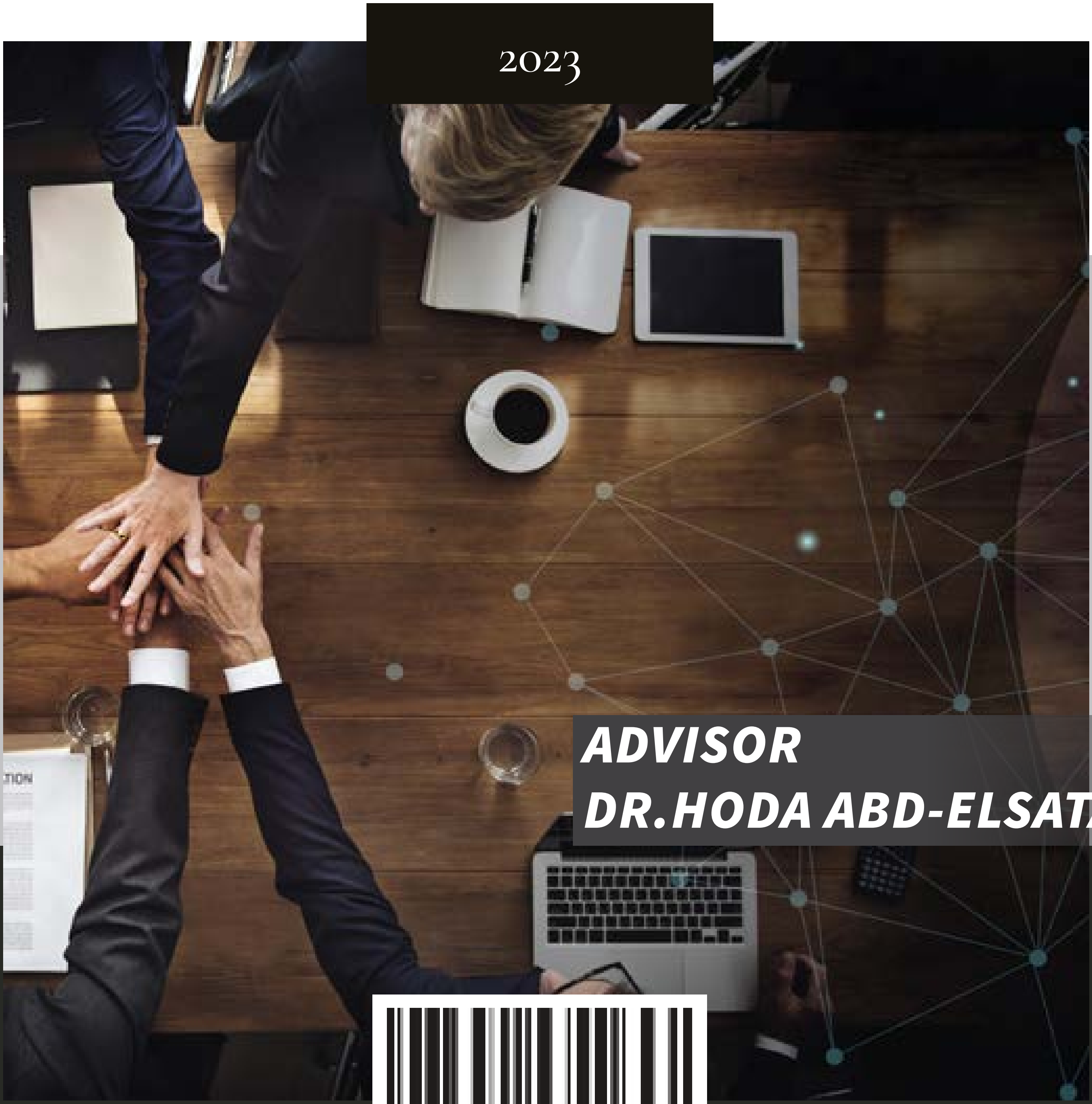
The High Institute of Engineering and Technology
Luxor - الأقصر

وزارة التعليم العالي والبحث العلمي
MINISTRY OF HIGHER EDUCATION
AND SCIENTIFIC RESEARCH

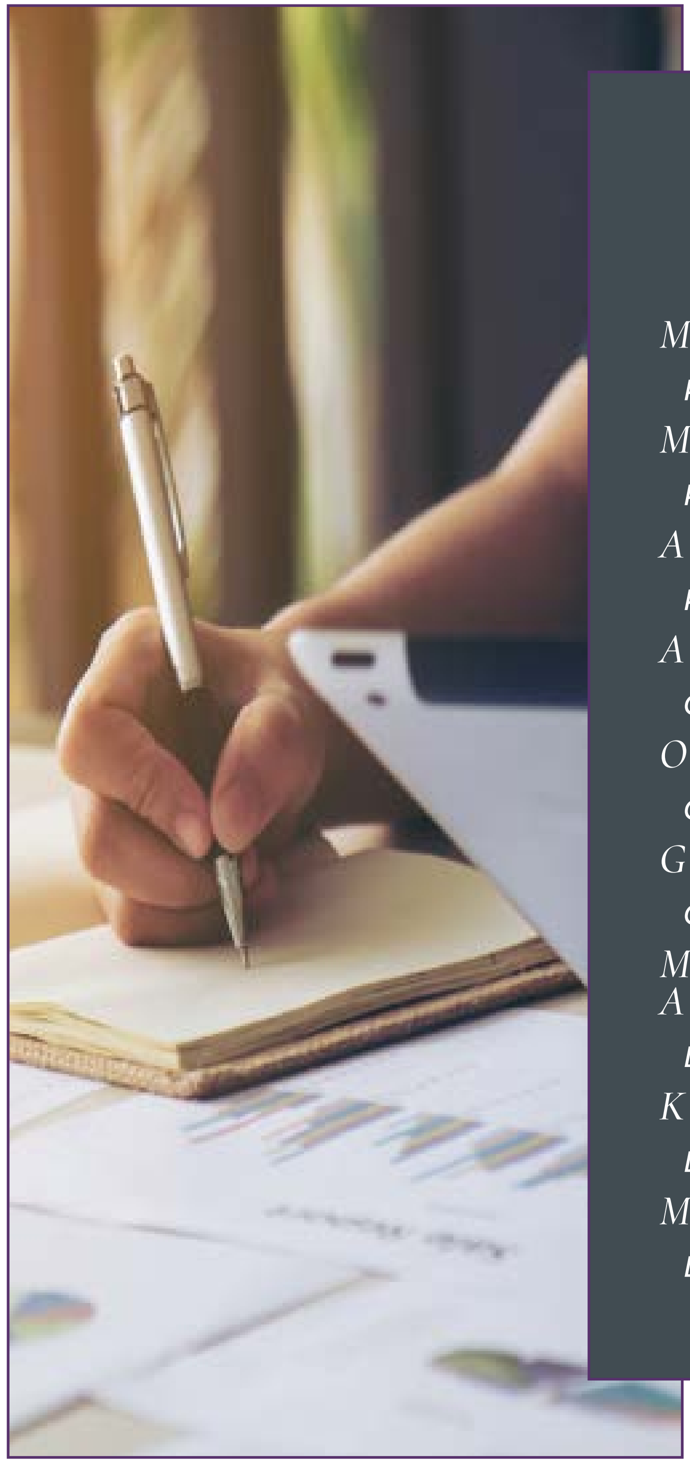
Virtual university networking structure

Fundamentals of networking

2023



ADVISOR
DR.HODA ABD-ELSATAR



Group Members

Marvy Nashaat Naiem
Presentation and book writing
Mona Alamir Monir
Presentation and book writing
Ahmed Mohamed Mahmoud
Presentation and book writing
Andro Ehab Khairy
Configuration & protocols
Osama Marzouk Rezk
Configuration & protocols
Gamal Abd-Elnaser
Configuration & protocols
Mohamed Mostafa Mohamed Abu-Elhagag
Lay-out & Components
Karim Ahmad
Lay-out
Mohamed kamal
Lay-out

Table of contents

INTRODUCTION TO PROJECT 5
0-1 Project description 6
0-2 Book contents 8

BASICS OF NETWORKING 11
1-1 Basic Undrstanding 11
1-1-1 Networking definition 11
1-1-2 Network types 11
1-1-3 OSI layers 15
1-2 LAN Basics 22
1-2-1 TCP/IP 22
1-2-2 LAN setup 23
1-2-3 Virtual LAN 24

FUNDAMENTAL COMPONENTS 27
2-1 Superstructure 28
2-1-1 PCs & Laptops 28
2-1-2 Mobile phones 29
2-1-3 smart board 30
2-1-4 RFID Gates 31
2-1-5 IP phones 32
2-1-6 Other devices 33

2-2 Infrastructure 34

2-2-1 Passive 34

2-2-2 Active 37

SOFTWARE APPLICATION 43

3-1 Diagram Programes 44

3-1-1 Autocad 44

3-2-1 Packet Tracer 45

3-2 Simulation Tools 45

3-2-2 VMWare workstation 45

3-2-3 EVE Comm 47

SOFTWARE APPLICATION 49

Table of figures

Figure 1: LAN 12

Figure 2: WAN 13

Figure 3: MAN 14

Figure 4: OSI 15

Figure 5: TCP/IP 22

Figure 6:Coaxial cable 34

Figure 8: Fiber-optic cable 35

Figure 9: Racks 35

Figure 7:Twisted cable 35

Figure 10: UPs 36

Figure 11: Rackmount monitor 36

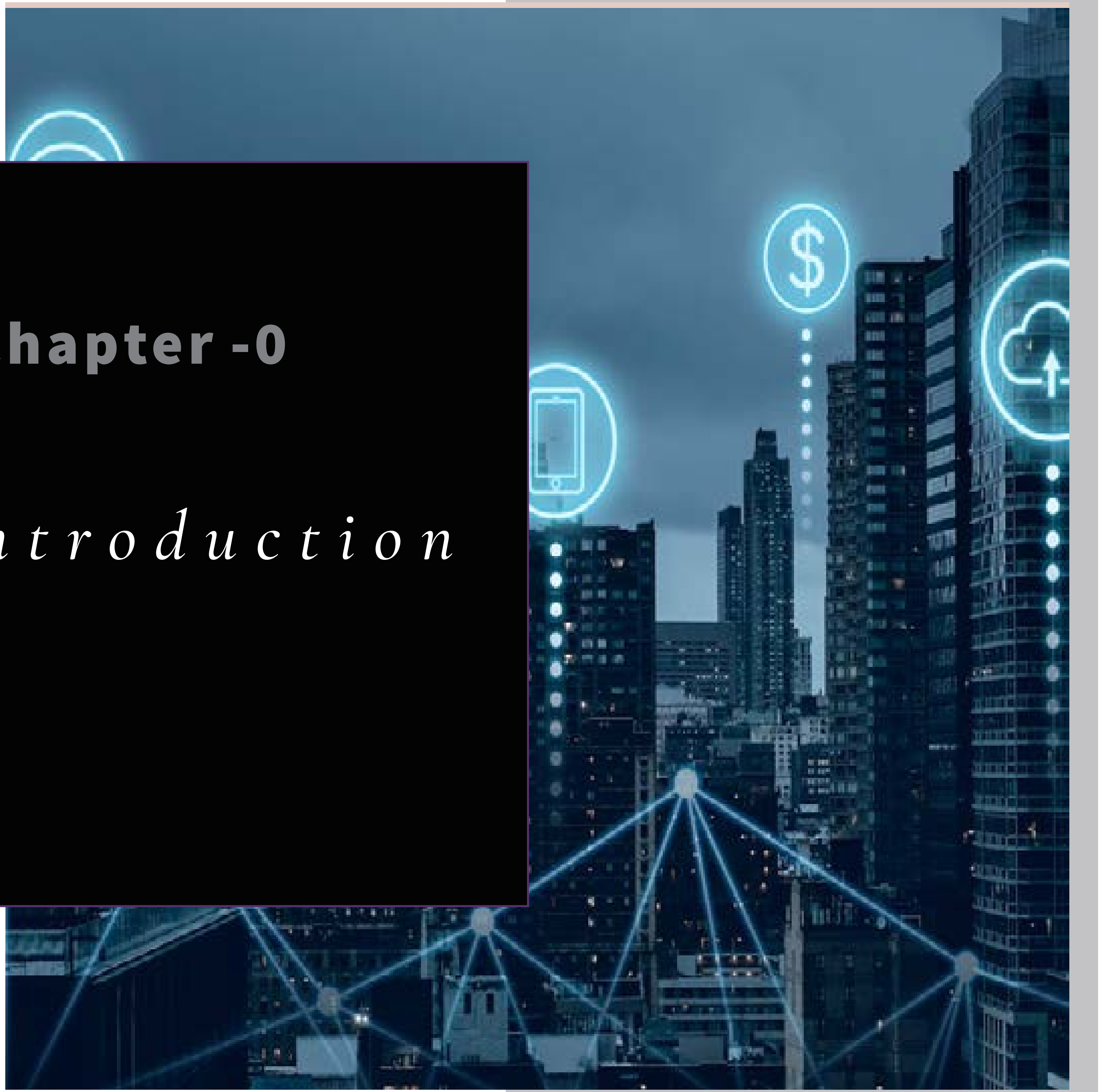
Figure 12: Switch 37

Figure 13: Router 38

Figure 14: Server 39

Figure 15: Firewall 40

Figure 16: Access point 41



Chapter -0

Introduction

Introduction to project

In the past, there was communication between people, but with poor quality and few and limited capabilities.

They were met with many problems in transferring data and exchanging information between them, such as the arrival of incomplete data or perhaps it was not clear at all.

Therefore, in our project, we will look forward to keeping pace with the times and the development of technology in transferring data and information and improving communication between people with each other.

And we will explain how to connect a large and high-quality communication network through technology and modern devices with various and high-quality systems.

We have a model to which we will apply this project: the Higher Institute of Engineering and Technology in Luxor

0-1 Project description

To keep pace with the developments of technology nowadays and achieve the proper education experience we need to establish the *university's networking infrastructure* and create an integrated system to establish seamless communication between students, professors, and university administration.

The networking structure will help the process of education with a lot of facilities and features :

- ***Ease of communication across the users doctors,student & administration***
- ***Synchronizing & securing databases with access on board***
- ***Automated systems for attendance of students and professors***
- ***Establishing of E-learning with the appropriate tools***
- ***Providing university E-platform & E-library***

A SIMPLE DEFINITION OF NETWORKING

Making connections and building relationships to exchange information

To establish the wanted infrastructure we need to understand the fundamentals basics of networking and the components of the system , then we start to plan and identify the system and program it to match the wanted result and achieve the benefits of *networking & E-learning*

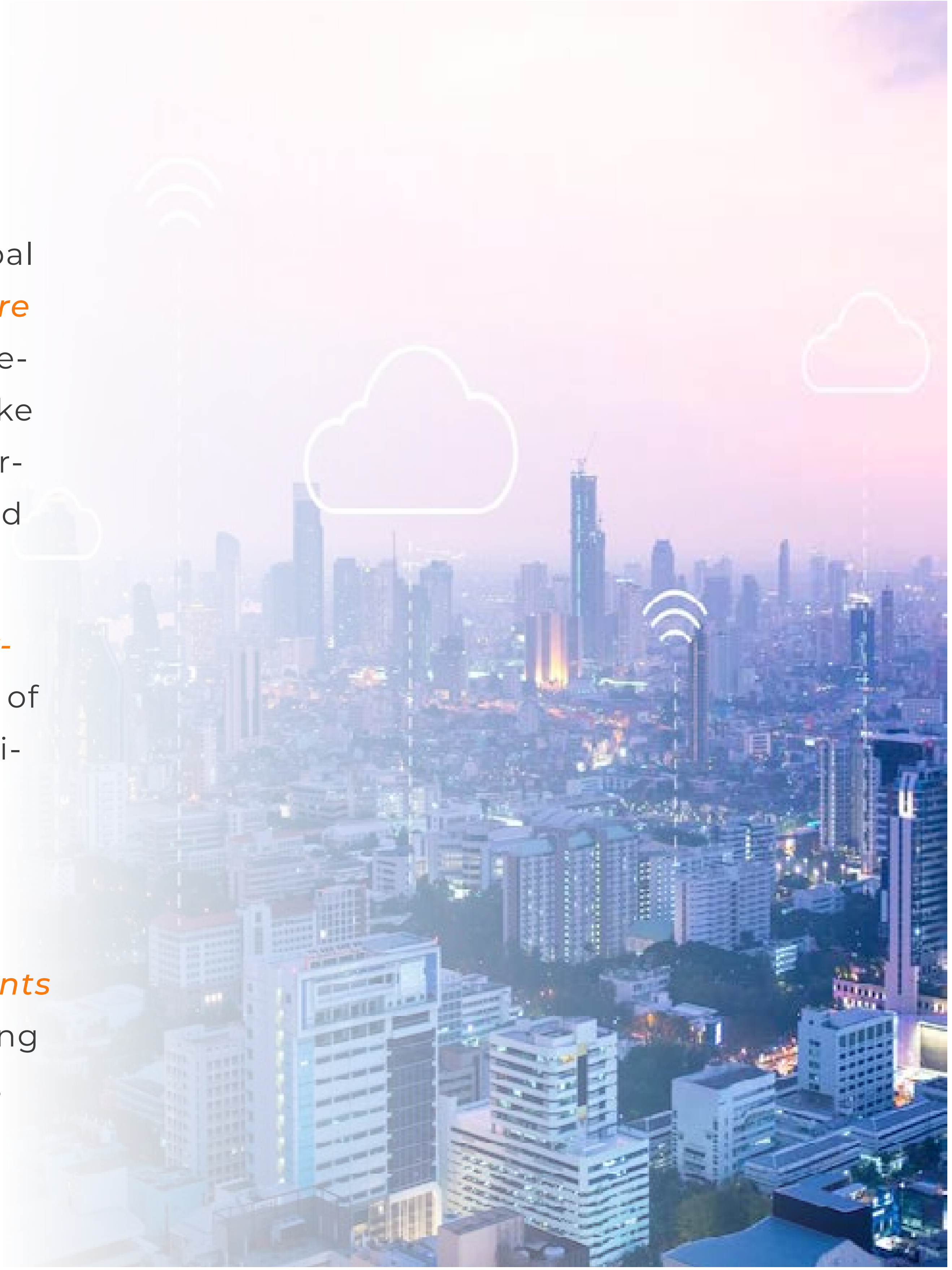
Therefore we have a cleared steps to bulid that infrastructure for the university [*Higher institute of engineering & technology El-Tod*]

0-2 Book contents

The book will discuss the principal steps of *designing the infrastructure of networking* in 5 chapters with detailed explaining of each step & make sure that we have a complete understanding of all components included at the system

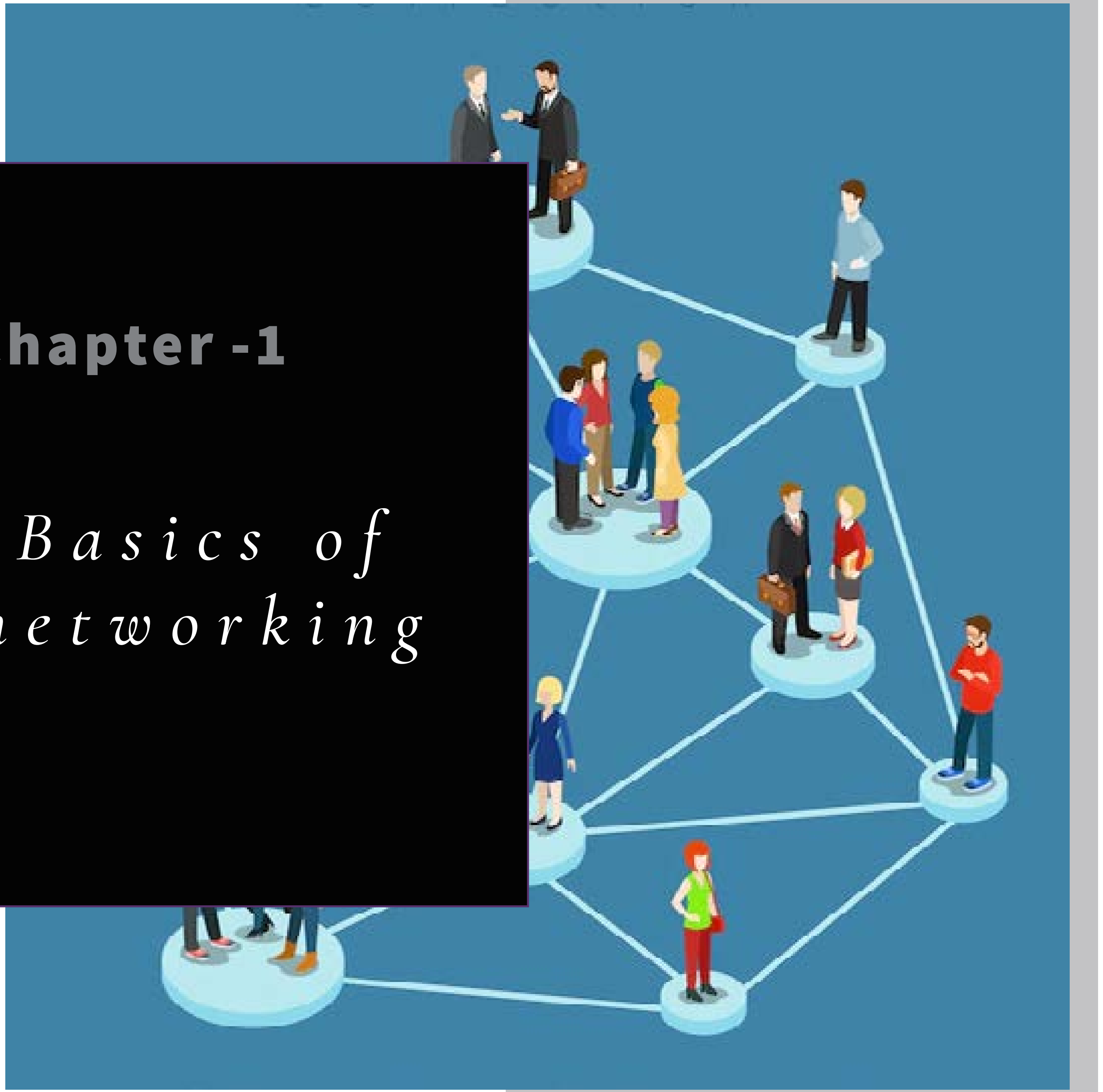
First chapter *''basics of networking''* explains the simple principles of a network , defines important definitions & shows deferences between network types

Second chapter of this book will discuss the *fundamental components* of the networking structure including superstructures and infrastructures



At the third chapter *''process of designing''* will define the general steps of the modulating system with 4 major procedure

Fourth chapter discusses the *features of system* with complete understanding of the engineering behind each feature



Chapter -1

Basics of networking

Basics of networking

At the beginning of our discussion we will define some definitions , understand the basic principles of networking and the differences between each network types .

1-1 Basic Undrstanding

1-1-1 Networking definition

it’s known as the practice of transporting and exchanging data between nodes over a shared medium in an information system .

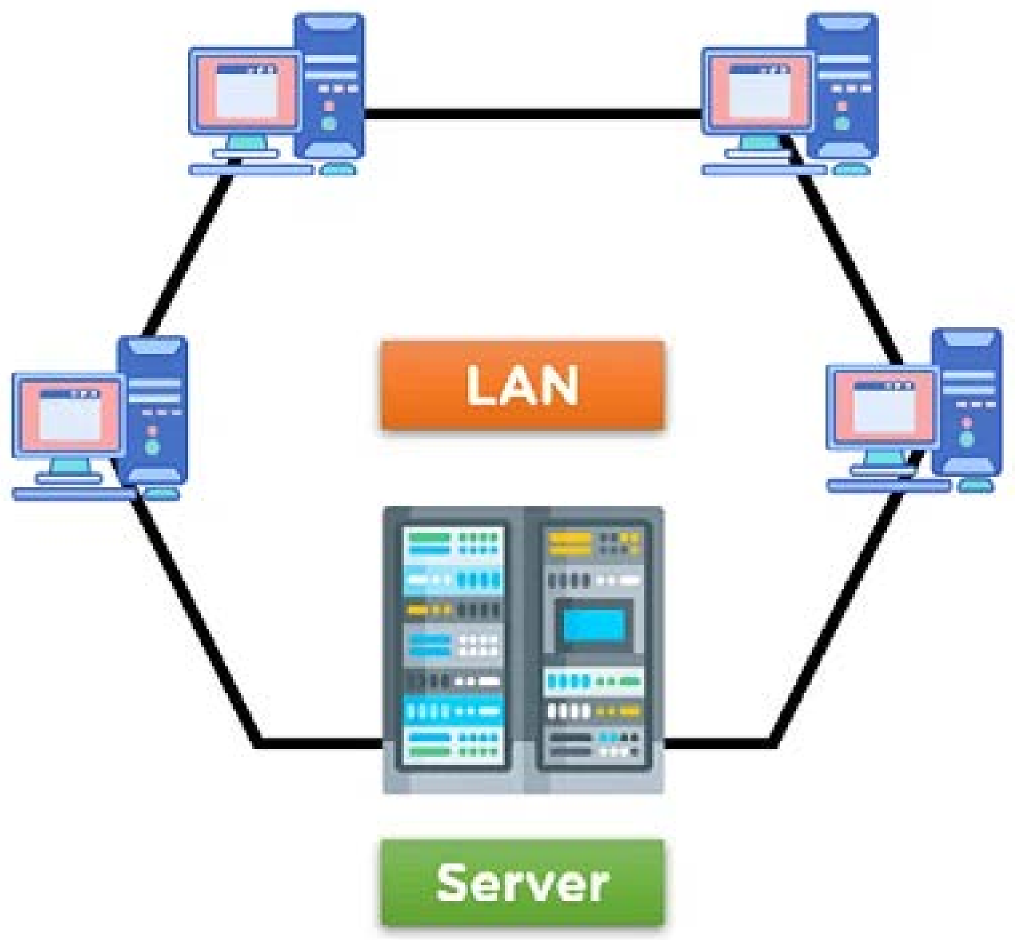
1-1-2 Network types

1. **LAN**
   (Local Area Network)
2. **WAN**
   (Wide Area Network)
3. **MAN**
   (Metropolitan Area Network)

1. LAN :

A computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media

*Cables + Switch + PC *(NIC)*



**NIC:*
Network interface card is the hardware device most essential to establishing communication between computers.

Figure 1: LAN

2. WAN :

It is a network that covers a broadarea using private or public network transports. Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations.

LAN [Cables + Switch + PC (NIC)]+Router

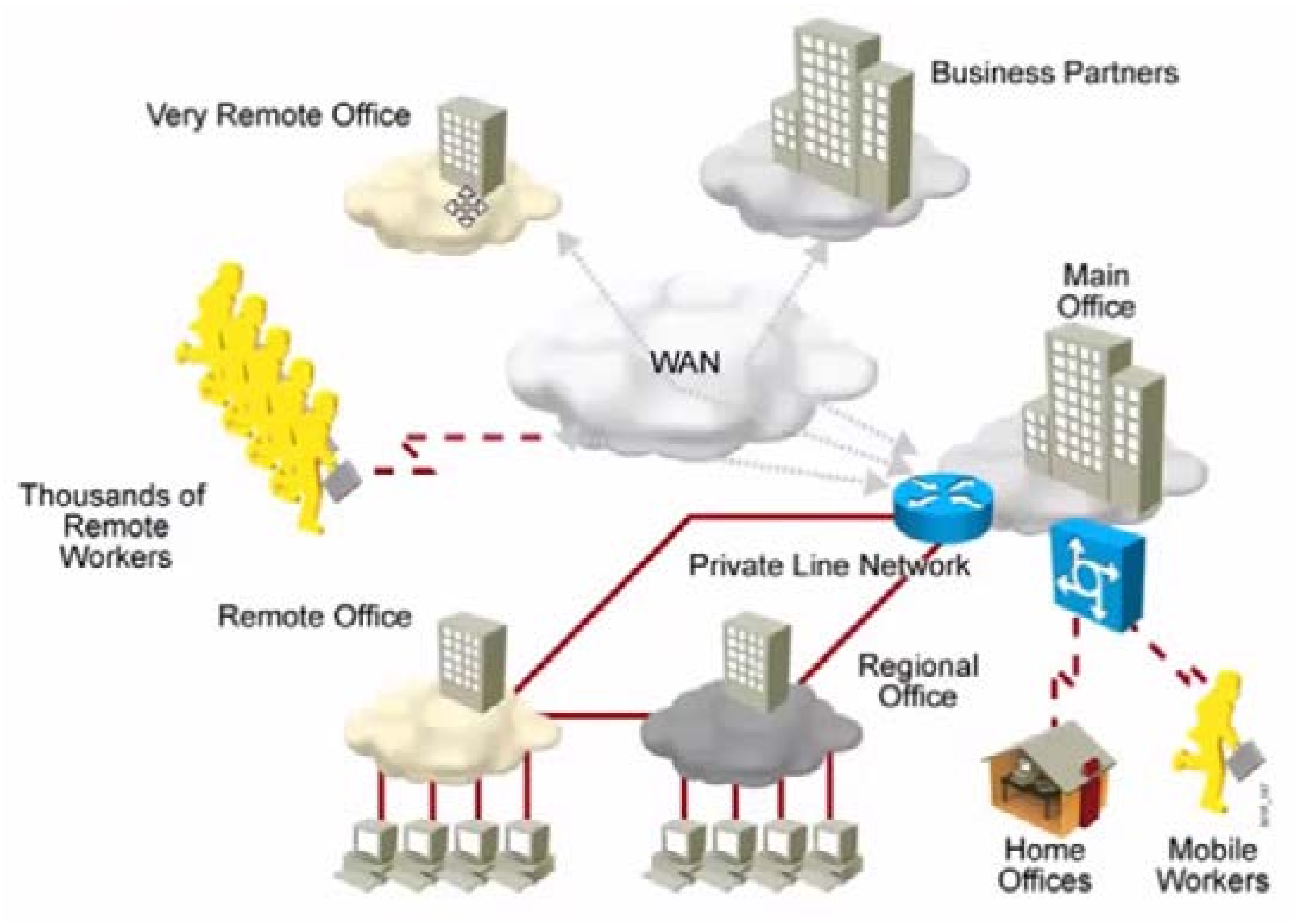


Figure 2: WAN

3. MAN :

It is a large computer network that usually spans a city or a large campus. A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet.

LAN +LAN +LAN + Fiber optics Cables

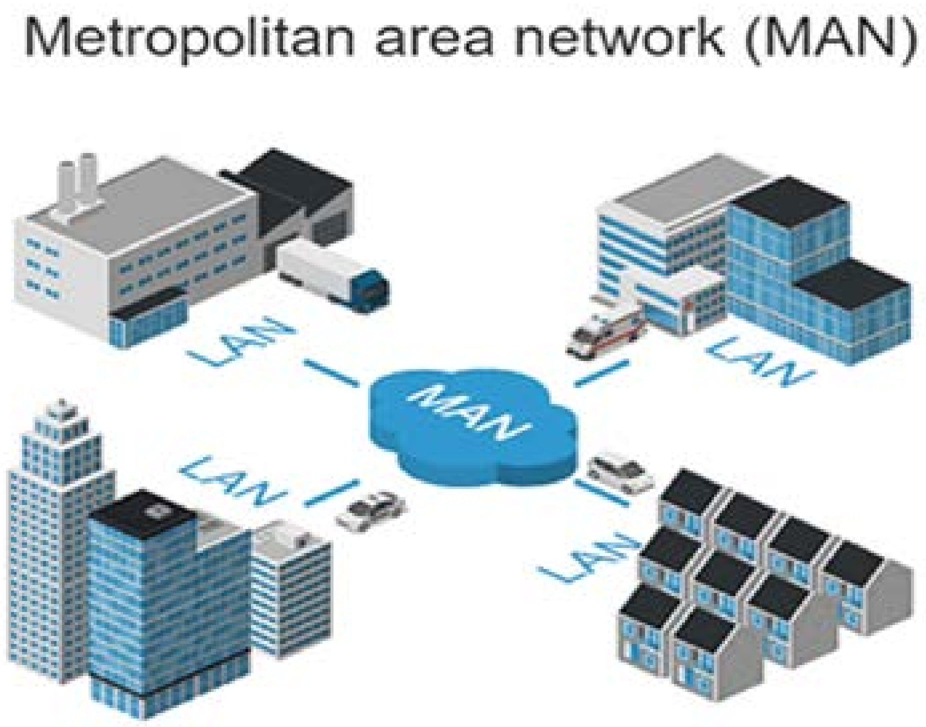


Figure 3: MAN

1-1-3 OSI layers

OSI stands for *Open Systems Interconnection.* It is a conceptual model that describes how data communication should take place between different systems or computers in a network. The OSI model is divided into seven layers, with each layer responsible for a specific function in the communication process

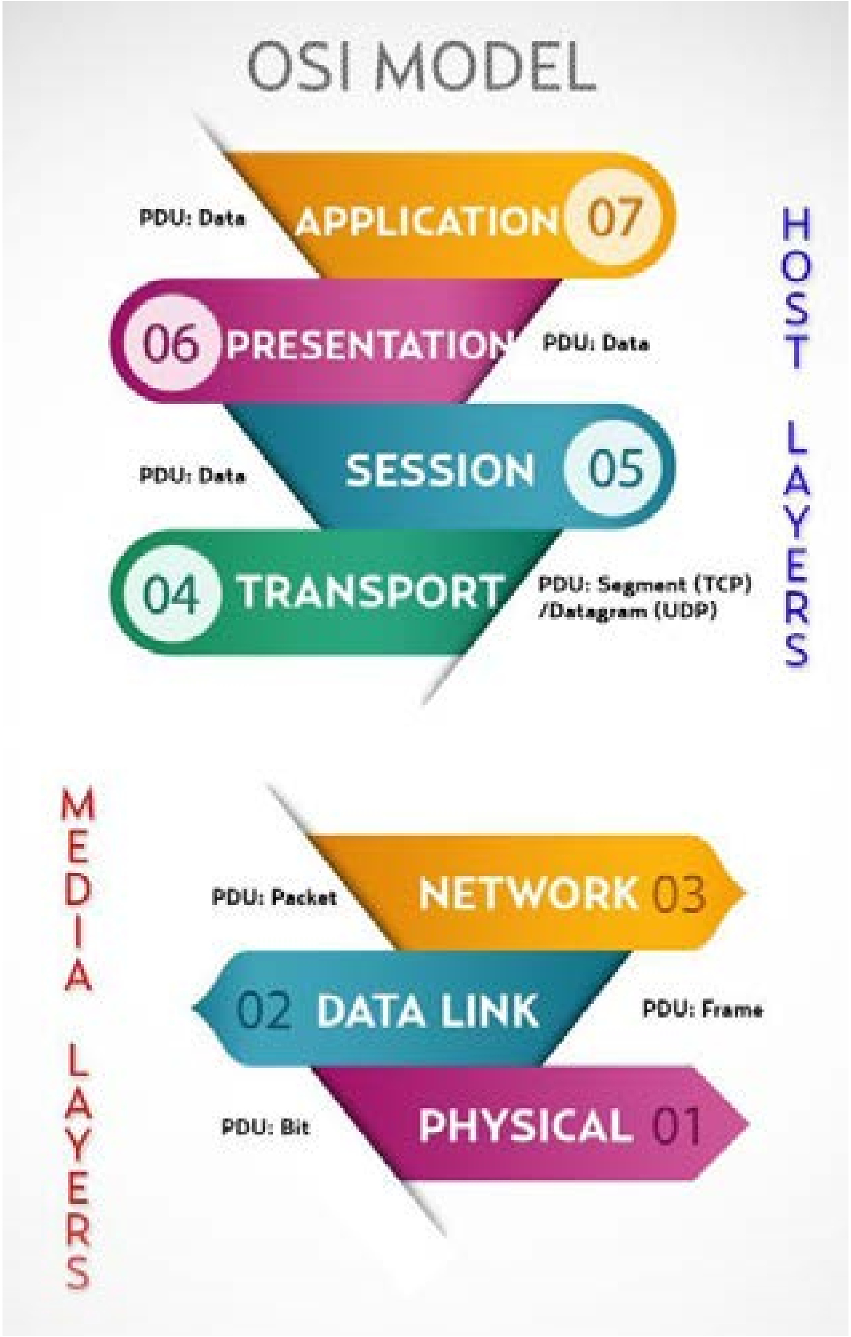


Figure 4: OSI

7. Applications layer

The application layer is the topmost layer in the Open System Interconnection (OSI) model. It provides various services and protocols that enable users and applications to access network resources and communicate with each other. Some examples of application layer protocols are HTTP, SMTP, FTP, Telnet, DNS and SNMP.

The application layer interacts with the presentation layer below it, which is responsible for translating data formats between different systems and ensuring data integrity. The presentation layer also handles encryption and decryption of data for security purposes. The application layer can request or receive data from the presentation layer using different methods, such as remote procedure calls (RPCs), sockets or message queues.

The application layer is also the interface between users and network applications. It displays incoming data to the user and receives user input. However, applications themselves do not reside at this layer; they use the services and protocols provided by this layer to communicate with other applications or systems. The application layer is independent of the underlying network architecture and can support different types of applications, such as web browsers, email clients, file transfer programs or network management tools.

The application layer performs several functions that are essential for any network communication process. These include:

- Identifying communication partners: The application layer helps users or applications find each other on a network using names or addresses. For example, DNS maps domain names to IP addresses.

- Establishing communication rules: The application layer defines how data should be exchanged between communication partners using protocols. For example, HTTP specifies how web servers and web browsers should interact.

- Synchronizing communication: The application layer ensures that both parties are ready to communicate and that data is sent and received in an orderly manner. For example, TCP provides reliable data delivery and flow control.

- Managing sessions: The application layer creates, maintains and terminates sessions between communication partners using session identifiers or cookies. For example, FTP uses a control connection and a data connection for file transfer sessions.

- Providing services: The application layer offers various services that facilitate network communication or provide additional functionality. For example, SMTP provides email delivery service; SNMP provides network monitoring service.

The application layer is a vital component of the OSI model as it enables users and applications to access network resources and communicate with each other across different platforms and systems.

6.Presentation layer

The presentation layer is the sixth layer in the OSI model. It is responsible for translating, formatting and encrypting data for transmission over the network. It also handles data compression and serialization to reduce bandwidth and ensure interoperability between different systems. The presentation layer acts as a bridge between the application layer and the session layer, converting data from user-dependent formats to common formats and vice versa. Some examples of protocols that operate at this layer are JPEG, GIF, MPEG, SSL and TLS.

The presentation layer performs several functions to ensure effective communication between applications on different nodes. Some of these functions are:

- Data translation: The presentation layer converts data from one format to another depending on the needs of the sender and receiver. For example, it can convert ASCII characters to EBCDIC characters or vice versa.

- Data encryption: The presentation layer can encrypt data to provide security and privacy for sensitive information. For example, it can use SSL or TLS protocols to encrypt data before sending it over the network.

- Data compression: The presentation layer can compress data to reduce the amount of bits that need to be transmitted over the network. For example, it can use JPEG or GIF protocols to compress images or MPEG protocol to compress videos.

- Data serialization: The presentation layer can serialize data structures or objects into a format that can be easily stored or transmitted over the network. For example, it can use XML or JSON protocols to serialize data into text strings.

The presentation layer is an important component of the OSI model as it enables applications on different systems to exchange data in a compatible and secure way. It also improves the efficiency and performance of data transmission by reducing its size and complexity.

5. Session layer

The session layer is the fifth layer of the OSI model. It is responsible for establishing, maintaining and terminating communication sessions between applications or devices. The session layer provides services such as authentication, authorization, synchronization, dialog control and data recovery. Some examples of protocols that operate at the session layer are RPC (Remote Procedure Call), SQL (Structured Query Language) and NFS (Network File System).

The session layer interacts with the transport layer below it and the presentation layer above it. The transport layer provides reliable or unreliable data transfer services to the session layer, while the presentation layer provides data formatting and encryption services to the session layer. The session layer can use different transport protocols depending on the requirements of the application or device. For example, a video conferencing application may use UDP (User Datagram Protocol) for real-time data transfer, while a file transfer application may use TCP (Transmission Control Protocol) for reliable data transfer.

The session layer can also create multiple sessions between applications or devices using different ports or sockets. A port is a logical endpoint that identifies a specific service or process on a device. A socket is a combination of an IP address and a port number that uniquely identifies a connection between two devices. The session layer can use different ports or sockets to multiplex or demultiplex data streams from different sources or destinations. For example, a web browser may use port 80 to communicate with a web server using HTTP (Hypertext Transfer Protocol), while using port 443 to communicate with another web server using HTTPS (Hypertext Transfer Protocol Secure).

4. Transport layer

The transport layer is the fourth layer of the OSI model. It is responsible for providing reliable and efficient communication between end systems or hosts. The transport layer performs several functions, such as:

- Segmenting and reassembling data: The transport layer divides the data received from the upper layers into smaller units called segments, and adds a header to each segment that contains information such as source and destination port numbers, sequence numbers, and checksums. The transport layer also reassembles the segments at the destination host and delivers them to the appropriate upper layer protocol.

- Flow control: The transport layer regulates the amount of data that can be sent by a sender or received by a receiver at any given time. This prevents network congestion and ensures that the receiver can handle the incoming data.

- Error control: The transport layer detects and corrects errors that may occur during data transmission. It uses mechanisms such as acknowledgements, timers, retransmissions, and checksums to ensure that data is delivered correctly and in order.

- Multiplexing and demultiplexing: The transport layer enables multiple applications to use the same network connection simultaneously. It assigns a unique identifier called a port number to each application or process on a host, and uses this port number to distinguish between different data streams. The transport layer also delivers data to the correct application or process based on the port number.

The two most common protocols used in the transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP provides reliable, connection-oriented, full-duplex communication with error detection and correction. UDP provides unreliable, connectionless, simplex communication with no error detection or correction.

3.Network layer

The network layer is one of the seven layers of the Open Systems Interconnection (OSI) model. It is responsible for the logical addressing and routing of data packets across different networks. The network layer provides services such as internetworking, error handling, congestion control and packet sequencing. The network layer also defines protocols that specify how devices on different networks can communicate with each other.

Some of the functions of the network layer are:

- Logical addressing: The network layer assigns a unique address to each device on a network, which is used to identify the source and destination of data packets. The most common logical addressing scheme is the Internet Protocol (IP) address.

- Routing: The network layer determines the best path for data packets to travel from one network to another, based on factors such as distance, cost and traffic. The network layer uses routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) to exchange routing information among routers.

- Internetworking: The network layer enables data communication between devices on different types of networks, such as local area networks (LANs), wide area networks (WANs) and wireless networks. The network layer uses protocols such as Internet Protocol (IP), Internet Control Message Protocol (ICMP) and Address Resolution Protocol (ARP) to facilitate internetworking.

- Error handling: The network layer detects and corrects errors that may occur during data transmission across networks. The network layer uses protocols such as Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP) to send error messages and feedback to other devices.

- Congestion control: The network layer monitors and regulates the flow of data packets across networks to avoid congestion and ensure optimal performance. The network layer uses protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Quality of Service (QoS) to implement congestion control mechanisms.

- Packet sequencing: The network layer ensures that data packets are delivered in the correct order at the destination device. The network layer uses protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Stream Control Transmission Protocol (SCTP) to assign sequence numbers to data packets and reorder them if necessary.

The network layer is an essential component of the OSI model that enables reliable and efficient data communication across heterogeneous networks.

2.Data Link layer

The data link layer is the second layer in the OSI model of computer networking. It is responsible for transferring data between adjacent network nodes in a wide area network (WAN) or between nodes on the same local area network (LAN) segment. The data link layer provides the functional and procedural means to establish and terminate a logical link between two nodes, to frame and unframe data packets for transmission and reception, to detect and correct errors that may occur in the physical layer, and to regulate the flow of data. The data link layer also defines the format of the media access control (MAC) address that uniquely identifies each node on a network.

The data link layer consists of two sublayers: the logical link control (LLC) sublayer and the media access control (MAC) sublayer. The LLC sublayer provides services such as multiplexing, flow control, error control, and acknowledgment to higher layers. It also handles protocol encapsulation and decapsulation, which involves adding or removing headers and trailers to or from data packets. The MAC sublayer deals with accessing the shared medium, such as Ethernet or Wi-Fi. It determines when a node can send or receive data on the medium, how to avoid or resolve collisions among multiple nodes competing for the medium, how to address and identify nodes on the medium, and how to handle broadcast and multicast transmissions.

1. Physical layer

The physical layer is the lowest layer in the OSI model. It is responsible for transmitting and receiving raw bits over a physical medium such as a cable or a wireless channel. The physical layer defines the characteristics of the medium, such as voltage levels, modulation schemes, bit rates, and connectors. The physical layer also handles error detection and correction, synchronization, and multiplexing of multiple signals on the same medium. The physical layer does not interpret the meaning or content of the bits; it only ensures that they are delivered reliably from one device to another.

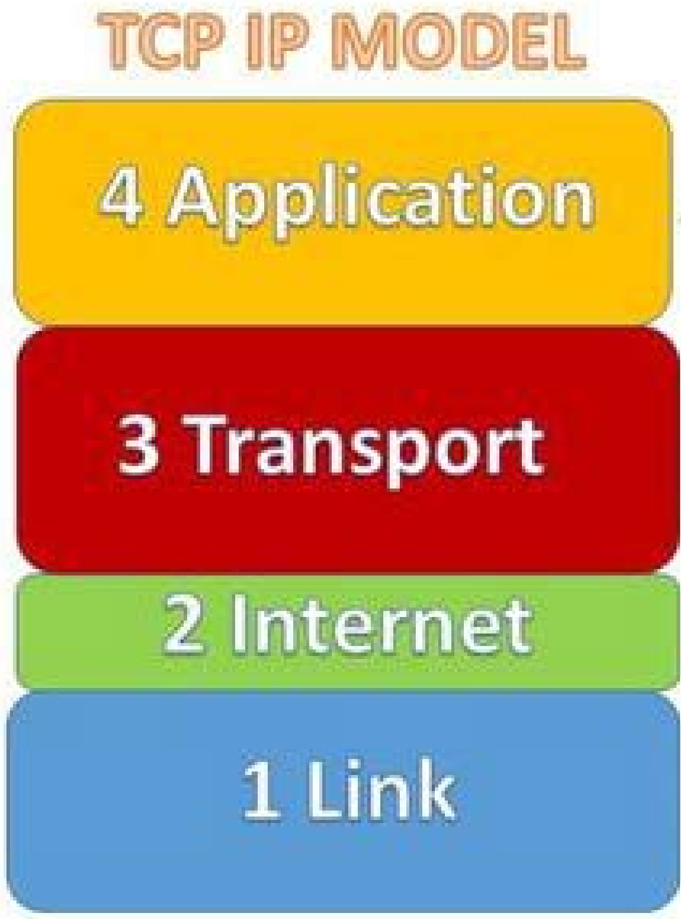


Figure 5: TCP/IP

1-2 LAN Basics

1-2-1 TCP/IP

TCP/IP is a suite of communication protocols that enables data transmission over the internet and other networks. TCP/IP stands for *Transmission Control Protocol/ Internet Protocol,* which are the two main protocols in the suite. TCP/IP is also known as the internet protocol stack because it consists of four layers: application, transport, internet and network interface.

4.The application layer

It provides services for different types of applications, such as web browsing, email and file transfer. The application layer uses protocols such as HTTP, SMTP and FTP to communicate with other applications.

3.The transport layer

It ensures reliable and ordered delivery of data packets between devices. The transport layer uses protocols such as TCP and UDP to segment and reassemble data, assign port numbers and perform error detection and correction.

2.The internet layer

It handles the routing and addressing of data packets across networks. The internet layer uses protocols such as IP, ICMP and ARP to assign IP addresses, determine the best path for each packet and handle network errors.

1.The network interface layer

It connects the device to the physical medium, such as Ethernet cable or wireless signal. The network interface layer uses protocols such as Ethernet, Wi-Fi and PPP to encode and decode data into bits and frames.

TCP/IP is widely used for communication over the internet because it is flexible, scalable and interoperable. TCP/IP can adapt to different network architectures, support a large number of devices and applications and work with different hardware and software vendors.

1-2-2 LAN setup

To set up a local area network (LAN), you will need some basic equipment and components. The main equipment you will need are:

A router: This is a device that connects multiple devices to a network and allows them to communicate with each other and the internet. A router can be wired or wireless, depending on your preference and needs. A wired router requires ethernet cables to connect the devices, while a wireless router uses radio waves to transmit data. Some routers have both wired and wireless capabilities.

A switch: This is a device that expands the number of ports on a router, allowing you to connect more devices to the network. A switch can be useful if you have a large number of devices or if your router does not have enough ports. A switch can also improve the performance and security of your network by reducing congestion and isolating traffic.

A network interface card (NIC): This is a hardware component that enables a device to connect to a network. A NIC can be built-in or external, depending on the device. For example, most computers and laptops have a built-in NIC, while some printers and scanners may require an external NIC. A NIC can also be wired or wireless, depending on the type of network you are using.

Ethernet cables: These are cables that connect devices to a router or a switch using RJ-45 connectors. Ethernet cables come in different categories and len`gths, depending on the speed and distance of data transmission. For example, Cat 5e cables can support up to 1 Gbps of data transfer over 100 meters, while Cat 6 cables can support up to 10 Gbps over 55 meters.

Wireless access points (WAPs): These are devices that extend the wireless coverage of a router by creating additional hotspots. WAPs can be useful if you have a large area to cover or if you have dead zones where the wireless signal is weak or nonexistent. WAPs can be connected to a router or a switch using ethernet cables or wireless bridges.

These are the essential equipment you will need to set up a LAN. Depending on your specific needs and preferences, you may also need other equipment such as firewalls, modems, servers, printers, scanners, etc.

1-2-3 Virtual LAN

A virtual LAN (VLAN) is a way of creating multiple logical networks on top of a single physical network. A VLAN allows devices to communicate with each other as if they were on the same LAN, even if they are physically separated by switches or routers. VLANs can improve network performance, security, and administration by reducing broadcast traffic, isolating sensitive or critical devices, and grouping devices according to their function or location.

To create a VLAN, network administrators assign a unique identifier (a VLAN ID) to each group of devices that belong to the same logical network. The VLAN ID is

added to the Ethernet frames of the devices as a tag. The tag tells the switches and routers how to handle the frames and which devices can receive them. Only devices that have the same VLAN ID can communicate with each other within a VLAN.

There are different types of VLANs depending on how they are configured and what they are used for. Some common types are:

- Static VLAN: A VLAN that is manually assigned to a switch port by the administrator. The port belongs to that VLAN regardless of which device is connected to it.

- Dynamic VLAN: A VLAN that is automatically assigned to a device based on its MAC address, IP address, username, or other criteria. The device can belong to different VLANs depending on where it is connected or who is using it.

- Native VLAN: A default VLAN that is assigned to untagged frames (frames without a VLAN ID). The native VLAN is usually VLAN 1, but it can be changed by the administrator.

- Management VLAN: A special VLAN that is used for remote access and configuration of network devices. The management VLAN should be separate from other VLANs for security reasons.

- Voice VLAN: A dedicated VLAN that is used for voice over IP (VoIP) traffic. The voice VLAN can have higher priority and quality of service (QoS) than other VLANs to ensure clear and uninterrupted voice communication.

Chapter -2

Fundamental Components

Fundamental Components of networking structures

The fundamental components of networking structure are the devices, media, and protocols that enable communication and data transfer among different nodes in a network. Devices are the hardware components that send, receive, process, or store data, such as computers, routers, switches, and firewalls. Media are the physical or wireless means that connect the devices and carry the data signals, such as cables, fibers, or radio waves.

The components are divided into two sections

1. *Superstructure*
    - ◊ *PCs &Laptops*
    - ◊ *Mobile phones*
    - ◊ *Smart board*
    - ◊ *RFID gates*
    - ◊ *Ip phones*
    - ◊ *other devices*
2. *Infrastructure*

- *passive*
    - ◊ *Cables*
    - ◊ *Racks*
    - ◊ *UPS*
    - ◊ *Rackmount monitor*
    - ◊ *ACs*
- *active*
    - ◊ *Routers*
    - ◊ *Switches*
    - ◊ *Servers*
    - ◊ *Firewalls*
    - ◊ *Access points*

2-1 Superstructure

2-1-1 PCs & Laptops

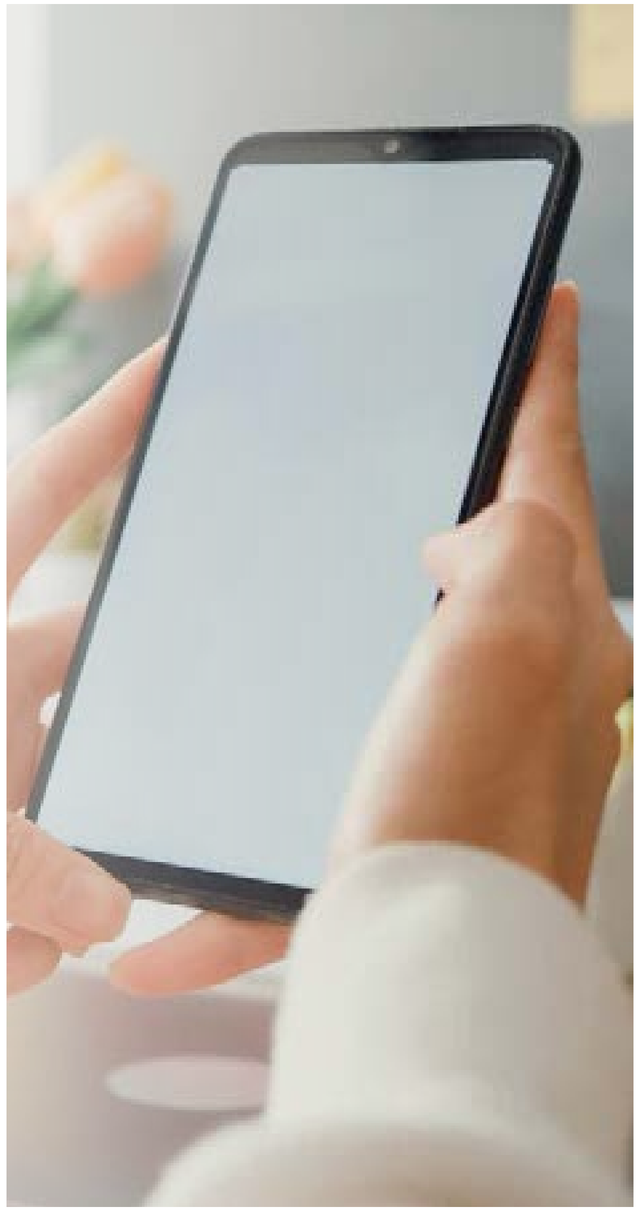
They are common devices in a networking structure. They can be connected to each other and to other network components such as routers, switches, servers, printers, etc. through wired or wireless connections.

They can communicate with each other and access shared resources on the network using protocols such as TCP/IP, HTTP, FTP, etc.

PCs and laptops can also have different roles on the network, such as clients, hosts, or peers. Clients are devices that request services from servers, which are devices that provide services to clients. Hosts are devices that have an IP address and can send and receive data on the network. Peers are devices that can act as both clients and servers on the network.

2-1-2 Mobile phones

Mobile phones are devices that can communicate wirelessly with other phones or networks using radio waves. They are part of a larger networking structure that includes cellular towers, base stations, switches, routers, and servers. Mobile phones can access various services and applications through the network, such as voice calls, text messages, internet browsing, social media, and video streaming. Mobile phones can also connect to other devices or networks using technologies such as Bluetooth, Wi-Fi, or NFC. Mobile phones have become an essential tool for personal and professional communication in the modern world.



2-1-3 smart board

A smart board is a type of interactive flat panel display (IFPD) that allows users to collaborate and share ideas on a large touchscreen monitor. A smart board can connect to a network supestructure, which is a system of interconnected networks that enables communication and data exchange among different devices and applications. A network supestructure can be composed of various types of networks, such as Ethernet, Wi-Fi, Bluetooth, cellular, or cloud-based networks.

By connecting a smart board to a network supestructure, users can benefit from several features and advantages. For example, they can access and use their favorite apps on the smart board, such as web browsers, video conferencing tools, or online whiteboards. They can also share their screen and annotations with other participants who are using different devices or locations. Moreover, they can save and sync their work on the cloud, and access it anytime and anywhere.

2-1-4 RFID Gates

RFID gates are devices that use radio frequency identification (RFID) technology to automatically identify and track items or load carriers passing through them. RFID gates can be used in various applications, such as logistics, inventory management, security, and access control. In a university network, RFID gates can be deployed to monitor the attendance of students and staff, to control the access to restricted areas, and to manage the circulation of books and equipment. RFID gates consist of RFID readers and antennas that communicate with RFID tags attached to the items or load carriers. The readers and antennas need to be optimally designed and configured to ensure a high coverage rate, a low interference rate, and a balanced load distribution. Several algorithms have been proposed in the literature to solve the RFID network planning problem, but most of them are not suitable for the design of RFID gates due to some limitations. Therefore, there is a need for a new RFID network planning algorithm that can support the design of RFID gates in a university network.

2-1-5 IP phones

IP phones are devices that use the Internet Protocol (IP) to transmit voice and data over a network. IP phones can be integrated into a network superstructure, which is the overall design and architecture of a network that includes its components, protocols, standards, and services. A network superstructure can provide various benefits for IP phones, such as scalability, security, reliability, and interoperability. Some examples of network superstructure components that support IP phones are:

- IP PBX: A private branch exchange (PBX) that uses IP to connect and manage IP phones and other endpoints within a network.

- SIP: A protocol that enables IP phones to establish, modify, and terminate multimedia sessions over a network.

- VoIP: A technology that converts voice signals into digital packets and transmits them over a network using IP.

- QoS: A mechanism that prioritizes and allocates network resources for different types of traffic, such as voice and data, to ensure optimal performance and quality for IP phones.

2-1-6 Other devices

There are other peripheral devices that can connect via the network by wired or wireless connection and connect to th system to be used easily or control it like

1. Cameras
2. Speakers
3. Printers
4. Scanners
5. POS machine

2-2 Infrastructure

Network infrastructure is the set of hardware and software components that enable the transmission and exchange of data across different devices and systems. It includes routers, switches, firewalls, servers, cables, wireless access points, and other network devices that facilitate communication and data processing. Network infrastructure is essential for providing reliable, secure, and efficient network services to users and applications. A well-designed network infrastructure can improve performance, scalability, availability, and security of the network .And it branches off to two categories ,passive and active.

2-2-1 Passive

Cables

Cables are essential components of network infrastructure, as they provide the physical medium for data transmission between computers and devices. There are different types of network cables, each with its own specifications and advantages. In this paragraph, we will briefly introduce three common types of network cables: coaxial, twisted-pair, and fiber-optic.

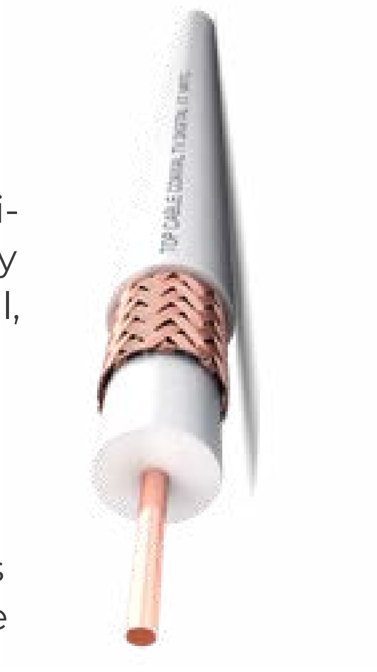


Figure 6:Coaxial cable

Coaxial cable consists of a central copper wire surrounded by insulation and a metallic shield. It was widely used for 10 Mbps Ethernet networks in the past, but it has been largely replaced by twisted-pair cable due to its stiffness and interference issues. Coaxial cable can still be found in some cable TV and radio systems.

Twisted-pair cable is composed of up to eight wires twisted together in pairs to reduce electromagnetic interference. It is the most popular type of network cable for Ethernet networks, ranging from 10 Mbps to 10 Gbps. Twisted-pair cable can be either unshielded (UTP) or shielded (STP), depending on whether it has an additional layer of protection against noise and crosstalk. UTP cable is cheaper and easier to install than STP cable, but it is more susceptible to external interference.

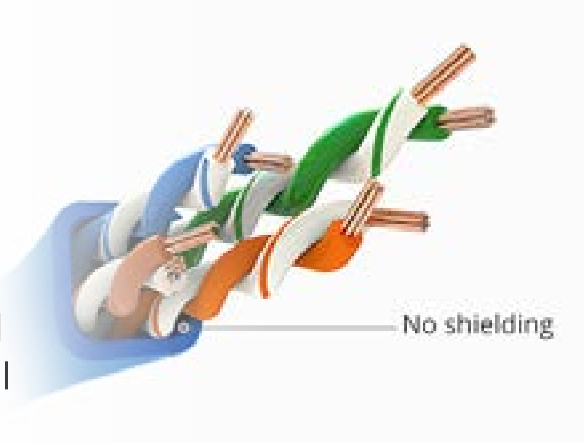


Figure 7:Twisted cable

Fiber-optic cable uses strands of glass or plastic to transmit data as pulses of light. It has several advantages over copper-based cables, such as higher bandwidth, longer distance, lower attenuation, and immunity to electromagnetic interference. Fiber-optic cable is widely used for long-distance and high-speed network applications, such as WANs and FDDI. Fiber-optic cable can be either single-mode or multimode, depending on the diameter and number of light paths in the fiber.

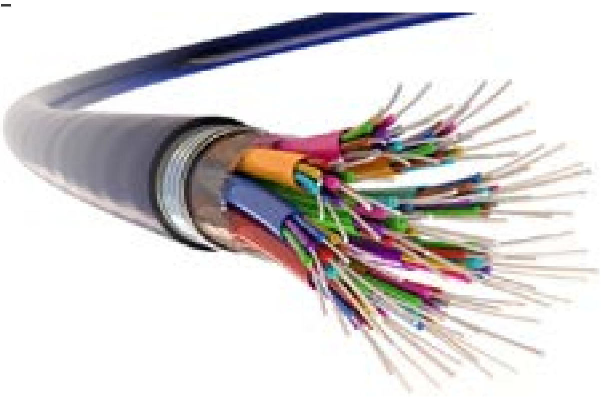


Figure 8: Fiber-optic cable

Racks

Racks are supporting frameworks that hold hardware modules, such as servers, switches, routers, and patch panels. They are commonly used in data centers or on-premise networking closets to organize IT equipment into standardized assemblies that make efficient use of space and other resources . There are different types of racks, such as open frame racks, rack enclosures, and wall-mount racks, each with its own advantages and disadvantages depending on the application and environment .

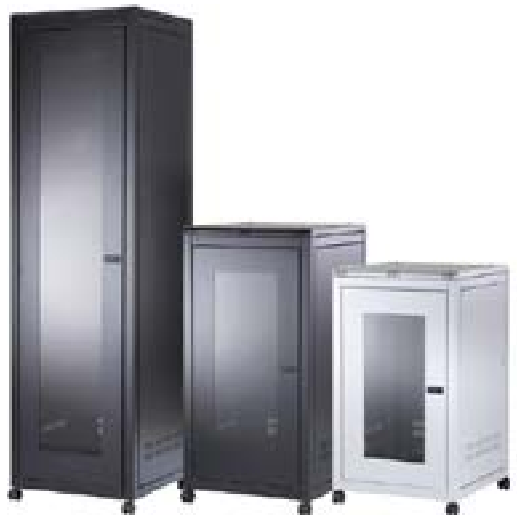


Figure 9: Racks

UPS

One of the challenges that network administrators face is ensuring the availability and reliability of the network infrastructure. A network outage can have serious consequences for the productivity and performance of an organization. Therefore, it is essential to implement backup power solutions, such as uninterruptible power supplies (UPS), to protect the network devices from power failures. UPS devices can provide continuous power to the network equipment in case of a power outage, and also regulate the voltage and frequency of the power supply to prevent damage from power surges or fluctuations. UPS devices can be classified into three types: offline, line-interactive, and online. Each type has its own advantages and disadvantages, depending on the level of protection and cost required. A network administrator should carefully evaluate the needs and budget of the organization before choosing the appropriate UPS solution for the network infrastructure.

Figure 10: UPs

Rackmount monitor

A rackmount monitor is a device that can be mounted on a standard 19-inch server rack and provides a graphical interface for managing the network infrastructure. Rackmount monitors are useful for monitoring the availability, performance, and resource utilization of hosts, containers, and other backend components in a data center or a remote location. Rackmount monitors can also save space and power consumption compared to standalone monitors.

Figure 11: Rackmount monitor

ACs

Air conditioning systems are essential components of network infrastructure, as they provide cooling and humidity control for the servers and equipment that run the network. Air conditioning systems can also improve the reliability and performance of the network by preventing overheating, dust accumulation, and corrosion. However, air conditioning systems also consume a significant amount of energy and require regular maintenance and monitoring. Therefore, network operators should optimize their air conditioning systems to achieve the best balance between cost and quality.

2-2-2 Active

switch

A switch is a device that connects multiple devices on a network and allows them to communicate with each other. Switches can operate at different layers of the network model, such as the data link layer or the network layer. Switches can also have different functions, such as learning the MAC addresses of the con nected devices, forwarding packets based on their destination IP addresses, or performing quality of service (QoS) operations.

Figure 12: Switch

Switches are an essential component of network infrastructure, as they enable scalability, efficiency, and security of the network. Switches can reduce the amount of broadcast traffic and collisions on the network by creating separate collision domains for each port. Switches can also create virtual LANs (VLANs) to logically separate devices on the same physical network based on their function, location, or security level. Switches can also implement access control lists (ACLs) to filter traffic based on various criteria, such as source and destination addresses, protocols, or ports.

Switches can be classified into two main types: unmanaged and managed. Unmanaged switches are simple plug-and-play devices that do not require any configuration or monitoring. They are suitable for small networks or home networks where performance and security are not critical. Managed switches are more advanced devices that offer more features and control over the network. They can be configured and monitored remotely using various protocols, such as SNMP, Telnet, SSH, or HTTP. They can also support advanced functions, such as spanning tree protocol (STP), link aggregation (LAG), port mirroring, or power over Ethernet (PoE).

Switches are an important part of network infrastructure that provide connectivity and functionality to the network devices. They can improve the performance and security of the network by reducing congestion and implementing policies. Switches can also adapt to the changing needs and demands of the network by offering flexibility and scalability.

Routers

A router is a device that connects multiple networks and forwards data packets between them. A router can perform various functions, such as routing protocols, network address translation, firewall, quality of service, and load balancing. In network infrastructure, routers play a vital role in ensuring the efficient and secure transmission of data across different networks.

Figure 13: Router

Routers operate at the network layer of the OSI model, which means they can analyze the header of each data packet and determine its destination based on the IP address. Routers can also use routing tables and algorithms to find the best path for each packet, taking into account factors such as bandwidth, congestion, and cost. Routers can also update their routing tables dynamically by exchanging information with other routers using routing protocols, such as RIP, OSPF, EIGRP, and BGP.

Routers can be classified into different types based on their functions and locations in the network infrastructure. For example, edge routers are located at the boundary of a network and connect it to other networks, such as the Internet. Core routers are located in the backbone of a network and handle high-speed data traffic between different subnets. Distribution routers are located between the core and the edge routers and aggregate traffic from multiple access routers. Access routers are located at the end-user premises and provide connectivity to local devices, such as computers and printers.

Servers

A server in network infrastructure is a high-powered computer that serves as a central repository for data and various programs shared by users within a network. A server can perform different functions depending on its type and configuration. For example, a file server stores critical business information that can be accessed by authorized clients, a web server hosts programs and data requested by users over the internet, and a virtual server allows multiple users to share the same physical resources while having full control over their own virtual machines.

Figure 14: Server

Servers are essential components of network infrastructure because they enable network connectivity and communication between users, devices, apps, the internet, and more. Servers also provide centralized management, security, backup, fault tolerance, and scalability for network resources. To ensure optimal performance and availability of servers, network administrators need to monitor various metrics such as CPU utilization, memory usage, disk space, network traffic, uptime, and response time. Server monitoring tools can help administrators collect, analyze, and visualize these metrics and alert them to any issues or anomalies that may affect the server's functionality or reliability.

Firewall

A firewall is a network security solution that protects your network from unwanted traffic. Firewalls block incoming malware based on a set of pre-programmed rules. These rules can also prevent users within the network from accessing certain sites and programs.

Figure 15: Firewall

Firewalls are based on the simple idea that network traffic from less secure environments should be authenticated and inspected before moving to a more secure environment. This prevents unauthorized users, devices, and applications from entering a protected network environment or segment.

Firewalls are essential for creating a proper cybersecurity system, as they offer essential monitoring and filtering of all traffic, including outgoing traffic, application-layer traffic, online transactions, communications and connectivity, and dynamic workflows.

There are different types of firewalls, such as proxy firewalls, stateful inspection firewalls, unified threat management (UTM) firewalls, next-generation firewalls (NGFW), and threat-focused NGFW. Each type of firewall has its own advantages and disadvantages, and can be deployed in different areas of the network infrastructure.

Firewalls have evolved over time in response to the growing variety and complexity of cyber threats. Firewalls are still considered to be the first line of defense against cyberattacks, but they need to be complemented by other security solutions and proper firewall configuration to provide maximum protection. 2-2-5 Firewall

Access point

An access point in network infrastructure is a device that allows wireless-capable devices to connect to a wired network. It is a common component of wireless network infrastructure, as it provides wireless network connectivity for users and devices. An access point can be configured in different ways, depending on the network requirements and design. For example, an access point can act as a root access point, a repeater access point, a bridge, a workgroup bridge, or a central unit in an all-wireless network. An access point can also support different wireless standards, such as Wi-Fi 6, which offers faster speeds and lower latency than previous generations. An access point can be managed either on-premises or through the cloud, depending on the level of security and customization needed. An access point is an essential device for enabling network communication and collaboration in any environment.

Figure 16: Access point

Chapter -3

Software Application

Software Application

The design of a network structure requires the use of various programs that can help with the planning, implementation and maintenance of the network. Some of the programs used in network design are:

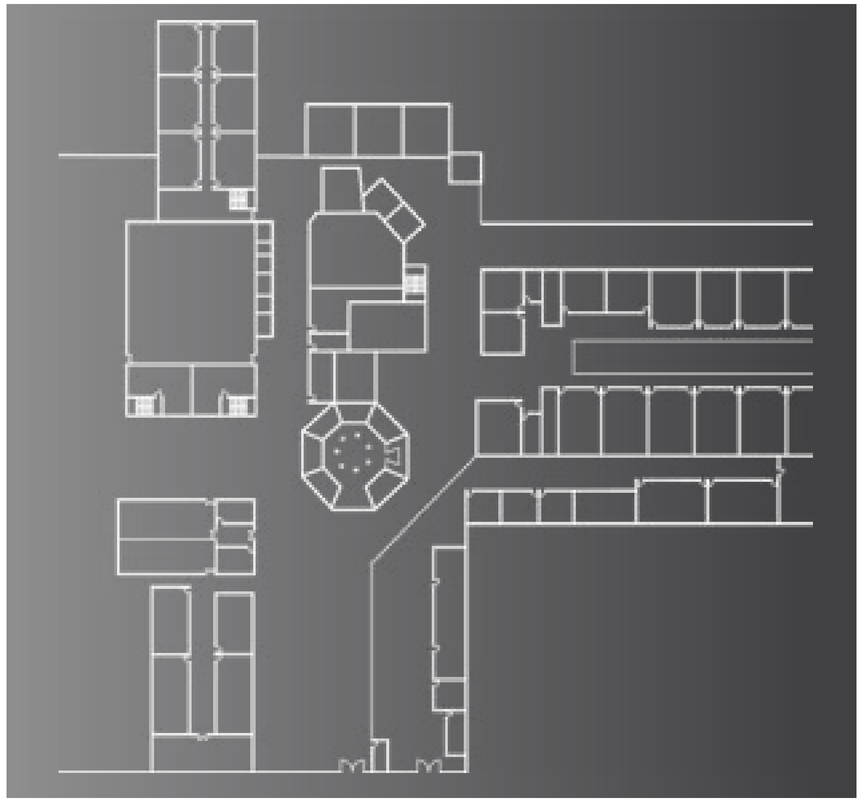
-Network simulation tools: These are programs that can model the behavior and performance of a network under different scenarios and conditions. They can help with testing the feasibility, reliability and efficiency of a network design before deploying it in the real world. Examples of network simulation tools are EVE , VM-Ware and Cisco Packet Tracer.

- Diagramming tools: These are programs that can create graphical representations of a network structure, showing the components, connections and configurations of the network. They can help with visualizing the network design and communicating it to others. Examples of diagramming tools are Auto Cad

3-1 Diagram Programes

3-1-1 Autocad

Autocad is a software application that allows users to create and edit 2D and 3D drawings and models. It is widely used in various fields of engineering, architecture, and design. One of the applications of Autocad is in designing networking infrastructure, such as routers, switches, cables, and servers layouts. Autocad can help network engineers to plan, design, and optimize the layout and performance of their networks. Autocad can also generate documentation and reports for the network infrastructure, such as wiring diagrams, network maps, and inventory lists. Autocad can also integrate with other software tools and platforms, such as simulation software, cloud services, and network management systems. Autocad can help network engineers to create and maintain efficient, reliable, and secure networking infrastructure for various purposes and environments



3-2 Simulation Tools

3-2-1 Packet Tracer

Packet Tracer is a powerful network simulation tool that allows users to practice networking, IoT, and cybersecurity skills in a virtual lab environment. Packet Tracer can be used to design networking infrastructure for various scenarios, such as small office networks, IoT smart home networks, or enterprise networks. Packet Tracer provides a graphical user interface that enables users to drag and drop network devices, connect them with different types of cables, and configure their settings and parameters. Packet Tracer also allows users to monitor and troubleshoot network performance and behavior using various tools and commands. Packet Tracer can be downloaded for free by enrolling in one of the self-paced courses offered by Cisco Networking Academy.

3-2-2 VMWare workstation

VMware is a leading provider of virtual networking solutions that enable organizations to design and deploy flexible, scalable, and secure networks across private, hybrid, and public clouds. VMware's virtual networking products include VMware NSX, VMware Cloud Networking, VMware NSX Advanced Load Balancer, and VMware Container Networking. These products offer various benefits such as:

- Automating network provisioning and operations with a cloud operating model

- Delivering consistent networking and security policies across different cloud environments

- Achieving high performance and availability for applications with advanced load balancing and threat prevention

- Simplifying container networking and policy management with a unified stack for multiple Kubernetes providers

- Supporting VLANs and other standard networking protocols for compatibility and interoperability

VMware's virtual networking solutions are based on the concept of virtual switches, which connect virtual machines to each other and to external networks. Virtual switches can be configured with different port groups, VLANs, security settings, and traffic shaping policies. Virtual machines can have one or more virtual Ethernet adapters, which are either paravirtualized (vmxnet) or emulated (e1000 or vlance). Paravirtualized adapters offer better performance and efficiency than emulated ones, but require VMware Tools to be installed in the guest operating system.

3-2-3 EVE Comm

Eve Comm is a software tool that allows users to design, simulate and test networking infrastructure in a virtual environment. Eve Comm supports various network devices, protocols and topologies, and enables users to create realistic scenarios for learning, testing and troubleshooting purposes. Eve Comm can be used for various applications, such as network security, cloud computing, routing and switching, voice and video, wireless and IoT. Eve Comm provides a user-friendly graphical interface, as well as a command-line interface for advanced users. Eve Comm can run on Windows, Linux and Mac OS platforms, and can be integrated with other software tools such as Wireshark, GNS3 and Packet Tracer. Eve Comm is a powerful and versatile tool for network engineers, students and enthusiasts who want to design and experiment with networking infrastructure in a cost-effective and flexible way.

Chapter -4

Designing of networking infrastructure

Software Application

The design of a network structure requires the use of various programs that can help with the planning, implementation and maintenance of the network. Some of the programs used in network design are:

-Network simulation tools: These are programs that can model the behavior and performance of a network under different scenarios and conditions. They can help with testing the feasibility, reliability and efficiency of a network design before deploying it in the real world. Examples of network simulation tools are NS2, NS3, OMNeT++, OPNET and Cisco Packet Tracer.

- Network diagramming tools: These are programs that can create graphical representations of a network structure, showing the components, connections and configurations of the network. They can help with visualizing the network design and communicating it to others. Examples of network diagramming tools are Microsoft Visio, Lucidchart, Draw.io and Dia.