol), NFS (Network File System).

**4.Print Servers**

These servers help to manage and distribute printing functionality instead of attaching printers for every workstation. Hence, a single print server can accept multiple printing requests from multiple clients at the same time.

**5.DNS Servers**

Larger business groups tend to have DNS servers. DNS (Domain Name System) convert host names to machine readable IP addresses. These servers contain database of public IP addresses with their associated host names. Hence, they help to resolve these names into IP addresses when requested.

**6. DHCP Servers**

DHCP (Dynamic Host Communication Protocol) server assigns IP addresses and default gateways automatically. This saves from troubles of manually configuring static IP addresses and other network settings to computers.

**7.Mail Servers**

These servers are used send and receive emails. These servers use email protocols such as SMTP(Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol) and POP3(Post Office Protocol version 3).

**8.Web Servers**

These servers are commonly used in today's market. This type of servers is specialized for storing, processing, and delivering web pages to users. This mainly uses HTTP protocol (Hypertext Transfer Protocol) for this intercommunication. Some of common Web Servers are Apache, Nginx, and Microsoft Internet Information Services.

**9.Database Servers**

Database Servers used to store and manage databases. These servers provide data access to authorized users, and they keep data in centralized location for back up. These servers are specially designed to respond multiple requests from many clients at the same time. Some of the common Database Servers applications are Oracle, MYSQL and Microsoft MQL.

**10.Proxy Servers**

Proxy Servers can translate traffic between networks and protocols. Since they provide gateway between users and internet, Proxy Servers helps to prevent cyber-attacks. Hence, they can act as a firewall and web filter. And also, Proxy Servers can cache data to speed up requests.

### 2.2.2 Things to know before buy a server

When decide to buy a new server, there are a lot of technical specifications that have to deal with. How a server looks from the outside is called “Form Factor.” With known in the form factor helps to estimate the size and the shape of a server.

There are several Forma Factors of a server.

1. Tower Server
2. Rach Server
3. Blade Server

**Tower Servers :**

General standing up servers called as Tower Servers. They have built in as an upright cabinet which very similar to Desktop PC but slightly larger. Because of the independent design of Tower Servers, they can add to networks easily. When compared to other servers, Tower Servers require less maintenance.

*Figure 2. 10 Tower Server*

**Rack Servers :**

They are designed to be keep inside racks. Though they can keep wherever want such as slide under TV stand. Since these servers designed to keep in racks, the size of these servers specified in terms of Rack Unit (RU).

Mainly the cooling fans generate a noise in Rack Servers. They are nosier than Tower Servers. Since rack server components are packed more densely than the Tower Server, the cooling fans of the Rack Server have to do more work when it comes to cool the components

*Figure 2. 11 Rack Server and how Rack Server mount in a rack*

**Blade Servers :**

Blade servers are designed to minimize the use of physical space hence they have stripped down architecture. With a blade server it is mandatory to buy blade enclosure with it. Which means Blade Servers can only runs with compatible Blade Enclosure. Because Blade Enclosure provide features of power, cooling, and networking all the Blade Servers packed in.

*Figure 2. 12 Blade Server and how Blade Server mount in an enclosure*

### 2.2.3 How to understand Server Name and Brands

The name of the server tells few things about CPU, supported hardware and expansion capabilities of the Server. Let's consider 2 famous brands of servers which are HP ProLiant and Dell Power Edge.

The 1st example is **HP ProLiant.**

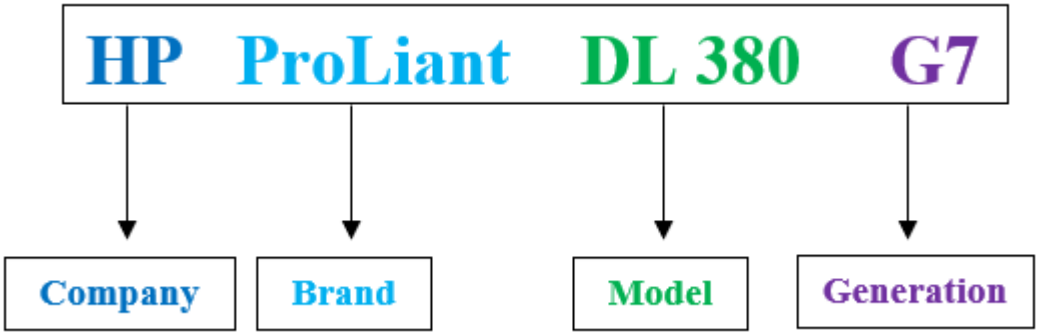



*Figure 2. 13 Understand Server Name and Brands of HP ProLiant*

Since Company and Brand self-explanatory, let's see Model. In model number DL stands for Density Line, which is another name for rack mountable server. Below figure shows other product lines of ProLiant servers. All these indicate the form factor of the server.

| Product Line | Meaning | Form Factor |
|---|---|---|
| ML | Modular Line | Tower. |
| DL | Density Line | Rack based for general purpose. |
| SL | Scalable Line | Rack based for data centers. |
| BL | Blade Line | Enclosure based. |
| Micro Servers | Entry Level | Small form factor. |

*Table 2. 1 HP ProLiant product lines with their form factor*

In model number 380 can break down into 3 constituent numbers as below.

380 → 300 + 80 + 0

300 is the Series. This indicates the number of processor sockets supported by the server. In HP ProLiant 300 series supports up to 2 processor sockets. That means it can have 2 physical CPUs in that server. Below figure shows other series of ProLiant servers with the number of supporting processor sockets.

| Series | Number of CPU sockets |
|---|---|
| 300 | 2 |
| 500 | 4 |
| 900 | 8 |

*Table 2. 2 HP ProLiant  different series with number of CPU sockets*

80 is a variation of 300 series. In 300 series there are 4 variants. They are 320, 360, 370 and 380. They each are different in terms of hardware as below picture shows.

**Side-by-Side Comparison**

| | HP ProLiant DL360 Gen 9 | HP ProLiant DL380 Gen 9 |
|---|---|---|
| **Processor** | Intel Xeon | Intel Xeon |
| **Maximum memory** | 3.0 TB | 3.0 TB |
| **Form factor** | 1U | 2U |
| **LFF HDDs** | 4 | 12 |
| **SFF HDDs** | 10 | 24 |
| **Cores per Socket** | 22 | 22 |
| **Memory** | DDR4 | DDR4 |
| **Upgradeability** | Up to 2 processors (44 cores) | Up to 2 processors (36 cores) |

*Figure 2. 14 Difference between server variants*

And the last digit which is 0 in this example indicate the processor type. 0 means it uses Intel processors. If the last digit is 5, it uses AMD processors.

The last part of the server's name is the Generation. The giving example is G& which means Generation 7. The G1 which means 1st Generation of HP ProLiant DL380 came in 1990s which had only 3 Pentium processors and supported up to 4GB of RAM. And the latest generation of HP ProLiant is 10th Generation which is indicate as G10. It can support up to 4TB of RAM and having Xeon processor which can go up to 28 cores as below table indicates.

| DL 380 | GEN 1 | GEN 10 |
|---|---|---|
| Processor Support | Intel Pentium III | Intel Xeon |
| Cores supported | 2 | 28 |
| Maximum RAM capacity | 4GB | 4TB |
| Maximum internal storage | 436.8GB | 459GB |

*Table 2. 3 DL 380 difference between generation 1 and generation 10*

The 2nd example is **Dell Power Edge.**

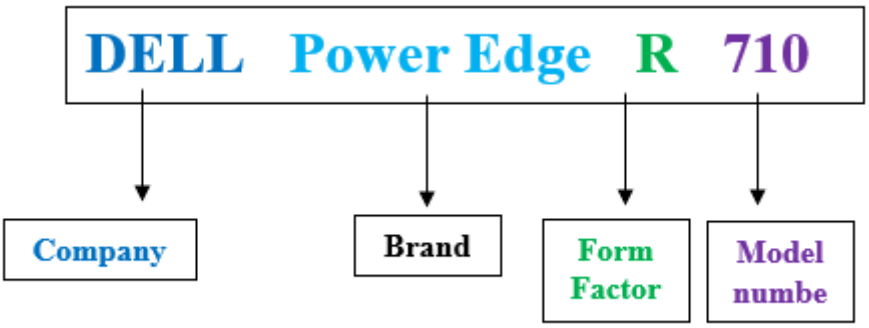



*Figure 2. 15 Understand Server Name and Brands of Dell Power Edge*

As HP ProLiant example the Company and Brand self-explanatory, let's see Form Factor. As in the above example server name the "R" indicates Rack Mountable server. And "T" indicates Tower server.

In the model number part, 1st digit indicates the number of CPU sockets. As below table show number of CPU sockets can be determine the value of the 1st digit. In our example the 1st digit is 7 which means according to below table it has 2 CPU sockets.

| Value of first digit | Number of CPU sockets |
|---|---|
| 1-3 | 1 |
| 4-7 | 2 |
| 8 | 2 or 4 |
| 9 | 4 |

*Table 2. 4 Dell PowerEdge First Digit vs the number of CPU sockets*

The 2nd digit indicates the Generation. 0 means it is 10th generation. And as in our example 1 means 11th generation.

And the last digit which is 0 in this example indicate the processor manufacturer. 0 means this server uses Intel processors. If the last digit is 5, it uses AMD processors.

### 2.2.4 Things to know before buy a server

When it comes to buy a server there are 4 options to choose as following.

1. New
2. Refurbished
3. Used
4. Buy for parts

Buying a New Server → New servers are the costliest among them. But most of time with new servers can get 3-5 years support contract with the vendor. This will ensure the quick availability of any failed components and on-site support if run into any issues. HP provide firmware updates only if buyer has support contract with them.

Buying a Refurbished Server → Refurbished servers are the servers which have previously returned to thew manufacturer for various reasons but not sold in the market. During refurbishing the seller will ensure the server is ready to deploy by cleaning the server, testing the components, ensuring the firmware updated and leave everything at its factory defaults. They are cost effective when compared to new servers.

Buying a Used Server → Used servers usually don't have refurbishment. And they have no warranty. Used servers are even cheaper than refurbished servers. But it is risky to buying it since there are no warranty.

Buying Server parts → When people want to build their own server or when want to upgrade their server, they are looking for buying server parts.

## 2.2.5 Other things to consider when buying a server

**Budget :**

Budget is important since it helps to control the spending and to focus on long term financial investment. Since servers are too expensive, it's necessary to track expenses of them. There are many servers with a range of price depending on specifications. If the running business is a long term, a suitable server will help to improve efficiency of the business. Considering the amount of spending money for the server is very important. Buyer can get very expensive server or cheaper server as prefer.

| Buying a cheaper server | Buying an expensive server |
|---|---|
| When renting cloud server may under $100 for month. | When renting cloud server may over $100 for month. |
| When buying dedicated may under $500 for 1 time payment. | When buying dedicated may over $1500 - $2000 for 1 time payment. |

*Table 2. 5 Pros and Cons of buying cheaper server and expensive server*

Small servers can buy for few hundred dollars but more powerful servers such as cloud servers can cost that much for per month or even thousands for on-site servers. Because of that. Buyer should buy a server for affordable price. It would be a waste of money for spending excessive amount of money for a server that exceed buyer requirements.

**Server's main function :**

Server could be different kind of computer or a software that specialized for various range of tasks. Server components such as RAM, processor, storage capacity play a major role before buying a server. Buyer has to consider details about these components before buy a server. Since different kind of servers performing different kind of functions, it is mandatory to buy a server which is matching buyer's requirement. Otherwise, it would be a waste of huge amount of money.

**Server Type :**

There are 2 types of servers as mentioned before. Physical Servers (On-Site Servers) and Virtual Servers (Cloud Servers). Physical servers have their own advantages and disadvantages. Since physical servers require space, installation and maintenance Cloud servers seems to be convenient compared to On-Site servers. Because we can access Cloud server from anywhere. And they provide better security. But in contrast the file transfer speed would be lower. Since buyer have to consider these advantages and disadvantages before making decision to buy a server.

| Advantages | Disadvantages |
|---|---|
| Have to pay 1 time to buy the hardware. (Enterprise grade hardware cost around $2000 - $3000) | To cool the server are power the server cost high electricity. (This could be cost $200-$400 per month) |
| No need to pay monthly fee to vendor | Need to set backup generator (This could be cost $2500 - $4500) |
| | Hardware replacement parts are expensive. |
| | Can't replace hardware immediately if a failure happens. |
| | Not having 24 x 7 customer support. |
| | Hardware becomes outdated quickly. |

*Table 2. 6 Advantages and disadvantages of having on-site server*

| Advantages | Disadvantages |
|---|---|
| Can have latest hardware | No need to pay monthly fee to vendor |
| Can upgrade and customize the hardware as buyer's requirement | Can't n access server physically. |
| Having 24 x 7 customer support. | |
| Benefit of having on-site staff for hardware replacement and maintenance. | |
| No additional charge to cool the server and power the server | |
| No need to buy backup generator | |

*Table 2. 7 Advantages and disadvantages of having cloud server.*

**Server Build :**

There are many preconfigured servers available in market ready to plug and play. And also, there are custom server which allows buyers to choose components and parts as they prefer. But its need expertise knowledge to decide the custom build and it would be requiring more work and effort to buy a server rather than buying preconfigured server.

**Security :**

Buyers has to consider the security of the server since it is dangerous to store all business data in one place and leave it open to attack. With a cloud server, buyer can customize the level of the protection by asking the provider. With the help of cybersecurity consultant, buyer can decide best suitable secured level server to operate.

**Maintenance :**

Physical Servers need to be monitored and require maintenance which costing lot of money to do that. Hence, business should hire onsite IT support to handle Physical Servers. But with having a Cloud Server, buyer doesn't need to maintain and handle them since the service provider handles it.

## 2.2.6 Server prices

### Tower Server Prices

HPE ProLiant ML350 Gen10

- Condition : Refurbished
- Processor 2x 6254 Xeon Gold (3.1 GHz / 24.75 MB Cache)
- Hard Drive 8x 1TB SATA 3.5" Hard Drives
- Memory 128GB (8x16Gb) Memory Installed - DDR4
- Power Dual 500W Power Supply
- Other : Battery, Fans, Heatsink included
- Price : $11 274

(Ebay, n.d.)

*Figure 2. 16 HPE ProLiant ML350 Gen10*

Dell PowerEdge T330

- Condition : Used
- Processor E3-1230 v5 with 4 Cores 3.40GHz
- Hard Drive 8x 1TB 7.2k 6Gbs SATA
- Memory 32GB Memory Installed - DDR4 U
- Power Supply2x 495W
- Other : DVD drive, Heatsink included
- Price : $849

(Ebay, n.d.)

*Figure 2. 17 Dell PowerEdge T330*

Lenovo Think System ST50

- Processor E-2124G Intel Xeon (3.4GHz 8MB Smart Cache)
- Memory : 8GB Memory Installed - DDR4-SD
- Hard Drive : Not installed
- Power Supply : 250W
- Other : DVD drive
- Price : $1 008

(Ebay, n.d.)

*Figure 2. 18 Lenovo Think System ST50*

**Rack Server prices:**

DELL PowerEdge R440 Server

- Condition : Refurbished
- Processor : 2x 4108 Xeon Silver (1.8 GHz / 11MB Cache)
- Hard Drive : 4x 1.92TB SATA 2.5" Hard Drives
- Memory : 256GB Memory Installed - DDR4
- Power : Dual 550W Power Supply
- Other : Battery, Fans, Heatsink included
- Price : $3 607

*Figure 2. 19 DELL PowerEdge R440 Server*

(Ebay, n.d.)

HP ProLiant DL380p G8 Server

- Condition : Refurbished
- Processor : Intel Xeon e5-2620v 6 Core (2.1Ghz/15Mb Cache)
- Hard Drive : 25x 146GB 6G SAS
- Memory : 192GB Memory Installed - DDR3
- Power : Dual 750W Power Supply
- Other : Battery, Fans included
- Price : $4 014

*Figure 2. 20 HP ProLiant DL380p G8 Server*

(Ebay, n.d.)

HP ProLiant DL380 Gen10

- Condition : Refurbished
- Processor 2x 5218R Gold (2.1 GHz 20C 27.5MB Cache)
- Hard Drive 24x 240GB SATA 2.5" Hard Drives
- Memory 384GB Memory Installed - DDR4
- Power Dual 800W Power Supply
- Other : Battery, Fans, Heatsink included
- Price : $8 323

*Figure 2. 21 HP ProLiant DL380 Gen10*

(Ebay, n.d.)

**Blade Server Prices**

Dell PowerEdge M520

- Condition : Refurbished
- Processor : 2 x Intel Xeon Quad-Core E5-2407 (2.2GHz)
- Hard Drive : 2 x Dell 300GB 15K SAS
- Memory : 16GB DDR3 RAM (2x 8GB)
- Price : $526

(Ebay, n.d.)

*Figure 2. 22 Dell PowerEdge M520*

HP ProLiant BL460c Gen8

- Condition : Used
- Processor : 2 x Intel Xeon Quad-Core E5-260 (2.4GHz)
- Hard Drive : 2 x 300GB 10K SAS
- Memory : 16GB DDR3 RAM (2x 8GB)
- Price : $477

(Ebay, n.d.)

*Figure 2. 23 HP ProLiant BL460c Gen8*

Fujitsu PY Primergy BX924 S4

- Condition : Used
- Processor : 2 x Intel E5-2667v2 8-Core XEON (3.3GHz)
- Hard Drive : 2 x Fujitsu 100GB SSD
- Memory : 192GB DDR3 1866MHz Fujitsu original memory
- Price : $3 289

(Ebay, n.d.)

*Figure 2. 24 Fujitsu PY Primergy BX924 S4*

Cisco B200 M3

- Condition : Used
- Processor : 2 x Intel Xeon 8-CORE E5-2650 (2.20GHz)
- Hard Drive : Not installed
- Memory : 96Gb DDR3 RAM
- Price : $1 644

(Ebay, n.d.)

*Figure 2. 25 Cisco B200 M3*

**Cloud Server Prices**

| Cores | RAM | Storage | Bandwidth | Monthly Rent |
|---|---|---|---|---|
| 1 CPU | 1GB | 25GB | 1TB | $5 |
| 1 CPU | 2GB | 50GB | 2TB | $10 |
| 2 CPU | 4GB | 80GB | 4TB | $20 |
| 2 CPU | 6GB | 100GB | 4TB | $30 |
| 4 CPU | 8GB | 160GB | 5TB | $40 |
| 6 CPU | 16GB | 320GB | 8TB | $80 |
| 8 CPU | 32GB | 640GB | 12TB | $150 |
| 12 CPU | 48GB | 960GB | 16TB | $250 |
| 16 CPU | 64GB | 1.5TB | 20TB | $350 |
| 20 CPU | 96GB | 2TB | 20TB | $500 |
| 24 CPU | 128GB | 3TB | 20TB | $650 |

*Table 2. 8 Cloud Servers price by "Server Mania"*

(Server Mania, n.d.)

**Hybrid Server Pricing**

| Series | V Cores | RAM | Storage | Cloud Backup | Monthly Rent |
|---|---|---|---|---|---|
| E3 VM SSD L1 | 2 | 8GB | 120GB SSD | 50GB | $30 |
| E3 VM SSD L2 | 2 | 8GB | 250GB SSD | 50GB | $40 |
| E3 VM SSD L3 | 2 | 8GB | 500GB SSD | 50GB | $50 |
| E3 VM SSD P1 | 4 | 16GB | 250GB SSD | 50GB | $60 |
| E3 VM SSD P2 | 4 | 16GB | 500GB SSD | 50GB | $70 |
| E3 VM SSD P3 | 4 | 16GB | 1TB SSD | 50GB | $80 |

*Table 2. 9 Hybrid Servers price by "Server Mania"*

(Server Mania, n.d.)

## 2.2.7 Choosing Servers for Matara Branch

Since Matara branch building dedicated space for servers, as a Network consultant I am recommending buying few Physical Servers. I'm not preferring to buy Cloud Server since transfer data across internet for cloud server is too risk. And since SYNTAX is software company, they would work with many important and highly confidential data. Because of that I can't take a risk to work with Cloud Servers. As mentioned before Cloud Server has many benefits but when it come security concerns, I am recommending Physical Servers to work with.

For a Physical Server, I prefer to buy HPE ProLiant ML350 Gen10 server. It is a good investment for businesses since this server can handle wide range of workloads. Such as databases, business analytics, virtualization, enterprise application and etc. And this is reliable and robust server to buy when compared to other physical servers.

As I mentioned before in the topic of "Tower Server Price List", this server supports dual processors with a high memory. This server can upgrade to impressive amount of storage and support a wide range of storage options. Since this includes Intel Xeon processor, this has an excellent performance. And also, there are number of configuration options available when customizing CPU, RAM, and storage. Hence, HPE ProLiant ML350 Gen10 server. is a highly flexible server to buy.

There are many racks, shelves. And universal rails available in market if we want to rackmount a Tower Server. Since HPE ProLiant ML350 Gen10 designed as a Tower Server, it can be easily converted into Rack Mount Server which giving flexibility for future growth.

*Figure 2. 26 HPE ProLiant ML350 Gen10 server*

## 2.3 Workstation Hardware and Networking Software

### 2.3.1 Interdependence of Workstation Hardware and Networking Software

Hardware is any element of a Computer or Workstation which physically includes. Such as keyboards, monitor, hard disk, CPU, RAM and etc. And software is a collection of various types of programs that tells hardware what to do and how to do. In other words, software is a collection of instruction in programming languages. Such as computer programs, applications, all types of OS, Microsoft office packages, video games, web browsers, photo editors and etc.

Despite the Hardware and Software are very different from each other, but they need one another to perform a particular task. To get a particular task done in a computer, both hardware and software has to perform together. In other words, they are complementary to each other. If it was only hardware, it would have a dead workstation. It wouldn't be operated since it can take any instruction without a software. On the other hand, if it was only software, there's no actual workstation to work on. It would be just a bunch of instructions, but there is nothing to perform and operate those instructions.

So, software work as an interface between client and the hardware. Hence, hardware needs software to get instructions. And also, software needs hardware in order to perform. We can say in other words hardware and software are the 2 sides of a same coin.

People consider hardware as a one-time expense. But when it comes to software, it is a continuing expense. Because 1 workstation or hardware can run many software and each software can perform different tasks. Since developing software very expensive, to get or update and software require mostly require to be purchased.

## 2.3.2 Networking Software

**Traditional network :**

Traditional network is a conventional way of networking. Traditional network uses fixed and dedicated hardware devices. For example, routers and switches use to control the traffic of the network. Hence, traditional network is based on hardware components. For example, as below figure traditional switches comes with both software and hardware together. The control plane is the software part, and the data plane is the hardware part.

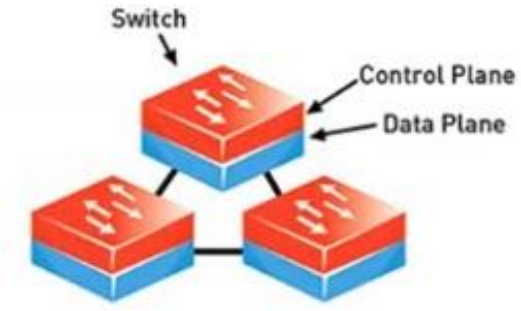



*Figure 2. 27 Three Switches interconnected as traditional network*

Now a days the network security and performance are the major concern for businesses. Hence, SDN (Software Define Network) has been developed and will be used more in future due to drawbacks of traditional network. The below figure shows the architecture of Traditional Network

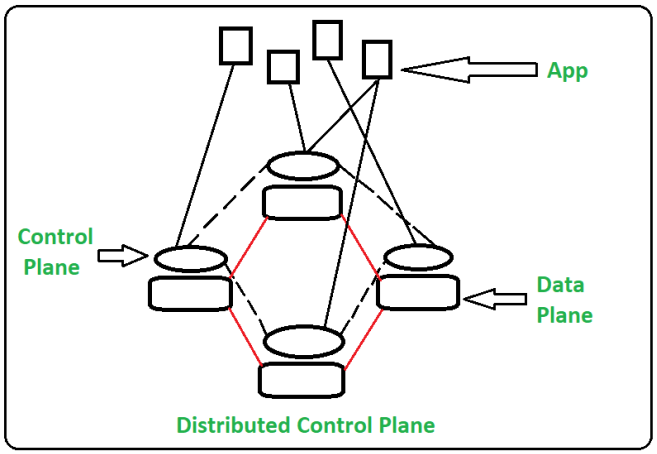



*Figure 2. 28 Architecture of Traditional Network*

**Software Define Networks (SDN) :**

SDN stands for Software Defined Network which is networking architecture approach. SDN helps to control and manage the network by using software applications. The network devices are controlled through software applications which improves the performance by network virtualization. For example, as below figure SDN switches comes software and hardware separately. The control plane is the software part, and the data plane is the hardware part. A single control plane part controlling all the switches. Hence, the cost price for switches has been reduced.

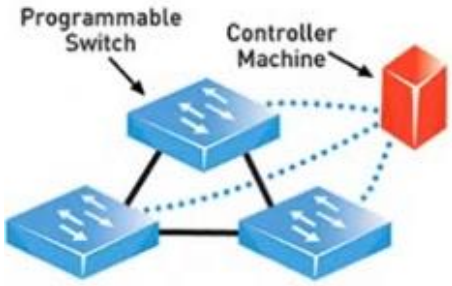



*Figure 2. 29 Three Switches interconnected as software define network*

So simple words, SDN create virtual network and it can control traditional network with the help of software. The below figure shows the architecture of Software Defined Network.

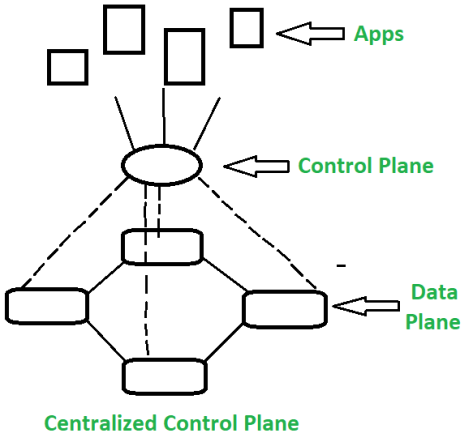



*Figure 2. 30 Architecture of Software Define Network*

| Differences | |
|---|---|
| **Traditional Network** | **Software Define Network (SDN)** |
| Old convectional networking approach. | Virtual networking approach. |
| Distributed control. | Centralized control. |
| Non-programmable. | Programmable. |
| Control plane and Data plane come together. | Control plane and Data plane come separately. |
| Because of manual configuration, it takes more time. | Because of automatic configuration, it takes less time. |
| Installation cost is high. | Installation cost is low. |
| Maintenance cost is high. | Maintenance cost is low. |
| Structural complexity is high. | Structural complexity is low. |
| Difficult to troubleshoot. | Easy to troubleshoot. |

Many large networking firms sell SDN controllers on the market. Cisco Open SDN controller, Juniper Contrail, Brocade SDN controller, and NEC PFC SDN controller are some examples of these controllers. Opendaylight, Floodlight, Beacon, Ryu, and other open source SDN controllers are also available on the market. What's great about these controllers is that they provide customers a solid idea of how SDN systems are built.

### 2.3.3 Functions of Network Software

- This helps to install computer networks.
- This helps clients to access network resources without any objection
- Allows network administrators to manage users in the network.
- Helps to configure the user access to data storage.
- With this network administrators can manage security system of the network.

## 2.3.4 Other Software

**Client Software :**

A Client Software is an application which installed in computer to performs specific task. This allows clients to access the shared resources of computer.

Ex:-

- System Software :- Windows operating systems (Windows 7, 8, 10, 11), MacOS, Android, Apple iOS.
- Application Software :- MS office, Adobe acrobat, web browsers (Google Chrome, Safari, In Microsoft Edge), graphic software (CorelDraw and Photoshop).
- Utility Software :- Anti Virus software (Windows defender, Windows firewall), Disk Cleanup, Disk Management, Disk Defragmenter, Backup utility, File Management System.
- Programming Software :- Python, Laravel, C++, C#, Java

**Server Software :**

A Server Software is an application which installed in server to performs specific task. This allows clients to access the shared resources of the server. Depending on the type or usage of server, service may be classified into various forms, such as followings.

Ex:-

- Web server software :- NGINX, Apache Tomcat, Apache Web Server, Lighttpd.
- Application server software :- IBM WebSphere Application Server, Plesk, Wildfly, Phusion Passenger, Oracle Tuxedo
- Database server software :- MySQL, Oracle RDBMS, IBM DB2, Microsoft SQL Server, Microsoft Access.
- FTP (File Transfer Protocol) server software :- Cerberus FTP Server, CrushFTP Server, FileZilla Client, FTP Voyager.
- Server OS :- Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2000, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Mac OS X Server.

## 2.3.5 Network Monitoring Software

If a network administrator has a responsibility to manage 100 routers and switches across the network, it is very difficult to manage and monitor them always. Clients would be complaining if anything goes wrong. So, network administrator has to figure out which one of his 100 routers and switches have the problem.

Hence, network administrator can use network monitoring software to monitor and fix problems of network easily. Network monitoring software is used to monitor the network, detect network faults, and configure remote devices.

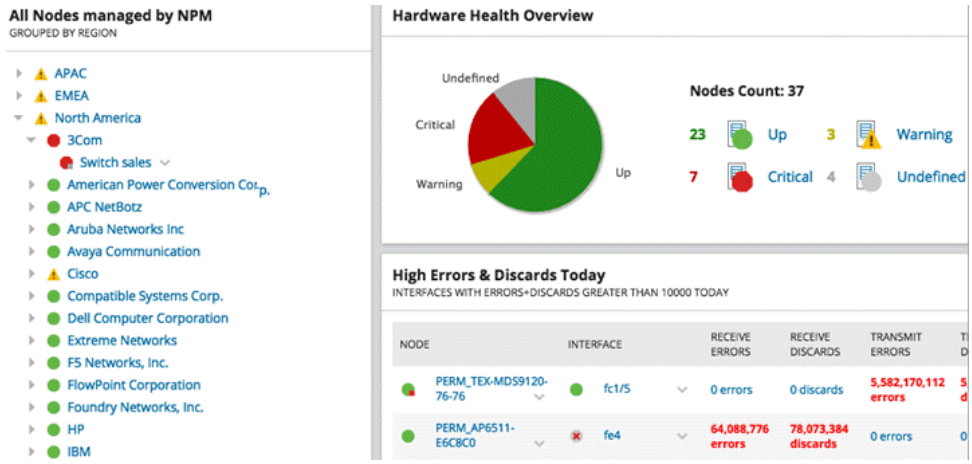



*Figure 2. 31 Monitoring network by network monitoring software*

**Example for network monitoring software :**

- SolarWinds Network Performance Monitor - Runs on Windows Server and Linux.
- ManageEngine OpManager - Runs on Windows Server and Linux.
- Paessler PRTG Network Monitor - Runs on Windows Server.
- Auvik – Web based system.
- Site24x7 Network Monitoring - Runs on Windows Server and Linux.
- Atera - Runs on Windows Server, Linux, Mac, Android, iOS.
- Nagios XI - Runs on Windows, Linux, Mac and Unix.
- Zabbix – Web based system.
- Incinga 2 - Runs on Linux.
- Progress WhatsUp Gold - Runs on Windows Server.
- ConnectWise Automate - Runs on Windows Server.

**Benefits of network monitoring software :**

- Stay ahead of outages :- Implementing network monitoring is one of the most fundamental and straightforward techniques to avoid outages in the first place. Network monitoring provides us with the visibility we require to keep ahead of possible problems. Network monitoring software lets us identify outages that could cause bottlenecks by displaying real network performance statistics in an easy-to-read interface.
- Fix issues faster :- For time-strapped network experts, network monitoring makes problem-solving easier and faster. Whether we're dealing with a setup fault or an unusual traffic fluctuation, network monitoring software assists us in resolving problems once and for all. Live network maps show us where problems are coming from, and status windows show us how things are going over time. Furthermore, network automation tools enable us to take things a step further. We can use network monitoring to detect problems and automatically resolve them without the need for a human intervention.
- Identify security threats :- Network monitoring can assist secure our business-critical data when we don't have the budget for intrusion detection software but still want a tier 1 solution to help protect against data breaches. That first layer of protection can be provided by a network monitoring tool. The most important benefit we receive is a picture of what "normal" performance for your business looks like, making it easy to notice anything out of the usual, whether it's a spike in traffic or an unfamiliar device connected to our network. We can adopt a proactive approach to network security by drilling down to determine when and on what device an event happened.
- Justify equipment upgrades :- Most employers aren't convinced by a gut feeling that a server needs to be upgraded. Network monitoring software provides us with historical data on how equipment has behaved over time, allowing us to justify network upgrades. Trends analysis aids us in determining whether our current technology can scale to meet company demands or whether we need to invest in new technology.

# Task 3

## 3.1 SYNTAX Solutions Matara branch LAN design

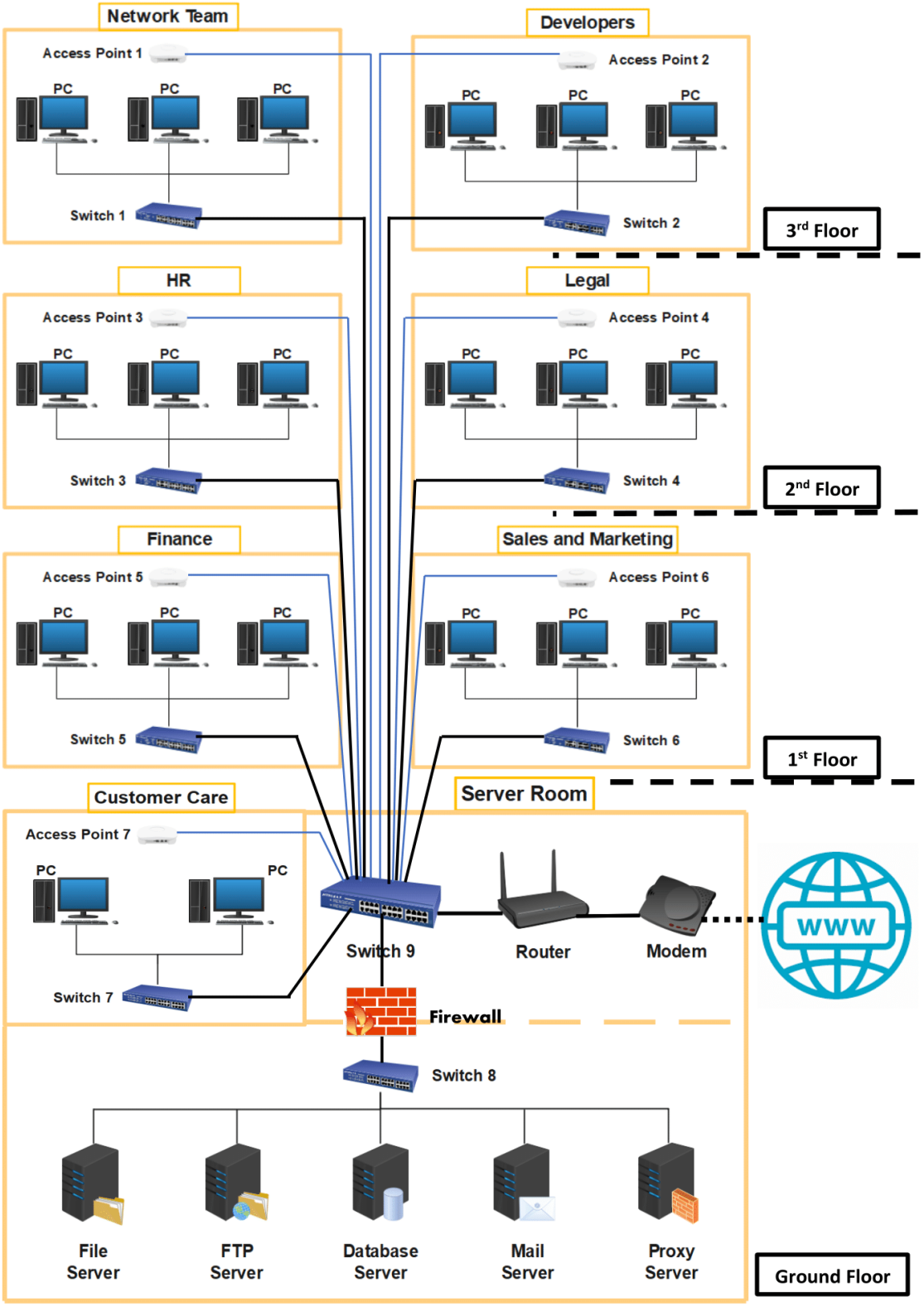



*Figure 3. 1 LAN design of SYNTAX Solutions Matara branch by "Wondershare EdarwMax" software.*

### 3.1.1 List of network devices and software for SYNTAX Solutions Matara branch

**Device / Software :** Computer

Since this is a well-known software company, high end PC for Network Team department and Developer department is recommended. For other departments, medium specification PC works fine.

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| For Network Team department and Developer department | | |
| 30 | CPU -Core i5 4th generation | $500 |
| | RAM – 8GB | |
| | Graphic Card – GTX 960, 2GB | |
| | 128GB SSD | |
| For other departments | | |
| 70 | CPU -Core i3 3rd generation | $200 |
| | RAM – 4GB | |
| | Graphic Card – 512MB | |
| | 128GB SSD | |

*Table 3. 1 Computer specifications and estimated unit price*

**Device / Software :** Switch

Cisco 350 Series Switch helps to improve the availability, efficiency of businesses and optimizing the network bandwidth. This type of switch helps to protect sensitive information, and this is very easy to use. Since there are maximum number of employees for each department is 25, a 24-port switch is recommended.

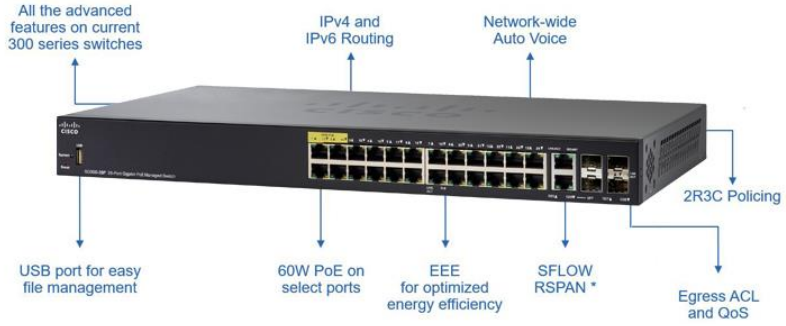



*Figure 3. 2 Cisco 350 Series*

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| 9 | Brand - Cisco 350 Series Switch SF350-24P | $300 (Brand New) |
| | 24 Port 10/100 Fast Ethernet Switch | |
| | 2 Gigabit Ethernet combo + 2 SFP | |
| | Internal Power Supply | |

*Table 3. 2 Switch specifications and estimated unit price*

**Device / Software :** Router

Cisco RV340 router is a recommended choice for small businesses since this can provide security, performance, and reliability. This router can give firewall protection. Without affecting internet access, this router can protect employees from malicious websites and unwanted contents. Since this has high speed internet access, it is recommended for software company. This has 2 WAN RJ-45 WAN ports for load balancing and resiliency, 4 LAN ports to give higher performance of connectivity, 2 USB ports for support 3G or 4G modem or flash drive, TCP with 900MBps to improve productivity, VPN functionality for secured connection.

*Figure 3. 3 Cisco RV340 router*

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| 1 | Brand - Cisco RV340 Dual WAN Gigabit VPN Router | $270 |
| | 2 WAN ports (RJ-45) | |
| | 4 LAN ports | |
| | 2 USB ports | |
| | TCP with 900MBps | |

*Table 3. 3 Router specifications and estimated unit price*

**Device / Software :** Modem

I'm recommending Motorola MB7621 cable modem for this company. As explained in task 2, I choose IEEE 802.11n standard as LAN standard for Matara branch (Click this hyperlink to see →1.8.4 Choosing IEEE 802.11 WLAN standards for Matara Branch). As told before this LAN standard supports maximum data rate 600Mbps. The selected modem Motorola MB7621 supports internet plans up to 600Mbps. Hence, it is very compatible modem for this network. And also, this modem is designed to minimize the shelf space and very attractive. The installation is very easy and can be done in fast.

*Figure 3. 4 Motorola MB7621 cable modem*

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| 1 | Brand - Motorola MB7621 modem | $90 (Brand New) |
| | Connectivity technology - Ethernet | |
| | 2-year warranty | |

*Table 3. 4 Modem specifications and estimated unit price*

**Device / Software :** Access Point

This supports up to 50 users which is very compatible with the designed LAN. Because still there are maximum users for departments is 25. This provides high secure wireless connection for small business workplace.

*Figure 3. 5 Cisco Business 100 Series Access Point*

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| 7 | Brand - Cisco Business 100 Series Access Point | $165 |

*Table 3. 5 Access Point specifications and estimated unit price*

**Device / Software :** Antivirus Software

I am recommending Bitdefender Gravity-Zone Elite anti-virus guard for this company since this is perfect virus guard for companies who looking for single platform to get prevention against sophisticated cyber threats. Despite there are budget friendly home virus guards in the market, I am recommending business security type of virus guard. Since virus guards can act as a host-based firewall, this saves us from spending lot of money to buy network-based firewall such as hardware firewall for the network. And not only that, but this is also very easy to manage and configure the protection and control.

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| 100 | Brand - Bitdefender Gravity-Zone Elite | $40<br>(1 year) |

*Table 3. 6 Anti-Virus Software specifications and estimated unit price*

**Device / Software :** Firewall Device

The hardware firewall helps to protect entire network while software firewall works at single computer. I am recommending implementing a hardware firewall for server room since they are the most important part of the entire network. Despite of installing software firewalls for each server, I prefer to add hardware firewall to protect entire server network as an additional security for the network.

I am recommending SonicWall TZ Series firewall since it is a perfect firewall for small network. This is a budget friendly device  but have lot of features. And this doesn't need any complicated setup requirements because of its Zero Touch Deployment technology.


*Figure 3. 6 SonicWall TZ350 series*

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| 1 | Brand - SonicWall TZ350 series | $600 (Brand New) |

*Table 3. 7 Firewall device specifications and estimated unit price*

**Device / Software :** Computer OS(Operating System)

Other older versions of windows such as Windows 7 and 8 doesn't have access DirectX 12, but Windows 10 has which brings 40% performance over DirectX 11. Likewise, there are many available features in Windows 10 Professional, but the retail key price is cost $200. We can buy OEM (Original Equipment Manufacturer) key for a low price, but it doesn't allow move the OS to different computer once installed. But since it is cost effective, I'd like to recommend buying OEM keys for the computers.

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| 100 | Brand – Windows 10 OEM product key | $10 |

*Table 3. 8 Computer OS specifications and estimated unit price*

**Device / Software :** Server OS(Operating System)

Windows Server 2019 is the latest server which have enhanced experience for developers. With windows 2019 server OS, developers can run Linux VM (Virtual Machine) through it. And this provides extra support and security compared to other old Windows Server Operating Systems such as Windows Server 2003, 2008, 2012 and 2016.

| Number of pieces | Recommending brand / specification | 1 Unit price in US dollar |
|---|---|---|
| 5 | Brand – Windows Server 2019 Standard - 16 Core License | $500 |

*Table 3. 9 Server OS specifications and estimated unit price*

**Total price for all hardware and software for the SYNTAX Solutions company Matara Branch :**

| Device / Software | Number of pieces | 1 Unit price in US dollar | Total Price in US dollar |
|---|---|---|---|
| Computers for IT department | 30 | $500 | $25,000 |
| Computers for other departments | 70 | $200 | $14,000 |
| Switches | 9 | $300 | $2,700 |
| Routers | 1 | $270 | $270 |
| Modem | 1 | $90 | $90 |
| Access Points | 7 | $165 | $1,155 |
| Antivirus Software | 100 | $40 | $4,000 |
| Firewall Devices | 1 | $600 | $600 |
| Computer OS | 100 | $20 | $2,000 |
| Server OS | 5 | $500 | $2,500 |
| Total | | | $52,315 |

*Table 3. 10 Total price for all hardware and software for the SYNTAX Solutions company Matara Branch*

## 3.2 Maintenance Schedule for designed network system

### 3.2.1 Importance of maintenance Schedule

Network maintenance, at its most basic level, entails all of the processes and systems in place to monitor, upgrade, and run your company's computer network before problems arise. The following are the essential elements of network maintenance and the foundation of a successful regular network maintenance plan.

- Network cybersecurity : Using firewalls, virtual private networks auto-generated security reports to implement robust and up-to-date network defense layers.
- Network performance: Examining the most common network performance issues that affect the speed of the devices. Such as bandwidth utilization, traffic patterns, regularly down or crashed servers, connection lags and more.
- Network scalability : refers to the software and hardware systems that are appropriate for company's existing operations, the number of network users, endpoint locations, and business processes.
- Update hardware and software on a regular basis: Scheduling updates are get distributed across network components and interfaces, which improves overall network performance and security.
- Data backups : The most important maintenance task is data backup. It's critical to be able to retrieve up-to-date data regardless of what kind of network calamity occurs. Some businesses only need an end-of-day backup, while others demand continuous backup.
- Preventative network repairs: Applying auto-generated reports and analytics to detect and fix utilization problems across the IT infrastructure. They need to be troubleshot before becoming serious problems.

(What Is Network Maintenance? | Network Maintenance Plans & Tips, 2018)

### 3.2.2 Maintenance Schedule for SYNTAX Solutions Matara branch

| Maintenance Task | Daily | Weekly | Monthly | Annually |
|---|---|---|---|---|
| **Updates** | | | | |
| PC software packages update and install | | X | | |
| Operating System update | | X | | |
| Server software update and install | | | X | |
| Update firewall and antivirus software | | X | | |
| **Security** | | | | |
| Server Access review | | X | | |
| Firewall rules review | | | X | |
| Force user to change password | | | | X |
| Run Spybot | | X | | |
| Run virus scan | | X | | |
| **Backups** | | | | |
| Automated System Recovery (ASR) | | | | X |
| Server data backup | | | X | |
| **Monitor** | | | | |
| Monitor resources usage | | X | | |
| PC hardware clean and check | | | X | |
| Server hardware clean and check | | | | X |
| Networking hardware clean and check | | | | X |
| Surveillance system check | | | | |
| Check internal connections and cables | | | | X |
| **File System Maintenance** | | | | |
| Disk defragmentation | | | X | |
| Unused application removes | | | X | |
| Disk integrity check | | | X | |
| Delete temporary internet files | X | | | |
| Delete temporary windows files | | X | | |
| Disk cleanup | | | X | |

*Table 3. 11 Maintenance Schedule for SYNTAX Solutions Matara branch*

### 3.2.3 User feedback form for SYNTAX Solutions Matara branch network

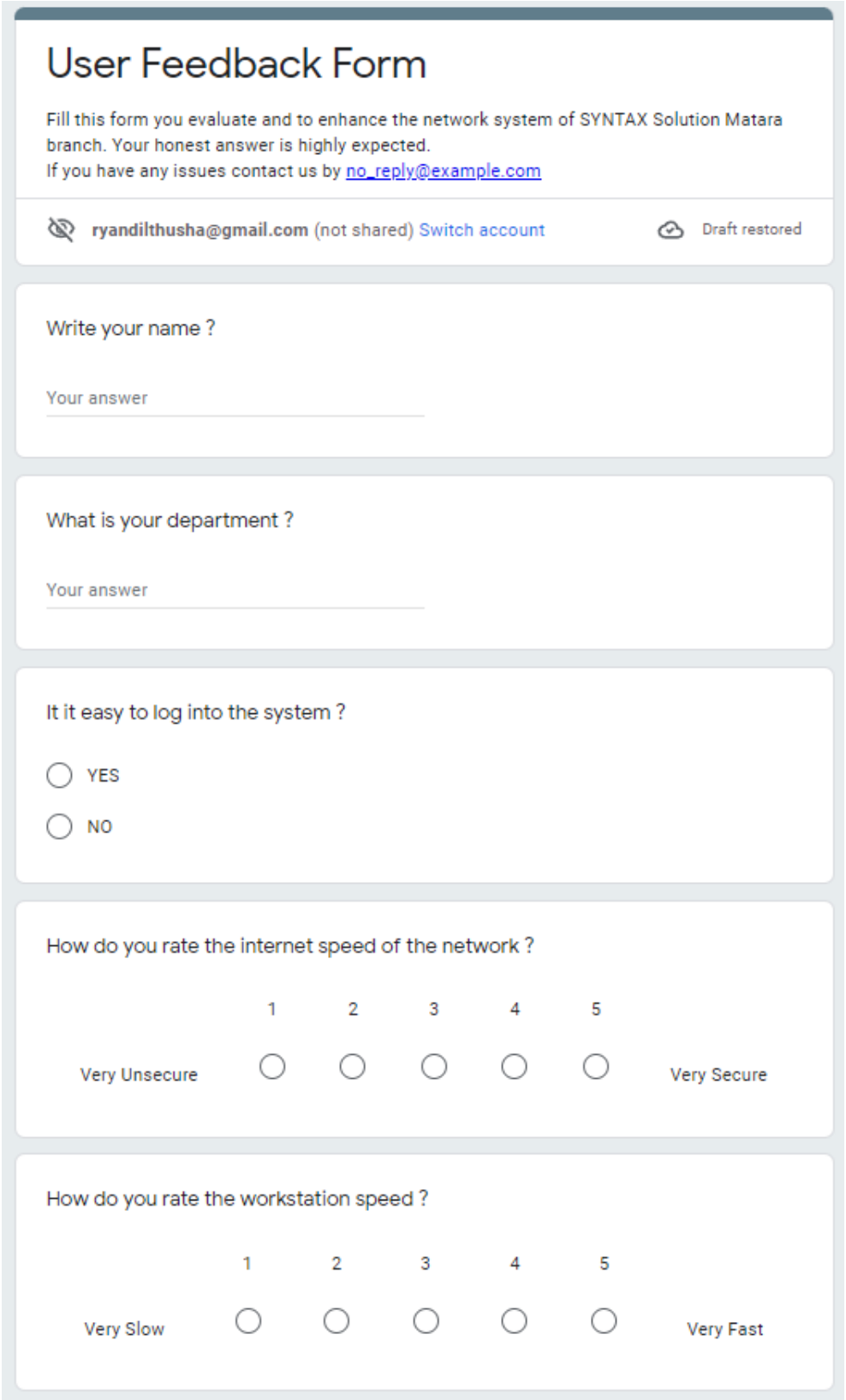



*Figure 3. 7 User feedback form for SYNTAX Solutions Matara branch network by Google Forms part 1*

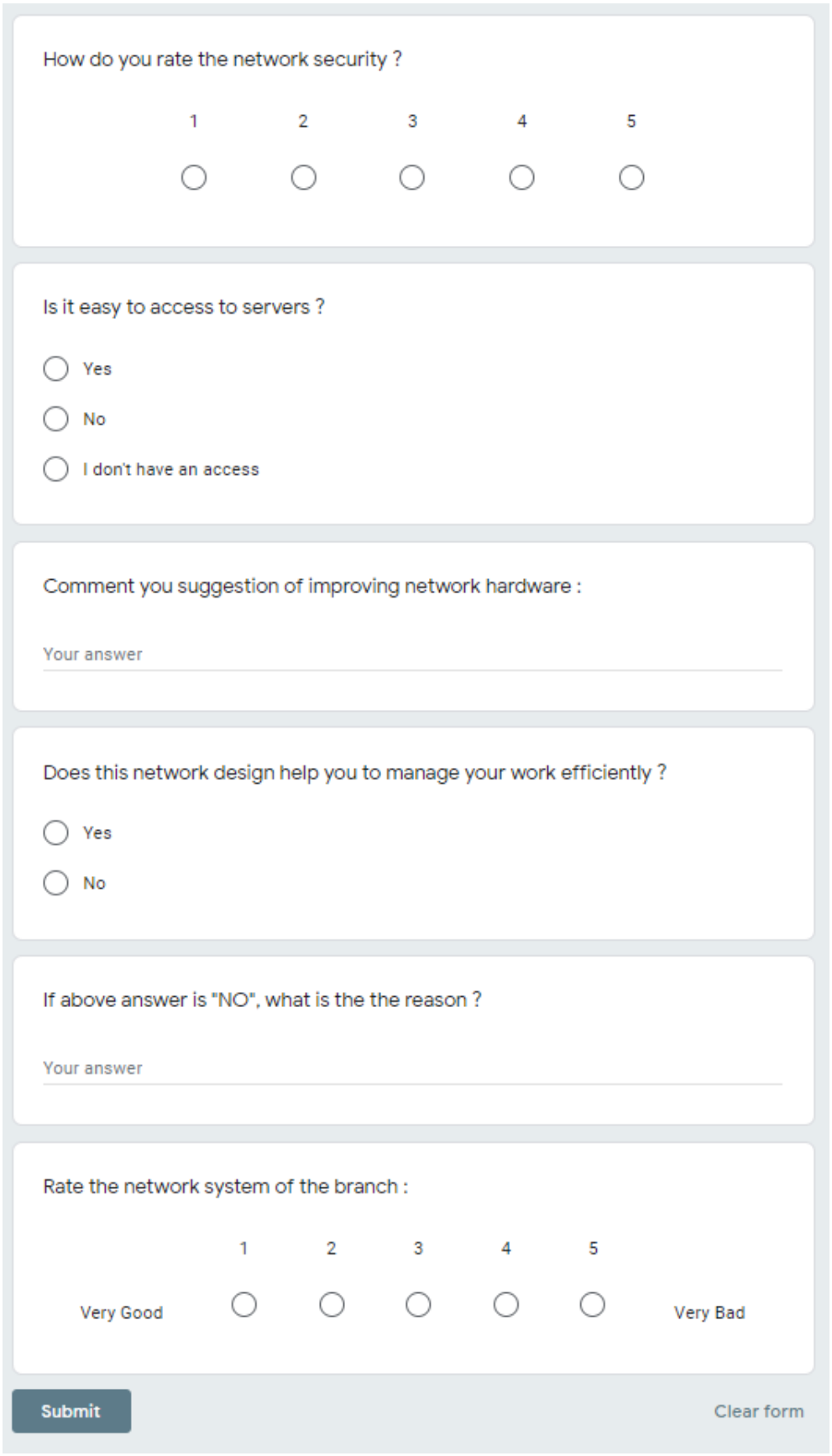



*Figure 3. 8 User feedback form for SYNTAX Solutions Matara branch network by Google Forms part 2*

## 3.3 IP Subnetting for Matara Branch

For IPV4 (Internet Protocol Version 4), there are 5 classes. Each class has a specific IP addresses range. If the IP address 1st octet in decimal belongs to range of 192 – 223, that class is C. The given Network IP for the SYNTAX Solutions Matara branch is 192. Hence, this Network ID range is belonging to IPV4 class C type. Class C can give total number of 2097152 (221) Network IP addresses and 254 (28-2) number of Host IP addresses.

### 3.3.1 IP subnetting by method no.1 :

The given Network ID = 192.168.10.0/24

Require number of subnets = 7

We can do IPV4 class C subnetting easily by using below table. According to that table's "Subnet" row there isn't number 7 which is the number of require number of subnets in our scenario. But we can choose number 8. Hence, we can ignore all other columns.

| Subnet | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |
|---|---|---|---|---|---|---|---|---|---|
| Host | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Subnet Mask | /24 | /25 | /26 | /27 | /28 | /29 | /30 | /31 | /32 |

*Figure 3. 9 IPV4 class C subnetting table*

Subnet row value is 4 → This means we can divide the Network into 4 subnets.

Host Row value is 64 → This means each subnet can has 32 Host ID (Including Network ID + Broadcast ID)

Subnet Mask value is /27 → This means new subnet mask for all 8 subnets.

New Subnet Mask for every subnet is →

**11111111 11111111 11111111 111** 00000 → /27

According to above information we can easily manage and get details such as host ID range, number of usable hosts, network ID, broadcast ID, gateway ID and VLAN number.

| Network IP | Host IP Range | Number of usable Hosts | Broadcast IP |
|---|---|---|---|
| For Departments | | | |
| 192.168.10.0 | 192.168.10.1 - 192.168.10.30 | 30 | 192.168.10.31 |
| 192.168.10.32 | 192.168.10.33 - 192.168.10.62 | 30 | 192.168.10.63 |
| 192.168.10.64 | 192.168.10.65 - 192.168.10.94 | 30 | 192.168.10.95 |
| 192.168.10.96 | 192.168.10.97 - 192.168.10.126 | 30 | 192.168.10.127 |
| 192.168.10.128 | 192.168.10.129 - 192.168.10.158 | 30 | 192.168.10.159 |
| 192.168.10.160 | 192.168.10.161 - 192.168.10.190 | 30 | 192.168.10.191 |
| 192.168.10.192 | 192.168.10.193 - 192.168.10.222 | 30 | 192.168.10.223 |
| 192.168.10.224 | 192.168.10.225 - 192.168.10.254 | 30 | 192.168.10.255 |
| For Server Room | | | |
| 10.254.1.0 | 10.254.1.1 - 10.254.1.254 | 254 | 10.254.1.255 |

*Table 3. 12 Subnetting given IP address with method 1 part 1*

Below table details will be useful when creating VLANs.

| Department | VLAN number | Network IP | Gateway IP | Broadcast ID | Subnet Mask |
|---|---|---|---|---|---|
| For Departments | | | | | |
| Network Team | 10 | 192.168.10.0 | 192.168.10.1 | 192.168.10.31 | 255.255.255.224 /24 |
| Developers | 20 | 192.168.10.32 | 192.168.10.33 | 192.168.10.63 | 255.255.255.224 /24 |
| HR | 30 | 192.168.10.64 | 192.168.10.65 | 192.168.10.95 | 255.255.255.224 /24 |
| Legal | 40 | 192.168.10.96 | 192.168.10.97 | 192.168.10.127 | 255.255.255.224 /24 |
| Finance | 50 | 192.168.10.128 | 192.168.10.129 | 192.168.10.159 | 255.255.255.224 /24 |
| Sales & Marketing | 60 | 192.168.10.160 | 192.168.10.161 | 192.168.10.191 | 255.255.255.224 /24 |
| Customer Care | 70 | 192.168.10.192 | 192.168.10.193 | 192.168.10.223 | 255.255.255.224 /24 |
| Extra Subnet | 80 | 192.168.10.224 | 192.168.10.225 | 192.168.10.255 | 255.255.255.224 /24 |
| For Server Room | | | | | |
| Server Rom | 100 | 10.254.1.0 | 10.254.1.1 | 10.254.1.255 | 255.255.255.224 /24 |

*Table 3. 13 Subnetting given IP address with method 1 part 2*

### 3.3.2 IP subnetting by method no.2 :

This is a general method to do subnetting.

The given Network ID = 192.168.10.0/24

Require number of subnets = 7

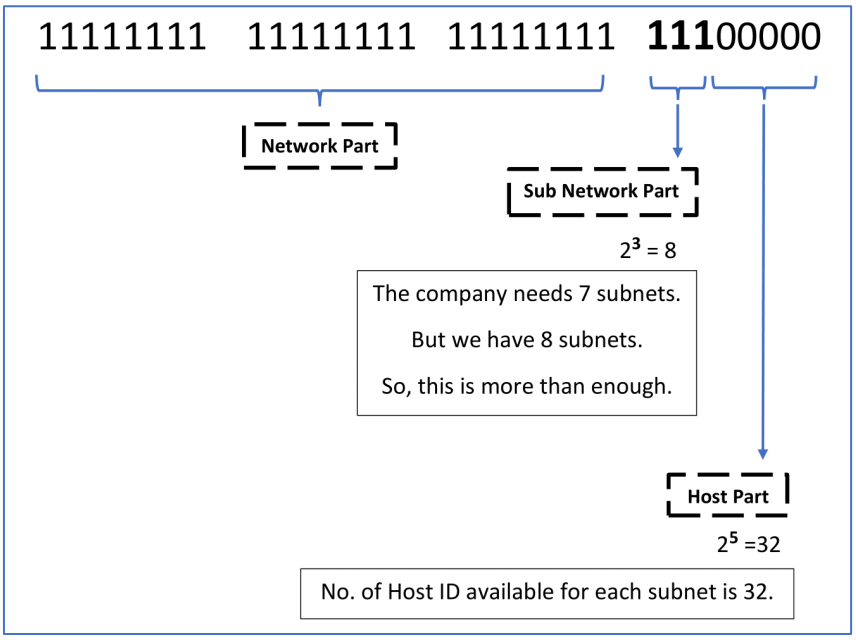



*Figure 3. 10 Parts of a IPV4 address in binary format*

New Subnet Mask is **11111111 11111111 11111111 111** 00000 → /27

| Network IP | Host IP Range | Number of usable Hosts | Broadcast IP |
|---|---|---|---|
| For Departments | | | |
| 192.168.10.0 | 192.168.10.1 - 192.168.10.30 | 30 | 192.168.10.31 |
| 192.168.10.32 | 192.168.10.33 - 192.168.10.62 | 30 | 192.168.10.63 |
| 192.168.10.64 | 192.168.10.65 - 192.168.10.94 | 30 | 192.168.10.95 |
| 192.168.10.96 | 192.168.10.97 - 192.168.10.126 | 30 | 192.168.10.127 |
| 192.168.10.128 | 192.168.10.129 - 192.168.10.158 | 30 | 192.168.10.159 |
| 192.168.10.160 | 192.168.10.161 - 192.168.10.190 | 30 | 192.168.10.191 |
| 192.168.10.192 | 192.168.10.193 - 192.168.10.222 | 30 | 192.168.10.223 |
| 192.168.10.224 | 192.168.10.225 - 192.168.10.254 | 30 | 192.168.10.255 |
| For Server Room | | | |
| 10.254.1.0 | 10.254.1.1 - 10.254.1.254 | 254 | 10.254.1.255 |

*Table 3. 14 Subnetting given IP address with method 2 part 1*

Below table details will be useful when creating VLANs.

| Department | VLAN number | Network IP | Gateway IP | Broadcast ID | Subnet Mask |
|---|---|---|---|---|---|
| For Departments | | | | | |
| Network Team | 10 | 192.168.10.0 | 192.168.10.1 | 192.168.10.31 | 255.255.255.224 /24 |
| Developers | 20 | 192.168.10.32 | 192.168.10.33 | 192.168.10.63 | 255.255.255.224 /24 |
| HR | 30 | 192.168.10.64 | 192.168.10.65 | 192.168.10.95 | 255.255.255.224 /24 |
| Legal | 40 | 192.168.10.96 | 192.168.10.97 | 192.168.10.127 | 255.255.255.224 /24 |
| Finance | 50 | 192.168.10.128 | 192.168.10.129 | 192.168.10.159 | 255.255.255.224 /24 |
| Sales & Marketing | 60 | 192.168.10.160 | 192.168.10.161 | 192.168.10.191 | 255.255.255.224 /24 |
| Customer Care | 70 | 192.168.10.192 | 192.168.10.193 | 192.168.10.223 | 255.255.255.224 /24 |
| Extra Subnet | 80 | 192.168.10.224 | 192.168.10.225 | 192.168.10.255 | 255.255.255.224 /24 |
| For Server Room | | | | | |
| Server Rom | 100 | 10.254.1.0 | 10.254.1.1 | 10.254.1.255 | 255.255.255.224 /24 |

*Table 3. 15 Subnetting given IP address with method 2 part 2*

The number of usable host IDs for each department is 30. This number won't be a problem since maximum number of employees for each department have 25.

## 3.4 Configure VLAN network devices by Cisco Packet Tracer

### 3.4.1 Cisco Packet Tracer VLAN design output for SYNTAX Solution Matara branch

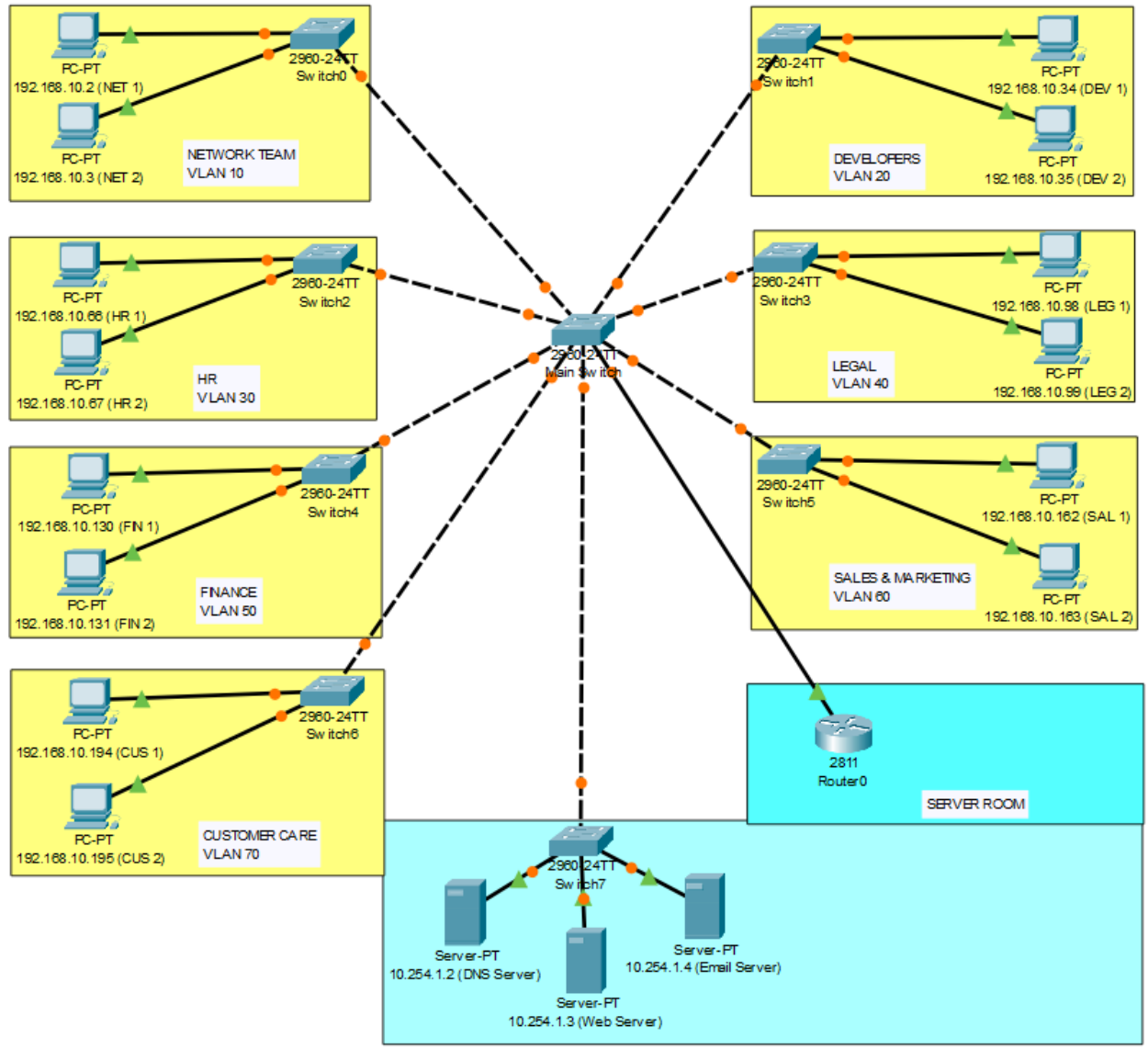



*Figure 3. 11 LAN design of SYNTAX Solutions Matara branch by Cisco Packet Tracer*

## 3.4.2 Comparison EdrawMax designed network system with Cisco Packet Tracer VLAN design

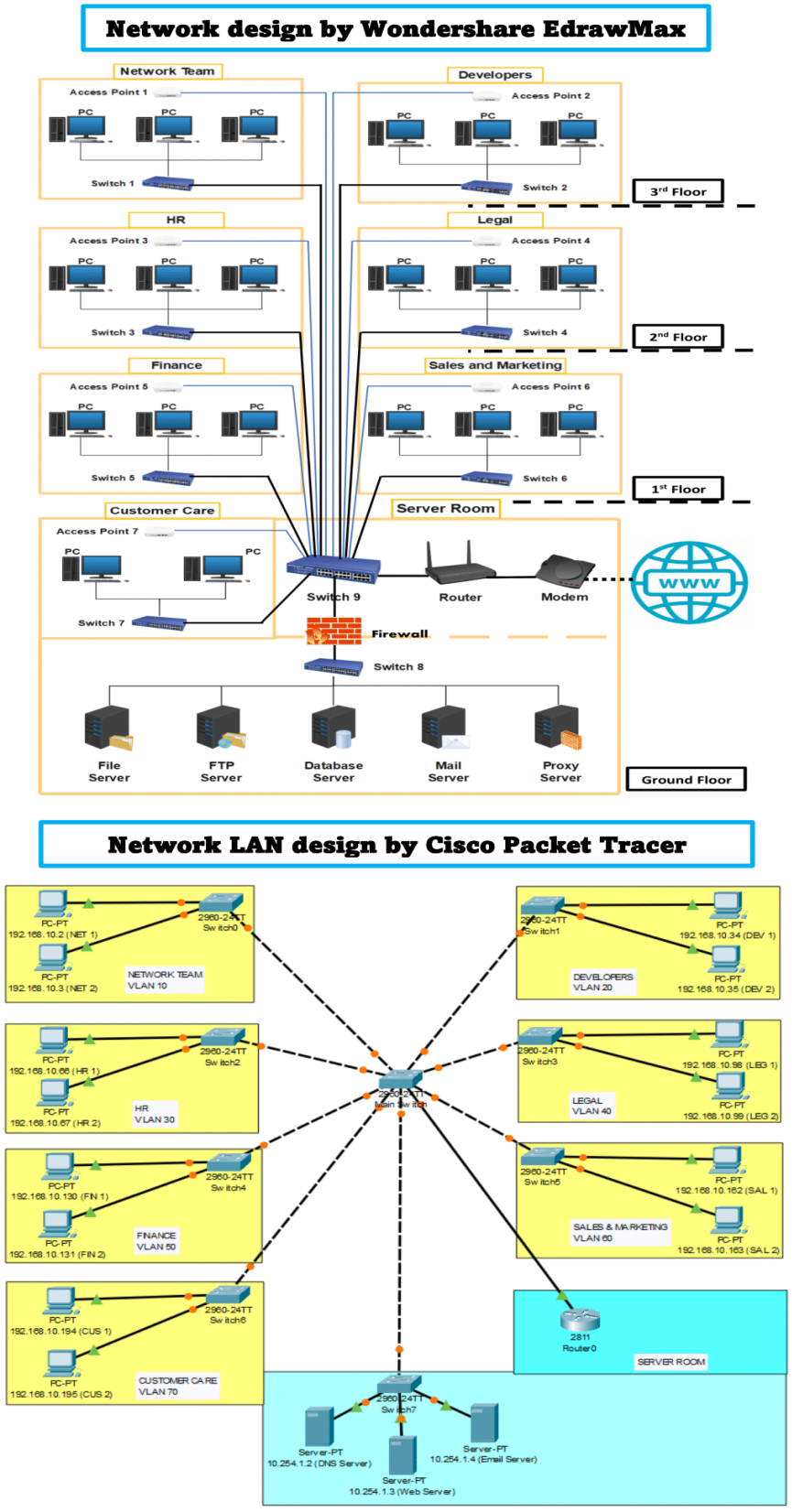



*Figure 3. 12 Comparison "EdrawMax" designed network system with "Cisco Packet Tracer" VLAN design*

## 3.4.3 Router Configuration

**Router show run :**

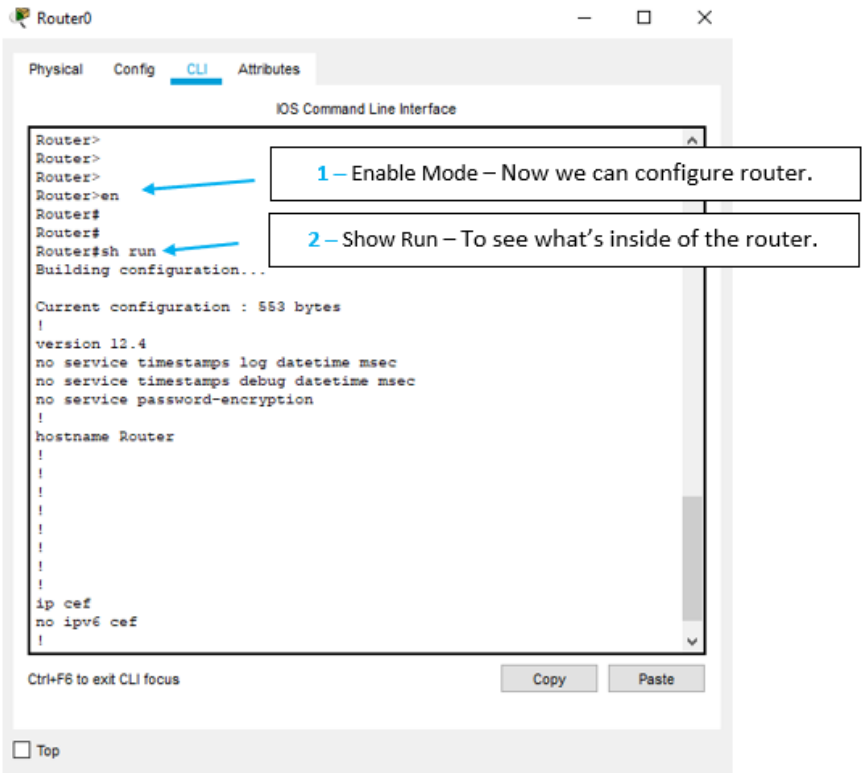



*Figure 3. 13 Router configuration → Router show run part 1*

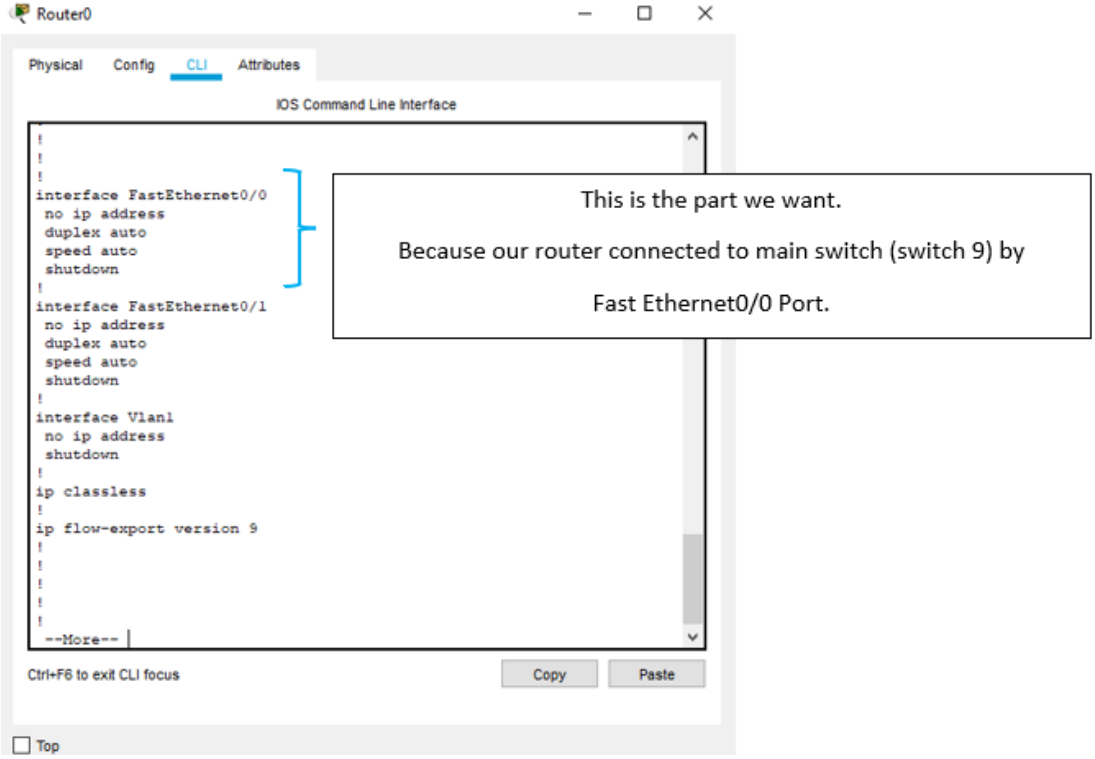



*Figure 3. 14 Router configuration → Router show run part 2*

## Creating VLANs from the Router :

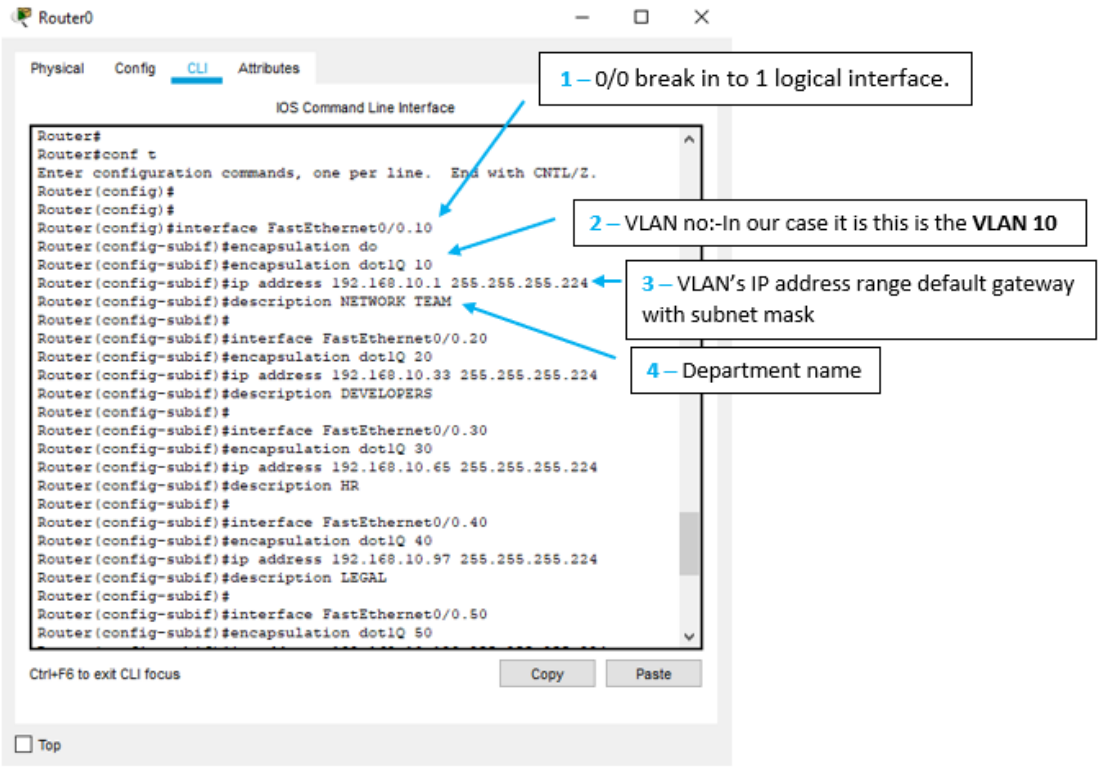



*Figure 3. 15 Router configuration → Creating VLANs from the Router part 1*

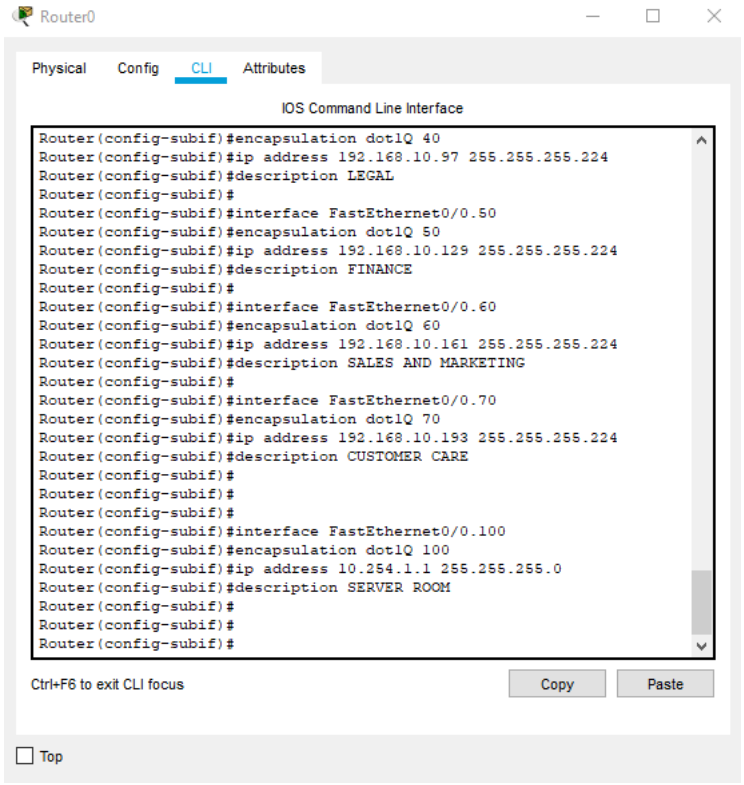



*Figure 3. 16 Router configuration → Creating VLANs from the Router part 2*

**Router show run and check status :**

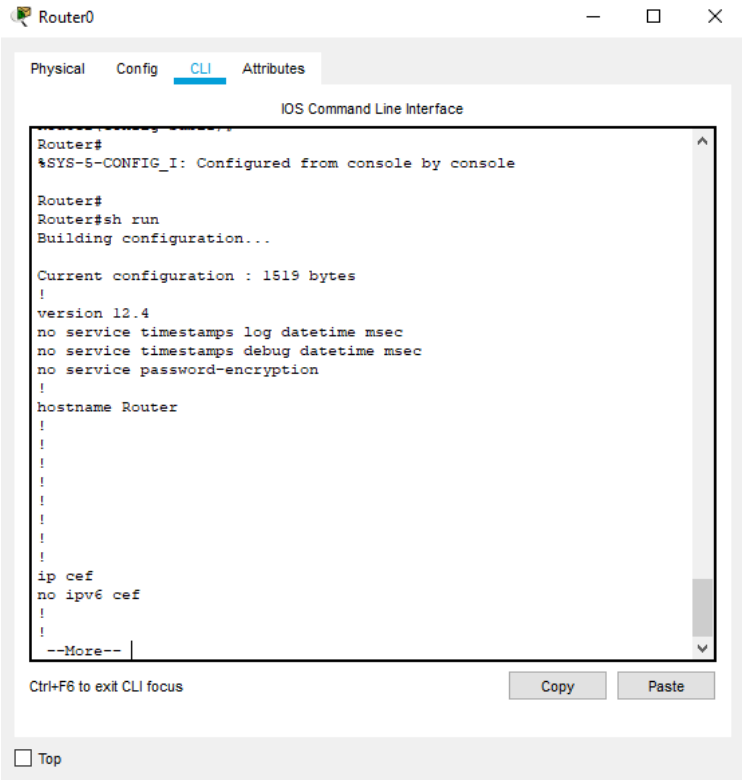



*Figure 3. 17 Router configuration → Router show run and check status part 1*

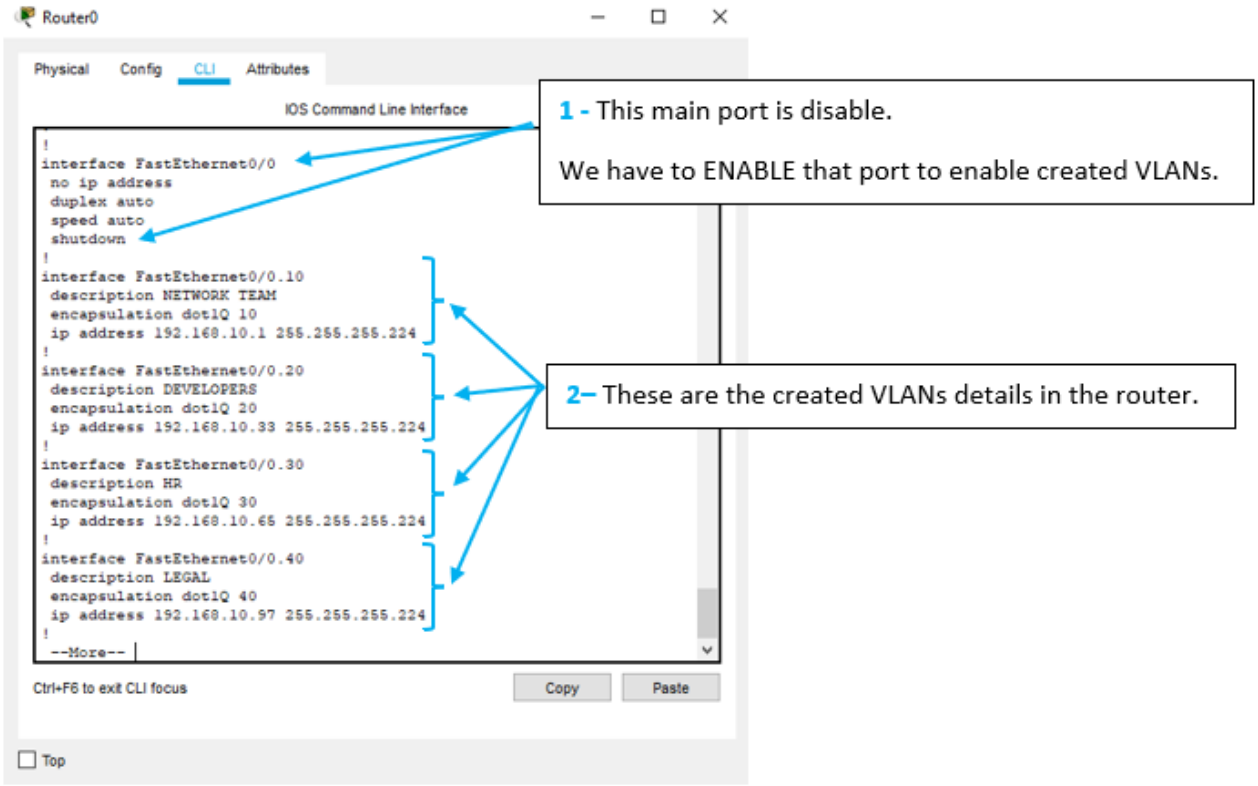



*Figure 3. 18 Router configuration → Router show run and check status part 2*

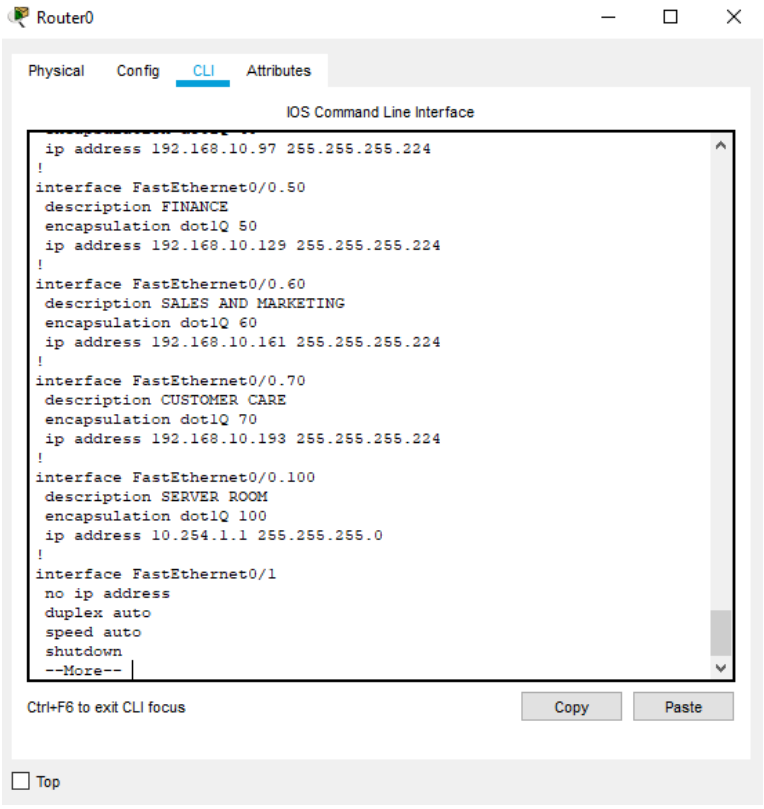



*Figure 3. 19 Router configuration → Router show run and check status part 3*

## Enable VLANs in the router :

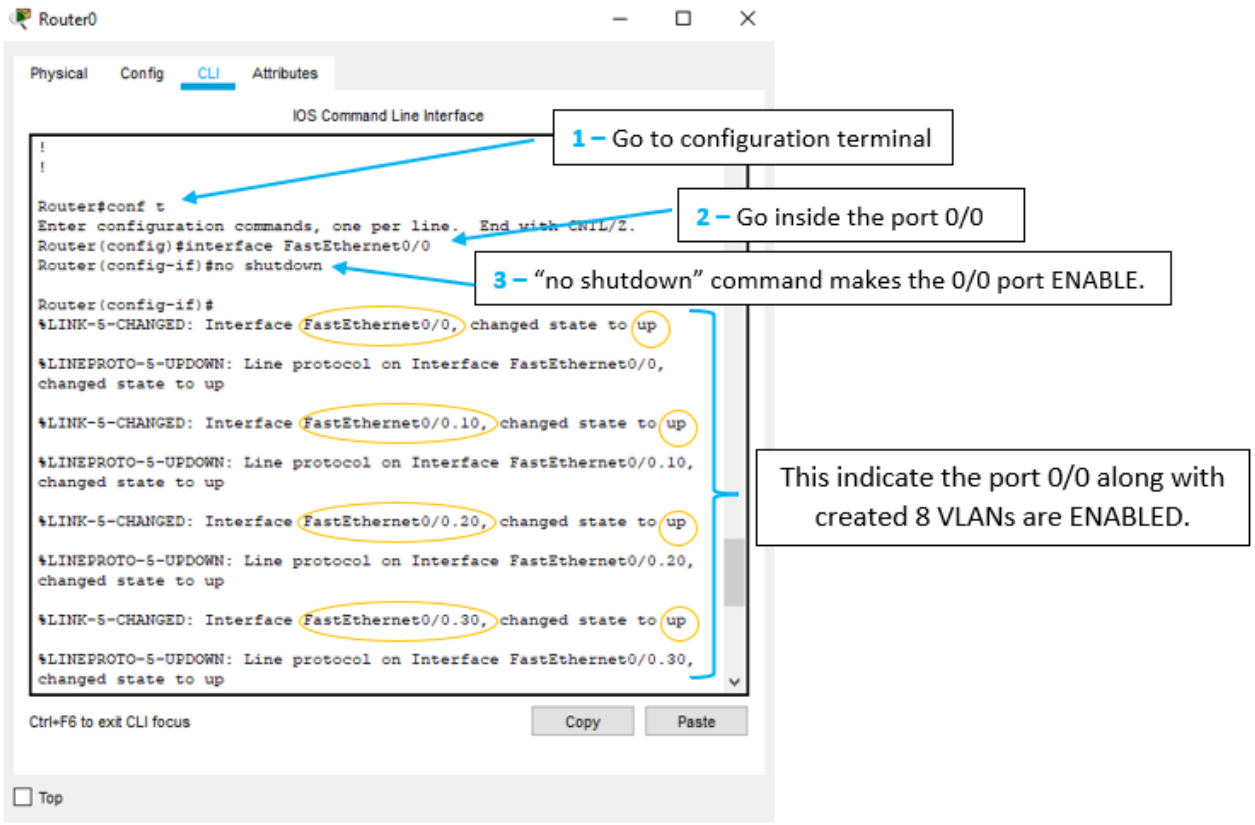



*Figure 3. 20 Router configuration → Enable VLANs in the router by "no shut" command part 1*

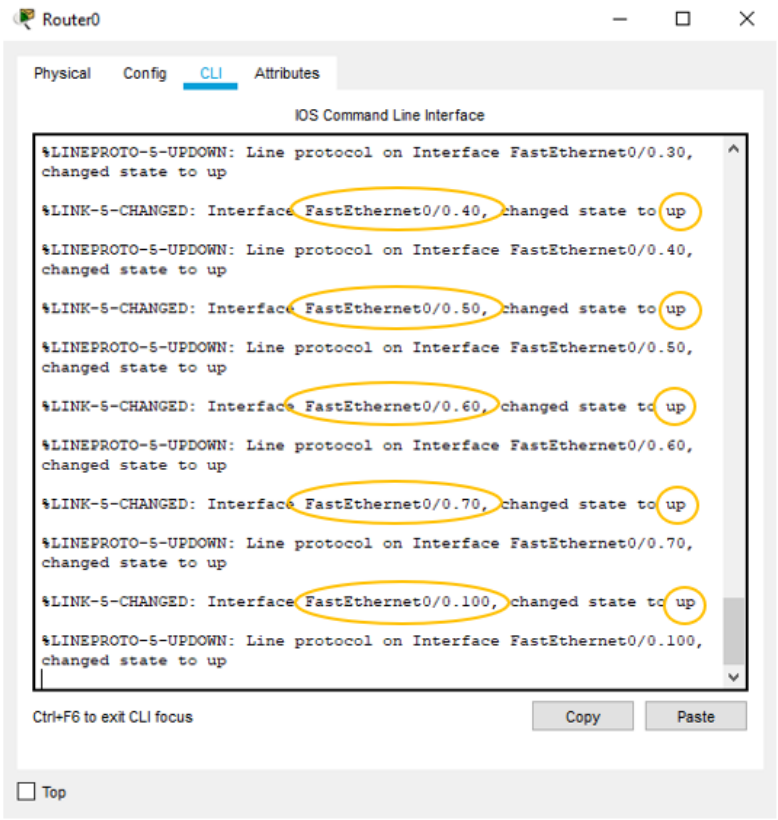



*Figure 3. 21 Router configuration → Enable VLANs in the router by "no shut" command part 2*

**Router show run and check enabled VLANs status :**

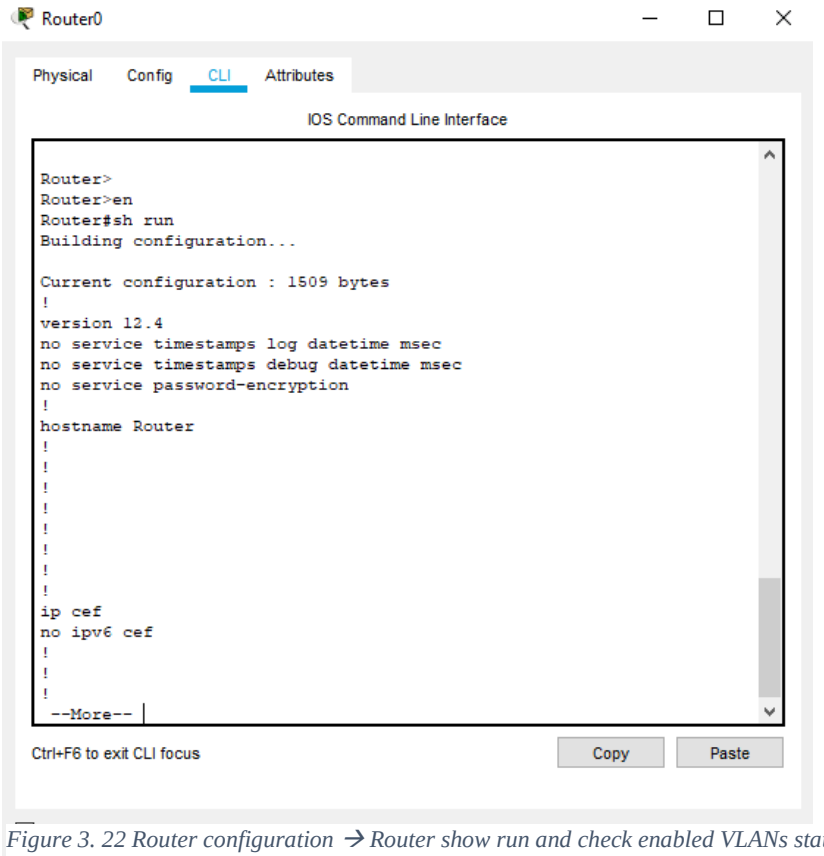



*Figure 3. 22 Router configuration → Router show run and check enabled VLANs status part 1*

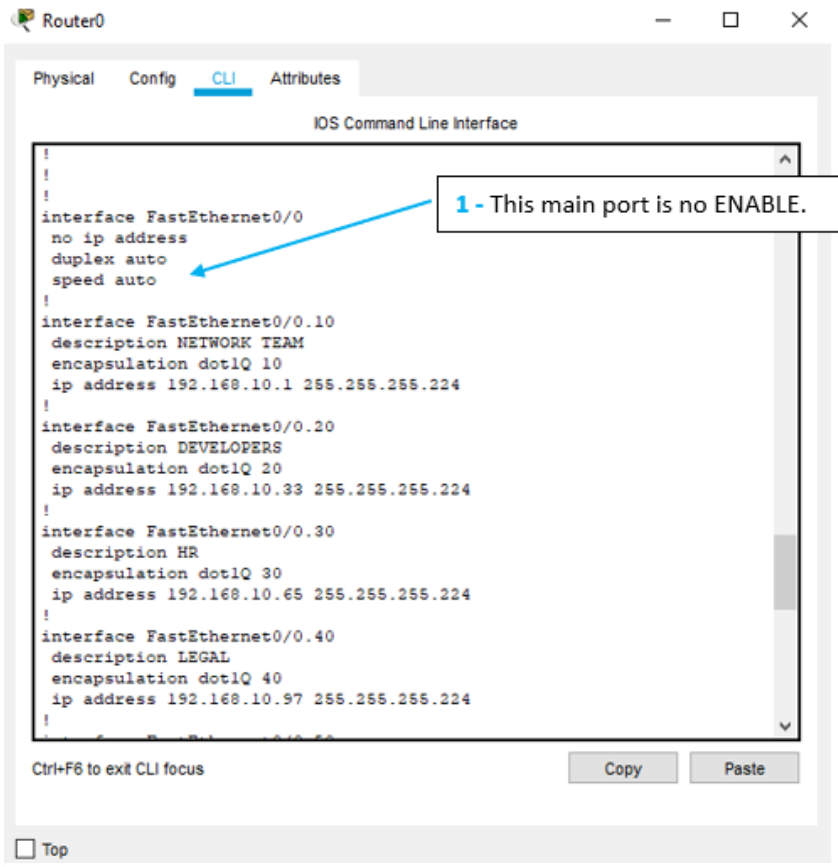



*Figure 3. 23 Router configuration → Router show run and check enabled VLANs status part 2*

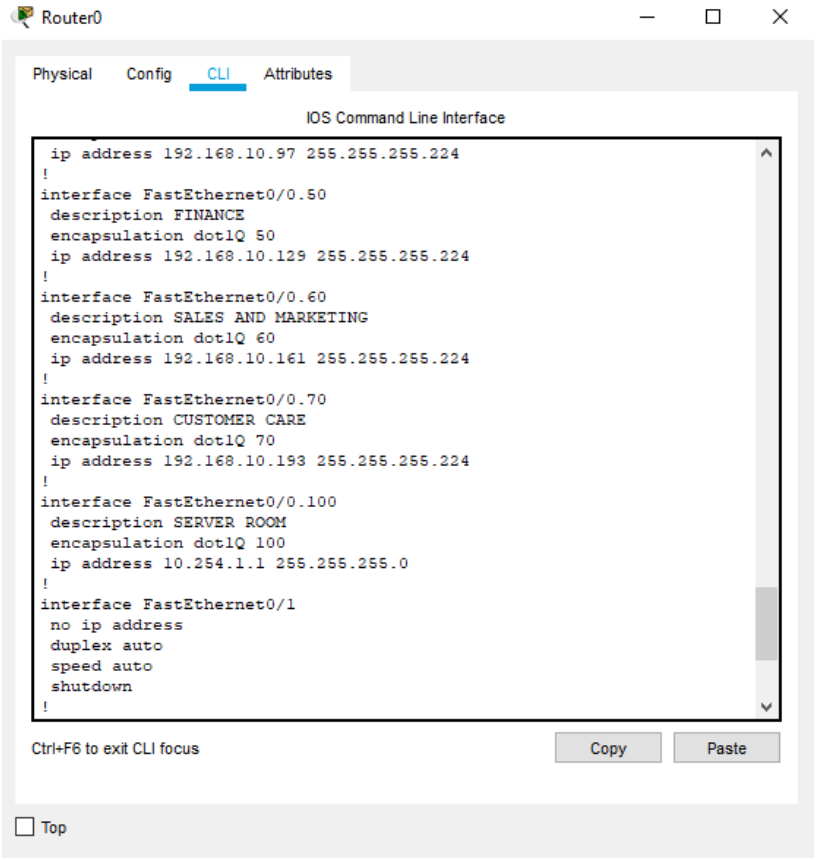



*Figure 3. 24 Router configuration → Router show run and check enabled VLANs status part 3*

**Telnet configuration :**

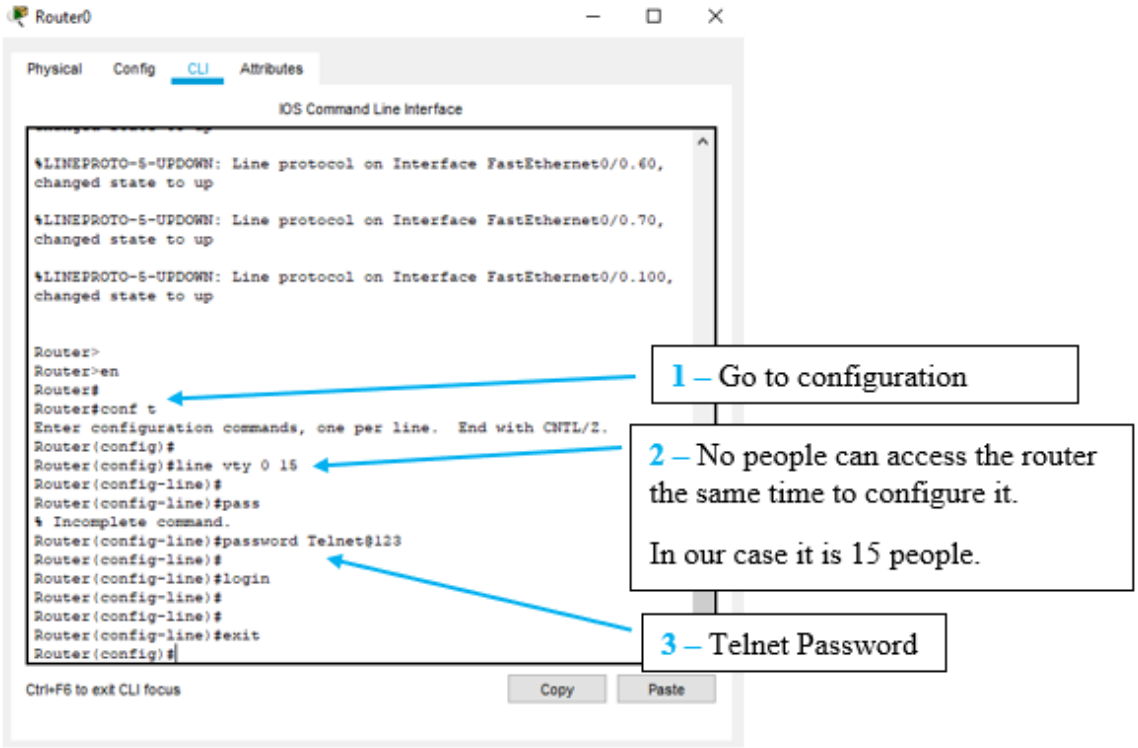



*Figure 3. 25 Router configuration → Telnet configuration from the router*

## 3.4.4 Main Switch Configuration

**Each department switch's cables attached ports configure into trunk :**

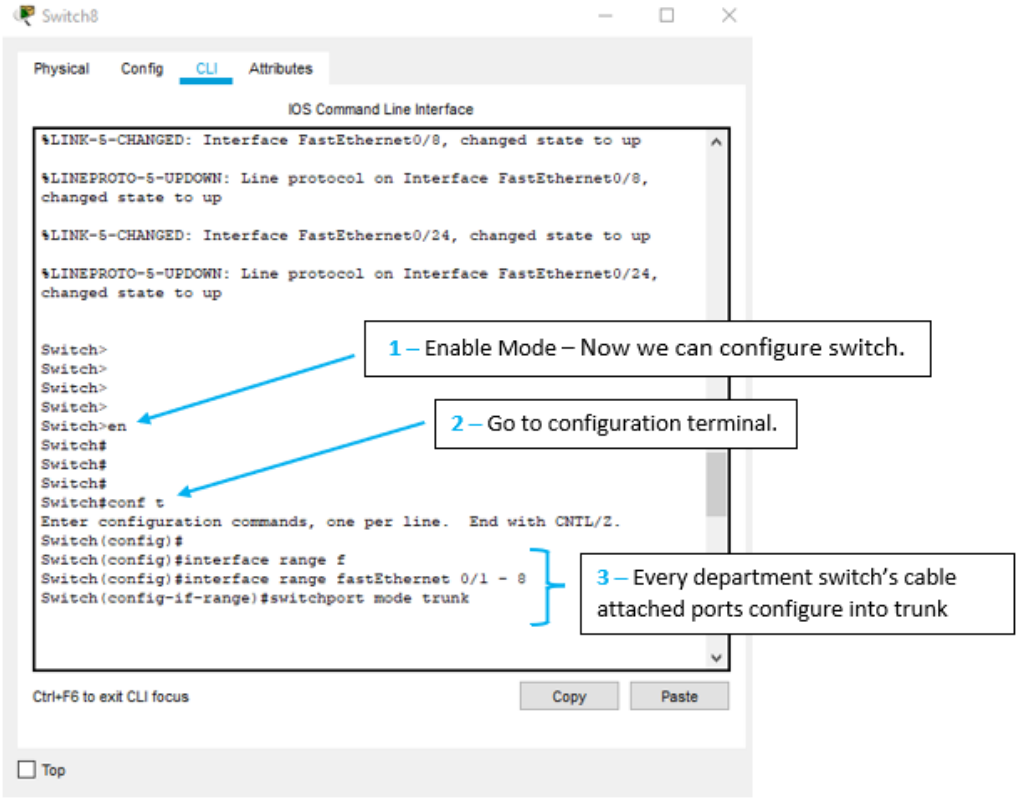



*Figure 3. 26 Main Switch configuration → Each department switch's cables attached ports configure into trunk part 1*

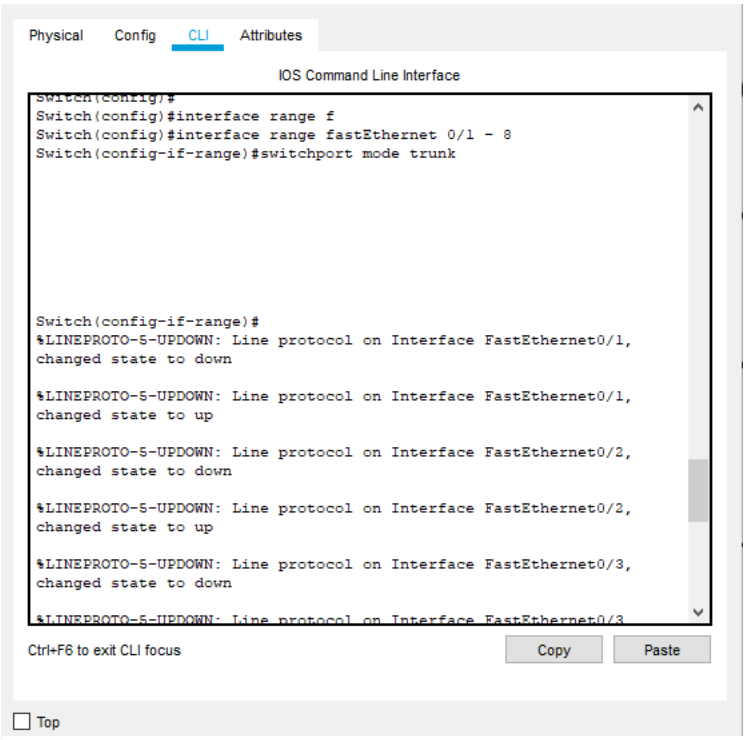



*Figure 3. 27 Main Switch configuration → Each department switch's cables attached ports configure into trunk part 2*

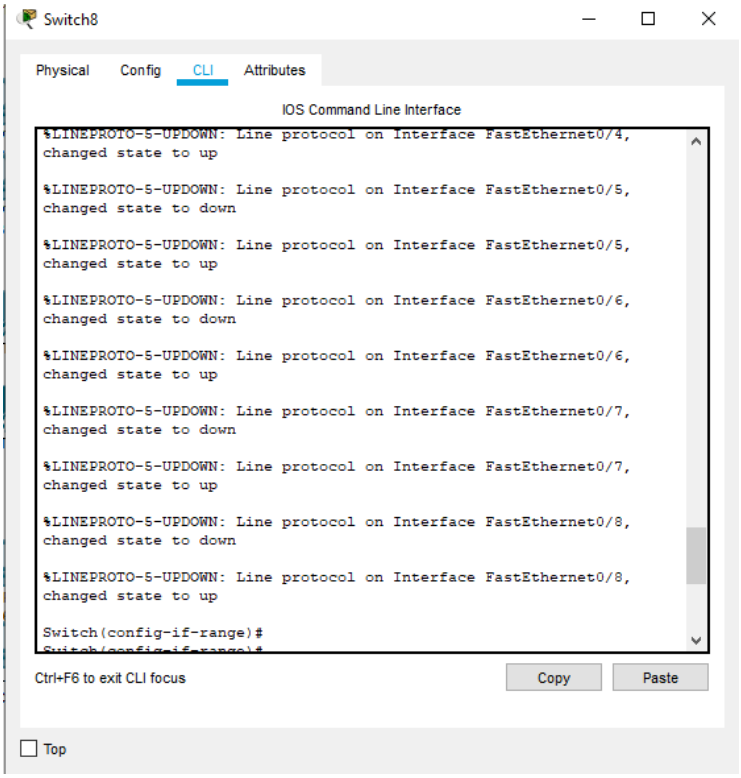



*Figure 3. 28 Main Switch configuration → Each department switch's cables attached ports configure into trunk part 3*

**Router cables attached ports configure into trunk :**

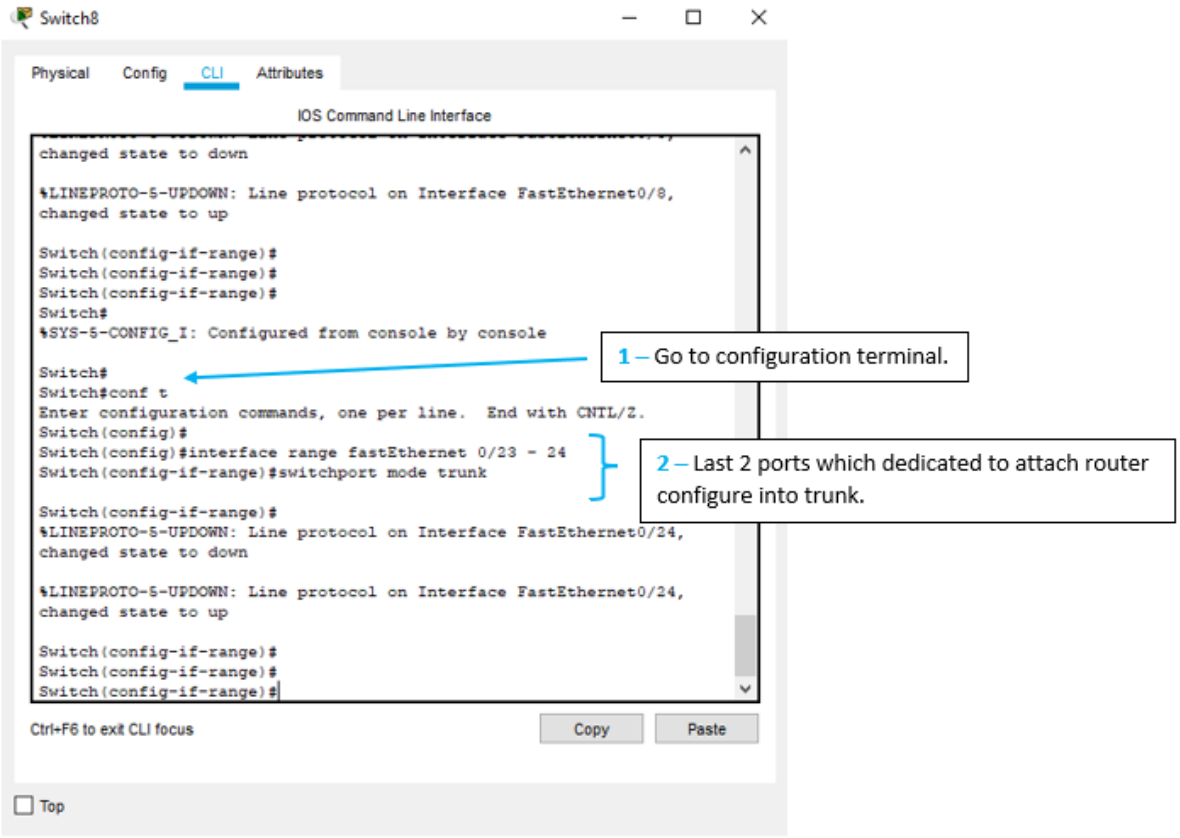



*Figure 3. 29 Main Switch configuration → Router cables attached ports configure into trunk part 1*

**Enter VLANs names into main switch for identification :**

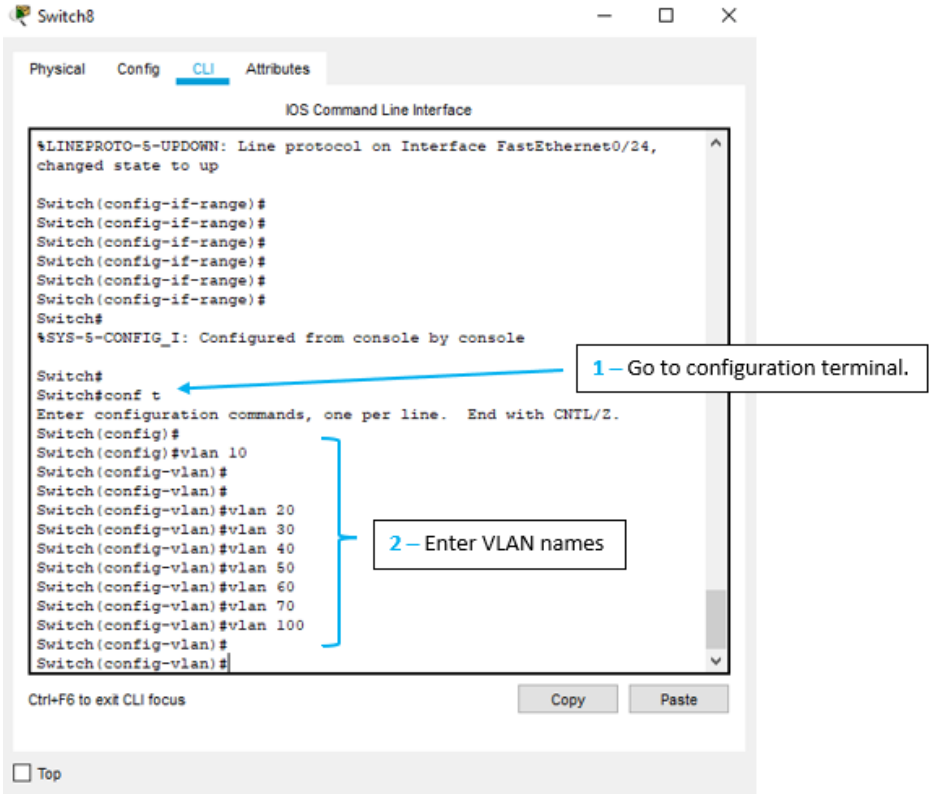



*Figure 3. 30 Main Switch configuration → Enter VLANs names into main switch for identification*

**Check main switch status :**

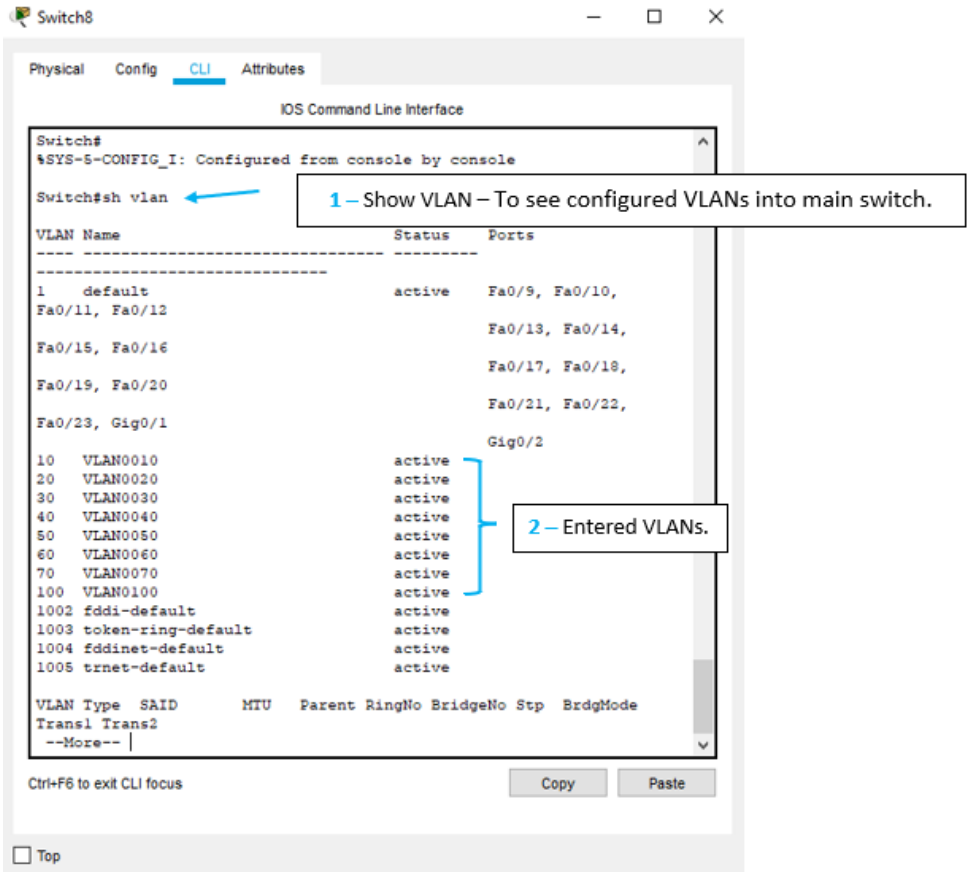



*Figure 3. 31 Main Switch configuration → Check main switch status by "show vlan" command*

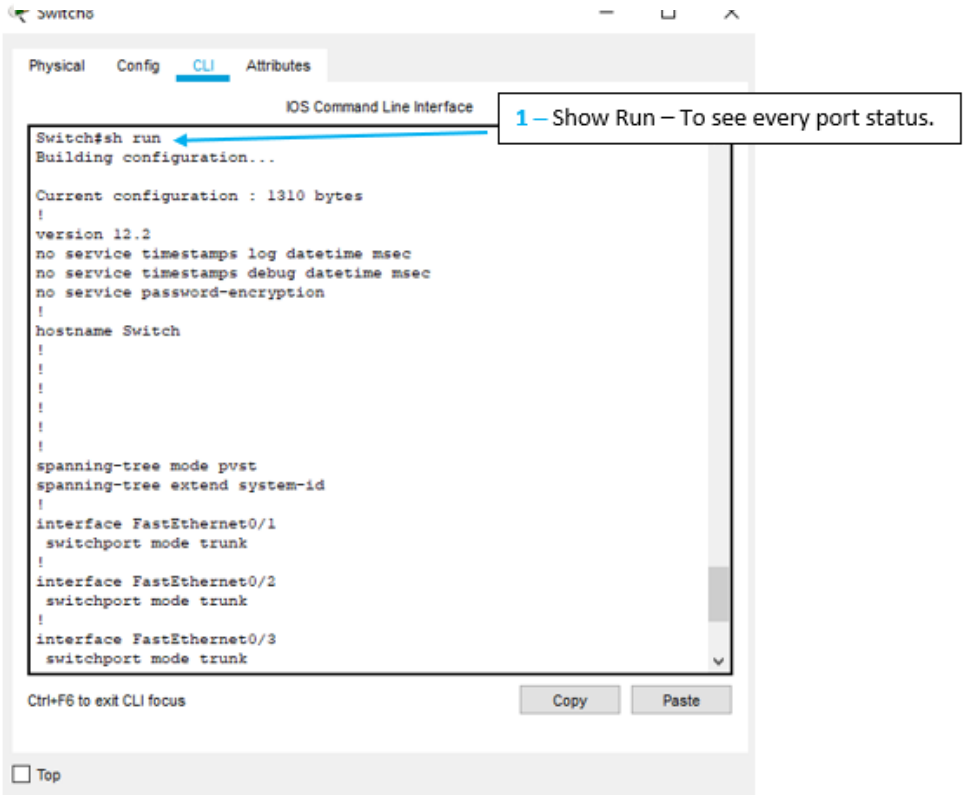



*Figure 3. 32 Main Switch configuration → Check main switch status by "show run" command part 1*

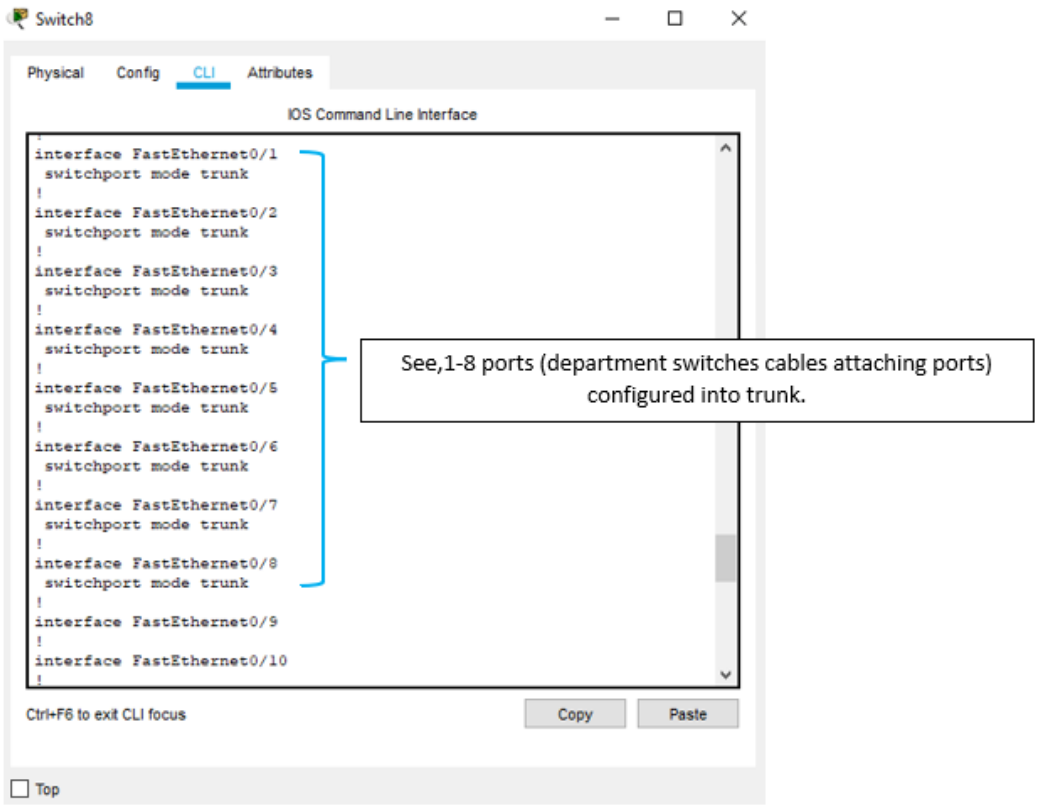



*Figure 3. 33 Main Switch configuration → Check main switch status by "show run" command part 2*

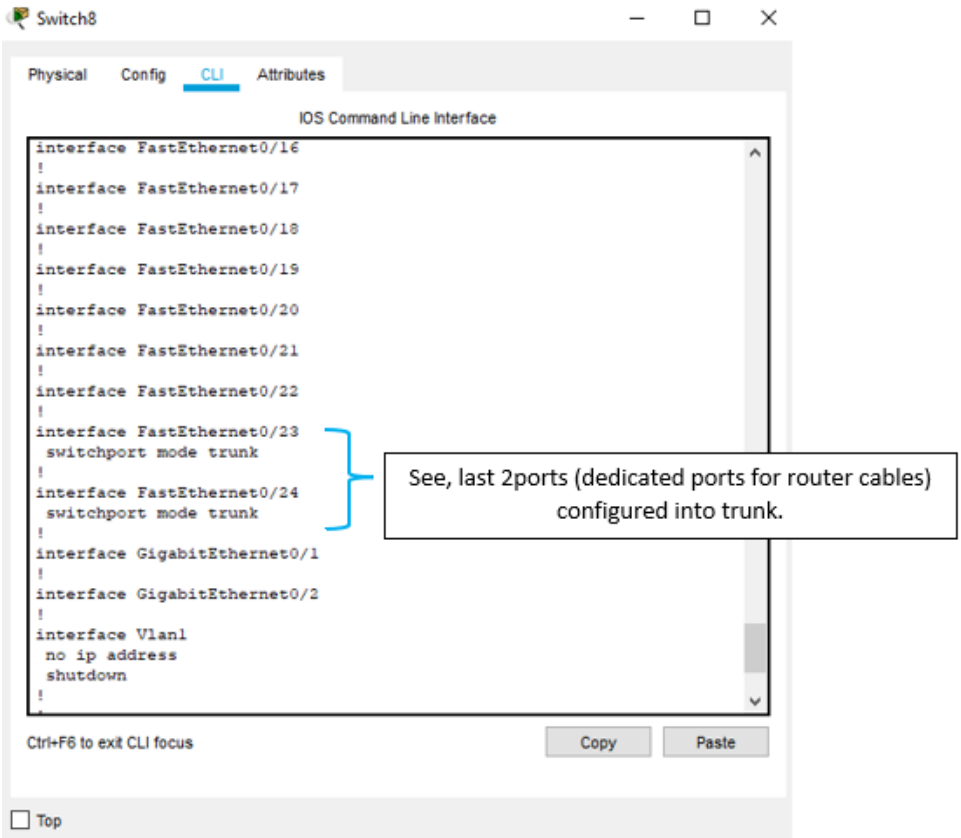



*Figure 3. 34 Main Switch configuration → Check main switch status by "show run" command part 3*

## 3.4.5 Department switches configuration

### Configure each department switches into VLAN and trunk :

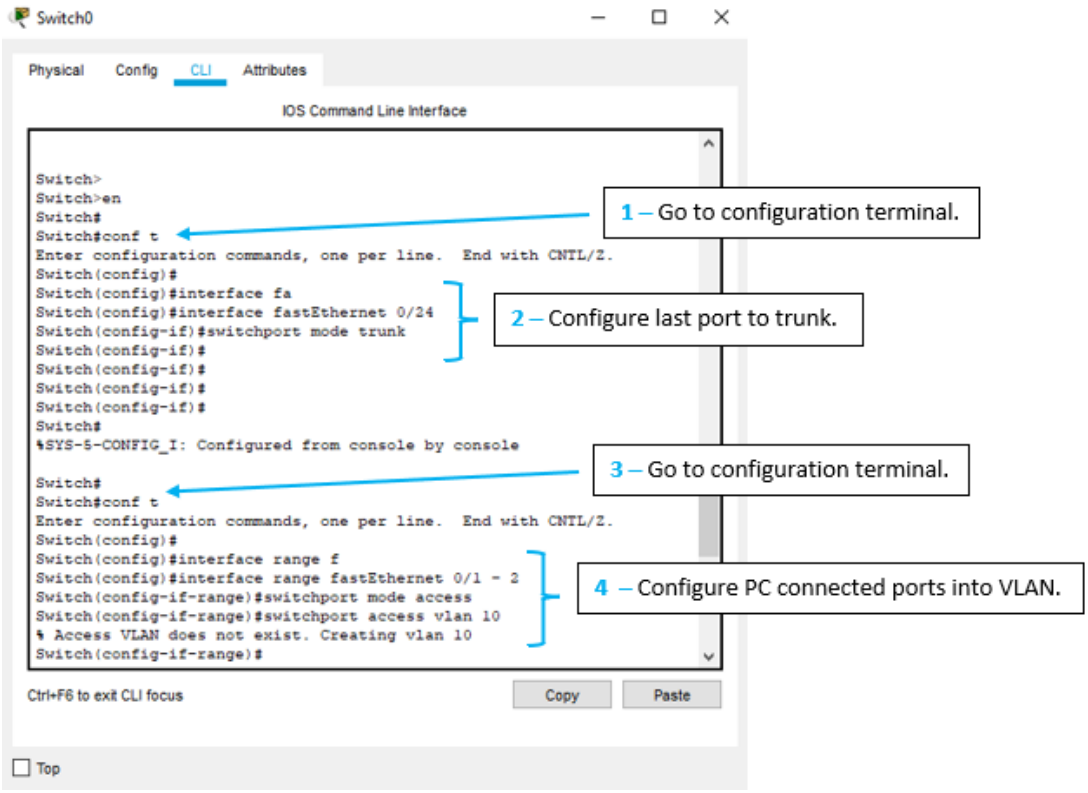



*Figure 3. 35 Department Switches configuration → Configure **Network Team** department switch into VLAN and trunk*

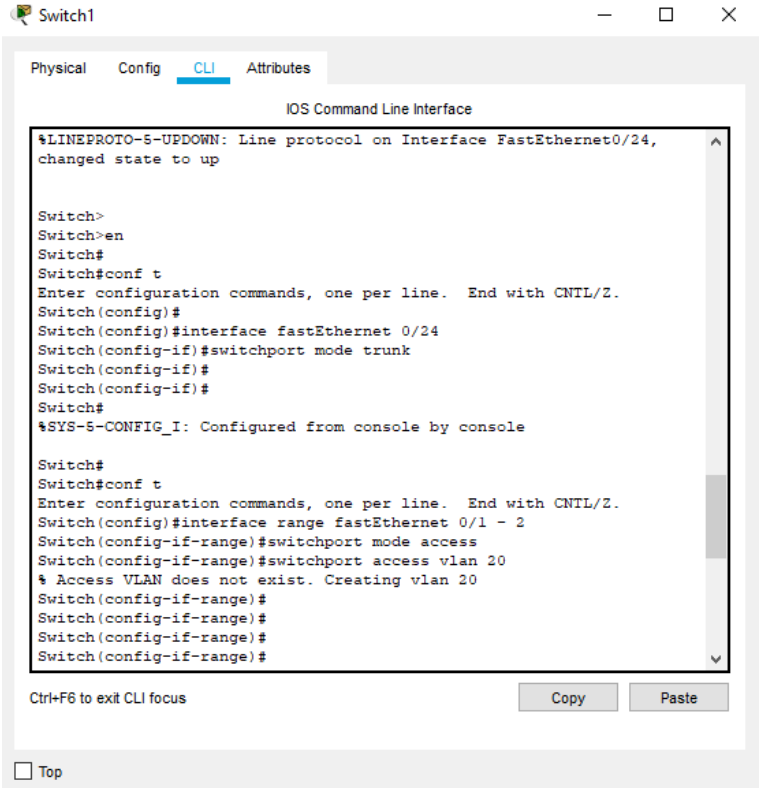



*Figure 3. 36 Department Switches configuration → Configure **Developers** department switch into VLAN and trunk*

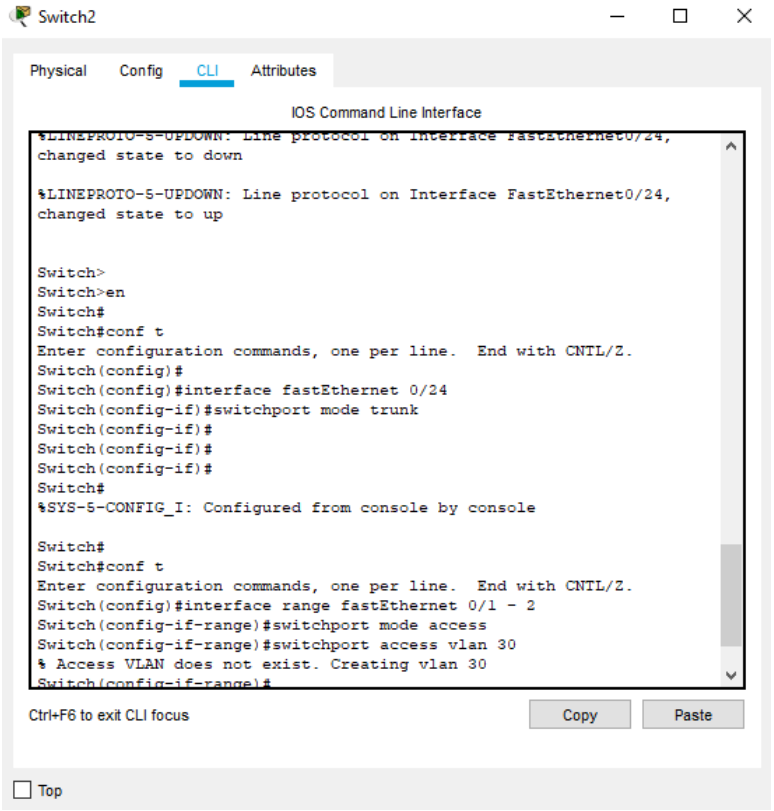



*Figure 3. 37 Department Switches configuration → Configure **HR** department switch into VLAN and trunk*

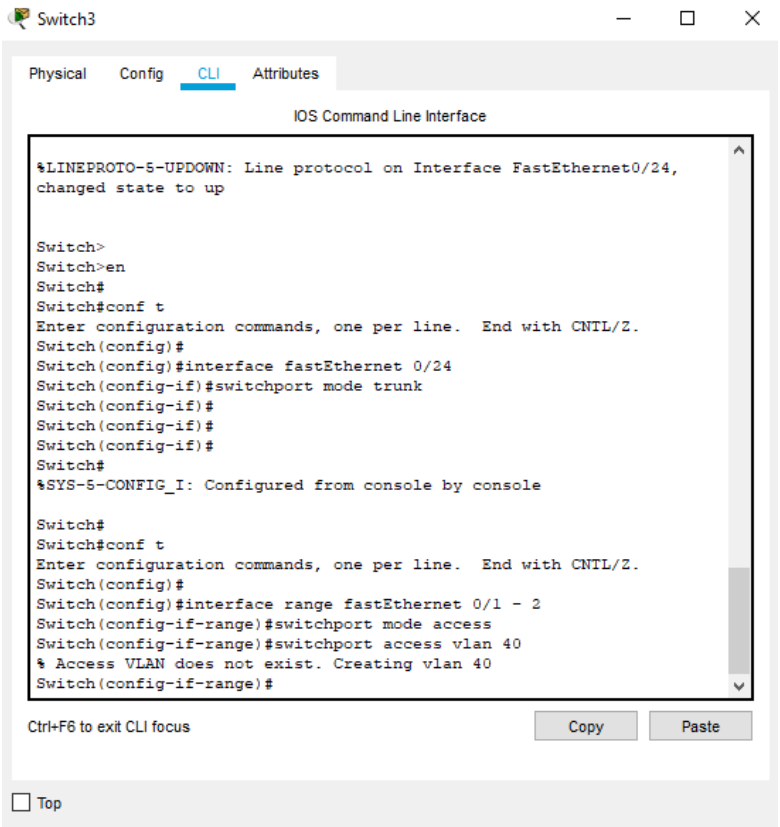



*Figure 3. 38 Department Switches configuration → Configure **Legal** department switch into VLAN and trunk*

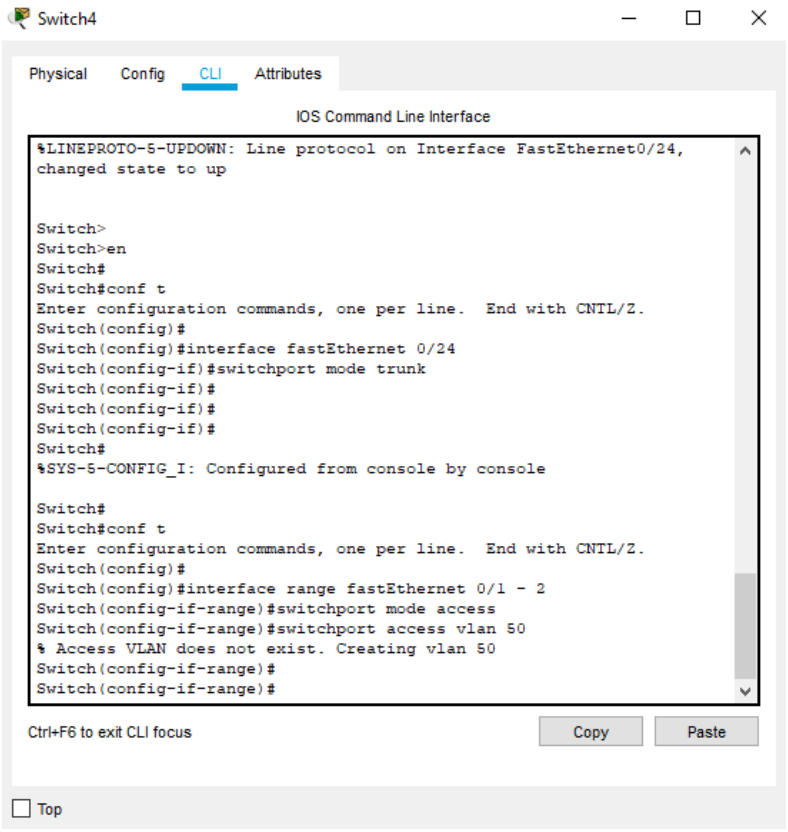



*Figure 3. 39 Department Switches configuration → Configure **Finance** department switch into VLAN and trunk*

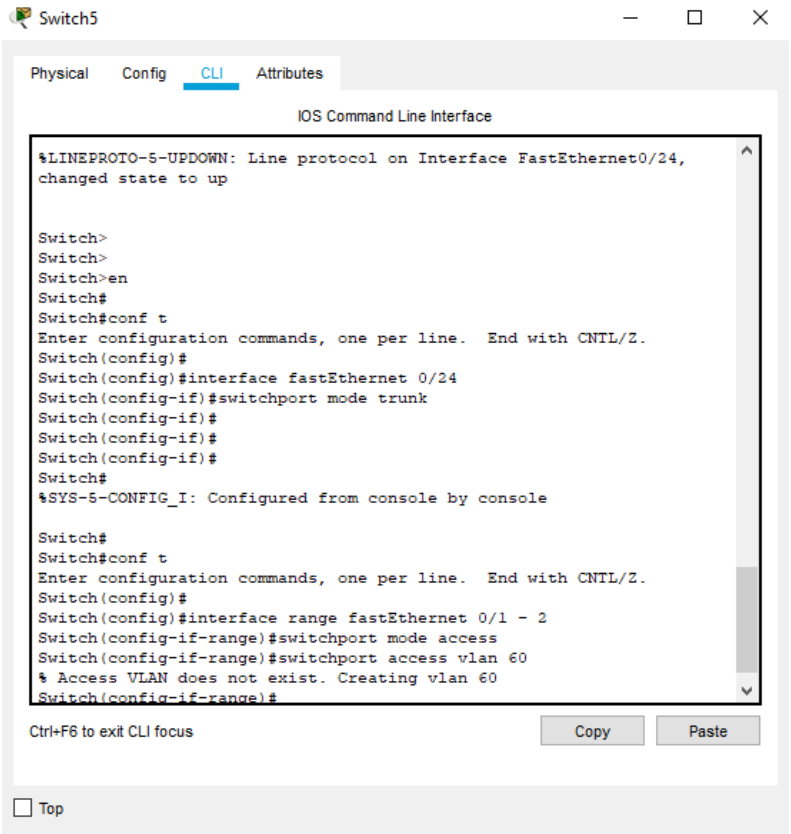



*Figure 3. 40 Department Switches configuration → Configure **Sales & Marketing** department switch into VLAN and trunk*

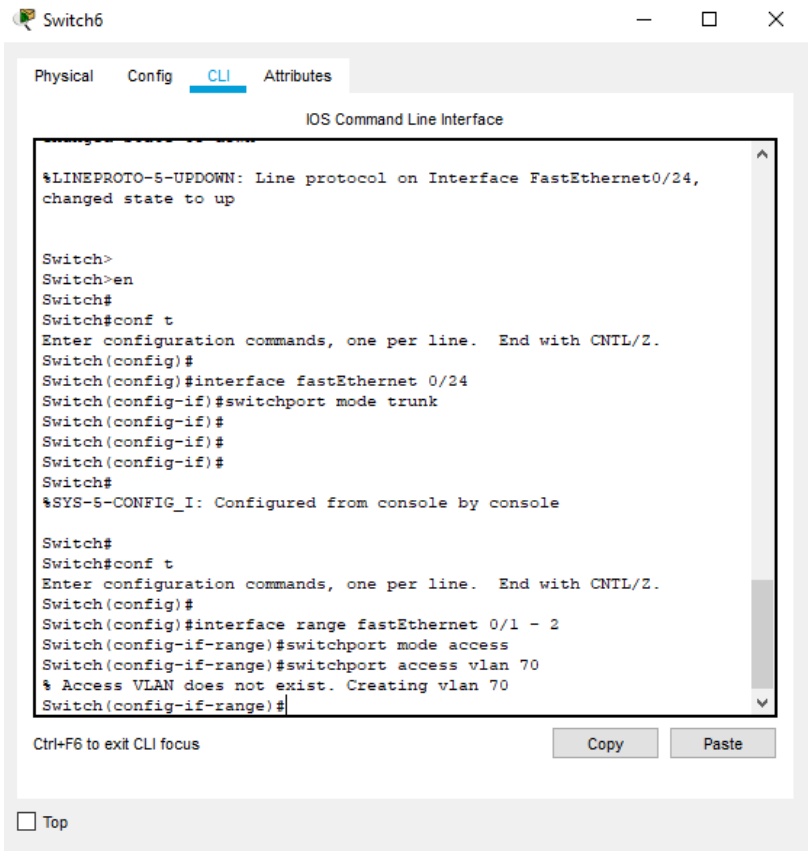



*Figure 3. 41 Department Switches configuration → Configure **Customer Care** department switch into VLAN and trunk*

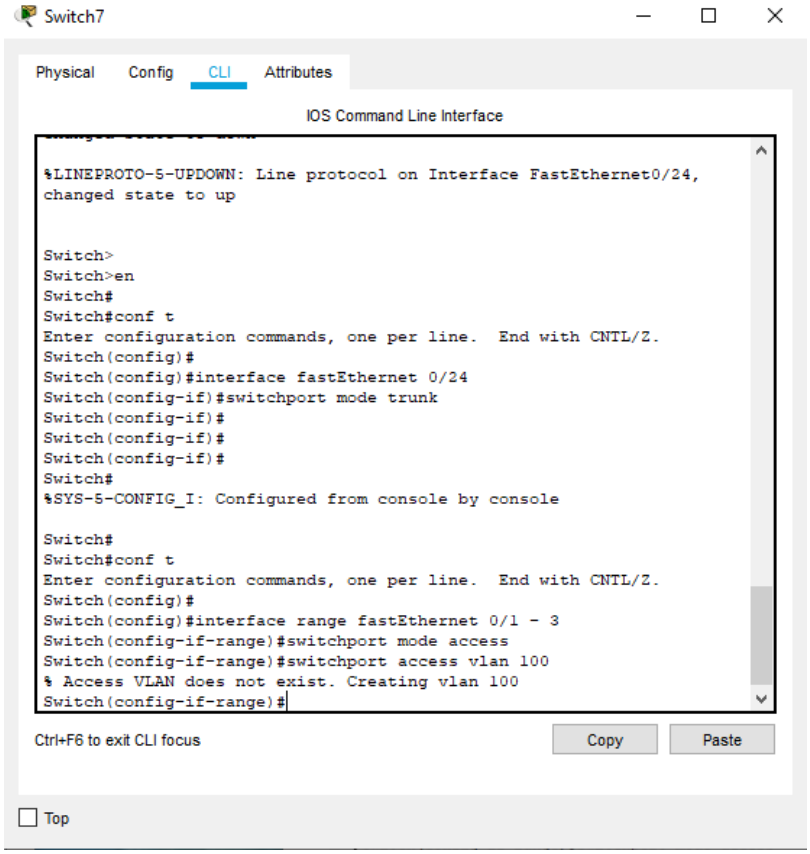



*Figure 3. 42 Department Switches configuration → Configure **Server Room** switch into VLAN and trunk*

## 3.4.6 Server configuration

**DNS Server configuration :**

The Domain Name System (DNS) Computer system that matches website hostnames (such as google.com) to their corresponding Internet Protocol (IP) addresses. A database of public IP addresses and their matching domain names is kept on the DNS server. DNS servers convert domain names into IP addresses that are understandable to machines.

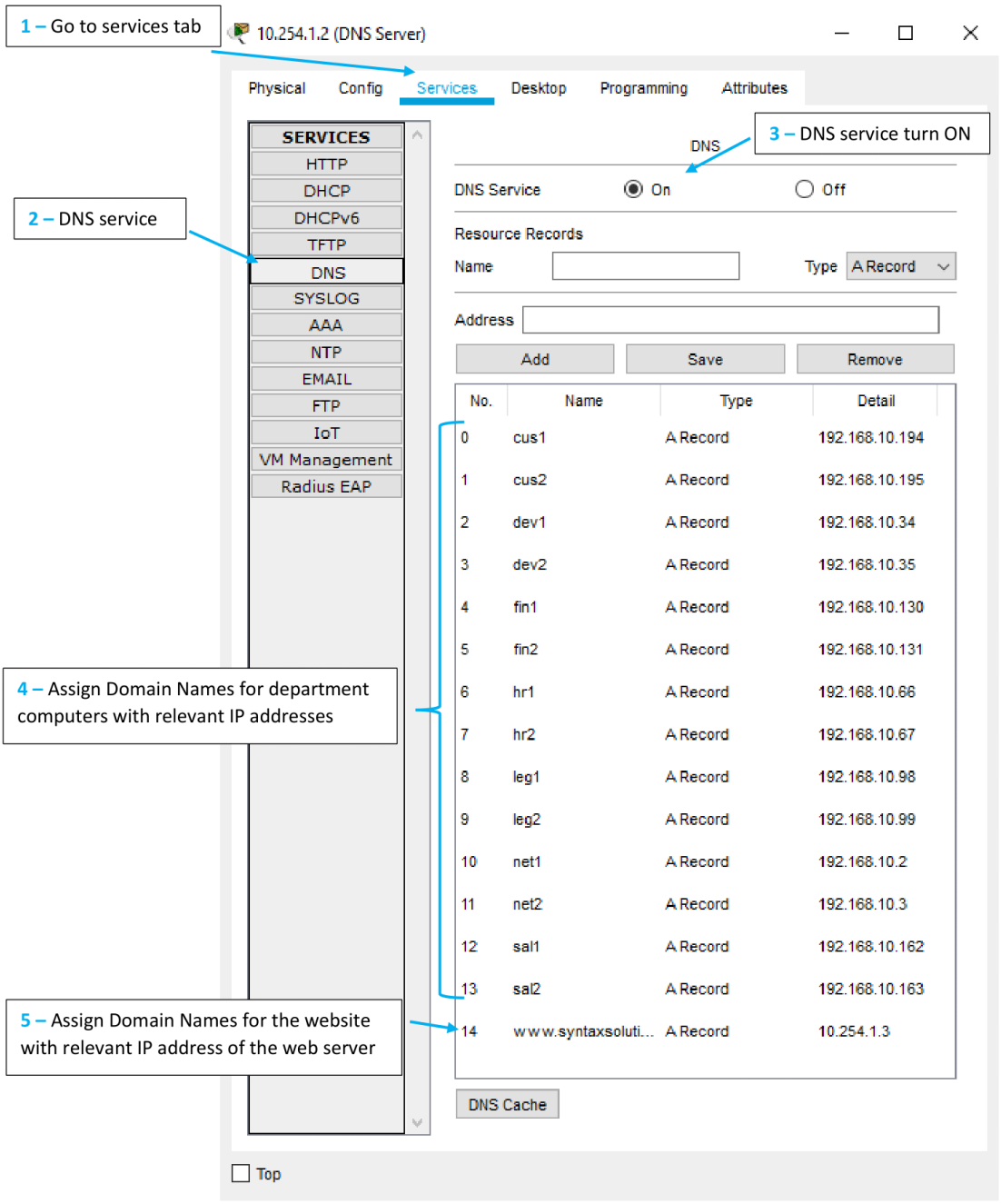



*Figure 3. 43 Server configuration → DNS Server configuration*

**Web Server configuration :**

A server is a device that manages the hosting of websites. It's a software program that requisitions web pages and distributes them as needed. The web server's primary goal is to store, process, and distribute web pages to users. The Hypertext Transfer Protocol is used for this intercommunication (HTTP).

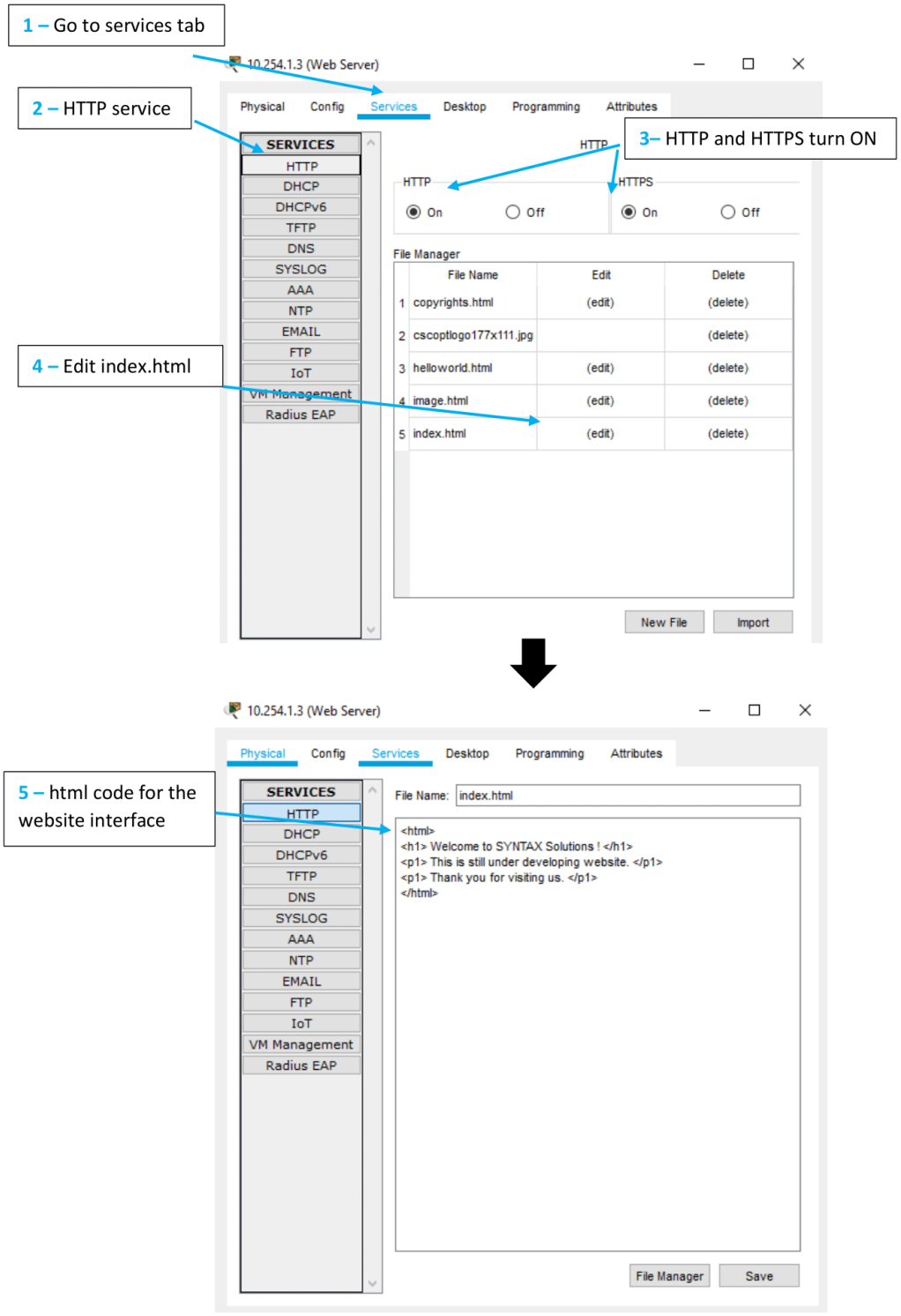



*Figure 3. 44 Server configuration → Web Server configuration*

**Email Server configuration :**

A mail transfer agent (MTA) is an e-mail server that is responsible for forwarding an e-mail message from sender to receiver, most typically using Simple Mail Transport Protocol (SMTP) to convey the message to the next server. We can't deliver your email to its intended recipient without an SMTP server. Our email messages are immediately translated into a string of codes and transmitted to our SMTP server when you click the "send" button from our email client. The codes are then processed, and the message is forwarded to the relevant email address.

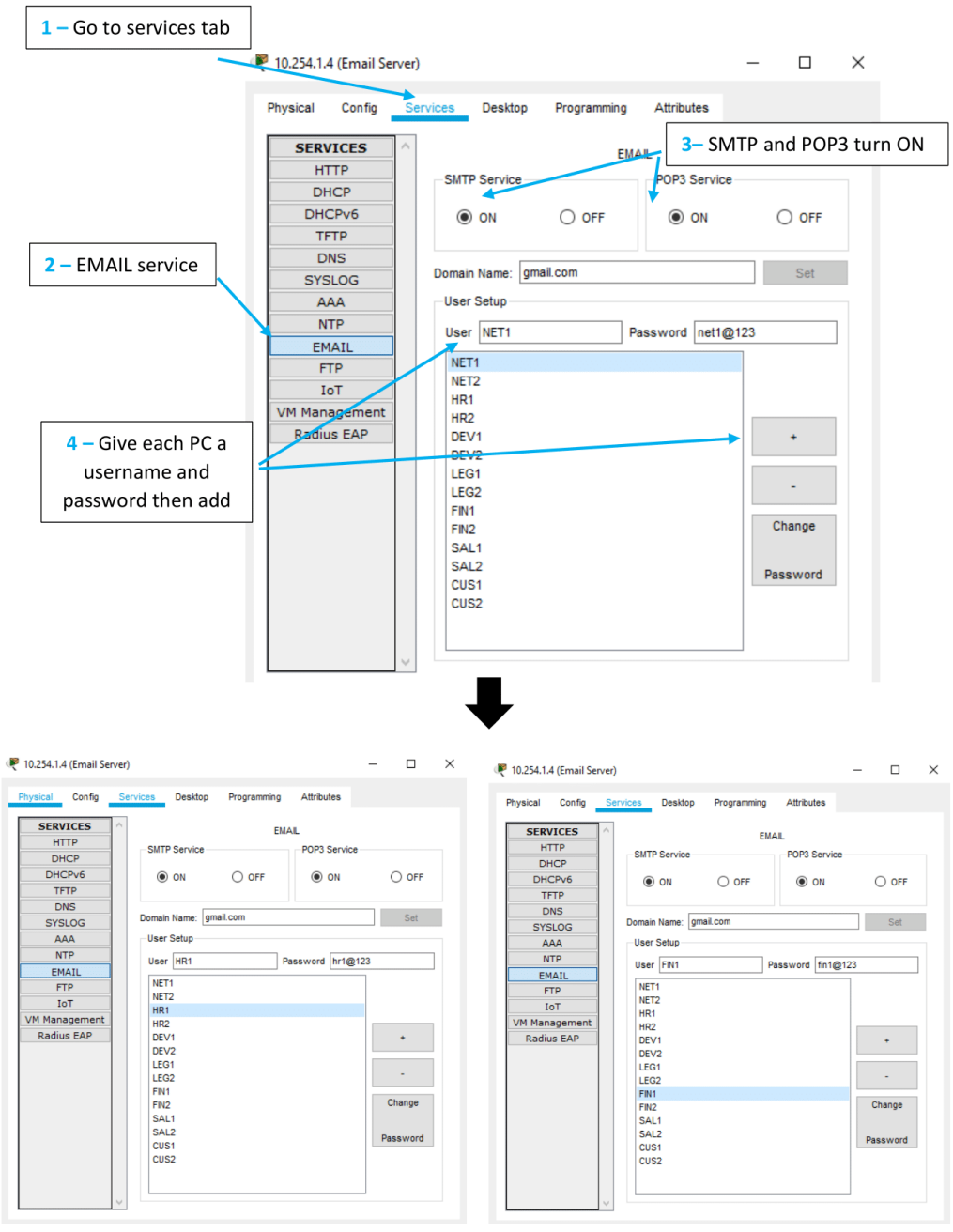



*Figure 3. 45 Server configuration → Email Server configuration*

## 3.4.7 PC configuration

### Configure PC with IP address, DNS Server address and Email details :

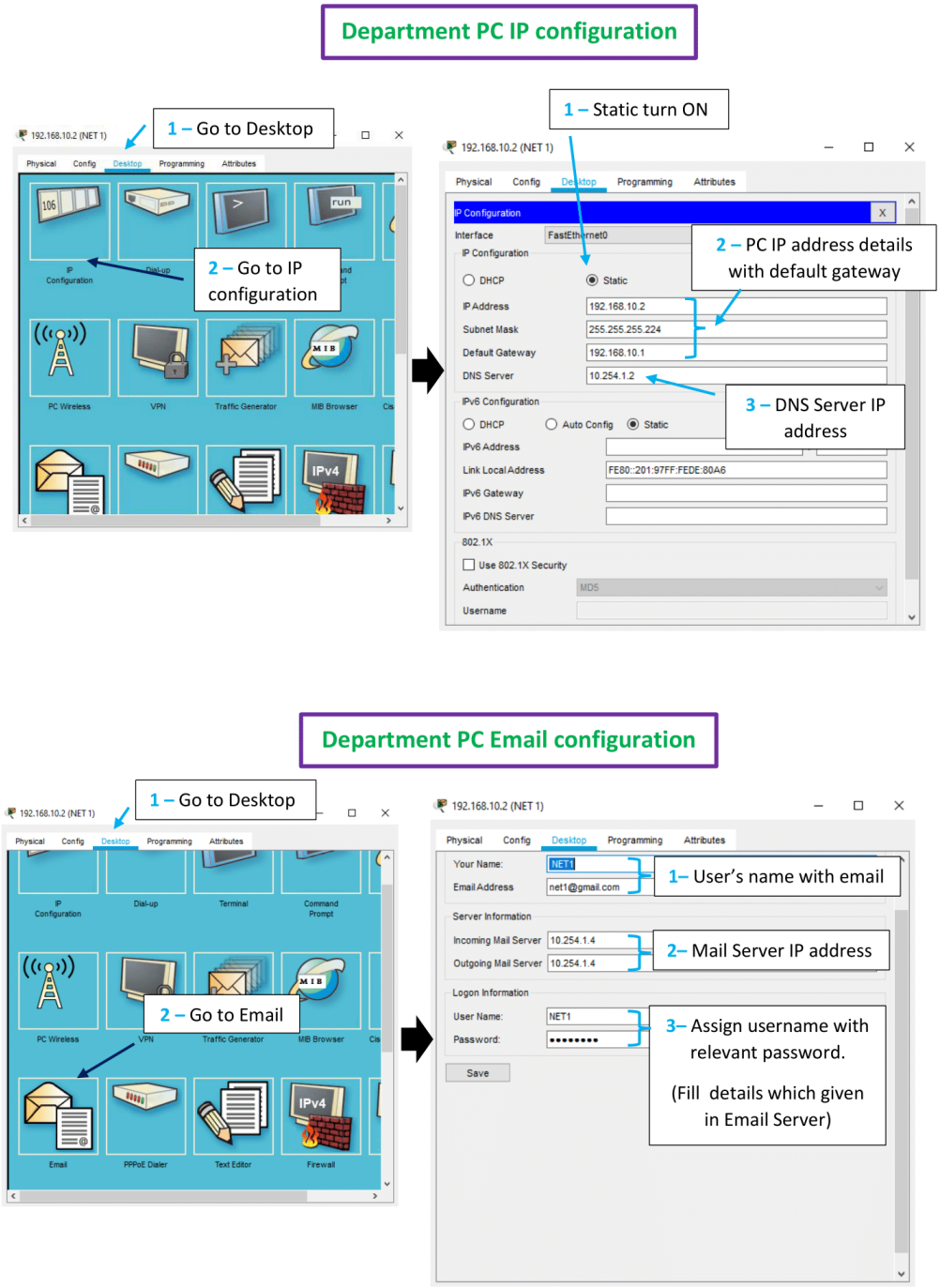
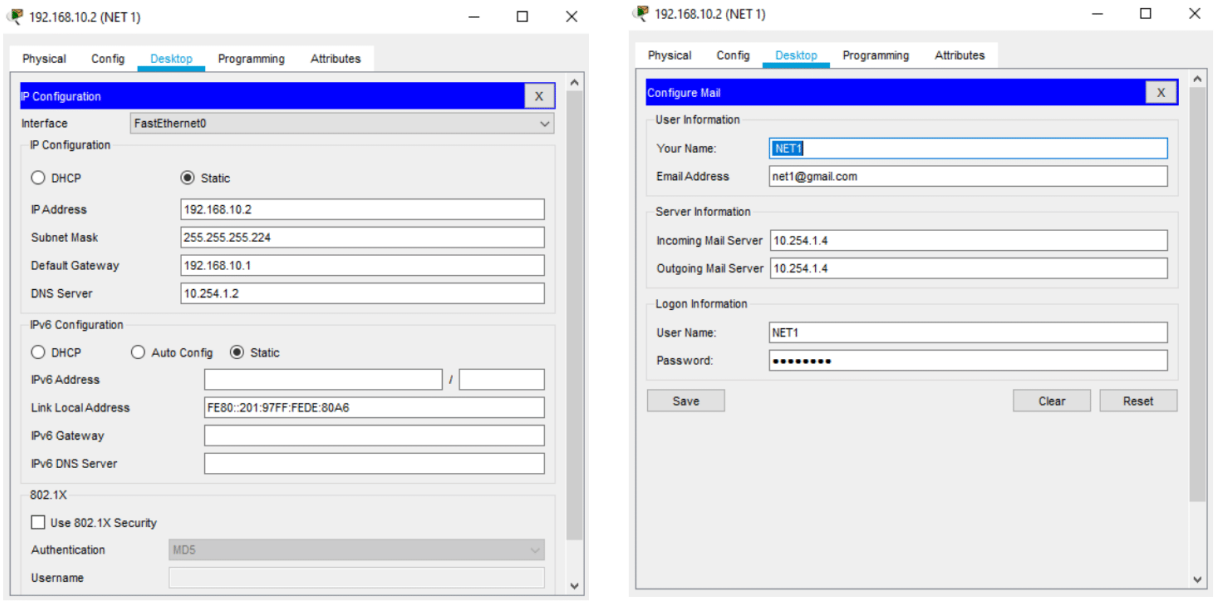



*Figure 3. 46 The way of configuring PC with IP address, DNS Server address and Email details*

**Configuration 1st PC in VLAN 10 (Network Team)**




**Configuration 1st PC in VLAN 20 (Developers)**

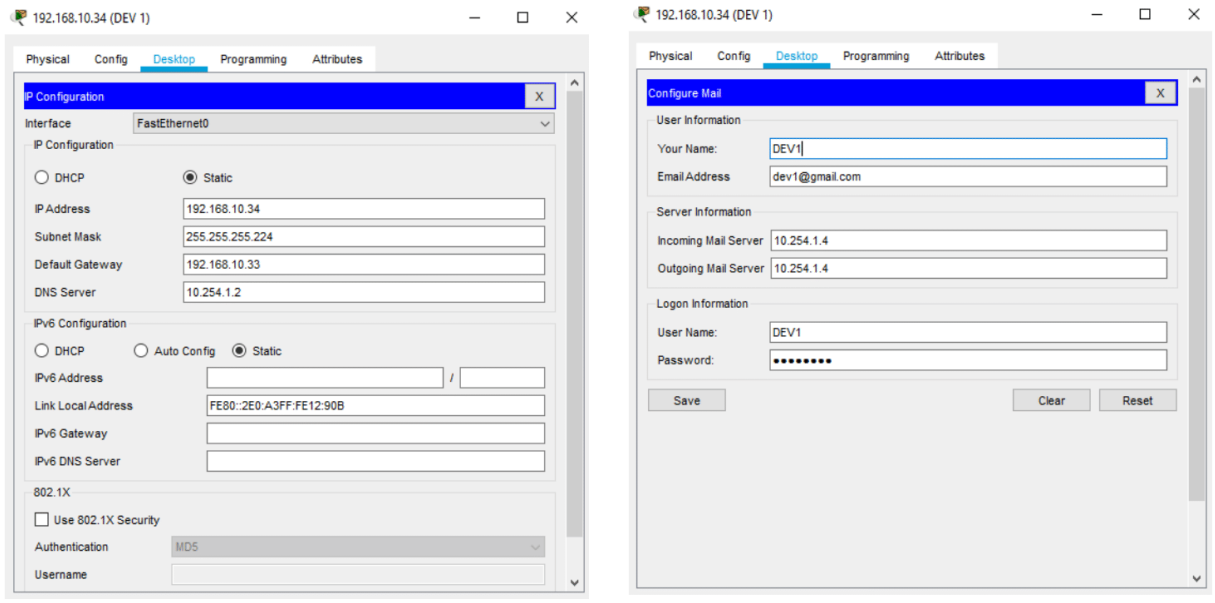
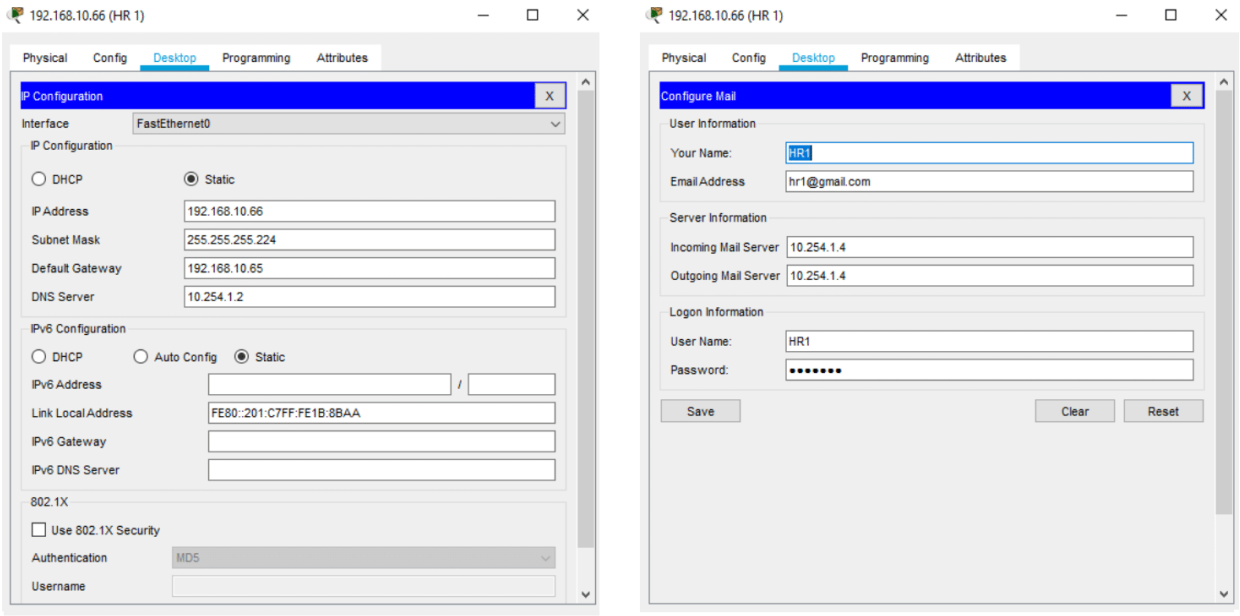



*Figure 3. 47 Configure Network Team department and Developers department PCs with IP address, DNS Server address and Email details*

**Configuration 1st PC in VLAN 30 (HR)**




**Configuration 1st PC in VLAN 40 (Legal)**

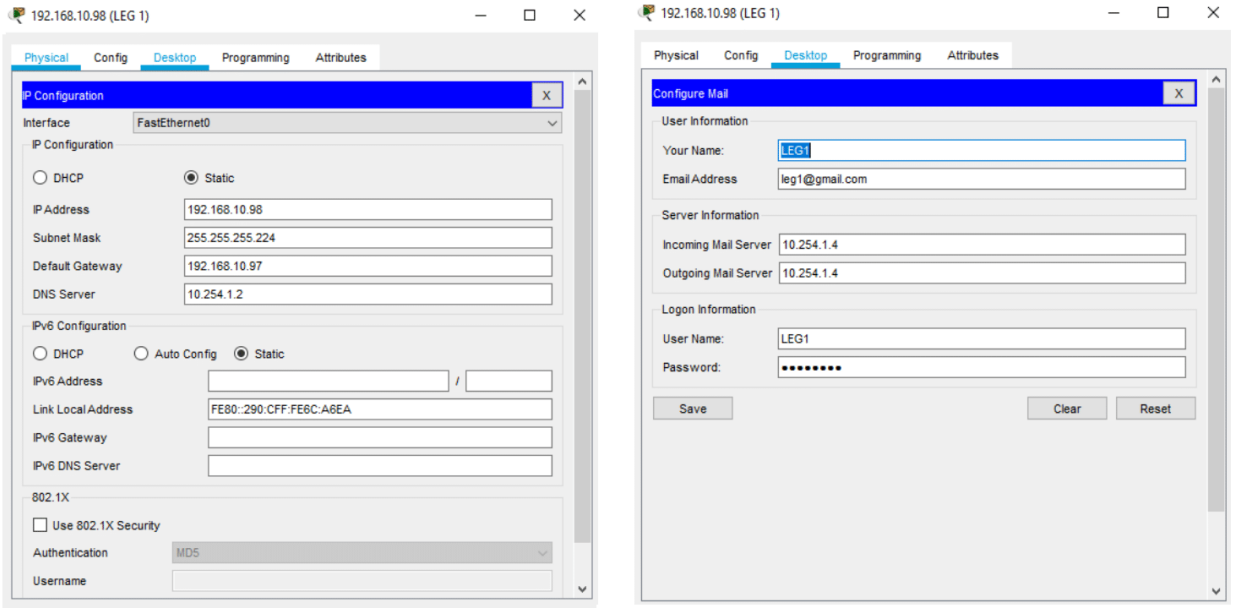
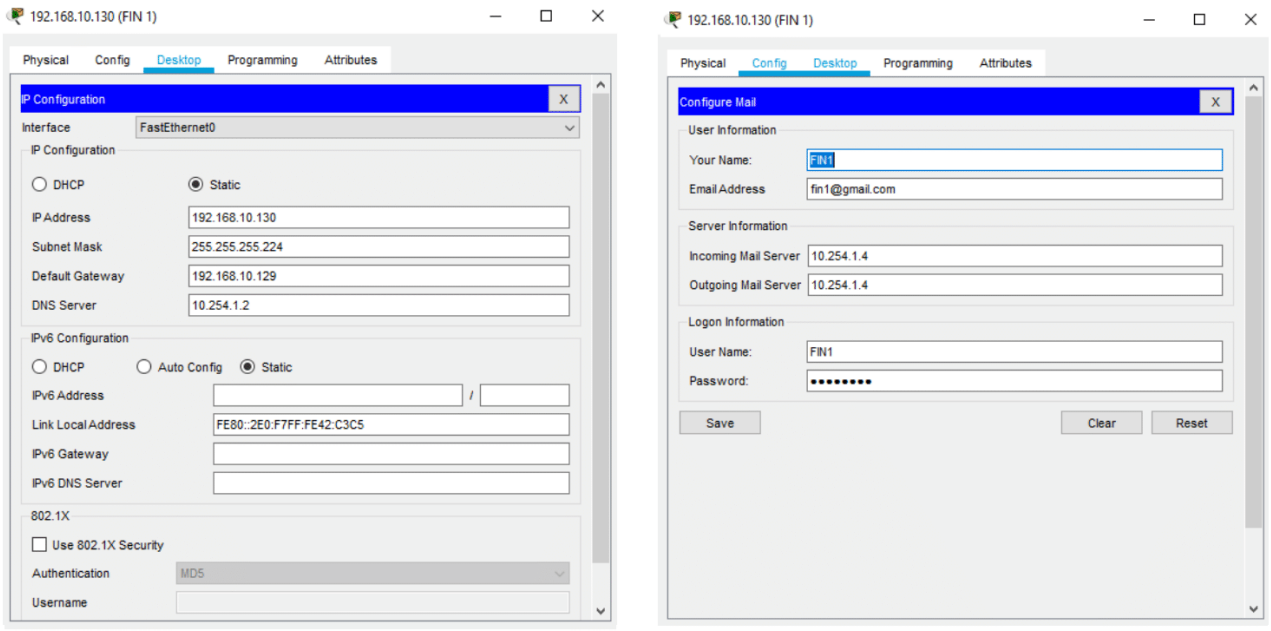



*Figure 3. 48 Configure HR department and Legal department PCs with IP address, DNS Server address and Email details*

**Configuration 1st PC in VLAN 50 (Finance)**




**Configuration 1st PC in VLAN 60 (Sales & Marketing)**

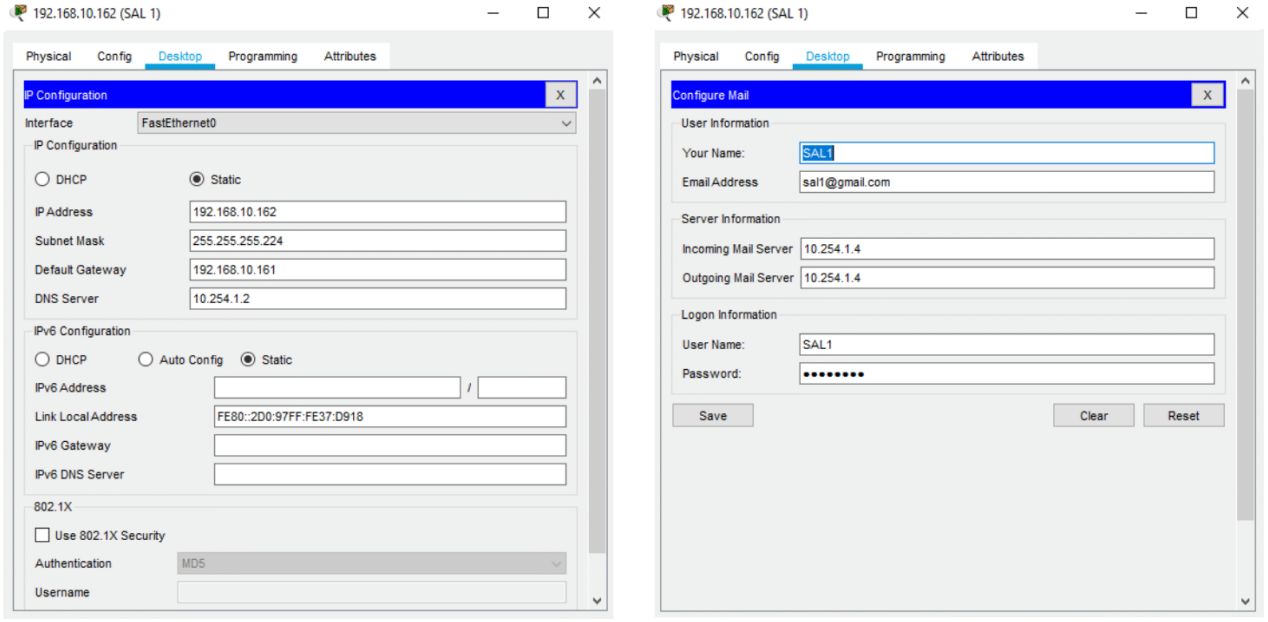



*Figure 3. 49 Configure Finance department and Sales & Marketing department PCs with IP address, DNS Server address and Email details*

**Configuration 1st PC in VLAN 70 (Customer Care)**

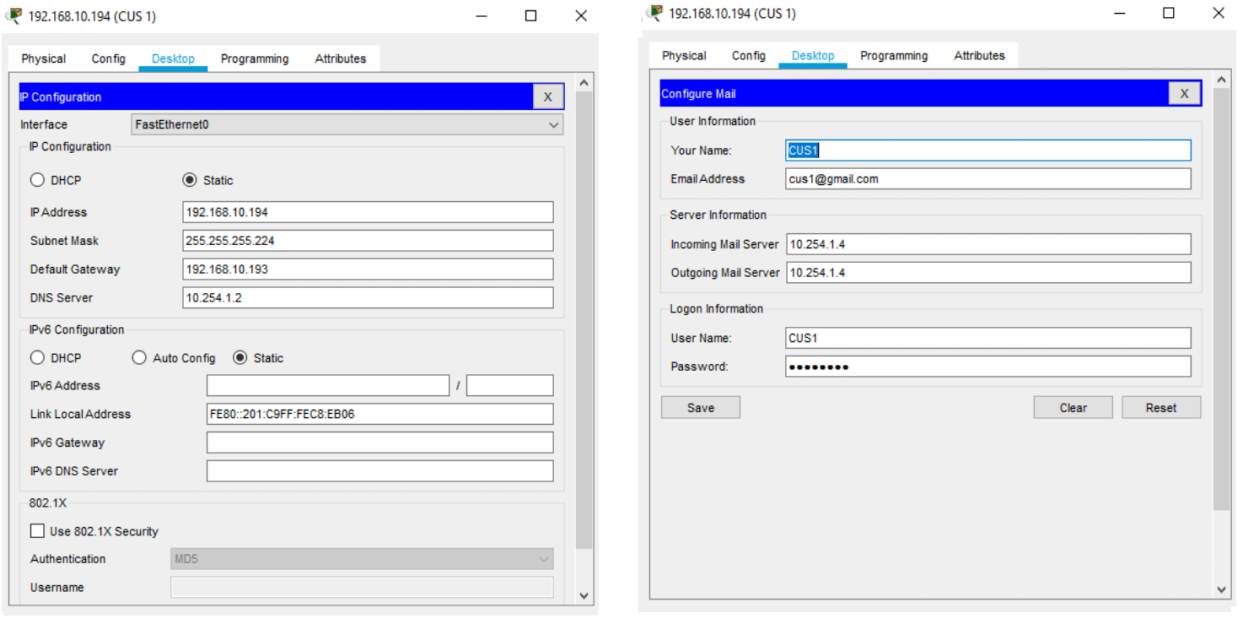



*Figure 3. 50 Configure Customer Care department PCs with IP address, DNS Server address and Email details*

# Task 4

## 4.1 Test cases of the SYNTAX Solution Matara branch LAN Network

### 4.1.1 Test Case 1: Test the Telnet

Telnet is a text-based application that allows to access and issue commands from the console of a router or other device. For configuration purposes, Telnet can be used to connect to networking devices (switches, routers).

Below figure show the way to go into router configuration by Developers department PC using TELNET. Hence, by any department PC, administrator can configure the router remotely.

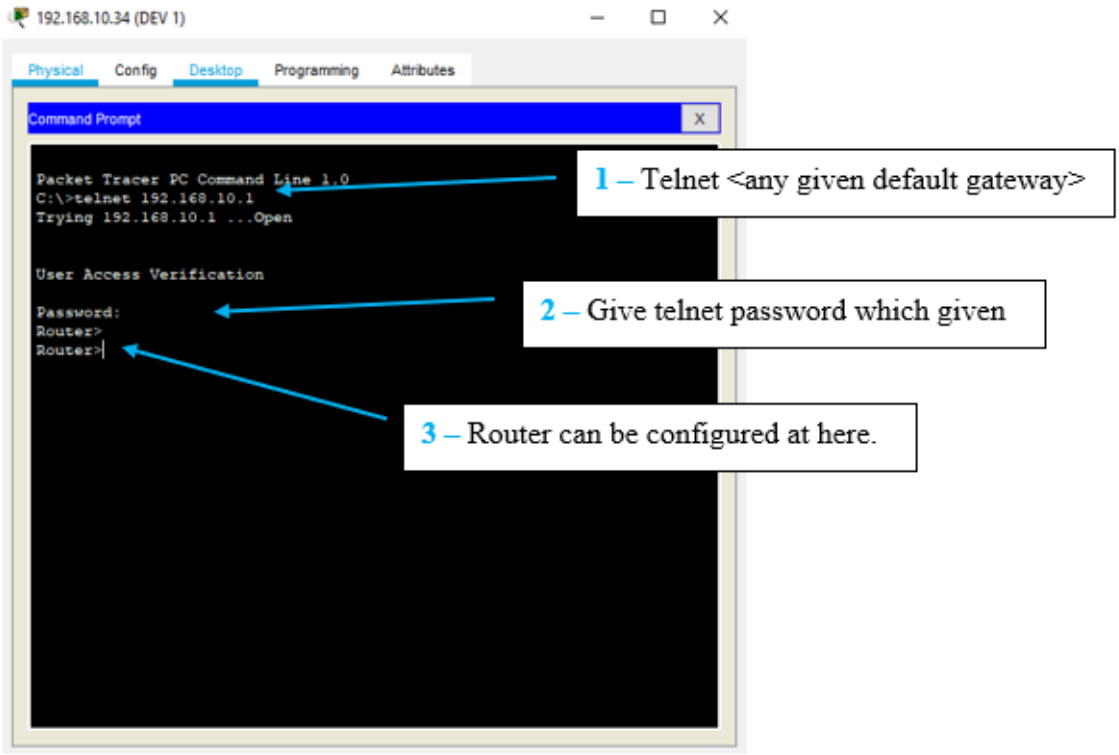



*Figure 4. 1 Go into router configuration by Developers department PC via TELNET*

### 4.1.2 Test Case 2: Test the Traceroute

Traceroute is a network diagnostic tool that tracks a packet's travel from source to destination on an IP network in real time, providing the IP addresses of all the routers it pings along the way. Traceroute also keeps track of the time it takes for each hop a packet takes on its way to its destination.

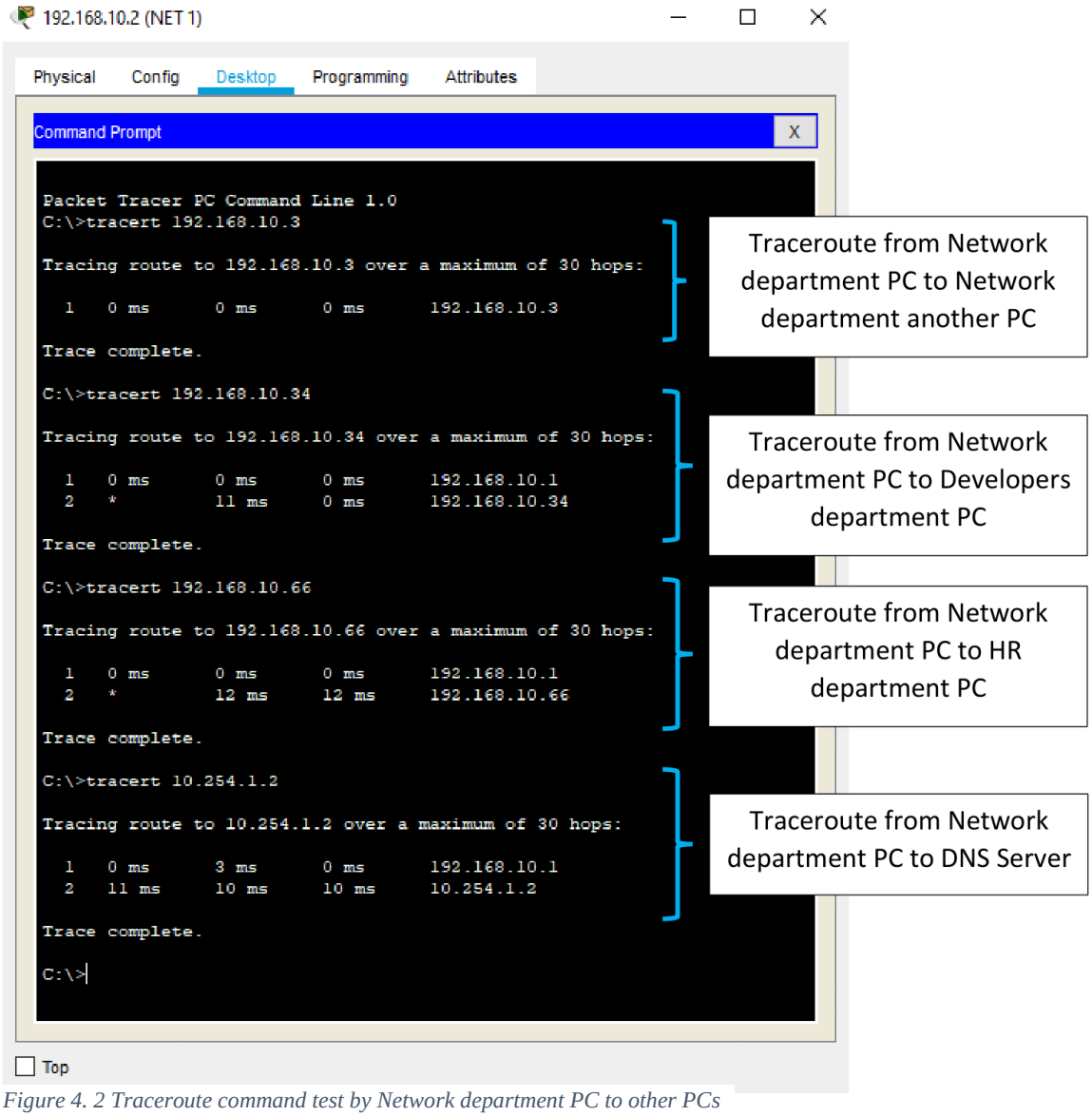



*Figure 4. 2 Traceroute command test by Network department PC to other PCs*

According to above figure packet is directly recived by same VLAN (Network department) PC. But when packet sending to another department PC, it first go through sender's VLAN gateway (Network VLAN Gateway) which is Router, then enter to destination PC.

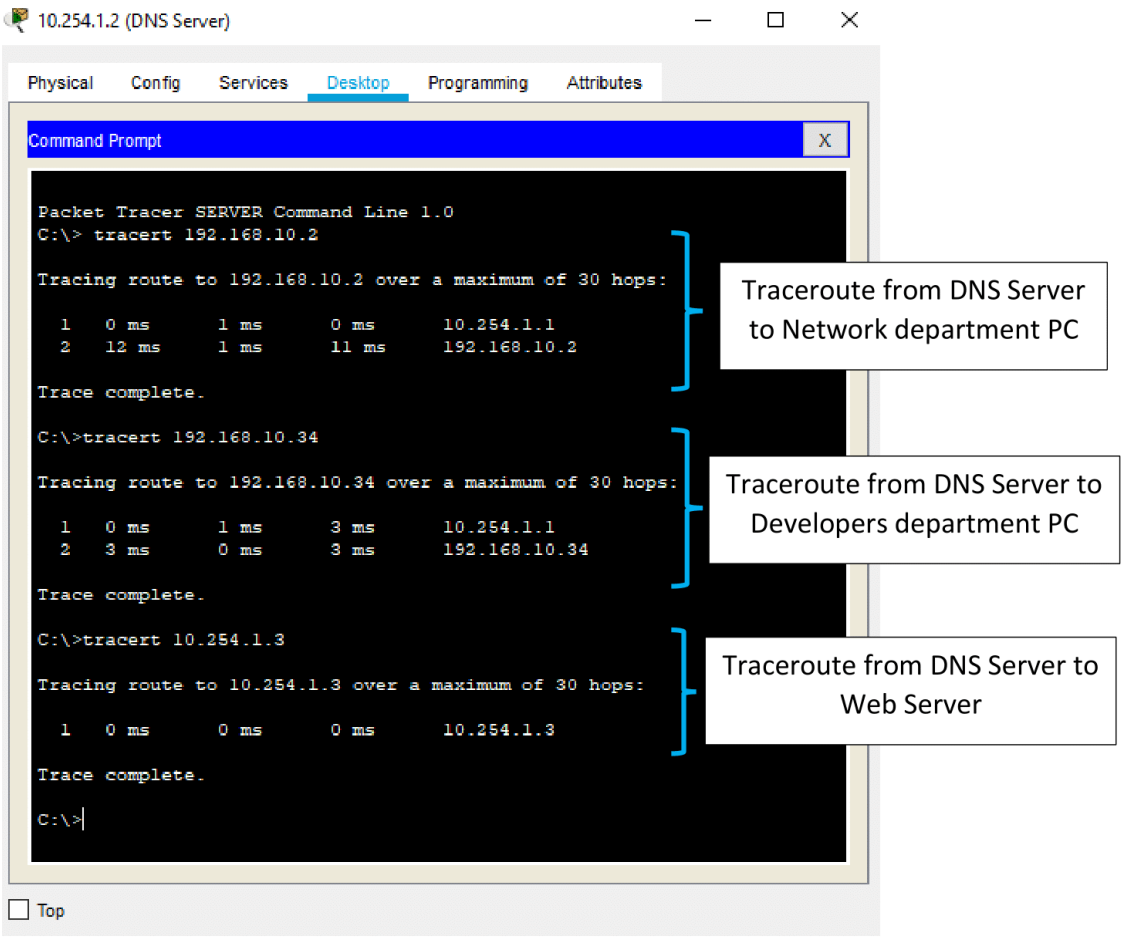



*Figure 4. 3 Traceroute command test by DNS Server to other PCs and Servers*

According to above figure packet is directly recived by same VLAN server. But when packet sending to another department PC, it first go through sender's VLAN gateway (Server VLAN Gateway) which is Router, then enter to destination PC.

### 4.1.3 Test Case 3: Ping within same department

The Ping tool is used to see if a specific host can be reached via an IP network. The time it takes for packets to be transferred from a local host to a destination computer and back is measured by a Ping. The Ping tool calculates and records the packet's round-trip duration as well as any losses encountered along the way.

**Ping from Network Team Department to Network Team Department :**

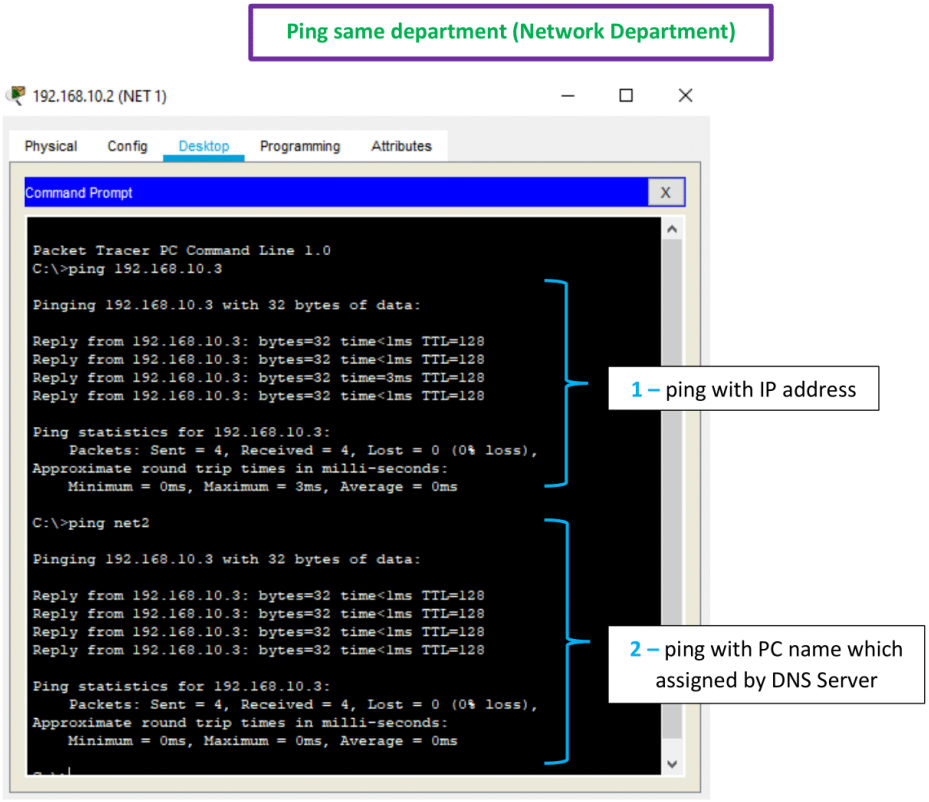



*Figure 4. 4 Ping from Network Team Department to Network Team Department*

### 4.1.4 Test Case 4: Ping within different department

**Ping from Network Team Department to HR Department :**

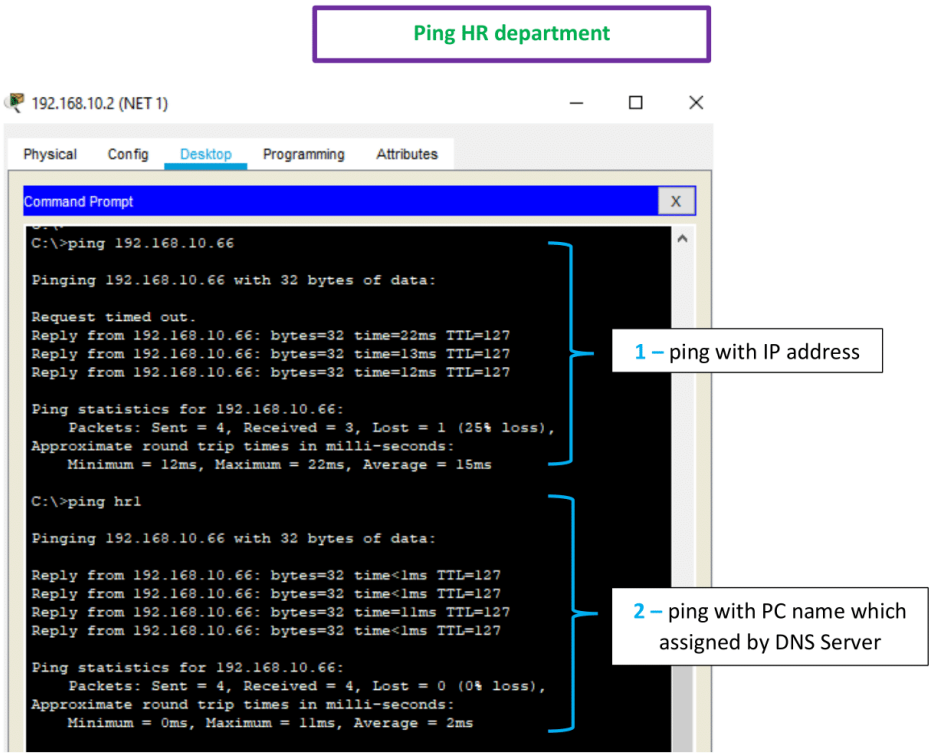



*Figure 4. 5 Ping from Network Team Department to HR Department*

**Ping from Network Team Department to Legal Department :**

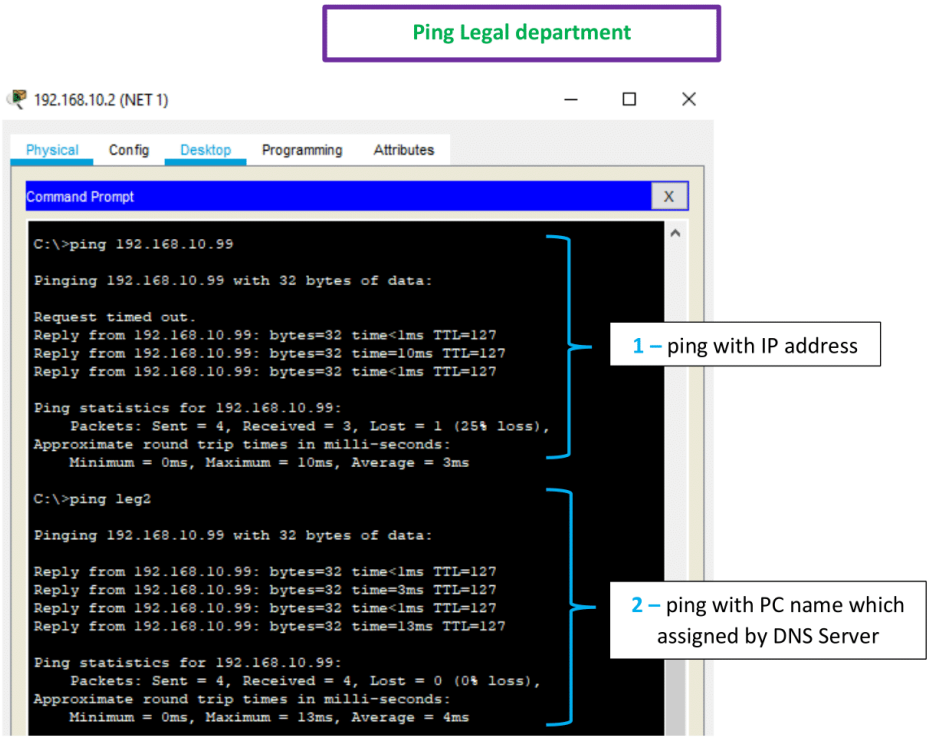



*Figure 4. 6 Ping from Network Team Department to Legal Department*

## Ping from Network Team Department to Finance Department :

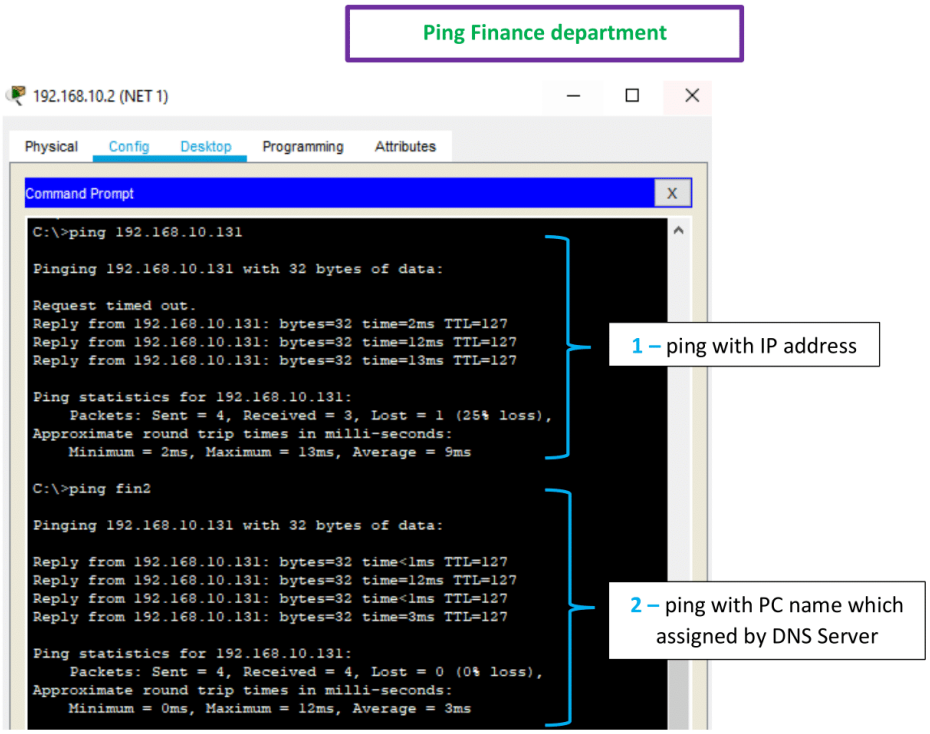



*Figure 4. 8 Ping from Network Team Department to Finance Department*

## Ping from Network Team Department to Sales & Marketing Department :

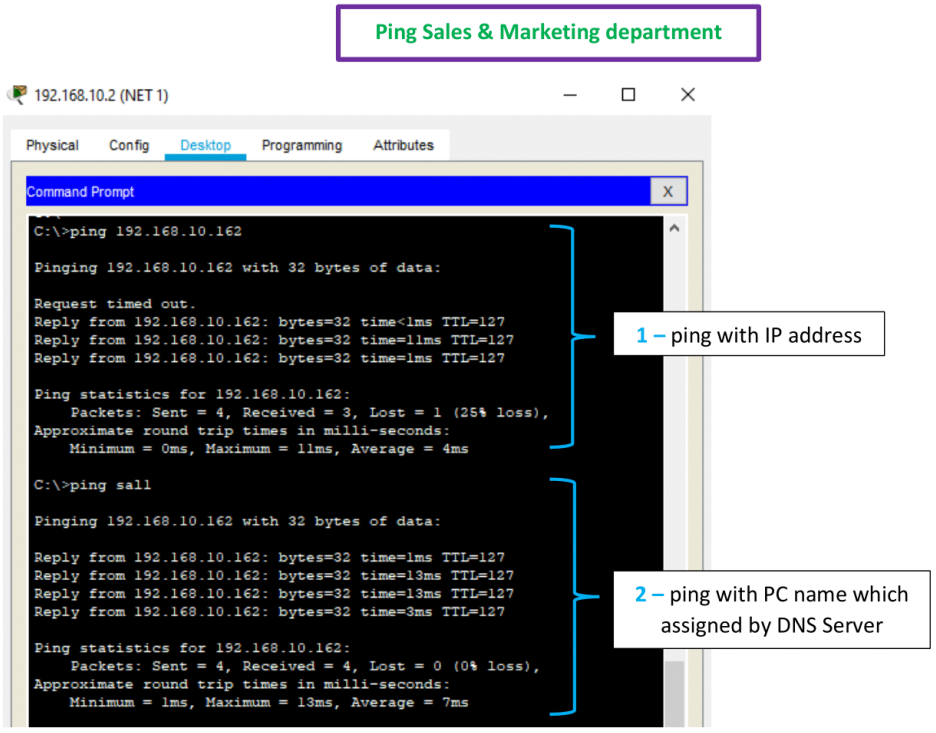



*Figure 4. 9 Ping from Network Team Department to Sales & Marketing Department*

## Ping from Network Team Department to Customer Care Department :

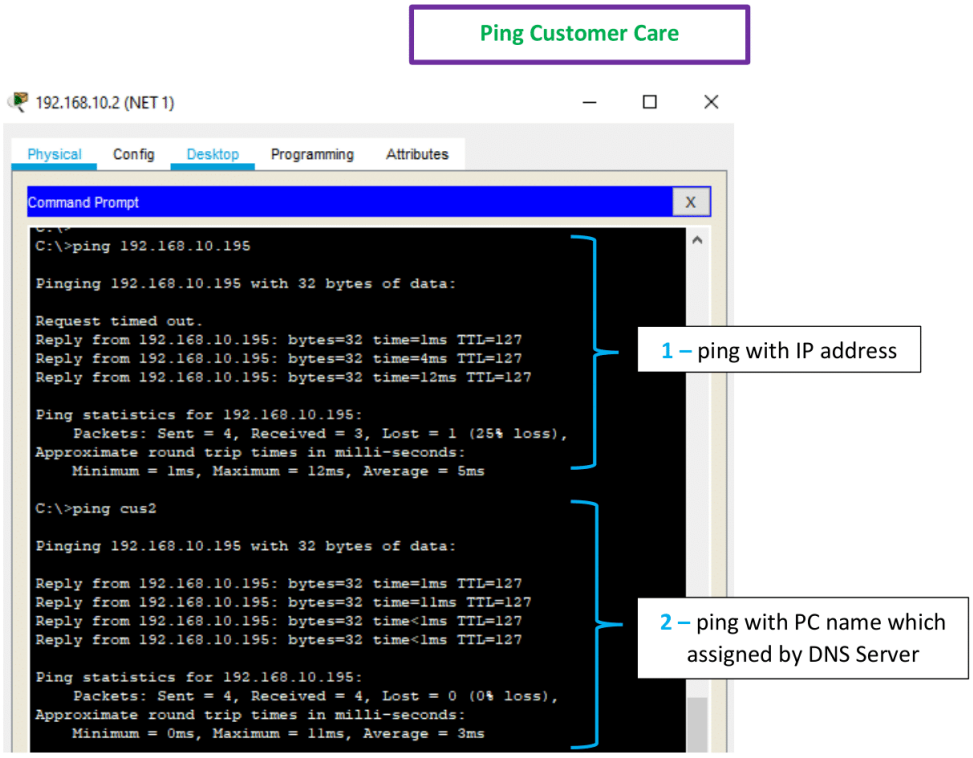



*Figure 4. 10 Ping from Network Team Department to Customer Care Department*

## Ping from Network Team Department to Developers Department :

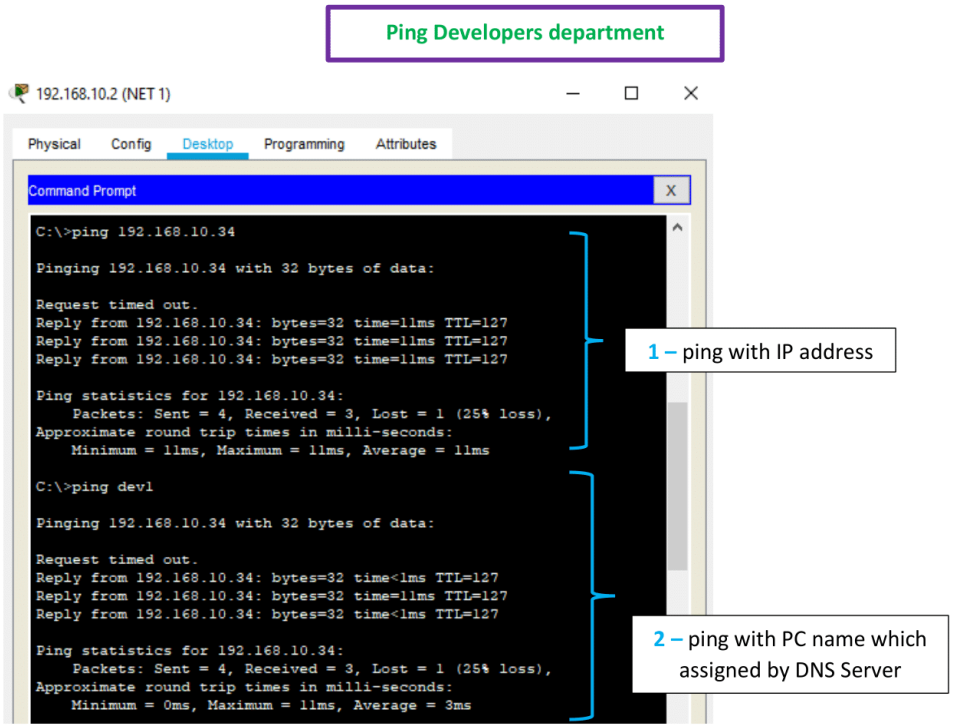



*Figure 4. 11 Ping from Network Team Department to Developers Department*

### 4.1.5 Test Case 5: Ping Servers by department PCs

**Ping from Network Team Department to Servers :**

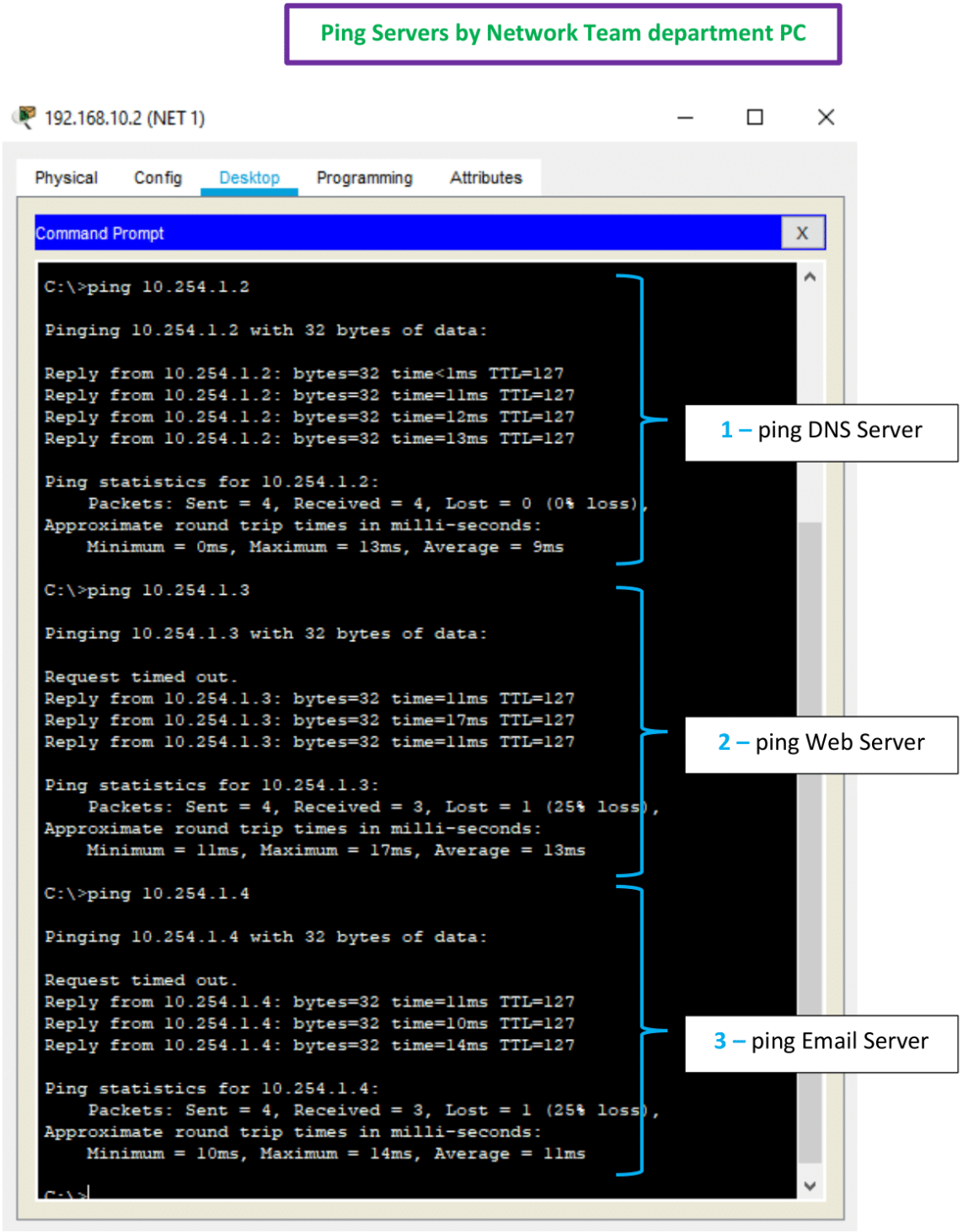



*Figure 4. 12 Ping from Network Team Department to Servers*

### 4.1.6 Test Case 6: Ping Servers by Servers

**Ping from DNS Server to other Servers :**

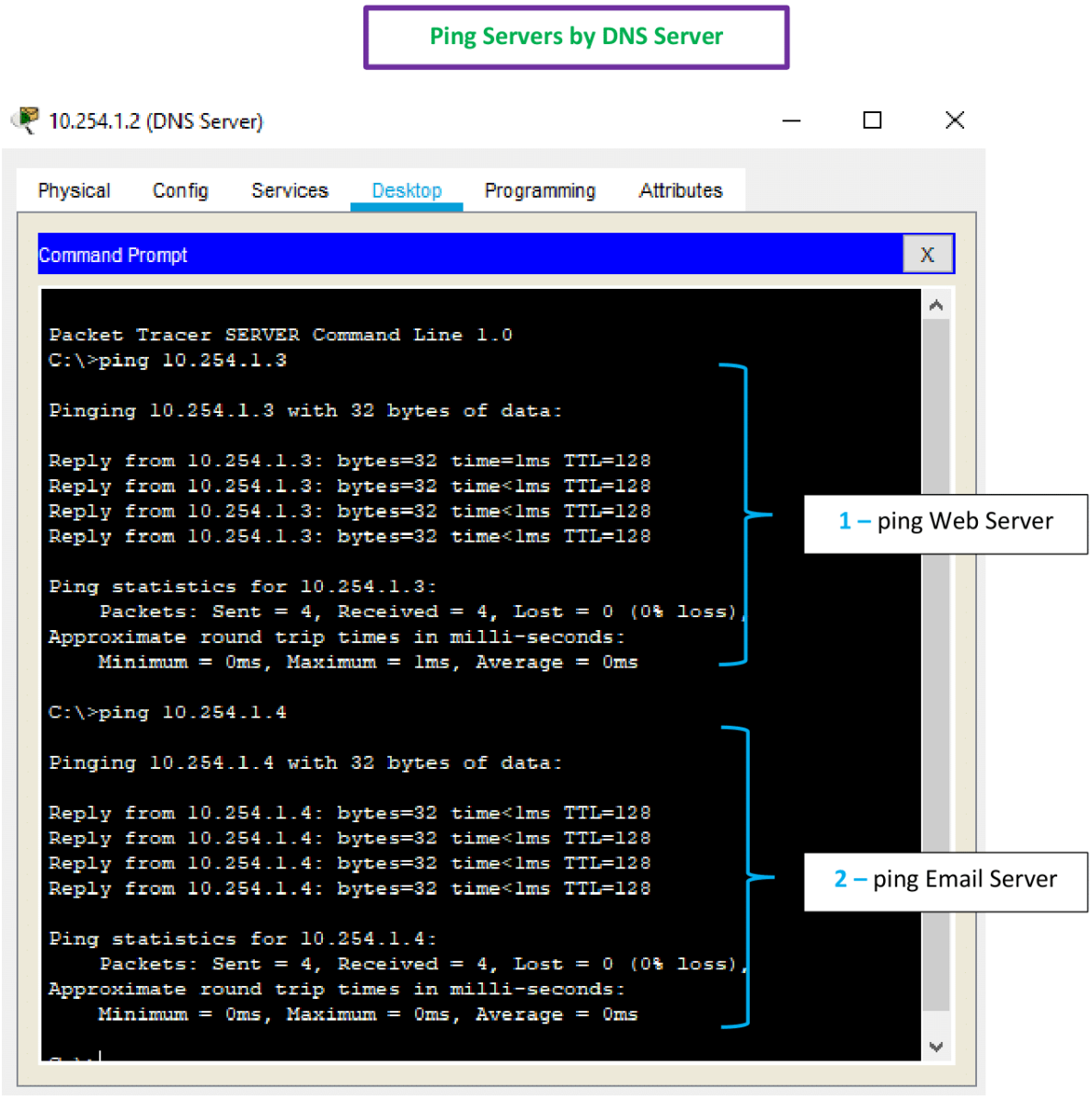



*Figure 4. 13 Ping from DNS Server to other Servers*

## 4.1.7 Test Case 7: Test Web Server access

**Test Web Server access from Network Department PC :**

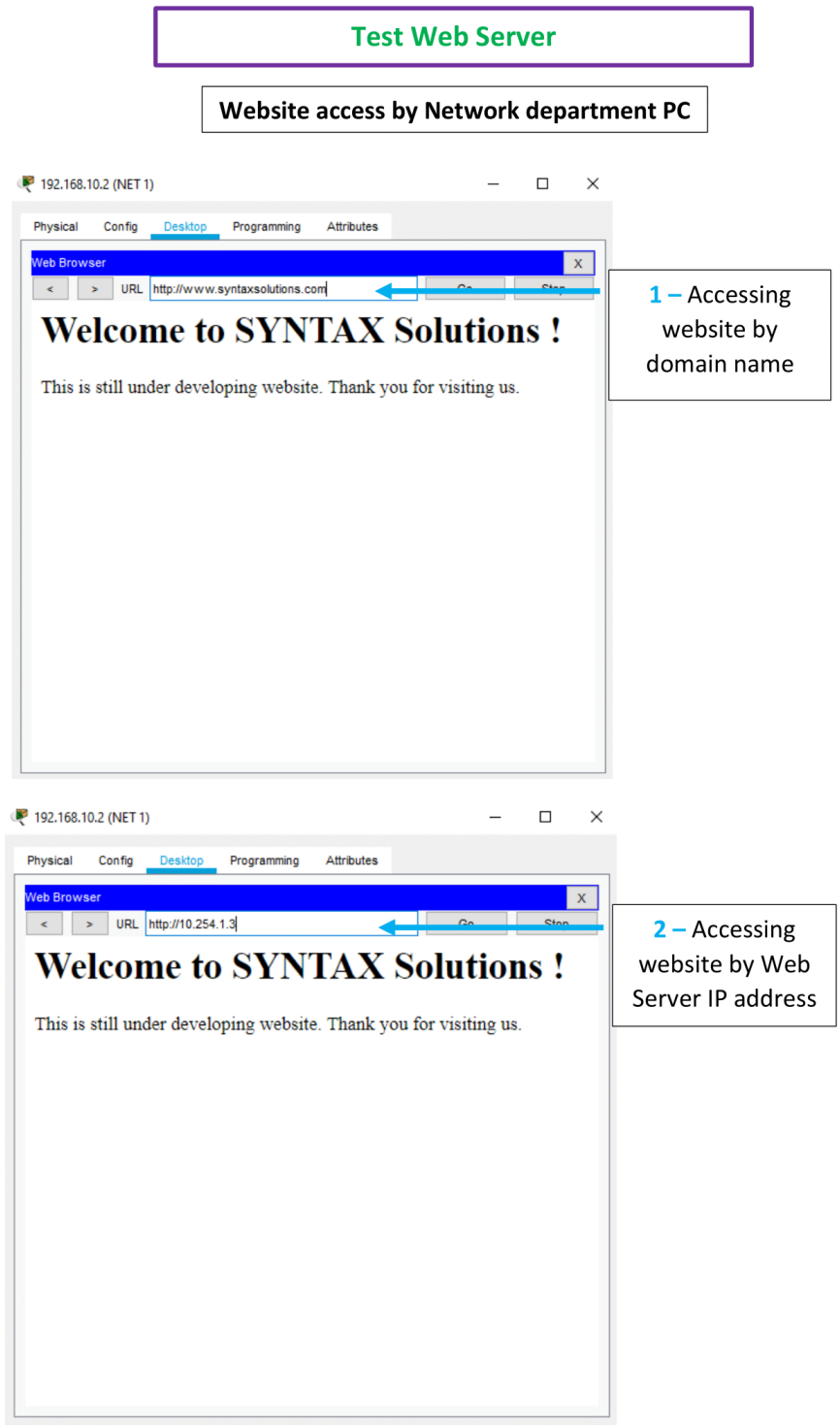



*Figure 4. 14 Test Web Server access from Network Department PC*

**Test Web Server access from Email Server :**

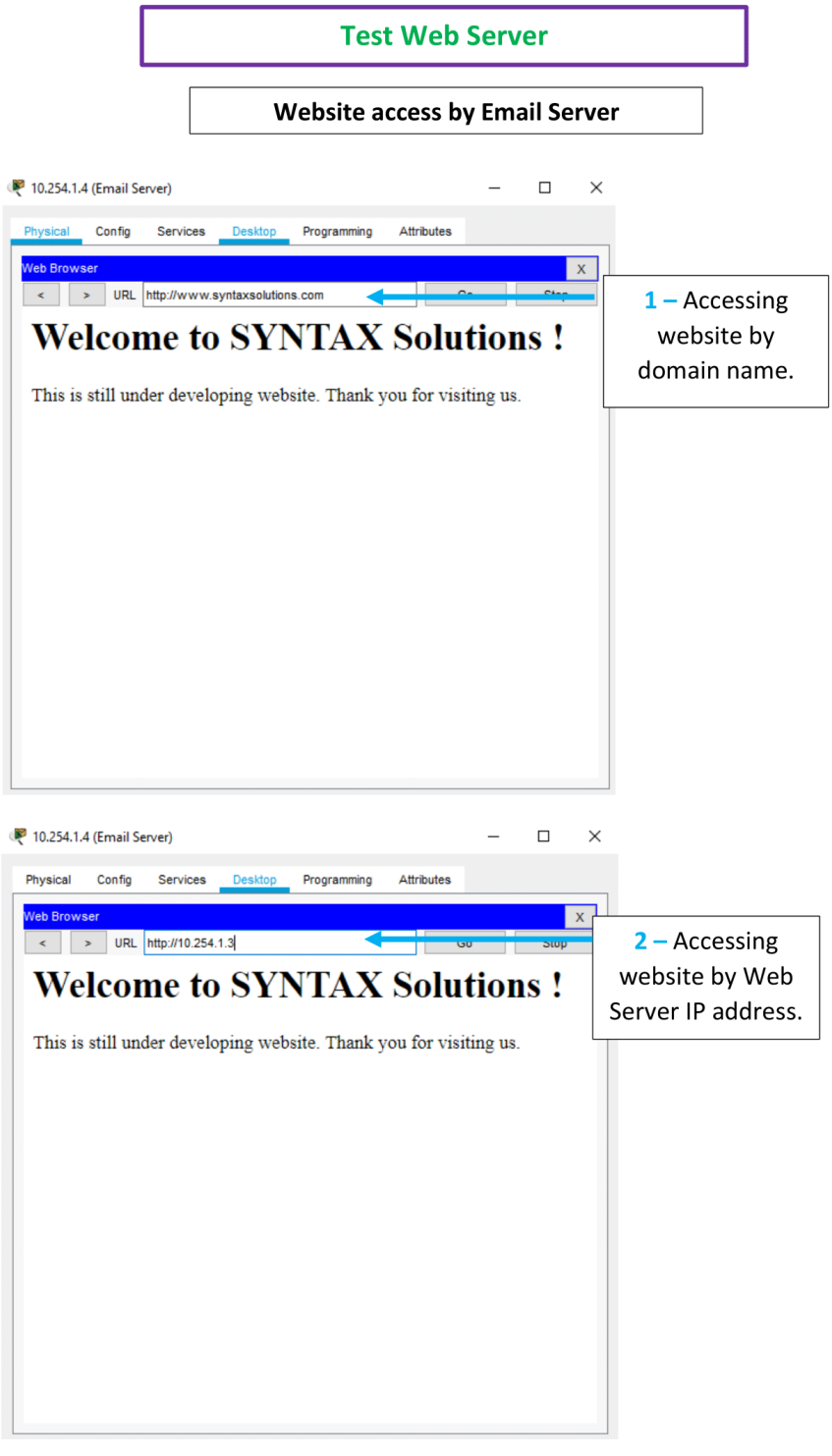



*Figure 4. 15 Test Web Server access from Email Server*

## 4.1.8 Test Case 8: Test Email Server access

**Send email from Network department to Network department :**

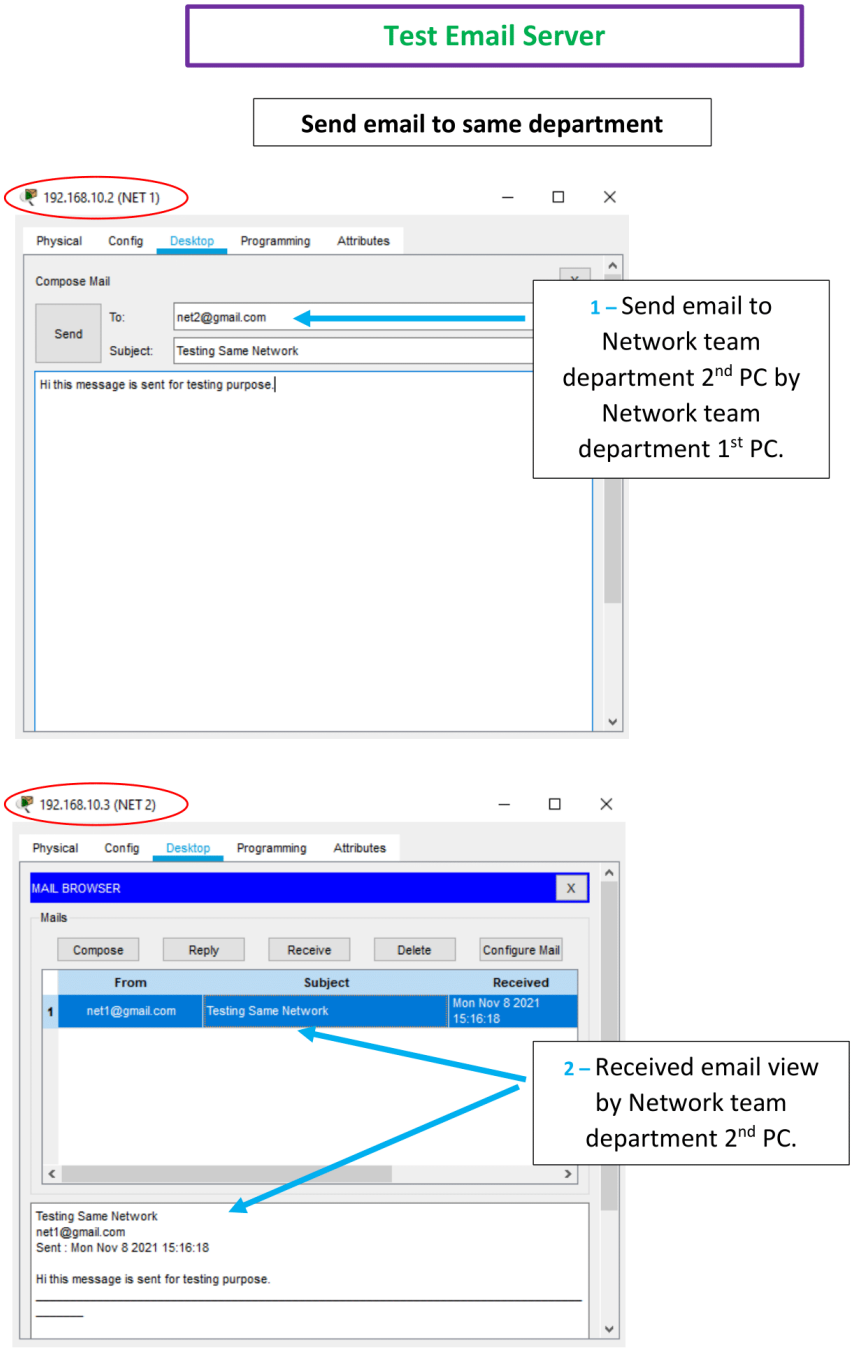



*Figure 4. 16 Send email from Network department to Network department*

**Send email from Network department to Developers department :**

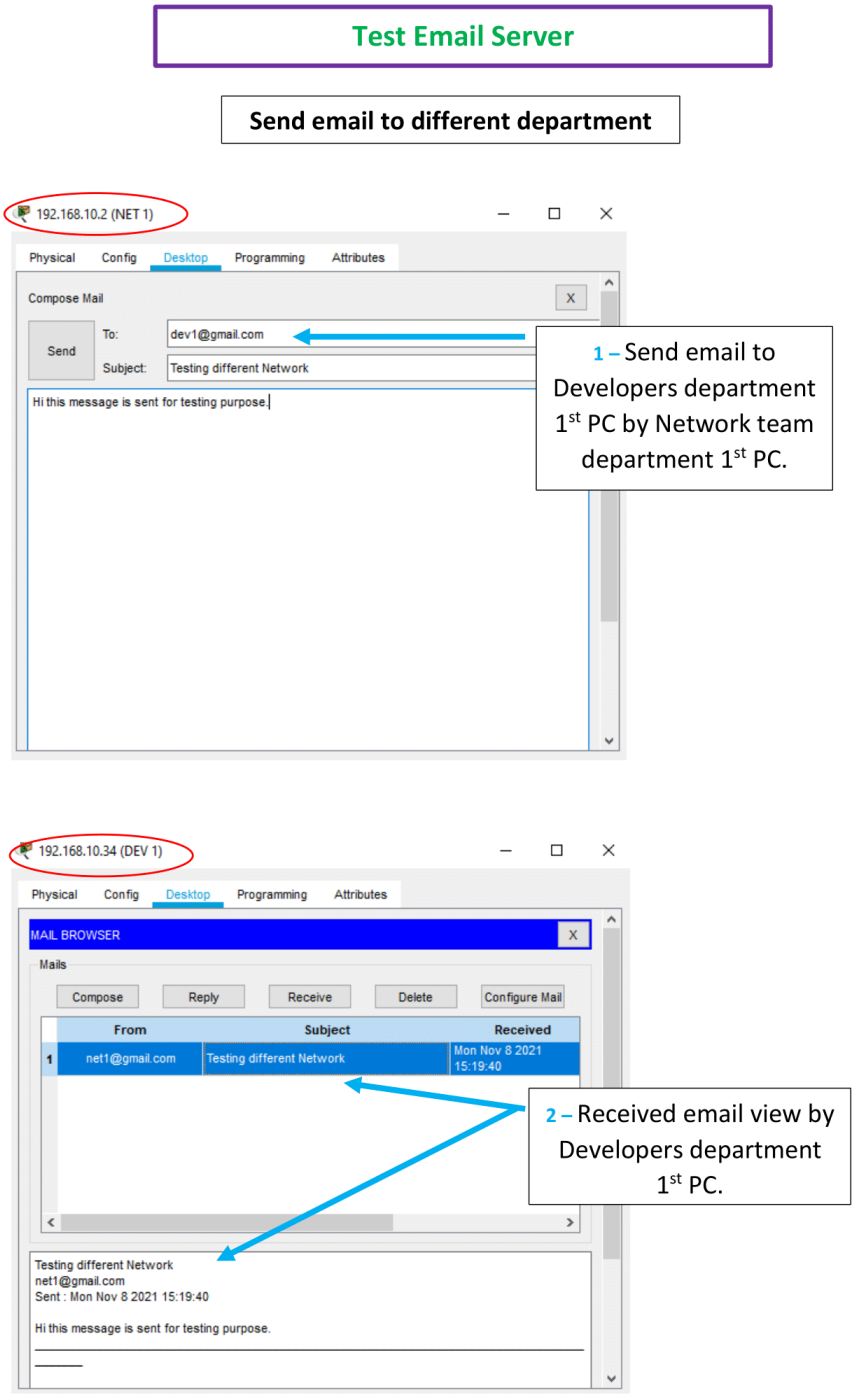



*Figure 4. 17 Send email from Network department to Developers department*

**Send email from Finance department to Sales & Marketing department :**

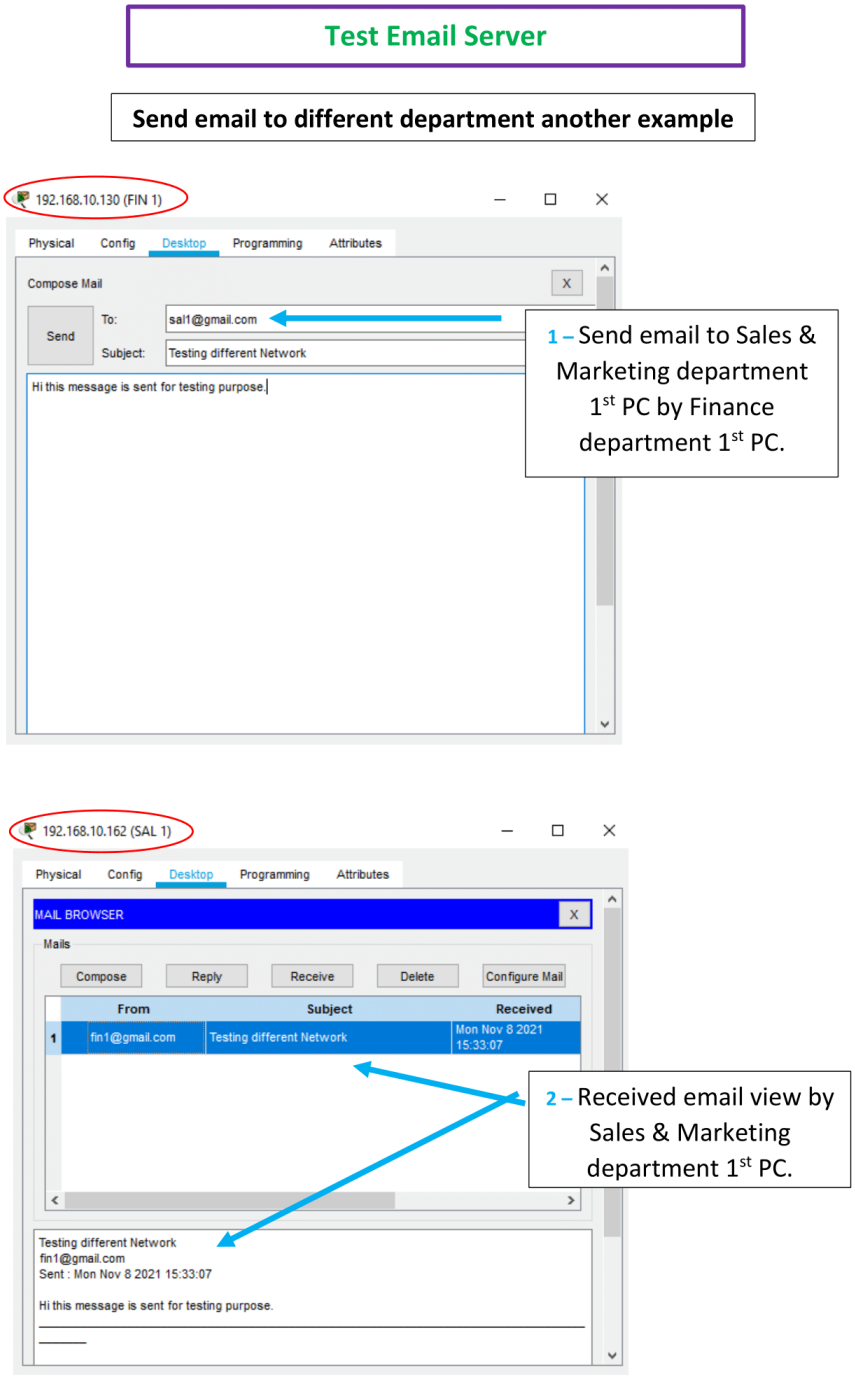



*Figure 4. 18 Send email from Finance department to Sales & Marketing department*

### 4.1.9 Test Case 9: DNS Server access

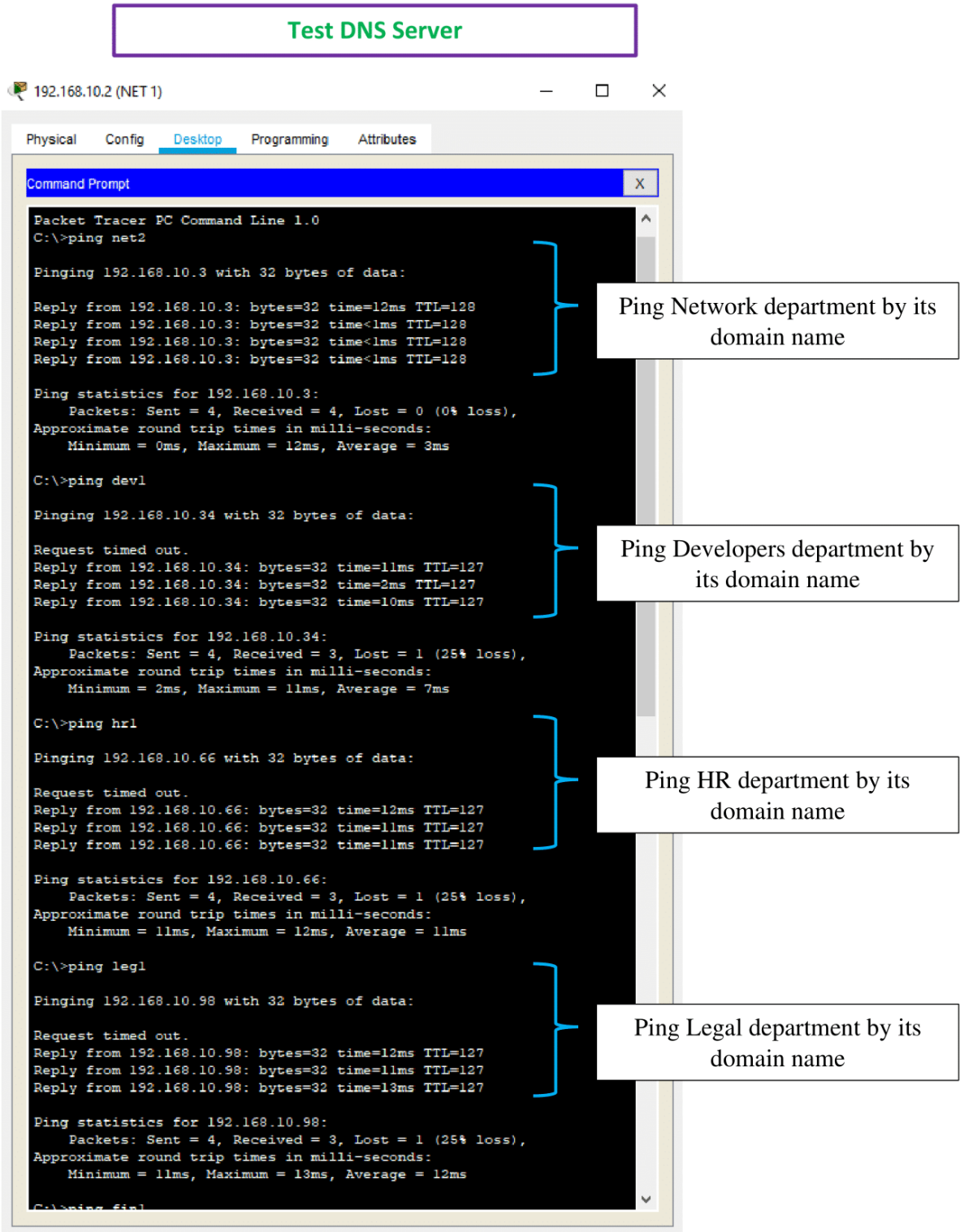



*Figure 4. 19 Test DNS Server access by Network department PC with pinging other department's part 1*

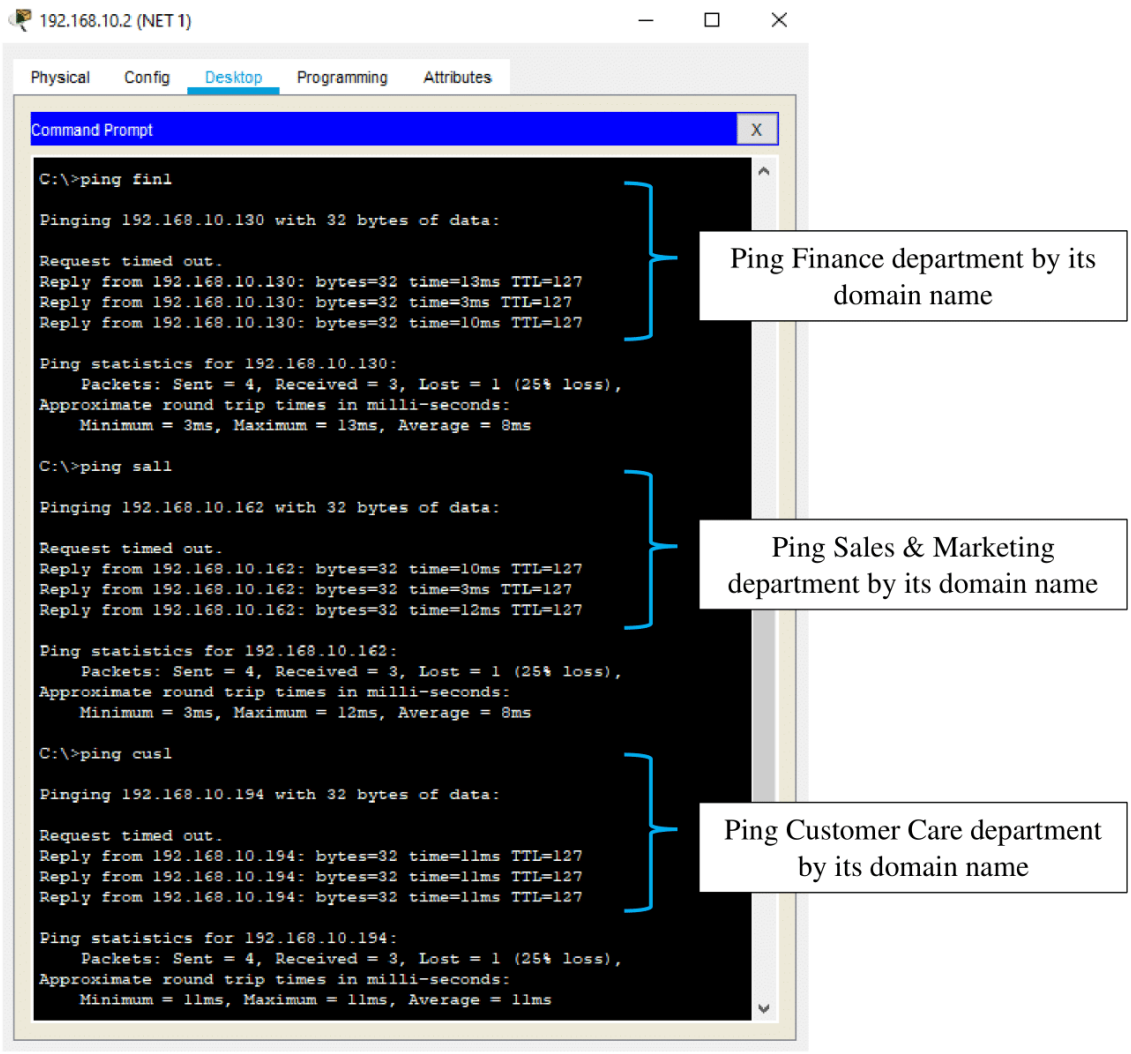



*Figure 4. 20 Test DNS Server access by Network department PC with pinging another department's part 2*

## 4.2 Potential future enhancement for designed LAN system for SYNTAX Solution Matara branch

An intranet is a private network which is heavily protected by many different networking devices such as router, firewall, proxy server, DMZ, Honeynet, IPS and IDS. Below diagram is an overly simplified version of the reality of it. I designed basic LAN network for the SYTAX Solutions Matara branch before. According to this figure for the further enhancement of the SYTAX Solutions Matara branch I prefer to apply Hybrid Firewall, Host based Firewall, Network Based Firewall, Proxy Firewall, Honeynet, DMZ, IPS and IDS for the LAN network of them.

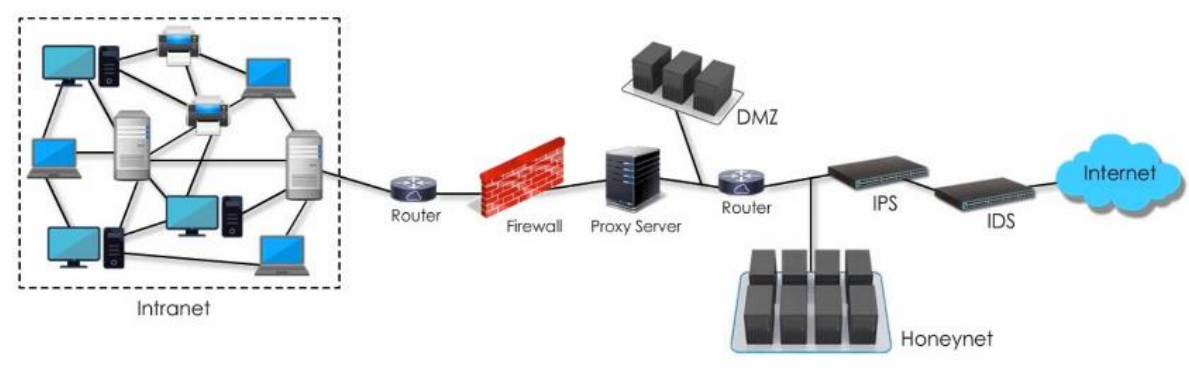



*Figure 4. 21 Designed future enhancement LAN system for SYNTAX Solution Matara branch*

From the next page there are some key characteristics and functions of each component I selected for future enhancement for designed LAN system for SYNTAX Solution Matara branch. And I have mentioned brief details about them for further knowledge.

### 4.2.1 Firewall

A firewall is a network security device that can be either hardware or software which use to monitor network traffic both inbound and outbound. The objective of a firewall is to create a barrier between an internal network and incoming traffic from external sources such as the internet, in order to prevent malicious traffic such as viruses and hackers from entering.

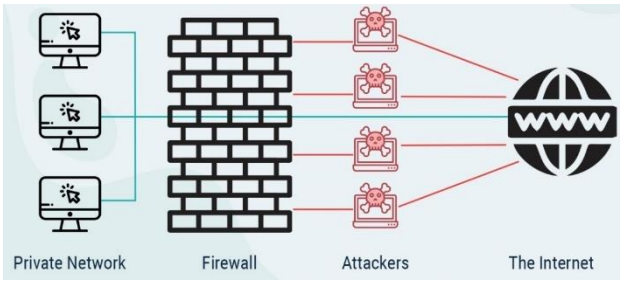



*Figure 4. 22 How firewall work in a LAN*

To prevent attacks, firewalls carefully examine incoming traffic using pre-defined rules and filter traffic from unsecured or suspect sources. Firewalls protect traffic at a computer's ports, which are the points where data is shared with external devices. For example, according to below figure "Any IP address can communicate with this PC using TCP protocol through port 80."

| Permission | IP Address | Protocol | Destination | Port |
|---|---|---|---|---|
| ALLOW | ANY | TCP | ANY | 80 |
| ALLOW | ANY | TCP | ANY | 25 |
| ALLOW | ANY | TCP | ANY | 110 |
| DENY | ANY | UDP | ANY | 23 |
| DENY | ANY | TCP | ANY | 3389 |

*Figure 4. 23 A typical way of firewall controlling incoming traffic*

Types of Firewalls :- Packet filtering firewall

Application/Proxy/Circuit Gateway Firewall

Hybrid Firewall

Host Based Firewall

Network Based Firewall

**Packet filtering firewall :-**

If someone downloads a file from the internet, the packet filtering firewall will work on the data packet when it comes. It merely looks at the IP addresses of the sender and receiver, as well as the port number in the data packet. ACL (Access Control List) refers to the rules that are written in the early stages of development . ACL is used to verify data packets. The data packet is allowed to travel across the firewall if everything is in order. Internet routers already have a packet filtering firewall. As a result, they are the most cost-effective and time-efficient method of implementation.

**Application/Proxy/Circuit Gateway Firewall :-**

A Proxy Firewall functions as a connection point for internal users to the internet. Proxy is, in fact, a server. It also has a firewall built in. If a user wishes to request something from the internet, the request is sent to the firewall, which makes the request on the user's behalf. Proxy firewalls keep the internet from knowing which machine is trying to access the requested website. During this process, the internet will believe that the proxy firewall is the one making the request. This Proxy Firewall, for example, protects us from internet attackers.

**Hybrid Firewall :-**

Packet Filtering Firewall and Application Firewall are combined in a Hybrid firewall. The security of the connection will be compromised if they are linked in parallel. Because packets will either pass through a Packet Filtering Firewall or an Application Firewall. The Application Firewall will be useless if packets pass through the Packet Filtering Firewall. As a result, Hybrid Firewall employs a series of Packet Filtering Firewalls and Application Firewalls. As a result, Hybrid Firewall offers the highest level of protection.

**Host Based Firewall :-**

This is type of Firewall that installed into computer to protect only that computer. For example, Microsoft Defender, Kaspersky (3rd party Firewall)

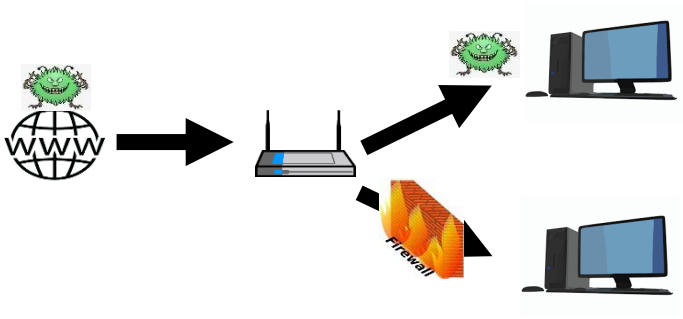



*Figure 4. 24 Typical way of how host-based firewall works*

**Network Based Firewall :-**

This is a combination of Hardware and Software. This operates at network layer. This is placed between Public Internet and Private network. This firewall protects the entire network.

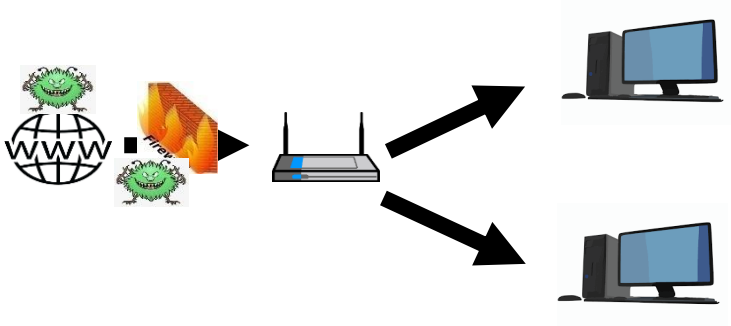



*Figure 4. 25 Typical way of how network-based firewall works*

As a Network consultant I recommend using both Network based, and Host based firewalls for maximum protection. If harmful data happens to get passed the Network Firewall, the Host based Firewall on each computer will be there to stop it. And as below figure I recommend applying Hybrid Firewall to SYNTAX Solutions Matara branch since it is a software company which handles many client's data.

| Firewall Type | Low Risk Environment (Florist Shop) | Medium Risk Environment (University) | High Risk Environment (Hospital) |
|---|---|---|---|
| Packet Filtering Firewall | **Recommended** | Gives minimal security | Unacceptable |
| Application Firewall | Acceptable | **Recommended** | Effective |
| Hybrid Firewall | Acceptable | Effective | **Recommended** |

*Figure 4. 26 Comparison of types of firewalls with different environments*

### 4.2.2 IDS

IDS is the acronym for Intrusion Detection System. The system is frequently installed on the intranet network, near the perimeter. When the IDS detects potentially harmful or suspicious traffic, it sends out notifications but leaves the action to the IPS.

Types of IDS :- Signature Based IDS

Anomaly Based IDS

Signature Based IDS :-

There is a database of known virus attacks with signatures. When packets arrive, IDS will check them against the database. The main limitation of this IDS is that it can only be used to detect known attacks. Also, when a typical packet stream fits the signature of an attack, IDS can produce a false warning.

Anomaly Based IDS :-

This sort of IDS generates a typical network traffic pattern. This IDS mode checks for statistically unexpected traffic patterns, such as odd packet loads. Any irregular traffic pattern is cause for concern. The difficulty in differentiating between routine and unexpected traffic is a limitation.

### 4.2.3 IPS

IPS is the acronym for Intrusion Prevention System. In contrast to IDS, IPS may actively block or prevent intrusions. It means IPS takes several actions as below.

- Inspection and Investigation :–

Inspection can include signature-based inspection and statical anomaly-based inspection. Investigation includes analyzing suspicious packets and activities.

- Action :–

Once unwelcome packets are identified, IPS would either put them in quarantine or simply drop them.

- Logs and reports :–

Like many security devices, IPS can log attacks and send reports.

IDS and IPS aren't always two different physical devices. They can be merged to form a single device. They also can be combined with other devices.

Ex:- Firewall / Router.

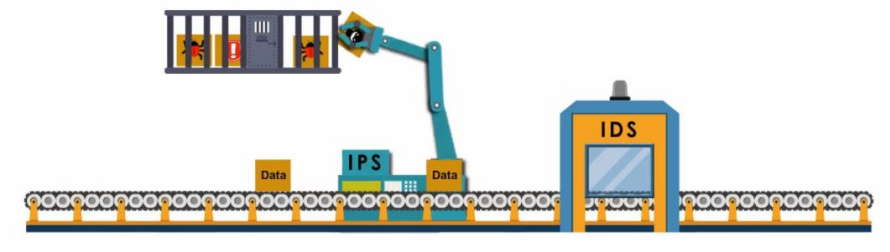



*Figure 4. 27 Typical way of how IDS and IPS works*

### 4.2.4 Honeynet

A Honeynet, often known as a "Honeypot," is a real network made up of real networking devices and servers. The Honeynet and Honeypots appear to be legitimate. They do, however, work together as a trap or bating system for two key reasons:

1) The setup of a Honeynet is intentionally vulnerable. The main purpose is inviting hackers to attack the system. So that hacking activities can be monitored, and their methods and patterns can be studied. Information could be valuable for IT professionals to protect a real company's intranet. To some extent, honeypots can serve as lightweight intrusion detection systems.

2) A Honeynet is also used to deflect hackers from attacking a real Internet and it resources. Once hackers thought they have got what they need, their attention could be diverted.


*Figure 4. 28 Honeynet servers*

### 4.2.5 DMZ

DMZ stands for “Demilitarized Zone.” A DMZ network is a network that is only lightly protected in the networking world. It is still part of company's LAN network, but it is less secure than the internet, which hosts crucial and sensitive data. We require a DMZ because we wish to provide public users with a convenient and efficient service. We also don't want to have too much control over traffic to the DMZ.

Within this company’s LAN there are 2 areas. 1st area is heavily protected internet. The company doesn’t want the internet users to access this part easily.

2nd part is DMZ. Which is lightly protected area where the file servers or web servers are hosted. The company wants the public user to access this service easily and smoothly like it wants as many public users as possible to access its webpages. If these servers are protected too much the traffic to the DMZ is restricted too much.

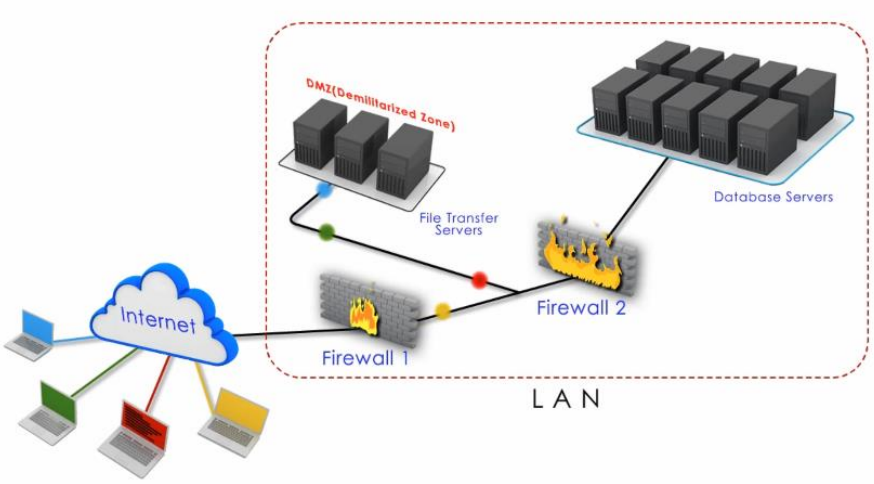



*Figure 4. 29 Typical way of how DMZ works in a LAN*

## 4.3 Critical reflection of my work

A company's computer network infrastructure is its backbone. All machines, software and applications and all other work of a company is built upon the computer network. As a result, any organization must prioritize the planning, design, purchase of hardware, and security of its computer network. Setting up a computer network in a business environment is significantly different from setting up a network at home or in a domestic setting.

When taking a business networking environment there is a high degree of complexity and security challenges. While the type of network a company needs will vary, the components of a computer network will remain consistent. Because of that before building a good network for this company I followed several steps as follows.

1. Understand business goals and technical requirements.
2. Creating a budget and acquiring components.
3. Designing the network.
4. Security and Connectivity.
5. Disaster Recovery Plan.
6. Training and scalability

**STEP 01 → Understand business goals and technical requirements :-**

SYNTAX SOLUTIONS is a privately owned, well-known Software company located in Colombo. The Management of SYNTAX SOLUTIONS has purchased a 3-story building in the heart of Matara and they wanted to make it one of the state-of-the-art companies in Matara with the latest facilities. According to this company's goals and objectives I expected to set my objectives and goals to build a good IT network for them. This supported me in selecting the appropriate resources and components.

Also, I've figured out what kind of data I'll be storing in the network. Because this is a well-known software company, they deal with a great deal of personal information from a large number of people. This company is responsible for ensuring that the personal data they hold is protected using proper security methods. As a result, I comprehended the needs and took the necessary steps to construct the most secure network possible for this organization. This helped me in selecting the appropriate software and hardware for the network.

**STEP 02 → Creating a budget and acquiring components :-**

One of the most significant parts of network construction is the budget. When IT costs are not adequately controlled, they can quickly spiral out of control. As a result, I had to ensure that capital was set aside for necessities. Getting the correct equipment is just as crucial as completing the budget. So, after purchasing the required equipment, the first thing I did was look at an example of a typical small company network setup, as seen below.

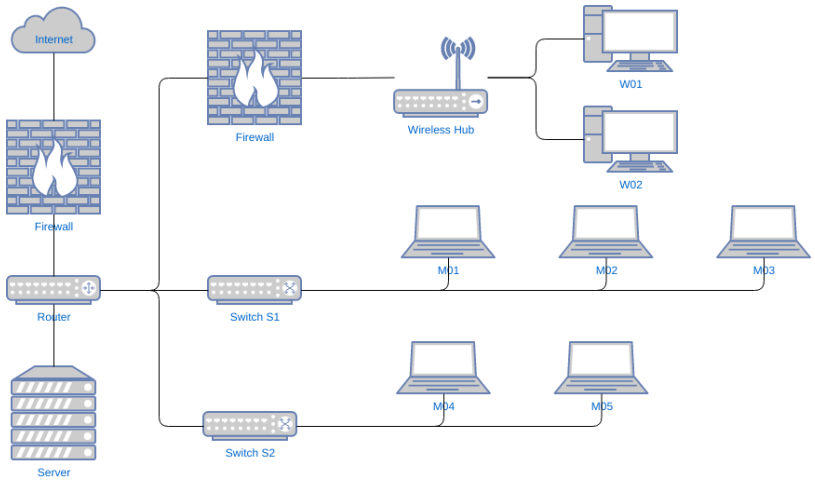



*Figure 4. 30 Typical small company network setup*

From using this smaller picture, I tried to design bigger picture of the LAN for this company. Then I made a list of the hardware components this network requires. After that, I made a separate note of how much each piece of hardware cost. Switches, servers, PCs, and all other necessary hardware components are critical to an IT network's performance. Because of that after research I listed out best hardware and software components for the designed network with the estimated cost for them.

**STEP 03 → Designing the network :-**

IT administrators can use network topology mapping software, often known as network topology software, to see how the total network infrastructure is arranged. I drew diagrams to help me comprehend and understand device networks and dependencies. I purchased a “Microsoft Visio” license and “Wondershare EdarwMax” license to develop a better network diagram for this company, and then used both of the software to produce a better network architecture.

As a result, I was able to efficiently administer the designed network. Knowing and visualizing each device's dependency made it simple for me to figure out which device or application was causing a bottleneck in the performance of other devices. This was possible for me with a better network topology mapping.

The SYNTAX Solutions Matara branch has 3-story building. Hence, I separated into each floor to different departments since the management was expecting to have 7 departments. Then I applied access points for each department to access internet wirelessly if they use wireless devices. And I separated each department into Virtual LANs to manage each department easily. To separate Virtual LANs, I did subnetting for given IP address. When I do subnetting for each department I got 1 extra subnet and I kept it as a redundancy for the future.

Then for setting PCs for each department I counted maximum number of employees for each department. Hence, I used 24- port switch for each department to manage a low cost. And I applied access points as a redundancy if management decide to have extra employees for each department. After that I connected every department switch into 1 switch and then connected it to Router.

Then I created the VLANs by Cisco Packet Tracer software as I leaned. Since I intended to configure 3 servers in server room, I went through heavy research to find a way to configure DNS server, Web server and Email server. I was quite challenging. After setting VLAN, I tested each computer and server connectivity with several test cases. The VLAN was successful since I did heavy research and follow every step with understanding. Every step was very useful to setup a successful network for the company and it helped me to evaluate my work eventually.

**STEP 04 → Security and Connectivity :-**

Network connectivity is expanding with time. Now, we can even use our mobile phones for connecting to business networks. Employees can use their mobile devices for accessing their company mail and etc. This will ensure that they can work from any remote location in the world. It is important to balance these needs while designing this network.

But I had to also consider the security challenges while designing the network. I had to ensure that even remote workers can access your network. But this can open many security holes in the network. I have to ensure this network is protected from threats. This will ensure that attackers can't use your network without proper authorization. Hence, I installed several third-party firewalls to protect the client PCs and Servers. And I choose best Switches, Routers and Modems for this network to enhance the protection of them.

And also, I had to figure out where I plan to store the data of this company. Some companies are using cloud-based solutions for storing their data, but I choose to buy servers to store the data since transfer data across internet for cloud server is too risk. So, in the network design I set up a server room for this company.

**STEP 05 → Disaster Recovery Plan :-**

Any network design should include a robust disaster recovery plan. When designing a network, I took into account when and how data is backed up, as well as where copies of the data are stored. Important data should be backed up at least once a day in most circumstances. Many businesses perform a complete weekly backup followed by daily incremental backups that replicate any files that have changed since the last weekly backup.

For backup server data into cloud, I planned to do it monthly basis in maintenance schedule. In the event of a building catastrophe, such as a fire, backup files should be maintained in a safe off-site location. For that I separated a database server in the server room to store data since it is most secure location in the building.

**STEP 06 → Training and scalability :-**

It is critical to educate staff about the new policies. Employees will be aware of the new network policies as a result of this. In addition, I need to give a cybersecurity seminar to the staff. Human mistake is to blame for the majority of network breaches. As a result, basic security terms must be taught to staff.

Another crucial aspect of any IT network is scalability. I should be required to upgrade and update the company's IT resources. As a result, I need to comprehend network expansion. This will assist me in avoiding unexpected expenses. It will also ensure that our company is prepared for expansion.

# Conclusion

This whole assignment demonstrates a successful implementation of a network architectural design for SYNTAX Solutions Matara branch. The 1st Task explains what is meant by computer network and it further explained by comparing different types of computer networks along with the communication methods of a computer system. After that along with common networking principles and types of different protocols have been explained. The IEEE standards and Network topologies of a network system is explained at the end of the task.

Then the 2nd tasks explain about networking devices and servers that are being used today. After that workstation hardware and software has been explained. At the end of the 2nd task, different types of software have been explained further.

3rd task demonstrate how I created LAN design for SYNTAX Solutions company Matara branch and maintenance schedule with user feedback form is given in the task. At the end of the task demonstrate how I created the virtual LAN for the company by using Cisco Packet Tracer.

The 4th task finally demonstrate how I tested the virtual LAN by different types of test cases. Then further explained how I can enhance the created LAN system in the future. Finally, I critically reflected my own work for further understanding the process I've been followed.

# References


GeeksforGeeks. 2021. Types of Computer Networks - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/types-of-computer-networks/.

[Accessed 17 October 2021].

BBC News. 2021. What happened to Facebook, WhatsApp, and Instagram? - BBC News.

[ONLINE] Available at: https://www.bbc.com/news/technology-58800670.

[Accessed 17 October 2021].

Green Garage. 2021. 14 Main Advantages and Disadvantages of Computer Networking – Green Garage.

[ONLINE] Available at: https://greengarageblog.org/14-main-advantages-and-disadvantages-of-computer-networking.

[Accessed 17 October 2021].

IT Release. 2021. What is Enterprise private network (EPN) with example - IT Release.

[ONLINE] Available at: https://www.itrelease.com/2021/06/what-is-enterprise-private-network-epn-with-example/.

[Accessed 17 October 2021].

GeeksforGeeks. 2021. Difference between Client-Server and Peer-to-Peer Network - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/difference-between-client-server-and-peer-to-peer-network/.

[Accessed 17 October 2021].

GeeksforGeeks. 2021. Cloud Computing - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/cloud-computing/.

[Accessed 20 October 2021].

GeeksforGeeks. 2021. Cloud Based Services - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/cloud-based-services/.

[Accessed 20 October 2021].

EasyTechJunkie. 2021. What is a Cluster Network? (with pictures).

[ONLINE] Available at: https://www.easytechjunkie.com/what-is-a-cluster-network.htm.

[Accessed 20 October 2021].

GeeksforGeeks. 2021. Comparison - Centralized, Decentralized and Distributed Systems - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/.

[Accessed 20 October 2021].

EDUCBA. 2021. What is Cluster Computing | A Concise Guide to Cluster Computing.

[ONLINE] Available at: https://www.educba.com/what-is-cluster-computing/.

[Accessed 24 October 2021].

GeeksforGeeks. 2021. Difference between Intranet and Extranet - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/difference-between-intranet-and-extranet/.

[Accessed 24 October 2021].

SearchNetworking. 2021. What are the IEEE 802 Standards?.

[ONLINE] Available at: https://www.techtarget.com/searchnetworking/reference/IEEE-802-Wireless-Standards-Fast-Reference.

[Accessed 24 October 2021].

NetworkByte. 2021. IEEE Standards | NetworkByte.

[ONLINE] Available at: https://network-byte.com/ieee-standards/.

[Accessed 24 October 2021].

YouTube. 2021. Lecture 36: IEEE Standards (802) and Ethernet (802.3) | Computer Networks - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=w56_kHprsU4.

[Accessed 30 October 2021].

Fiber Optic Solutions. 2021. Fast Ethernet vs Gigabit Ethernet: What's the Difference?.

[ONLINE] Available at: http://www.fiber-optic-solutions.com/fast-ethernet-vs-gigabit-ethernet.html.

[Accessed 30 October 2021].

GeeksforGeeks. 2021. Difference between Fast Ethernet and Gigabit Ethernet - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/difference-between-fast-ethernet-and-gigabit-ethernet/.

[Accessed 30 October 2021].

dummies. 2021. How to Choose the Proper Wireless Network Standard - dummies.

[ONLINE] Available at: https://www.dummies.com/computers/pcs/how-to-choose-the-proper-wireless-network-standard/.

[Accessed 30 October 2021].

YouTube. 2021. The Evolution of IEEE 802.11 Standards | 802.11 Wireless Standards | WiFi 802.11 a/b/g/n/ac Standard - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=rnwHa4IttLs.

[Accessed 30 October 2021].

YouTube. 2021. The Evolution of IEEE 802 11 standards - BAG NAC - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=qZLPq5mebFM&t=114s.

[Accessed 1 November 2021].

YouTube. 2021. The Evolution of IEEE 802 11 standards - BAG NAC - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=qZLPq5mebFM&t=114s.

[Accessed 1 November 2021].

YouTube. 2021. Token ring network and how it works - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=p72R2uGglnU.

[Accessed 1 November 2021].

YouTube. 2021. Network topology types (Bus, Star, Ring, Mesh, Hybrid, Logical, Physical) | TechTerms - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=e0CWszGpgAE.

[Accessed 1 November 2021].

Network Direction. 2021. Hierarchical Network Model - Network Direction.

[ONLINE] Available at: https://networkdirection.net/articles/network-theory/hierarchicalnetworkmodel/.

[Accessed 1 November 2021].

Hierarchical Network Design Overview (1.1) > Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design | Cisco Press . 2021.

[ONLINE] Available at: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4.

[Accessed 1 November 2021].

Wikipedia. 2021. Hierarchical internetworking model - Wikipedia.

[ONLINE] Available at: https://en.wikipedia.org/wiki/Hierarchical_internetworking_model.

[Accessed 3 November 2021].

Cisco Three Layer / Three-tier Hierarchical Network Model. 2021. Cisco Three Layer / Three-tier Hierarchical Network Model.

[ONLINE] Available at: https://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php.

[Accessed 3 November 2021].

What are Repeaters in Computer Network?. 2021. What are Repeaters in Computer Network?.

[ONLINE] Available at: https://www.tutorialspoint.com/what-are-repeaters-in-computer-network.

[Accessed 3 November 2021].

GeeksforGeeks. 2021. Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter) - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/.

[Accessed 3 November 2021].

What are Hub and Switch in Computer Network?. 2021. What are Hub and Switch in Computer Network?.

[ONLINE] Available at: https://www.tutorialspoint.com/what-are-hub-and-switch-in-computer-network.

[Accessed 5 November 2021].

What are Switches in Computer Network?. 2021. What are Switches in Computer Network?.

[ONLINE] Available at: https://www.tutorialspoint.com/what-are-switches-in-computer-network.

[Accessed 5 November 2021].

What are Routers in Computer Network?. 2021. What are Routers in Computer Network?.

[ONLINE] Available at: https://www.tutorialspoint.com/what-are-routers-in-computer-network.

[Accessed 5 November 2021].

Uses of Bridges in Computer Network. 2021. Uses of Bridges in Computer Network.

[ONLINE] Available at: https://www.tutorialspoint.com/uses-of-bridges-in-computer-network.

[Accessed 5 November 2021].

TechGenix. 2021. What is a layer 3 switch and why would your network need it?.

[ONLINE] Available at: https://techgenix.com/layer-3-switch/.

[Accessed 5 November 2021].

What are Gateways in Computer Network?. 2021. What are Gateways in Computer Network?.

[ONLINE] Available at: https://www.tutorialspoint.com/what-are-gateways-in-computer-network.

[Accessed 5 November 2021].

Fiber Transceiver Solution. 2021. What Is a Multilayer Switch and How to Use It?.

[ONLINE] Available at: http://www.fiber-optic-transceiver-module.com/what-is-a-multilayer-switch-and-how-to-use-it.html.

[Accessed 9 November 2021].

Techopedia. 2021. What is a Multilayer Switch? - Definition from Techopedia.

[ONLINE] Available at: https://www.techopedia.com/definition/8465/multilayer-switch.

[Accessed 9 November 2021].

Comparing Top-of-the-Line Servers: HP ProLiant DL360 Gen9 vs. DL380 Gen9. 2021. Comparing Top-of-the-Line Servers: HP ProLiant DL360 Gen9 vs. DL380 Gen9.

[ONLINE] Available at: https://www.aventissystems.com/blog-smb-comparing-top-of-the-line-servers-s/12994.htm#:~:text=The%20primary%20difference%20between%20the,be%20fitted%20with%20more%20drives..

[Accessed 9 November 2021].

YouTube. 2021. Buying a SERVER - 3 things to know - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=AcCkrHfA_gU&ab_channel=diyinfosec.

[Accessed 9 November 2021].

Paessler. 2021. Server - Definition and details.

[ONLINE] Available at: https://www.paessler.com/it-explained/server.

[Accessed 9 November 2021].

Networks Training. 2021. 8 Different Types of Servers in Computer Networks.

[ONLINE] Available at: https://www.networkstraining.com/different-types-of-servers/.

[Accessed 9 November 2021].

RedNight Consulting. 2021. 6 things to consider when buying a server for your business.

[ONLINE] Available at: https://www.rednightconsulting.com/6-things-to-consider-when-buying-a-server-for-your-business/.

[Accessed 9 November 2021].

Dell Technologies. 2021. Five Things to Consider When Buying Your First Server - Dell Technologies.

[ONLINE] Available at: https://www.delltechnologies.com/en-us/blog/five-things-to-consider-when-buying-first-server/.

[Accessed 9 November 2021].

Jones IT | Managed IT Services, IT Support, IT Consulting. 2021. Best Servers For Small And Medium Businesses | Jones IT.

[ONLINE] Available at: https://www.itjones.com/blogs/2021/2/1/best-servers-for-small-and-medium-businesses.

[Accessed 9 November 2021].

Small Business Servers: How To Choose Best Server In 2021. 2021. Small Business Servers: How To Choose Best Server In 2021.

[ONLINE] Available at: https://blog.servermania.com/choosing-a-small-business-server/.

[Accessed 9 November 2021].

YouTube. 2021. CAIB | Relationship between software and Hardware | Hardware and Software are two sides of same coin - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=PLPWIPH7KD8.

[Accessed 10 November 2021].

YouTube. 2021. DIT / ICT / Definition of Software and Hardware, Relationship between Software and Hardware - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=TF1ifwP7Dxo.

[Accessed 10 November 2021].

GeeksforGeeks. 2021. Difference between Software Defined Network and Traditional Network - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/difference-between-software-defined-network-and-traditional-network/.

[Accessed 10 November 2021].

Network Software. 2021. Network Software.

[ONLINE] Available at: https://www.tutorialspoint.com/Network-Software.

[Accessed 10 November 2021].

Network Software. 2021. Network Software.

[ONLINE] Available at: https://www.tutorialspoint.com/Network-Software.

[Accessed 10 November 2021].

Gustavo Carvalho. 2021. Web server examples: The top 5 servers - Copahost.

[ONLINE] Available at: https://www.copahost.com/blog/web-server-examples/.

[Accessed 10 November 2021].

DigitalThinkerHelp. 2021. What is Database Server: Definition, Types, Examples, Functions, Working.

[ONLINE] Available at: https://digitalthinkerhelp.com/what-is-database-server-definition-types-examples-functions-working/.

[Accessed 10 November 2021].

Webopedia. 2021. What is A Server Operating System? | Webopedia.

[ONLINE] Available at: https://www.webopedia.com/definitions/server-operating-system/.

[Accessed 10 November 2021].

Cisco SF350-24P | Comms Express. 2021. Cisco SF350-24P | Comms Express.

[ONLINE] Available at: https://www.comms-express.com/products/cisco-sf350-24p/.

[Accessed 10 November 2021].

Cisco. 2021. Cisco RV340 Dual WAN Gigabit VPN Router - Cisco.

[ONLINE] Available at: https://www.cisco.com/c/en/us/products/routers/rv340-dual-gigabit-wan-vpn-router/index.html.

[Accessed 10 November 2021].

Wirecutter: Reviews for the Real World. 2021. The Best Cable Modem | Reviews by Wirecutter.

[ONLINE] Available at: https://www.nytimes.com/wirecutter/reviews/best-cable-modem/.

[Accessed 11 November 2021].

Cisco. 2021. Cisco Business 100 Series Access Points - Cisco Business 100 Series Access Points - Cisco.

[ONLINE] Available at: https://www.cisco.com/c/en/us/products/wireless/business-100-series-access-points/index.html.

[Accessed 11 November 2021].

Business Pundit. 2021. The Best Firewall for Small Business Owners: 6 Top Products.

[ONLINE] Available at: https://www.businesspundit.com/best-firewall-for-small-business/.

[Accessed 11 November 2021].

. 2021. Bitdefender Business Cybersecurity Solutions Comparison.

[ONLINE] Available at: https://www.bitdefender.com/business/compare.html.

[Accessed 11 November 2021].

SearchNetworking. 2021. Key tasks in a network maintenance checklist.

[ONLINE] Available at: https://www.techtarget.com/searchnetworking/tip/Key-tasks-in-a-network-maintenance-checklist.

[Accessed 11 November 2021].

Worldwide Services. 2021. What Is Network Maintenance? | Network Maintenance Plans & Tips.

[ONLINE] Available at: https://worldwideservices.net/network-maintenance-guide-upkeep/.

[Accessed 11 November 2021].

HitechWhizz - The Ultimate Tech Experience. 2021. 7 Advantages and Disadvantages of LAN | Limitations & Benefits of LAN .

[ONLINE] Available at: https://www.hitechwhizz.com/2020/07/7-advantages-and-disadvantages-drawbacks-benefits-of-lan.html.

[Accessed 11 November 2021].

Why Fast Ethernet. 2021. Why Fast Ethernet.

[ONLINE] Available at: http://www.dewassoc.com/support/networking/whyfast.htm.

[Accessed 11 November 2021].

Worldwide Supply. 2021. The Benefits of Switching to 10 Gigabit Ethernet | Worldwide Supply.

[ONLINE] Available at: https://worldwidesupply.net/blog/benefits-switching-10-gigabit-ethernet/.

[Accessed 11 November 2021].

www.qorvo.com. 2021. No page title.

[ONLINE] Available at: https://www.qorvo.com/resources/d/qorvo-the-wi-fi-evolution-white-paper#:~:text=Over%20the%20past%2020%20years,(Wi%2DFi%206)..

[Accessed 11 November 2021].

Danny Mareco. 2021. Benefits of Using 802.11n Wifi Access Points.

[ONLINE] Available at: https://www.securedgenetworks.com/blog/benefits-of-using-80211n-wifi-access-points.

[Accessed 13 November 2021].

blossoms.mit.edu. 2021. No page title.

[ONLINE] Available at: https://blossoms.mit.edu/sites/default/files/video/download/Notes-on-Hybrid-topology.pdf.

[Accessed 13 November 2021].

GeeksforGeeks. 2021. Components of Data Communication System - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/components-of-data-communication-system/.

[Accessed 13 November 2021].

Teach Computer Science. 2021. Simplex, Half Duplex, Full Duplex | Definition, Comparison & Information.

[ONLINE] Available at: https://teachcomputerscience.com/simplex-half-duplex-full-duplex/.

[Accessed 13 November 2021].

GeeksforGeeks. 2021. Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex) - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/transmission-modes-computer-networks/.

[Accessed 13 November 2021].

GeeksforGeeks. 2021. Line Configuration in Computer Networks - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/line-configuration-computer-networks/.

[Accessed 13 November 2021].

GeeksforGeeks. 2021. Differences between Point-to-Point and Multi-point Communication - GeeksforGeeks.

[ONLINE] Available at: https://www.geeksforgeeks.org/differences-between-point-to-point-and-multi-point-communication/.

[Accessed 13 November 2021].

SearchNetworking. 2021. What is network bandwidth and how is it measured?.

[ONLINE] Available at: https://www.techtarget.com/searchnetworking/definition/bandwidth.

[Accessed 13 November 2021].

Lifewire. 2021. What is Bandwidth and How Much Do You Need?.

[ONLINE] Available at: https://www.lifewire.com/what-is-bandwidth-2625809.

[Accessed 16 November 2021].

Classic Hotspot | Guest WiFi, Social Login and Paid WiFi. 2021. Network Bandwidth - How to Calculate WiFi Bandwidth Need?.

[ONLINE] Available at: https://www.tanaza.com/tanazaclassic/blog/how-to-calculate-network-bandwidth-requirements/.

[Accessed 16 November 2021].

Which model is better, OSI or TCP/IP?. 2021. Which model is better, OSI or TCP/IP?.

[ONLINE] Available at: https://afteracademy.com/blog/which-model-is-better-osi-or-tcpip.

[Accessed 16 November 2021].

dummies. 2021. Network Administration: TCP/IP Protocol Framework - dummies.

[ONLINE] Available at: https://www.dummies.com/programming/networking/network-administration-tcpip-protocol-framework/.

[Accessed 16 November 2021].

YouTube. 2021. IDS and IPS - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=cMH4yGE73iQ.

[Accessed 16 November 2021].

Forcepoint. 2021. What is a Firewall? Defined, Explained, and Explored | Forcepoint .

[ONLINE] Available at: https://www.forcepoint.com/cyber-edu/firewall.

[Accessed 16 November 2021].

Jigsaw Academy. 2021. Packet Filtering Firewall All you need to know In 3 Easy Steps.

[ONLINE] Available at: https://www.jigsawacademy.com/blogs/cyber-security/packet-filtering-firewall/#Packet-Filtering-Firewall-Diagram.

[Accessed 19 November 2021].

SearchSecurity. 2021. What is a Proxy Firewall? - Definition from WhatIs.com.

[ONLINE] Available at: https://searchsecurity.techtarget.com/definition/proxy-firewall.

[Accessed 19 November 2021].

YouTube. 2021. What is a Firewall? - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=kDEX1HXybrU.

[Accessed 19 November 2021].

YouTube. 2021. Firewall - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=RV2QznoyEBU.

[Accessed 19 November 2021].

YouTube. 2021. Honeynet and DMZ - YouTube.

[ONLINE] Available at: https://www.youtube.com/watch?v=FihkG72z7MQ.

[Accessed 19 November 2021].