University of Swat

Aspiring For Quality Education With Relevance

NETWORK MANAGEMENT

By:

M. Zeeshan Khan(Visiting Lecturer)

Department of Computer Science & Software Engineering,

University of Swat.

CHAPTER -1

INTRODUCTION TO NETWORKING

NETWORK

A network is defined as a group of two or more computer systems linked together. There are many types of computer networks, including the following:

- **local-area networks (LANs):** The computers are geographically close together (that is, in the same building).
- **wide-area networks (WANs):** The computers are farther apart and are connected by telephone lines or radio waves.
- **campus-area networks (CANs):** The computers are within a limited geographic area, such as a campus or military base.
- **metropolitan-area networks MANs):** A data network designed for a town or city.
- **home-area networks (HANs):** A network contained within a user's home that connects a person's digital devices.

LAN - local-area network

- A ***local-area network (LAN)*** is a computer network that spans a relatively small area. Most often, a LAN is confined to a single room, building or group of buildings, however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

WAN - Wide-area network

- A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

- Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

- A system of LANs connected in this way is called a wide-area network (WAN). The difference between a LAN and WAN is that the wide-area network spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs) and are often connected through public networks.

MAN - Metropolitan Area Network

- Short for ***M**etropolitan **A**rea **N**etwork*, a data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media

Network Characteristics

In addition to these types, the following characteristics are also used to categorize different types of networks:

- **topology** : The geometric arrangement of a computer system. Common topologies include a bus, star, and ring. See the Network topology diagrams in the Quick Reference section of Webopedia.
- **protocol** : The protocol defines a common set of rules and signals that computers on the network use to communicate. One of the most popular protocols for LANs is called *Ethernet*. Another popular LAN protocol for PCs is the *IBM token-ring network* .
- **architecture** : Networks can be broadly classified as using either a *peer-to-peer* or *client/server architecture*.

Computers on a network are sometimes called *nodes*. Computers and devices that allocate resources for a network are called *servers*.

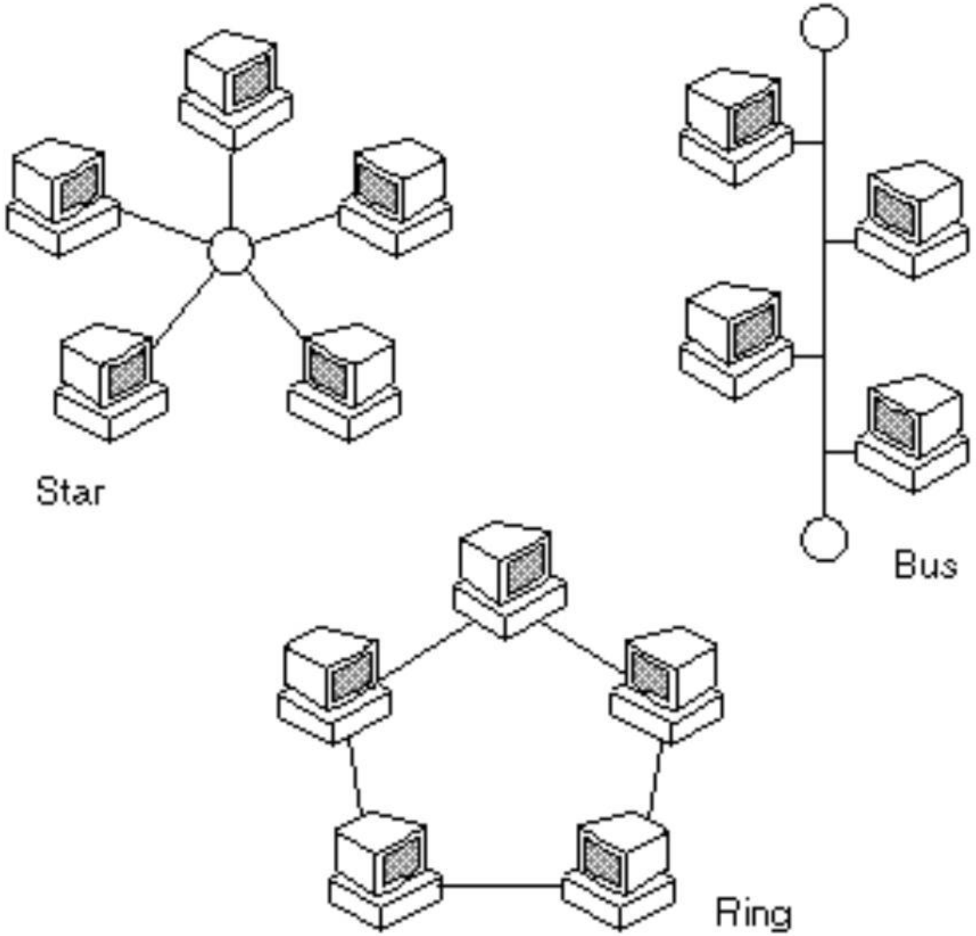


Image: Network Topology diagram

Networking Devices

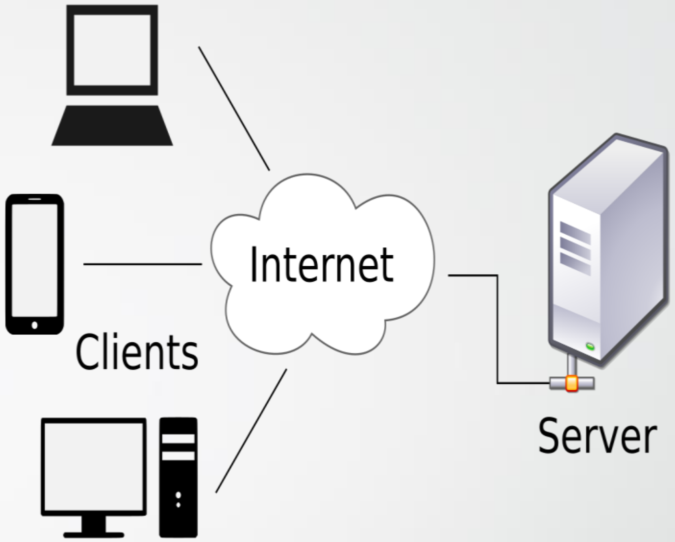
- Some of the basic hardware components that can be used in networks include:
- **Interface Cards:** These allow computers to communicate over the network with a low-level addressing system using media access control (MAC) addresses to distinguish one computer from another.
- **Repeaters:** These are electronic devices that amplify communication signals and also filter noise from interfering with the signals.
- **Hubs:** These contain multiple ports, allowing a packet of information/data to be copied unmodified and sent to all computers on the network.

Networking Devices

- **Bridges:** These connect network segments, which allows information to flow only to specific destinations
- **Switches:** These are devices that forward, make forwarding decisions and otherwise filter chunks of data communication between ports according to the MAC addresses in the packets of information.
- **Routers:** These are devices that forward packets between networks by processing the information in the packet.
- **Firewalls:** These reject network access requests from unsafe sources, but allow requests for safe ones.

Server vs Client Computer

- A **server** is a software or hardware device that accepts and responds to requests made over a network. The device that makes the request, and receives a response from the server, is called a client. On the Internet, the term "server" commonly refers to the computer system which receives a request for a web document, and sends the requested information to the client.



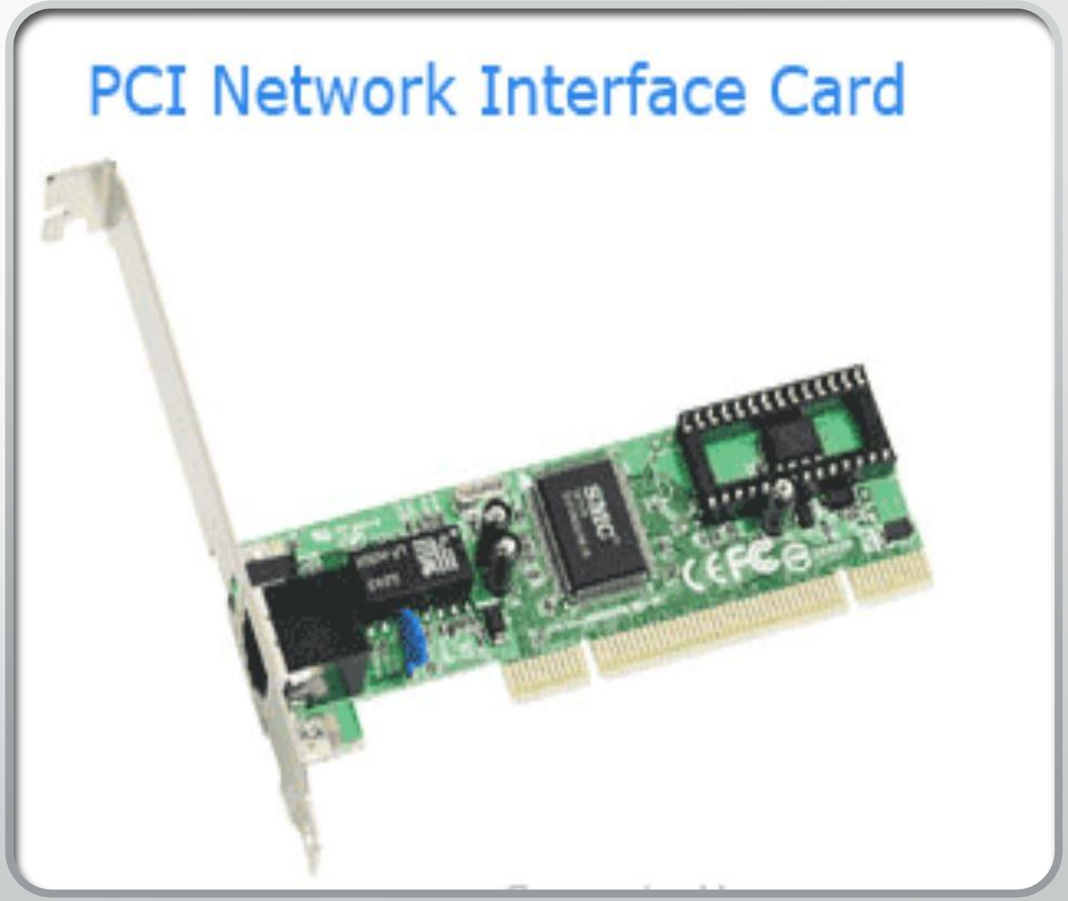
Examples of Servers

The following list contains links to various server types.

- Application server
- Blade server
- Cloud server
- Database server
- Dedicated server
- Domain name service
- File server
- Mail server
- Print server
- Proxy server
- Standalone server
- Web server

NIC

- Short for **network interface card**, the **NIC** is also referred to as an **Ethernet card** and **network adapter**. A NIC is a computer expansion card for connecting to a network (e.g., home network or Internet) using an Ethernet cable with an RJ-45 connector.



Switch

- A switch, in the context of networking is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN). A LAN switch operates at the data link layer (Layer 2) or the network layer of the OSI Model and, as such it can support all types of packet protocols.

- A switch in an Ethernet-based LAN reads incoming TCP/IP data packets/frames containing destination information as they pass into one or more input ports. The destination information in the packets is used to determine which output ports will be used to send the data on to its intended destination.

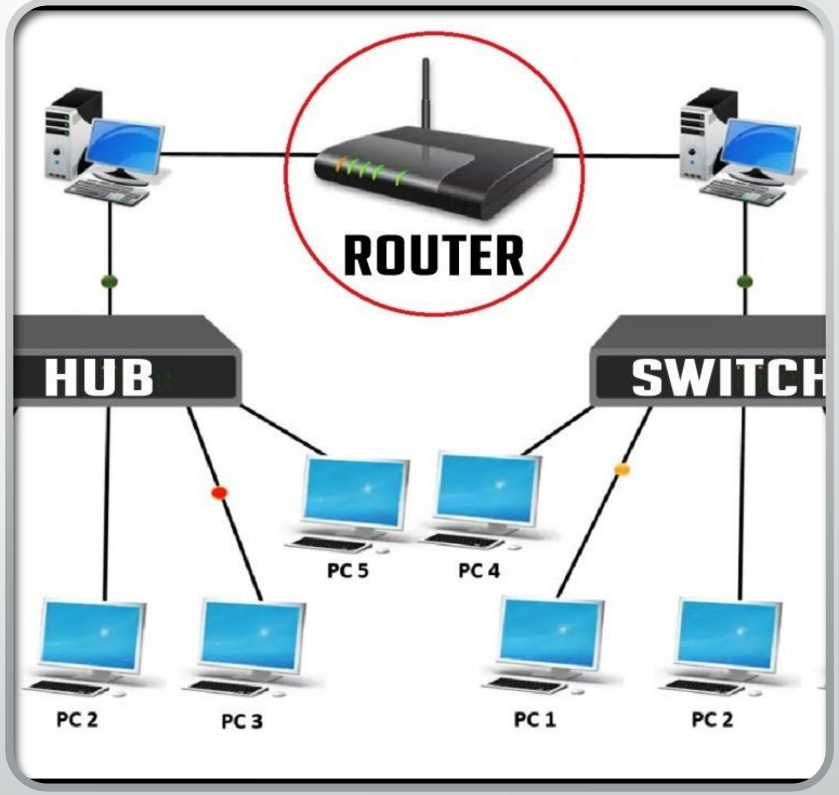
HUB

- A hub, in the context of networking, is a hardware device that relays communication data. A hub sends data packets (frames) to all devices on a network, regardless of any MAC addresses contained in the data packet.
- A switch is different than a hub in that it keeps a record of all MAC addresses of all connected devices. Thus, it knows which device or system is connected to which port. When a data packet is received, the switch immediately knows which port to send it to

Router

- A router is a device that analyzes the contents of data packets transmitted within a network or to another network. Routers determine whether the source and destination are on the same network or whether data must be transferred from one network type to another, which requires encapsulating the data packet with routing protocol header information for the new network type.

- Large routers determine interconnectivity within an enterprise, between enterprises and the Internet, and between different internet service providers (ISPs); small routers determine interconnectivity for office or home networks. ISPs and major enterprises exchange routing information using border gateway protocol (BGP).



Fire-Wall

- A **firewall** is a software utility or hardware device that acts as a filter for data entering or leaving a network or computer. You could think of a firewall as a security guard that decides who enters or exits a building. A firewall works by blocking or restricting network ports. Firewalls are commonly used to help prevent unauthorized access to both company and home networks.

Repeater

A **repeater** is an object that increases a signal's strength, so it can be transmitted and received over a greater distance without a loss in quality. These devices are commonly used with networks to help the lines running between network devices reach farther destinations.

CHAPTER -2

NETWORK MANAGEMENT

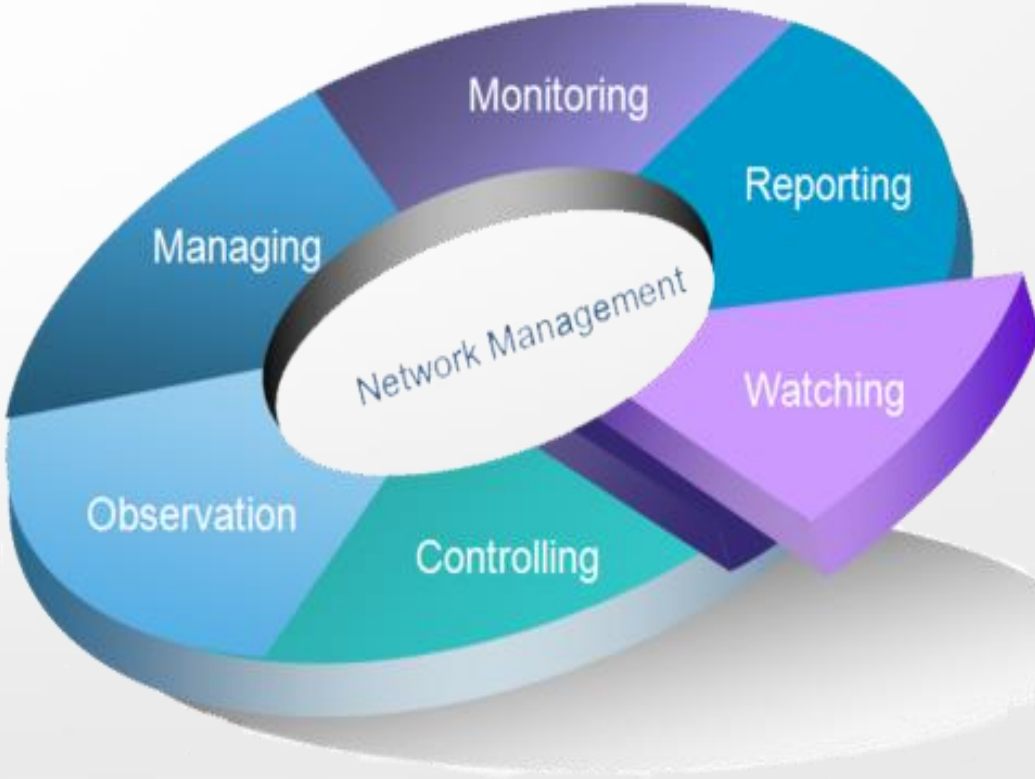
NETWORK MANAGEMENT

Network management refers to the broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:

- **Security:** Ensuring that the network is protected from unauthorized users.
- **Performance:** Eliminating bottlenecks in the network.
- **Reliability:** Making sure the network is available to users and responding to hardware and software malfunctions.

What Is Network Management?

- Network management refers to the processes, tools and applications used to administer, operate and maintain a network infrastructure. Performance management and fault analysis are also included in network management. To put it simply, network management is the process of keeping your network healthy, which keeps your business healthy.

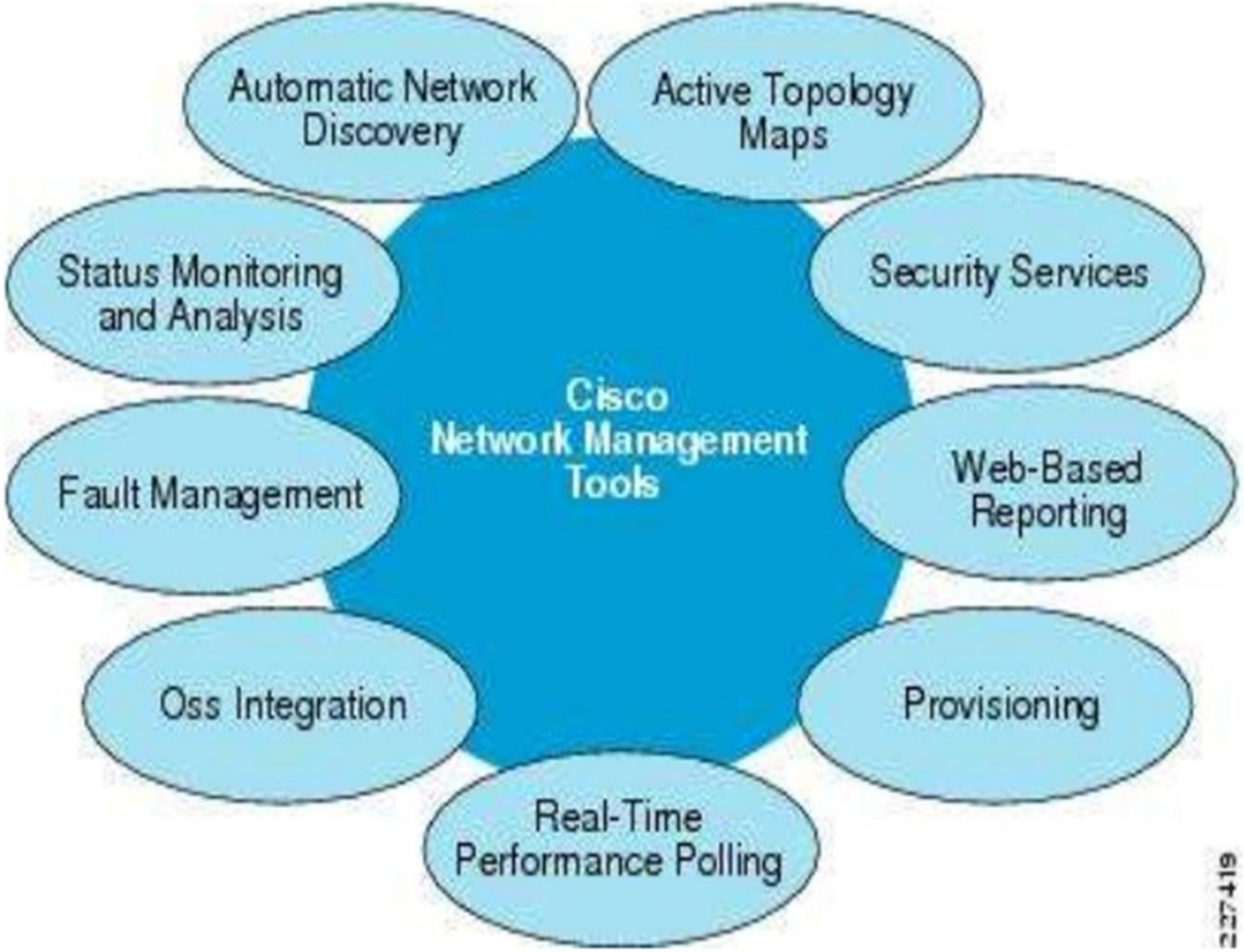


What Are the Components of Network Management?

The definition of network management is often broad, as network management involves several different components. Here are some of the terms you’ll often hear when network management or network management software is talked about:

- Network administration
- Network maintenance
- Network operation
- Network provisioning
- Network security

NETWORK MANAGEMENT


Automatic Network Discovery
Active Topology Maps
Status Monitoring and Analysis
Security Services
Cisco Network Management Tools
Fault Management
Web-Based Reporting
Oss Integration
Provisioning
Real-Time Performance Polling
227419

Why Is Network Management so Important When It Comes to Network Infrastructure?

The whole point of network management is to keep the network infrastructure running smoothly and efficiently. Network management helps you:

- Avoid costly network disruptions
- Improve IT productivity
- Improve network security
- Gain a holistic view of network performance

What Are the Challenges of Maintaining Effective Network Management and Network Infrastructure?

- Network infrastructures can be complex. Because of that complexity, maintaining effective network management is difficult. Advances in technology and the cloud have increased user expectations for faster network speeds and network availability. On top of that, security threats are becoming ever more advanced, varied and numerous. And if you have a large network, it incorporates several devices, systems and tools that all need to work together seamlessly. As your network scales and your company grows, new potential points of failure are introduced. Increased costs also come into play.
- In short, the list of challenges surrounding network management is a long one. Fortunately, there are solutions. Look no further than network management software.

Main areas of Network Management

While there is no precise definition of the term due to it being such a broad concept, some of the main areas are summarized below:

- Network Administration: This involves tracking and inventorying the many network resources such as monitoring transmission lines, hubs, switches, routers, and servers; it also involves monitoring their performance and updating their associated software – especially network management software, network operating systems, and distributed software applications used by network users.
- Network Operation: This involves smooth network functioning as designed and intended, including close monitoring of activities to quickly and efficiently address and fix problems as they occur and preferably even before users are aware of the problem.

Main areas of Network Management

- Network Maintenance: This involves timely repair and necessary upgrades to all network resources as well as preventive and corrective measures through close communication and collaboration with network administrators. Example work includes replacing or upgrading network equipment such as switches, routers and damaged transmission lines.
- Network Provisioning: This involves configuring network resources to support the requirements of a particular service; example services may be voice capabilities or increasing broadband requirements to facilitate more users.

IP (Internet Protocol)

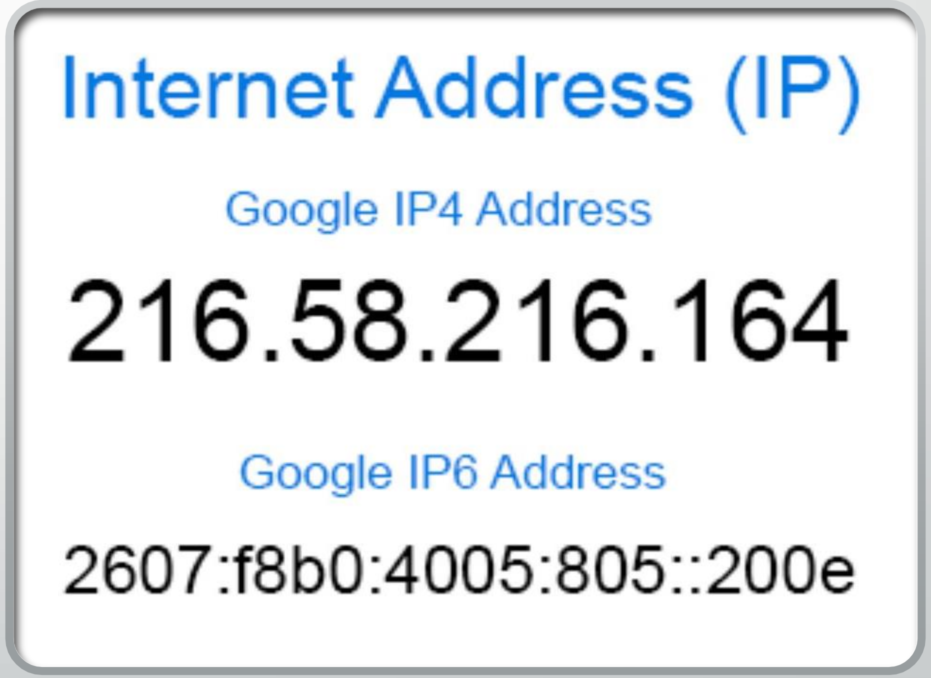
- The **IP** (**Internet Protocol**) is the fundamental protocol for communications on the Internet. It specifies the way information is packetized, addressed, transferred, routed, and received by networked devices.

IP Address

- An **IP address** is a number identifying of a computer or another device on the Internet. It is similar to a mailing address, which identifies where postal mail comes from and where it should be delivered. IP addresses uniquely identify the source and destination of data transmitted with the Internet Protocol.

IPv4 and IPv6 addresses

IPv4 addresses are 32 bits long (four bytes). An example of an IPv4 address is **216.58.216.164**, which is the front page of Google.com.



Internet Address (IP)

Google IP4 Address

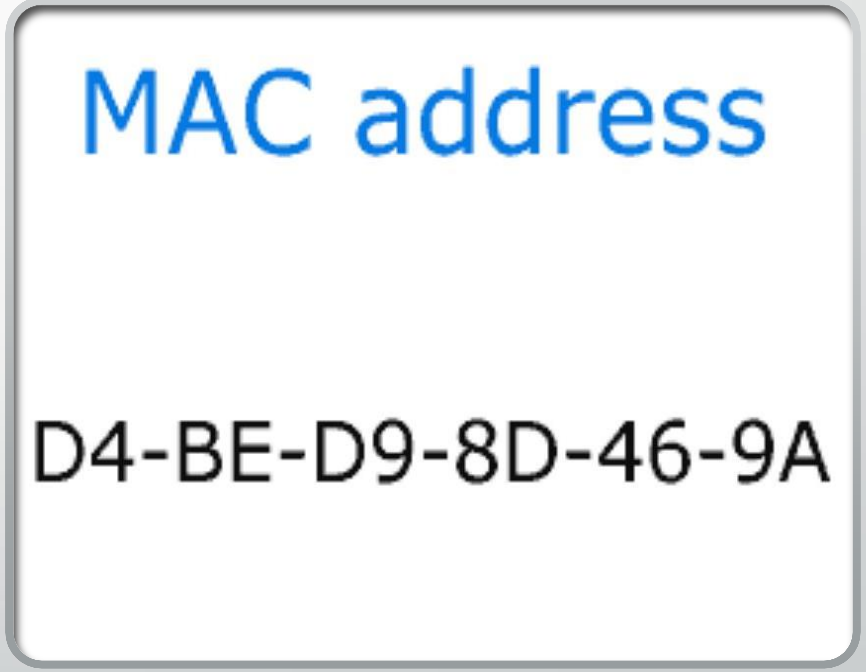
216.58.216.164

Google IP6 Address

2607:f8b0:4005:805::200e

MAC Address

- Short for **medium access control**, or **MAC address**. Known as a **physical address** and **hardware address** whose number is uniquely formatted in hexadecimal format and given to each computer or network device on a computer network. The addresses are usually assigned by the hardware manufacturer, and these ID's are considered burned into the firmware of the network access hardware. Because of this process, some vendors use specific formats in the hardware address. Below is an example of a MAC address. **[D4-BE-D9-8D-46-9A]**
- Because a MAC address is a unique address, devices on a network do not share the same MAC address.

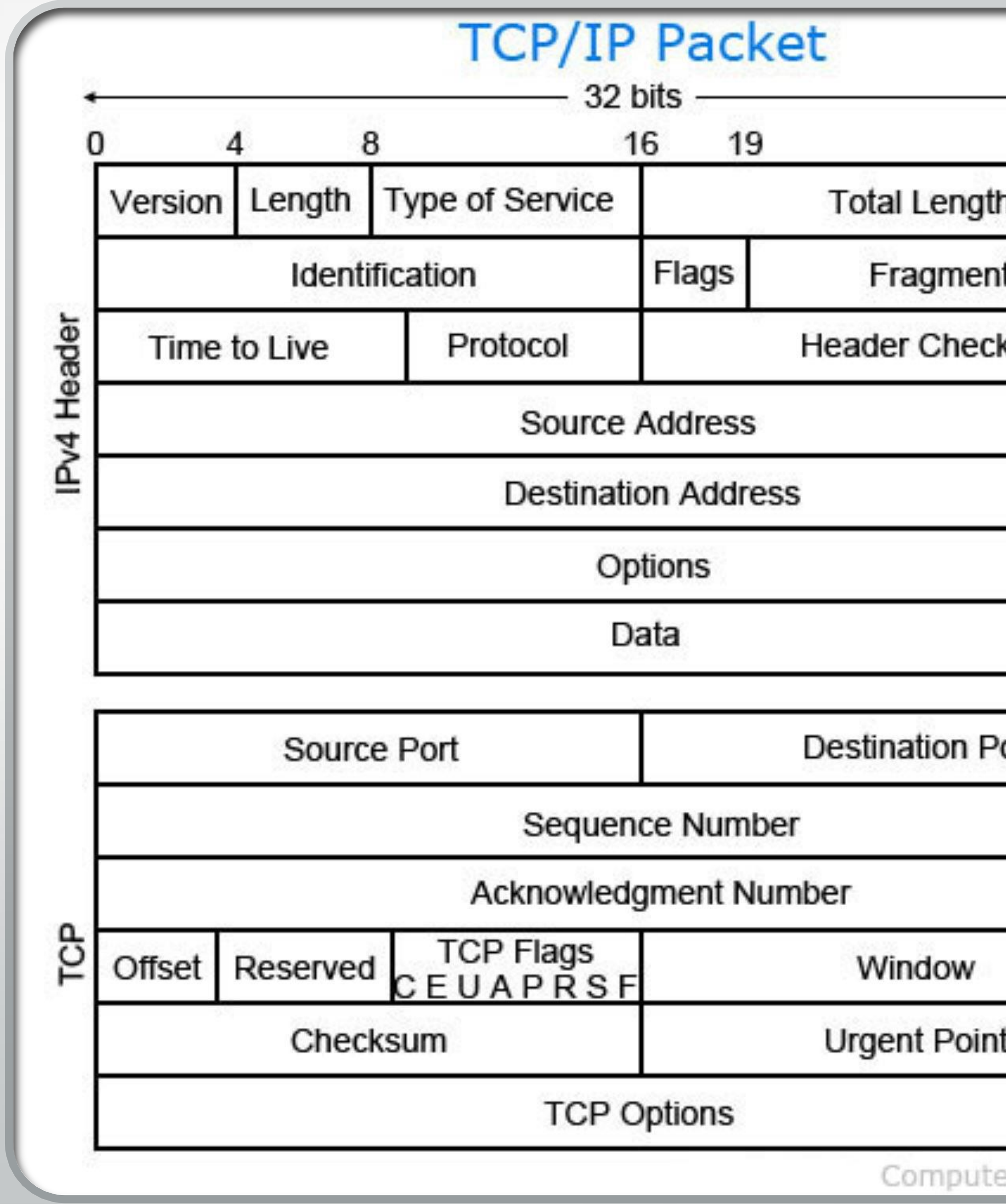


MAC address

D4-BE-D9-8D-46-9A

What is in a packet?

- A packet contains a source, destination, data, size, and other useful information that helps packet make it to the appropriate location and get reassembled properly. Below is a breakdown of a TCP packet.



TCP/IP Packet

32 bits

0 4 8 16 19

IPv4 Header

Version | Length | Type of Service | Total Lengt

Identification | Flags | Fragment

Time to Live | Protocol | Header Check

Source Address

Destination Address

Options

Data

TCP

Source Port | Destination Po

Sequence Number

Acknowledgment Number

Offset | Reserved | TCP Flags C E U A P R S F | Window

Checksum | Urgent Point

TCP Options

Compute

Network packet basics

- Another name for a packet is a **datagram**.
- Data transferred over the Internet is sent as one or more packets. The most common packet sent is the TCP packet.
- The size of a packet is limited, so most data sent over a network is broken up into multiple packets before being sent out and then put back together when received.
- When a packet is transmitted over a network, network routers and switches examine the packet and its source to help direct it to the correct location.
- During its transmission, network packets can be dropped. If a packet is not received or an error occurs, it is sent again.

AGGREGATE

- **Aggregate** may refer to any of the following:
- 1. In general, an **aggregate** is data composed of smaller pieces that form a larger whole.
- 2. An **aggregator** is a software program designed to collect data from multiple sources. For example, a user could use an RSS aggregator that collects their favorite web pages RSS feeds and instantly see all updates on those pages, without having to visit each site.

AGGREGATION

- 3. In programming, **aggregation** is a type of object composition where not all the containing objects should be destroyed when the owning object is destroyed.
- 4. In networking, **link aggregation** is combining many network connections to enable more data to be sent at one time or provide a backup connection if one of the connections fail.
- 5. In networking, when transferring packets, **packet aggregation** is combining many packets to make the transmission of packets require fewer server requests.
- 6. In networking, **route aggregation** refers to forming a supernet (combining two or more networks into one routing prefix).

ASSIGNMENT-1

i. Briefly Explain various Networking devices.

ii. Explain Network Topology? Discuss Various Network topologies and its importance.

email: **zeeshanuswat@gmail.com**

Submission deadline: 12-July-2020

CHAPTER -3

OSI REFERENCE MODEL

OSI Reference Model

1 - **Physical layer** - responsible for the electrical, mechanical, and timing across the link.

2 - **Data link layer** (also known as the **link layer**) - responsible for transmitting data across a link.

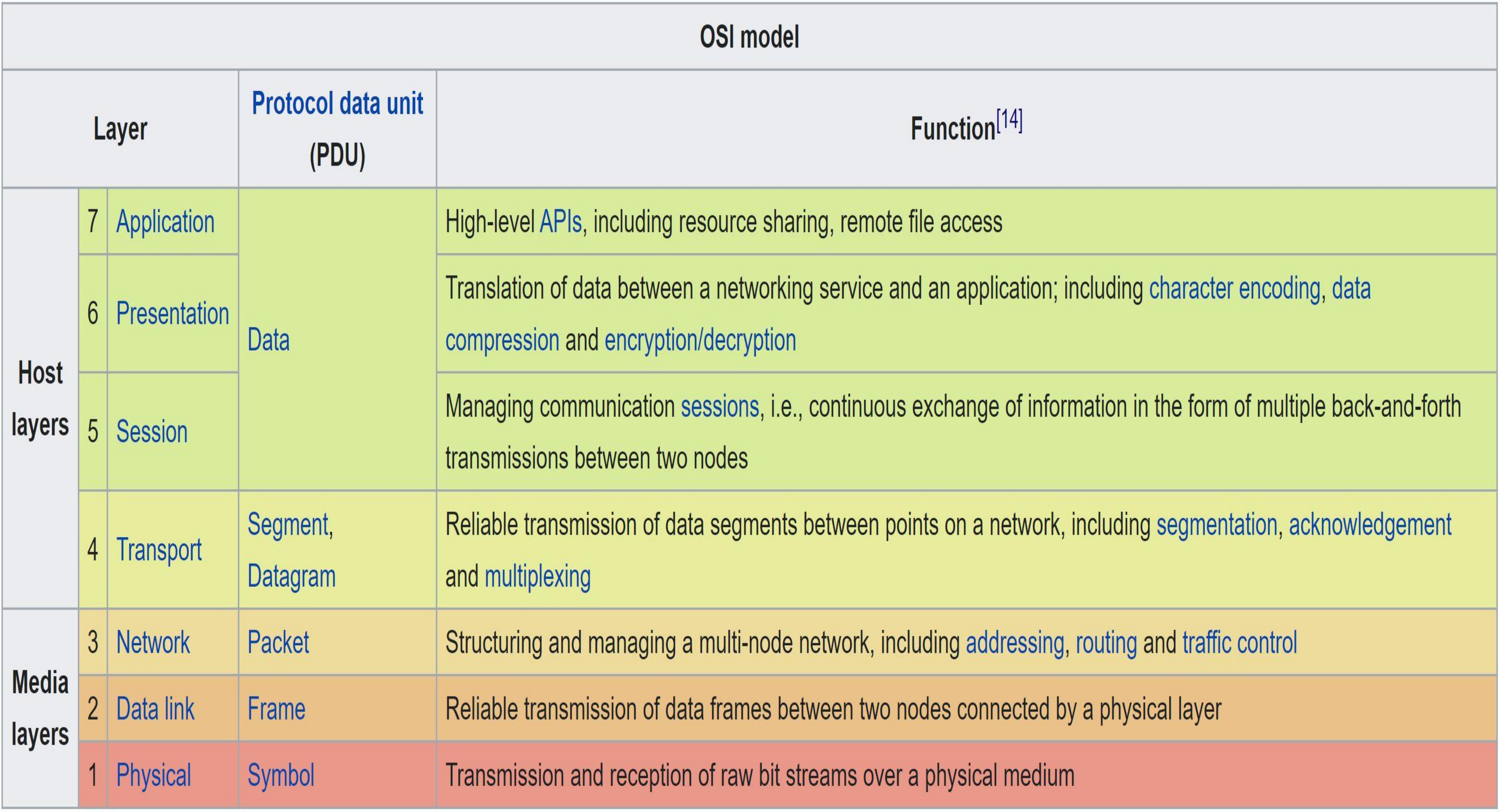
3 - **Network layer** - responsible for routing information through the network and allowing systems to communicate.

4 - **Transport layer** - responsible for transferring information between endpoints on the network and deals with errors, such as lost or duplicate packets.

5 - **Session layer** - responsible for managing a session between two applications.

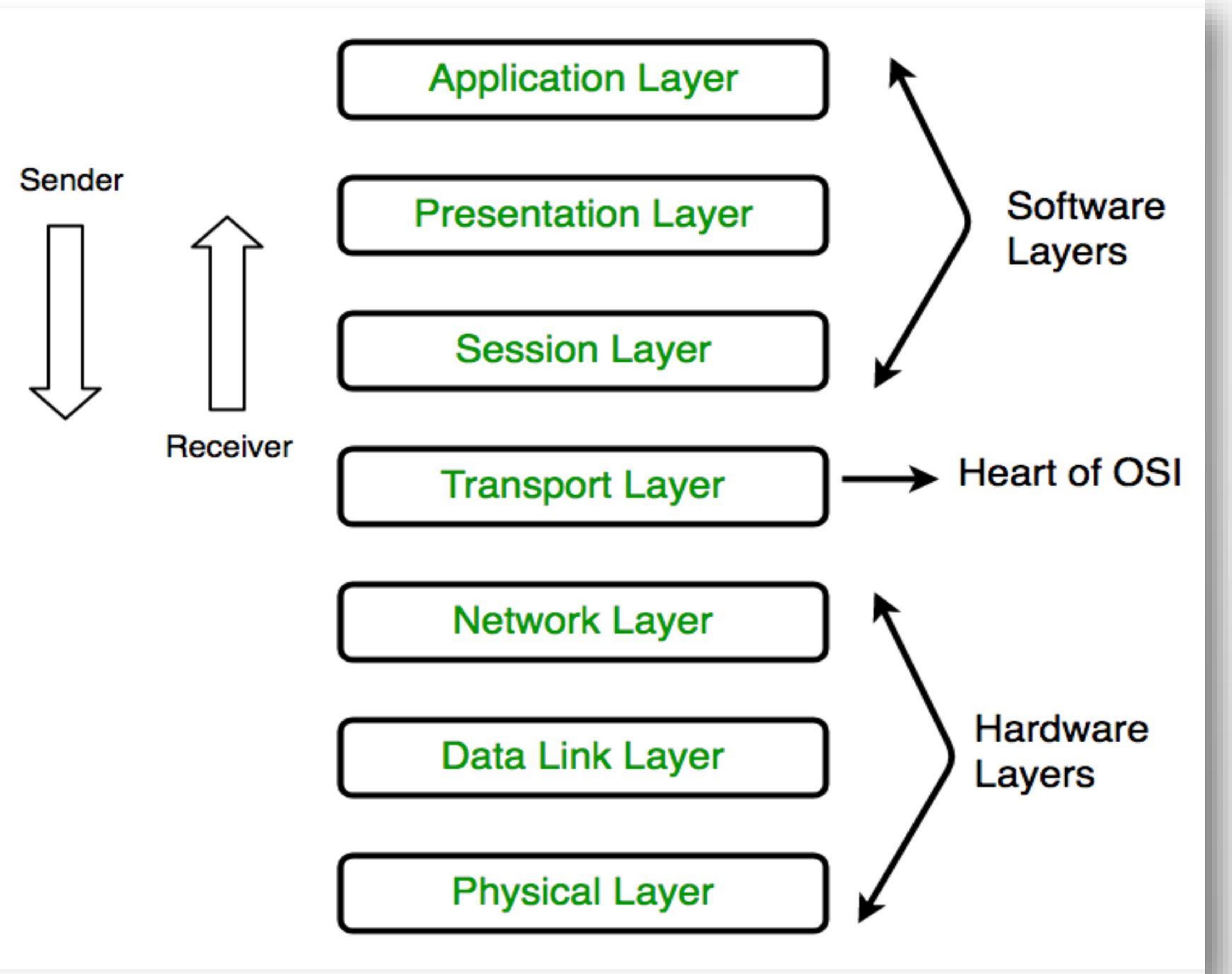
6 - **Presentation layer** - responsible for the data formatting and display, allowing for compatibility.

7 - **Application layer** - responsible for user interaction. An example of an OSI application is the FTAM.



OSI model

Layer			Protocol data unit (PDU)	Function[14]
Host layers	7	Application	Data	High-level APIs, including resource sharing, remote file access
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1	Physical	Symbol	Transmission and reception of raw bit streams over a physical medium



Sender
Receiver
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Software Layers
Heart of OSI
Hardware Layers

1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

1. Physical Layer (Layer 1) :

The functions of the physical layer are :

1.Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

2.Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

3.Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.

4.Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.

** Network Layer, Data Link Layer and Physical Layer are also known as **Lower Layers** or **Hardware Layers**

2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

1.Logical Link Control (LLC)

2.Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

2. Data Link Layer (DLL) (Layer 2) :

- The functions of the data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

- ** Packet in Data Link layer is referred as **Frame**.*
  *** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
  **** Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP address are placed in the header by the network layer.

The functions of the Network layer are :

1.Routing: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.

2.Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver’s IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* *Segment* in Network layer is referred as **Packet**.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

- Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

  - **At sender's side:**

  Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

  Note: The sender need to know the port number associated with the receiver's application.

  Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

  - **At receiver's side:**

  Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

4. Transport Layer (Layer 4) :

- The functions of the transport layer are :
- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

4. Transport Layer (Layer 4) :

- The services provided by the transport layer :
- **Connection Oriented Service:** It is a three-phase process which include

  – Connection Establishment

  – Data Transfer

  – Termination / disconnection

  In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
- **Connection less service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.
- ** Data in the Transport Layer is called as **Segments**.*

  *** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*

  *Transport Layer is called as **Heart of OSI** model.*

5. Session Layer (Layer 5) :

- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
  The functions of the session layer are :
- **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
- **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.
- ***All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as "Application Layer".*
  ***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

6. Presentation Layer (Layer 6) :

- Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

  The functions of the presentation layer are :

- **Translation :** For example, ASCII to EBCDIC.
- **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

  Compression: Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Ex: Application – Browsers, Skype Messenger etc.

***Application Layer is also called as Desktop Layer.*

The functions of the Application layer are :

1.Network Virtual Terminal

2.FTAM-File transfer access and management

3.Mail Services

4.Directory Services

OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model.

CHAPTER -4

TCP/IP NETWORK MODEL & NETWORK-PROTOCOLS

The TCP/IP Network Model

- The TCP/IP Model separates networking functions into discrete layers. Each layer performs a specific function and is transparent to the layer above it and the layer below it. Network models are used to conceptualize how networks should work, so that hardware and network protocols can interoperate. The TCP/IP model is one of the two most common network models, the other being the OSI Model.
- The TCP/IP Model of networking is a different way of looking at networking. Because the model was developed to describe TCP/IP, it is the closest model of the Internet, which uses TCP/IP.

The TCP/IP Network Model

The TCP/IP network model breaks down into four (4) layers:

- Application Layer
- Transport Layer
- Internet Layer
- Network Access Layer

TCP/IP Model Layers

- **Application Layer**
- The Application Layer provides the user with the interface to communication. This could be your web browser, e-mail client (Outlook, Eudora or Thunderbird), or a file transfer client.
- The Application Layer is where your web browser, a telnet, ftp, e-mail or other client application runs. Basically, any application that rides on top of TCP and/or UDP that uses a pair of virtual network sockets and a pair of IP addresses.

The Application Layer sends to, and receives data from, the Transport Layer.

TCP/IP Model Layers

- **Transport Layer**
- The Transport Layer provides the means for the transport of data segments across the Internet Layer. The Transport Layer is concerned with end-to-end (host-to-host) communication.
- Transmission Control Protocol provides reliable, connection-oriented transport of data between two endpoints (sockets) on two computers that use Internet Protocol to communicate.
- User Datagram Protocol provides unreliable, connectionless transport of data between two endpoints (sockets) on two computers that use Internet Protocol to communicate.
- The Transport Layer sends data to the Internet layer when transmitting and sends data to the Application Layer when receiving.

TCP/IP Model Layers

- **Internet Layer**
- The Internet Layer provides connectionless communication across one or more networks, a global logical addressing scheme and packetization of data. The Internet Layer is concerned with network to network communication.
- The Internet Layer is responsible for packetization, addressing and routing of data on the network. Internet Protocol provides the packetization, logical addressing and routing functions that forward packets from one computer to another.
- The Internet Layer communicates with the Transport Layer when receiving and sends data to the Network Access Layer when transmitting.

TCP/IP Model Layers

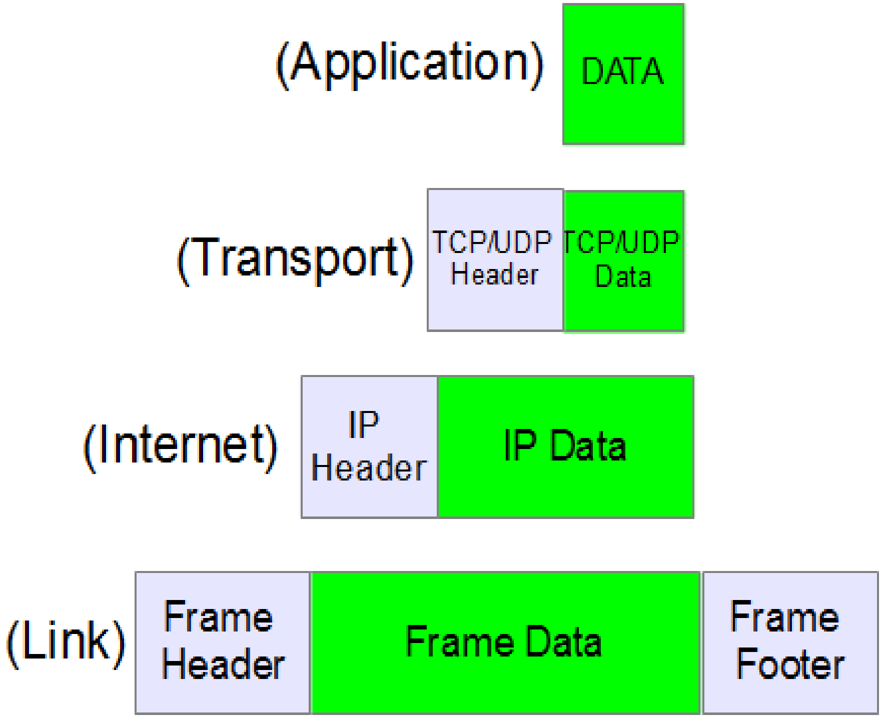
- **Network Access Layer**
- The Network Access Layer provides access to the physical network.
- This is your network interface card. Ethernet, FDDI, Token Ring, ATM, OC, HSSI, or even Wi-Fi are all examples of network interfaces. The purpose of a network interface is to allow your computer to access the wire, wireless or fiber optic network infrastructure and send data to other computers.
- The Network Access Layer transmits data on the physical network when sending and transmits data to the Internet Layer when receiving.

TCP/IP Model Layers

- All Internet-based applications and their data, whether it is a web browser downloading a web page, Microsoft Outlook sending an e-mail, a file, an instant message, a Skype video or voice call; the data is chopped into data segments and encapsulated in Transport Layer Protocol Data Units or PDU's (TCP or UDP segments). The Transport Layer PDU's are then encapsulated in Internet Layer's Internet Protocol packets. The Internet Protocol packets are then chopped into frames at the Network Access layer and transmitted across the physial media (copper wires, fiber optic cables or the air) to the next station in the network.
- The OSI Model uses seven layers, and differs quite a bit from the TCP/IP model. The TCP/IP model does a better job of representing how TCP/IP works in a network, but the OSI Model is still the networking model most technical people refer to during troubleshooting or network architecture discussions.

Layer Names	Protocols
Application	HTTP,FTP,POP3, SMTP,SNMP
Transport	TCP,UDP
Networking	IP,ICMP
Datalink	Ethernet, ARP

TCP/IP Networking Model



(Application) DATA

(Transport) TCP/UDP Header | TCP/UDP Data

(Internet) IP Header | IP Data

(Link) Frame Header | Frame Data | Frame Footer

Network Protocol

Simply, a protocol is a set of rules. A network protocol is a set of rules followed by the network. Network protocols are formal standards and policies made up of rules, procedures and formats that defines communication between two or more devices over a network. Network protocols conducts the action, policies, and affairs of the end-to-end process of timely, secured and managed data or network communication. They define rules and conventions for communication. They incorporate all the processes requirement and constraints of initiating and accomplishing communication between computers, routers, servers and other network enabled devices. Network protocols must be confirmed and installed by the sender and receiver to ensure network\data communication. It also applies software and hardware nodes that communicate on a network. There are several types of network protocols

Internet Protocol Suite

Internet protocol suite is the set of communication protocols that implement the protocol stack on which the internet runs. The Internet protocol suite is sometimes called the TCP/IP protocol suite, after TCP\IP, which refers to the important protocols in it, the Transmission Control Protocol(TCP) and the Internet Protocol(IP). The Internet protocol suite can be described by the analogy with the OSI model, but there are some differences. Also not all of the layers correspond well.

Internet Protocol Suite

Internet Protocol Suite

- Internet protocol suite is the set of communication protocols that implement the protocol stack on which the internet runs. The Internet protocol suite is sometimes called the TCP/IP protocol suite, after TCP\IP, which refers to the important protocols in it, the Transmission Control Protocol(TCP) and the Internet Protocol(IP). The Internet protocol suite can be described by the analogy with the OSI model, but there are some differences. Also not all of the layers correspond well.

Protocol Stack

- A protocol stack is the complete set of protocol layers that work together to provide networking capabilities.

Transmission Control Protocol (TCP)

- **Transmission Control Protocol (TCP)**
- The Transmission Control Protocol is the core protocol of the internet protocol suite. It originated in the network implementation in which it complemented the Internet Protocol. Therefore the entire suite is commonly referred to as TCP/IP. TCP provides reliable delivery of a stream of octets over an IP network. Ordering and error-checking are main characteristics of the TCP. All major Internet applications such as World Wide Web, email and file transfer rely on TCP.

Internet Protocol(IP)

- **Internet Protocol(IP)**
- The Internet Protocol is the principal protocol in the Internet protocol suite for relaying data across networks. Its routing function essentially establishes the internet. Historically it was the connectionless datagram service in the original Transmission Control Program; the other being the connection oriented protocol(TCP). Therefore, the Internet protocol suite is referred as TCP/IP.

Common Protocols Used and Their Ports

- **Hypertext Transfer Protocol (HTTP)**
- The HTTP is the foundation of data communication for the World Wide Web. The hypertext is structured text that uses hyperlinks between nodes containing texts. The HTTP is the application protocol for distributed and collaborative hypermedia information system.
- The default port of HTTP is 80 and 443 is the secured port.

Common Protocols Used and Their Ports

File Transfer Protocol (FTP)

- The FTP is the most common protocol used in the file transferring in the Internet and within private networks.
- The default port of FTP is 20/21.

Secured Shell (SSH)

- SSH is the primary method used to manage the network devices securely at the command level. It usually used as the alternative of the Telnet which does not support secure connections.
- The default port of SSH is 22.

Common Protocols Used and Their Ports

Telnet

- Telnet is the primary method used to manage network devices at the command level. Unlike SSH, Telnet does not provide a secure connection, but it provides a basic unsecured connection.
- The default port of Telnet is 23.

Simple Mail Transfer Protocol (SMTP)

- SMTP is used for two primary functions. It is used to transfer email from source to destination between mail servers and it is used to transfer email from end users to a mail system.
- The default port of SMTP is 25 and secured (SMTPS) is 465 (Not standard)

Common Protocols Used and Their Ports

Domain Name System (DNS)

- Domain name system is used to convert the domain name to IP address. There are root servers, TLDs and authoritative servers in the DNS hierarchy.
- The default port of DNS is 53.

Post Office Protocol version 3 (POP 3)

- The Post Office Protocol version 3 is one of the two main protocols used to retrieve mail from the internet. It is very simple as it allows the client to retrieve complete content from the server mail box and deletes contents from the server.
- The default port of POP3 is 110 and secured is 995.

Common Protocols Used and Their Ports

Internet Message Access Protocol (IMAP)

- IMAP version 3 is another main protocol that used to retrieve mail from a server. IMAP does not delete the content from the mail box of the server.
- The default port of IMAP is 143 and secured is 993.

Simple Network Management Protocol (SNMP)

- The Simple Network Management Protocol is used to manage networks. It has abilities to monitor, configure and control network devices. SNMP traps can also be configured on network devices to notify a central server when specific action are occurring.
- The default port of SNMP is 161/162.

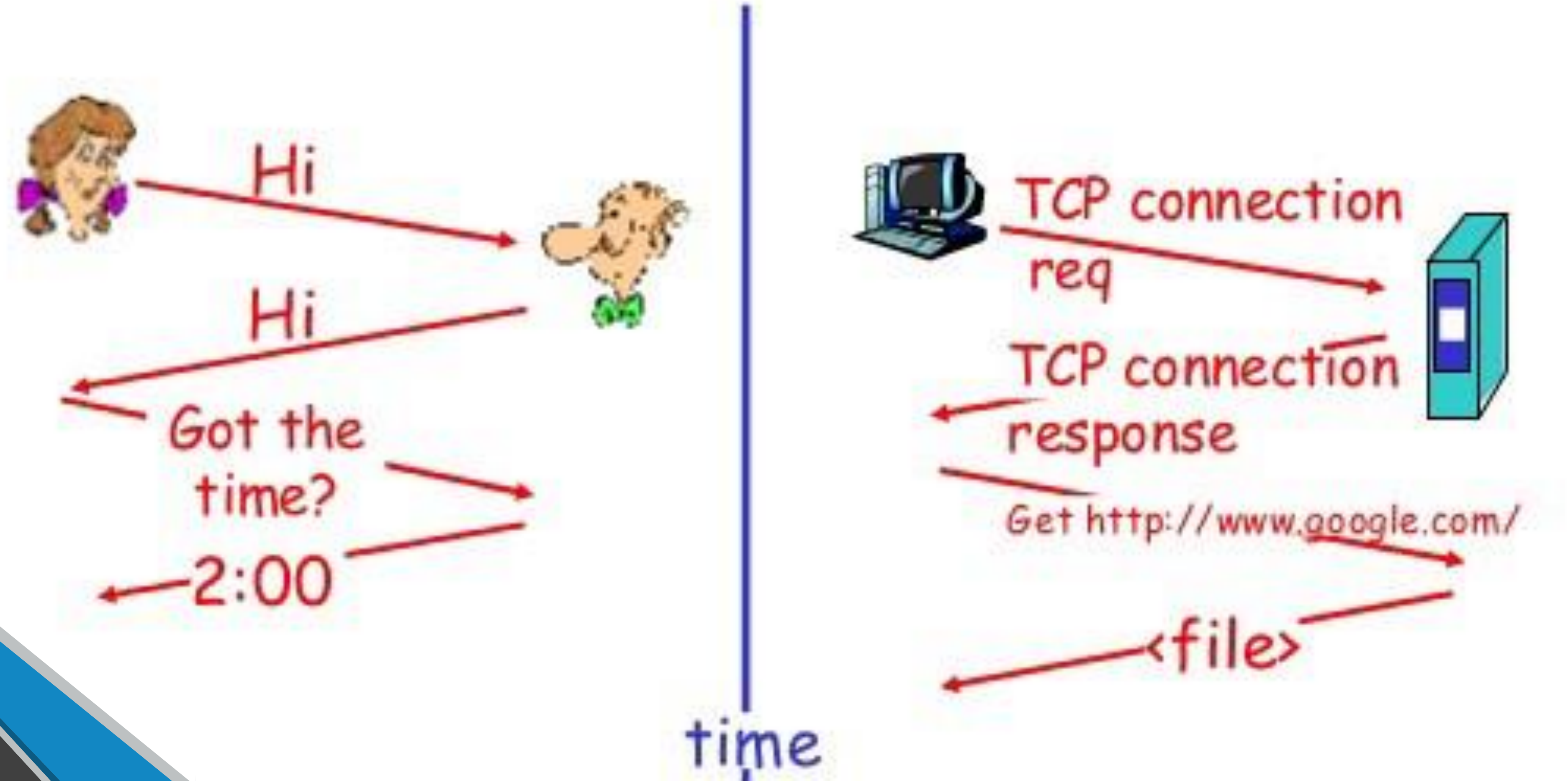
Common Protocols Used and Their Ports

Hypertext Transfer Protocol over SSL/TLS (HTTPS)

- HTTPS is used with HTTP to provide same services, but with a secured connection which is provided by SSL or TLS.
- The default port of HTTPS is 443.

What’s a protocol?

a human protocol and a computer network protocol:

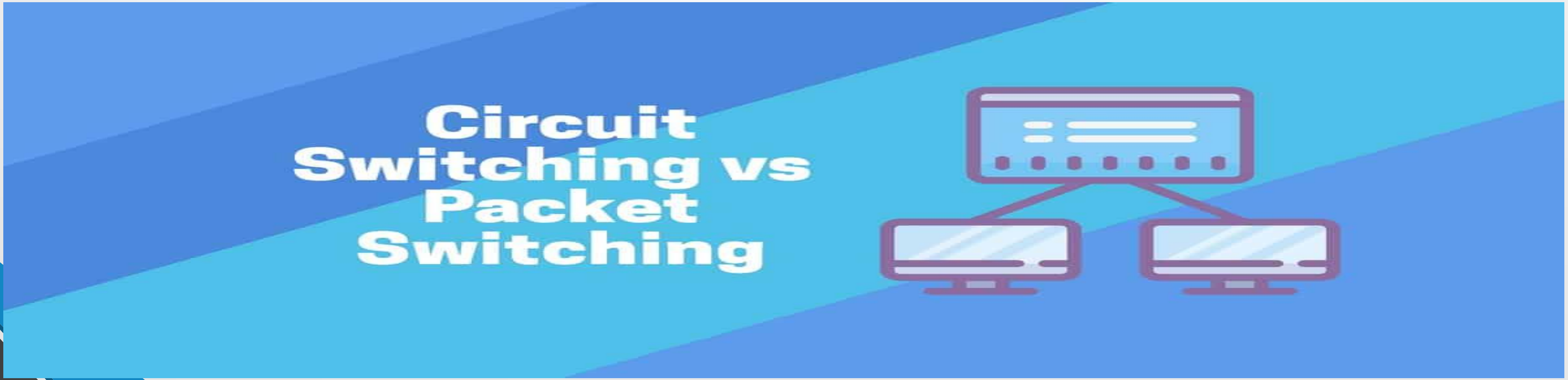


Chapter -5

Switching, Coding, Multiplexing

Circuit Switching vs Packet Switching

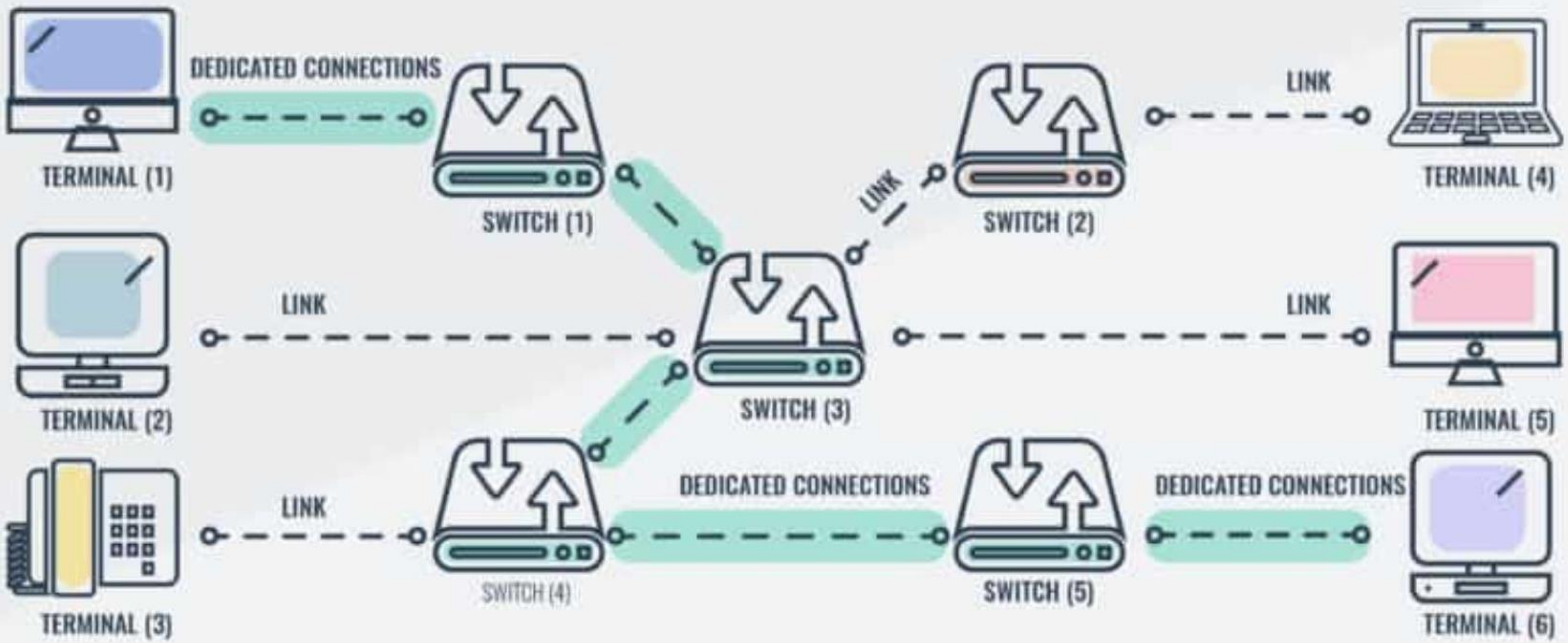
- Understanding how devices connect to each other is one of the most important elements of networking. The more you know about how your network is tied together the better you are able to respond to performance issues and run in-depth troubleshooting.
- **Circuit Switching** and **Packet Switching** are two of the main models used to facilitate connections within enterprise networks. In this article, we’re going to look at circuit switching vs packet switching to see how these two models differ from each other.



What is Circuit Switching?

- Circuit switching is when a dedicated channel or circuit needs to be established before users can speak to each other on a call. A channel used in circuit switching is kept reserved at all times and is used once the two users communicate. Circuit switching connections are classified as **half duplex** or **full duplex**. Half duplex communications allocate one channel and full duplex communications allocate two channels.
- Circuit switching is most commonly-used to sustain telephone systems so that whenever the phone is picked up the conversation can begin. Circuit switching is considered to be distinct from packet switching because it **provides a physical path between the source and destination**. Packet switching offers no such physical path for packets which travel independently through a range of routes.

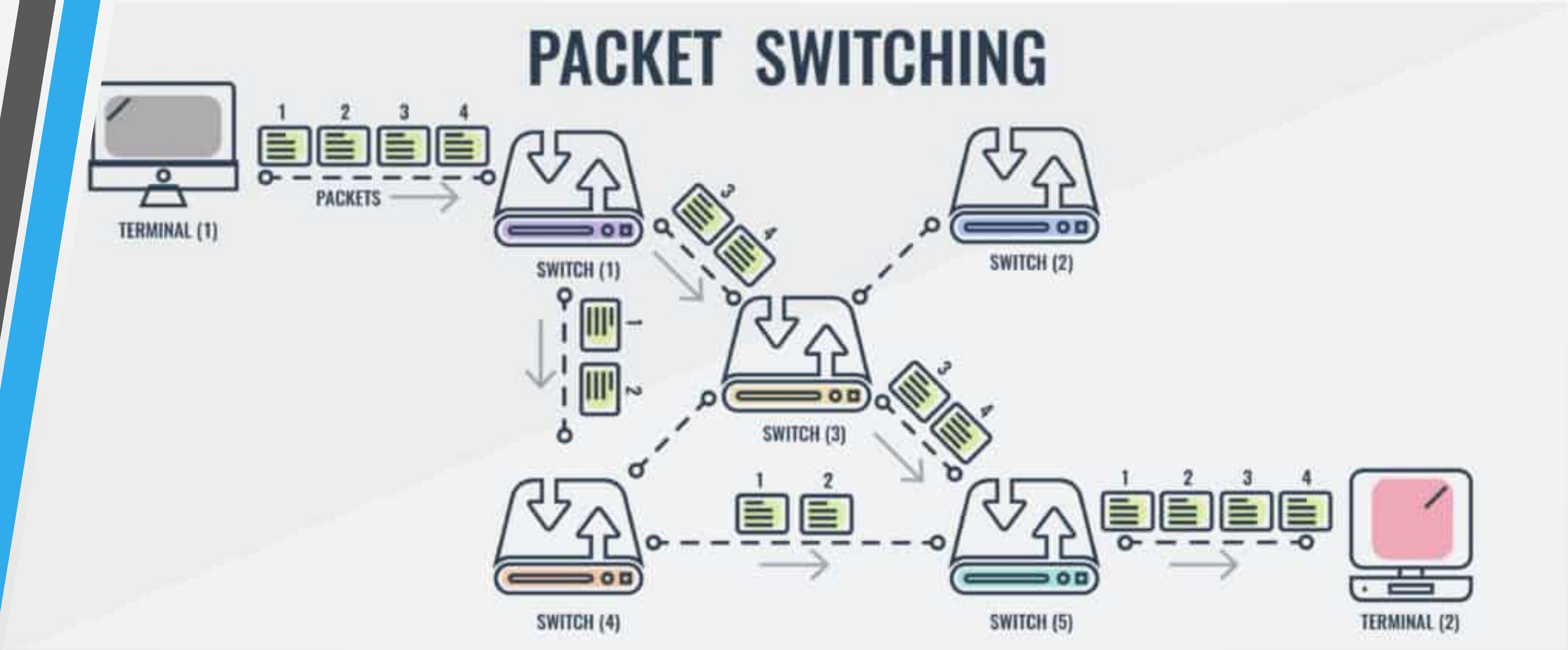
CIRCUIT SWITCHING



What is Packet Switching?

- Packet switching is different from circuit switching because there is no requirement to establish a channel. The channel is available to users throughout the network. Long messages are broken down into packets and sent individually to the network. These packets are handled by datagram or virtual circuit. Datagram sends each packet individually and can travel any route. The problem with this method is that packets can arrive out of sequence or even be lost in transit altogether.

- On the other hand, a virtual circuit establishes a predefined route before the packets are transmitted. As a consequence routing decisions don’t need to be made for the packet path as they are with a datagram. Every packet contains a virtual circuit identifier (VCI) so that the packets can reach their destination. Call requests and accept messages are used to identify the route before packets are in transit. Packet switching is used to sustain data and voice applications that don’t require real-time service.


PACKET SWITCHING
TERMINAL (1)
1
2
3
4
PACKETS
SWITCH (1)
3
4
1
2
SWITCH (2)
SWITCH (3)
3
4
1
2
SWITCH (4)
SWITCH (5)
1
2
3
4
TERMINAL (2)

Circuit Switching vs Packet Switching

- **Circuit Switching vs Packet Switching**
- **Circuit switching and packet switching are undeniably two of the most widely-used techniques for transferring data across enterprise networks.** Both of these two techniques have their own space within modern networking. Using circuit switching allows you to keep a channel established for high priority voice calls to give the users the best chance to communicate with each other. In contrast, packet switching uses a more malleable approach so that traffic can travel a variety of paths.

MULTIPLEXING

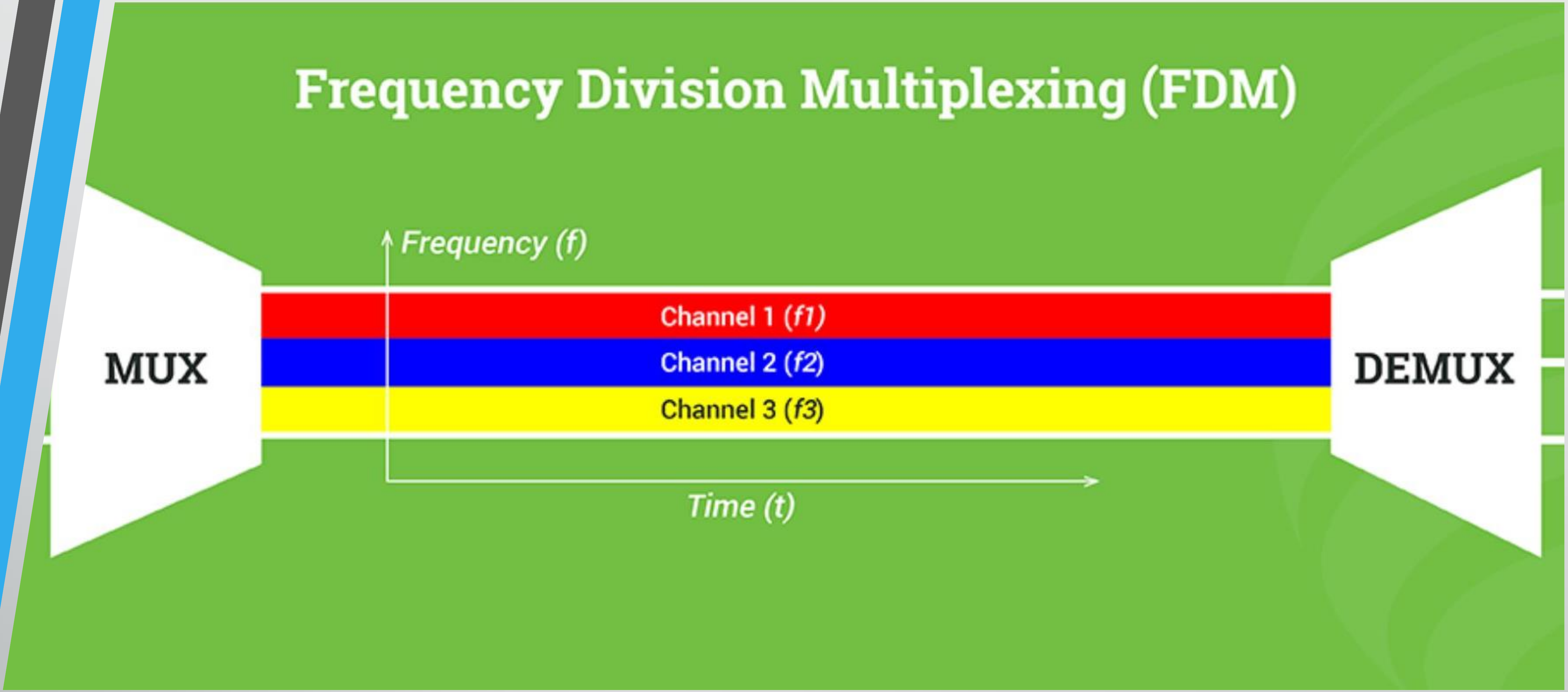
- Multiplexing (or *muxing*) is a way of sending multiple signals or streams of information over a communications link at the same time in the form of a single, complex signal; the receiver recovers the separate signals, a process called *demultiplexing* (or *demuxing*).

Networks use multiplexing for two reasons:

- To make it possible for any network device to talk to any other network device without having to dedicate a connection for each pair. This requires shared media;
- To make a scarce or expensive resource stretch further -- e.g., to send many signals down each cable or fiber strand running between major metropolitan areas, or across one satellite uplink.

Frequency-division multiplexing

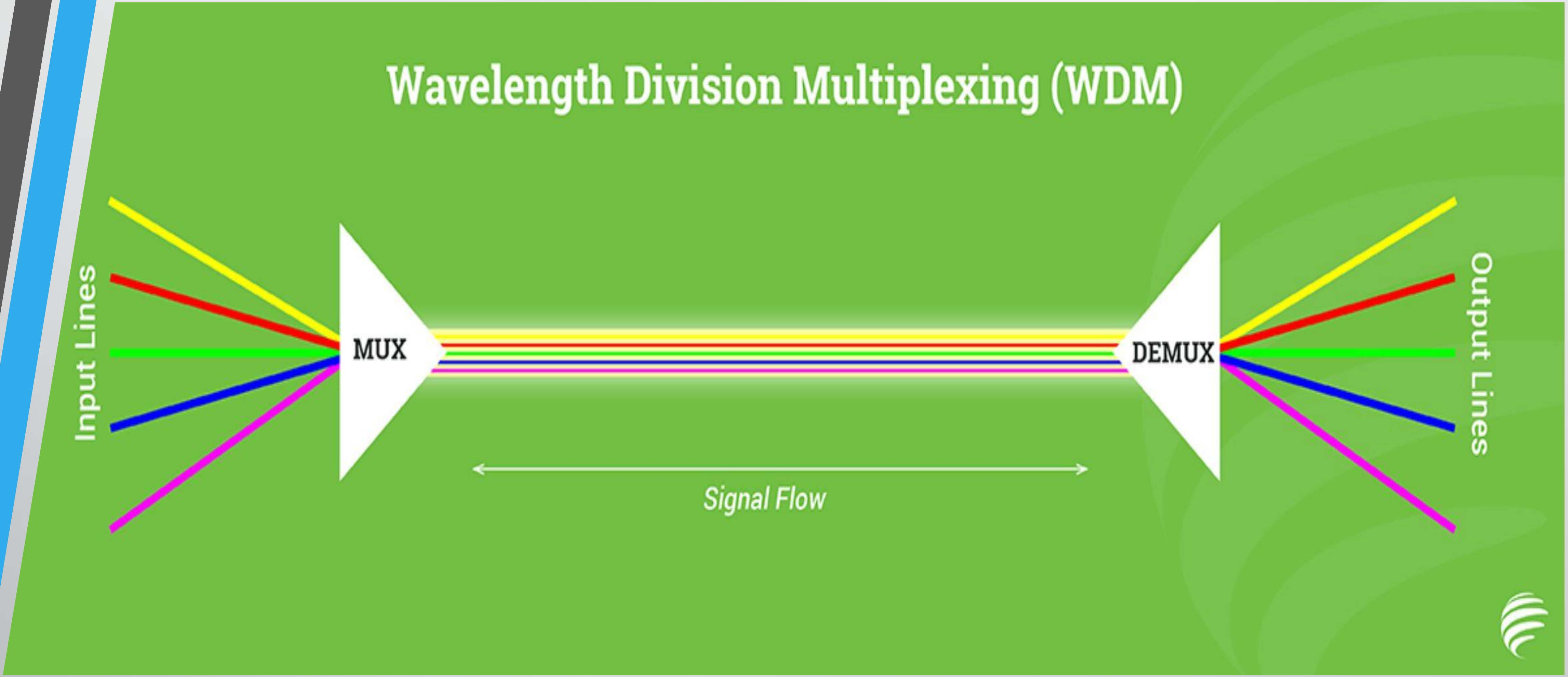
- In analog radio transmission, signals are commonly multiplexed using frequency-division multiplexing (FDM), in which the bandwidth on a communications link is divided into subchannels of different frequency widths, each carrying a signal at the same time in parallel. Analog cable TV works the same way, sending multiple channels of material down the same strands of coaxial cable.



Frequency Division Multiplexing (FDM)

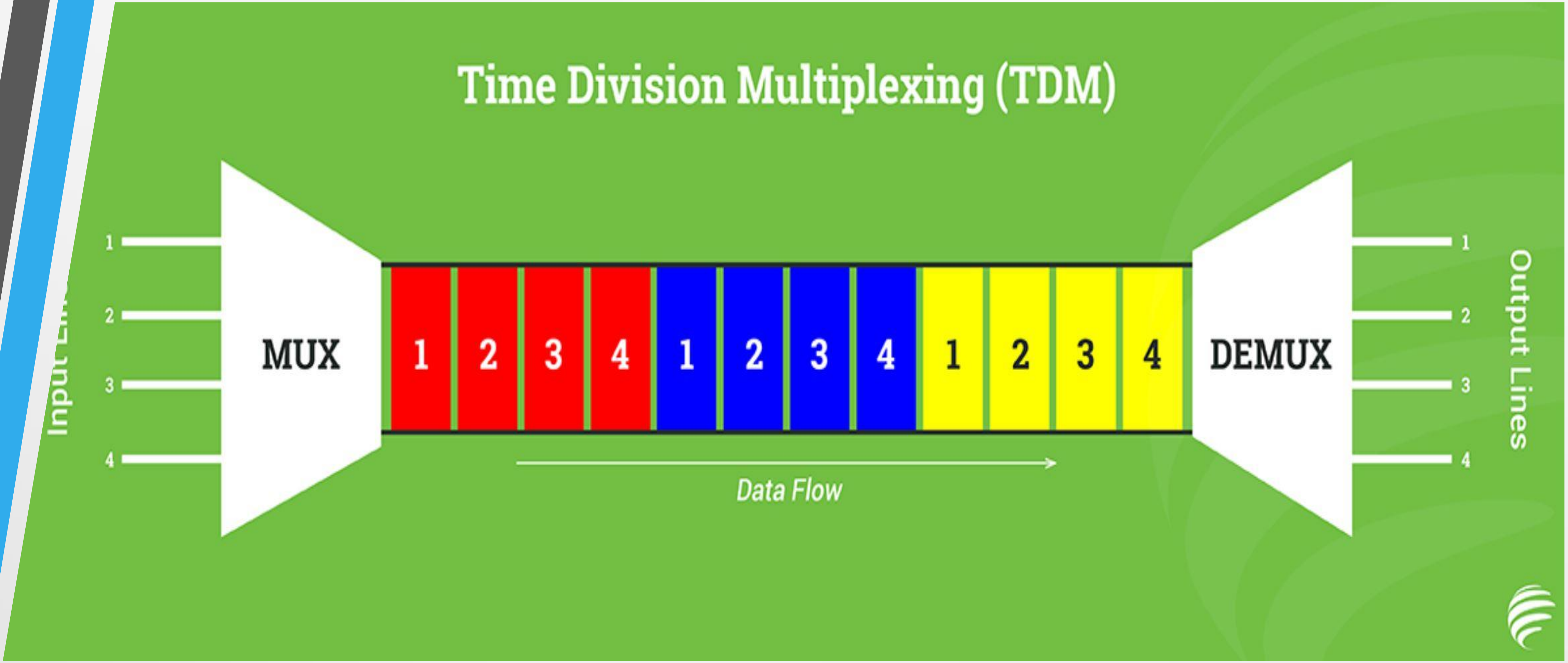
wave-length division multiplexing (WDM).

- Similarly, in some optical networks, data for different communications channels are sent on lightwaves of different wavelengths, a variety of multiplexing called *wave-length division multiplexing* (WDM).
- These techniques are all basically use the same concept. FDM describes fields that traditionally discuss frequencies (like radio and television broadcasting). WDM is used in fields that traditionally talk about wavelengths, like telecommunications and computer networks that use laser systems (which generate the signals sent over fiber optic cables). Variations include coarse WDM (CWDM) and dense WDM (DWDM), which put relatively fewer or more channels of information, respectively, on the medium at the same time. Other variations use light polarization to multiplex.


Wavelength Division Multiplexing (WDM)
Input Lines
MUX
DEMUX
Output Lines
Signal Flow

time-division multiplexing (TDM),

- In digital transmission, signals are commonly multiplexed using time-division multiplexing (TDM), in which the multiple signals are carried over the same channel in alternating time slots. For example, TDM is used on SONET links that used to be a mainstay of enterprise WAN and Internet connectivity.


Time Division Multiplexing (TDM)
Input Lines
1
2
3
4
MUX
1
2
3
4
1
2
3
4
1
2
3
4
DEMUX
1
2
3
4
Output Lines
Data Flow

Code-Division Multiple Access (CDMA).

- Code Division Multiplexing (CDM) uses identifying codes to distinguish one signal from another on a shared medium. Each signal is assigned a sequence of bits called the spreading code that is combined with the original signal to produce a new stream of encoded data; a receiver that knows the code can retrieve the original signal by subtracting out the spreading code (a process called *dispreading*). CDM is widely used in digital television and radio broadcasting and in 3G mobile cellular networks. Where CDM allows multiple signals from multiple sources, it is called Code-Division Multiple Access (CDMA).

THANKS

submit your assignment on:
zeeshanuswat@gmail.com