SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

3040233303
COMPUTER NETWORK

UNIT-1:INTRODUCTION TO NETWORKING & NETWORK MODELS

SEMESTER: 5

PREPARED BY: Ms. Dimple Shah

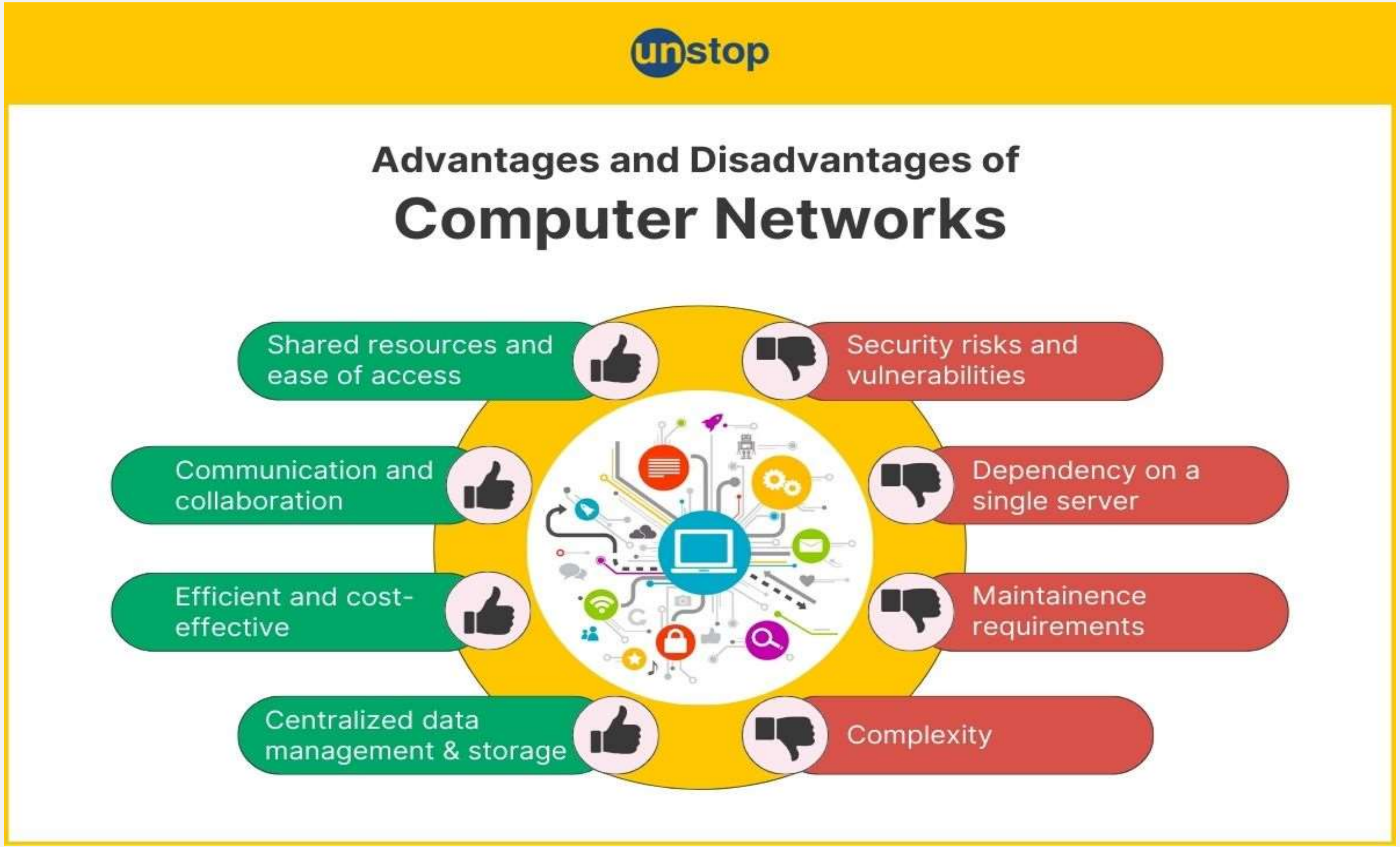
INTRODUCTION

Computer Network

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

Computer networking refers to interconnected computing devices that can exchange data and share resources with each other.

ADVANTAGES AND DISADVANTAGES OF COMPUTER NETWORKS



Advantages and Disadvantages of Computer Networks

- Shared resources and ease of access
- Communication and collaboration
- Efficient and cost-effective
- Centralized data management & storage

- Security risks and vulnerabilities
- Dependency on a single server
- Maintainence requirements
- Complexity

ADVANTAGES

- **Resource Sharing:**

  Allows multiple users to access and utilize the same resources like printers, files, and software.

- **Centralized Management:**

  Data and resources can be managed from a central location, simplifying administration and security.

- **Improved Communication and Collaboration:**

  Facilitates faster and more efficient communication and collaboration among users.

- **Cost Reduction:**

  Reduces the need for individual hardware and software licenses, leading to overall cost savings.

- **Increased Flexibility and Scalability:**

  Networks can be easily expanded or modified to accommodate changing needs.

- **Centralized Data Management:**

  Data can be stored and managed in a central location, improving data consistency and security.

- **Enhanced Security:**

  Advanced security measures can be implemented to protect sensitive data and resources.

DISADVANTAGES

- **High Initial Cost:**

  Setting up a computer network can be expensive due to the cost of hardware, software, and installation.
- **Security Risks:**

  Networks are susceptible to various security threats like viruses, malware, and hacking attempts.
- **Dependence on Infrastructure:**

  Network failures or downtime can disrupt operations and lead to loss of productivity.
- **Complexity:**

  Managing and maintaining a complex network requires specialized knowledge and expertise.
- **Potential for Data Loss:**

  In case of system failures, data loss can occur if backups are not properly maintained.
- **Vulnerability to Viruses and Malware:**

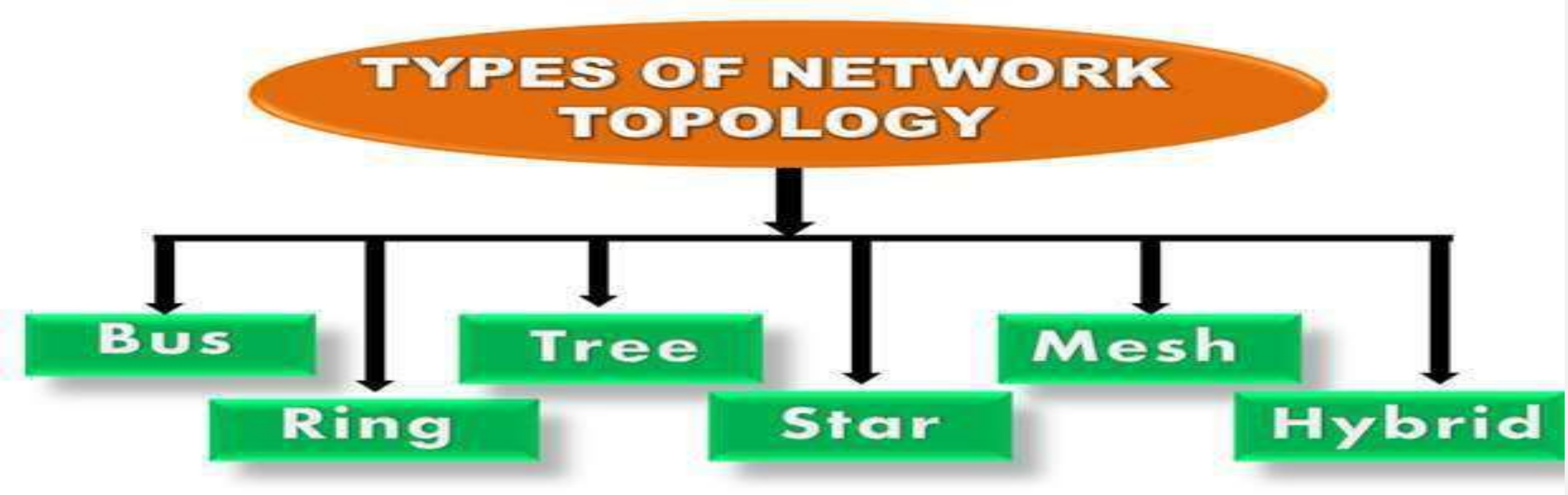
  Viruses and malware can spread rapidly through a network, potentially affecting all connected devices.

Applications of Computer Network

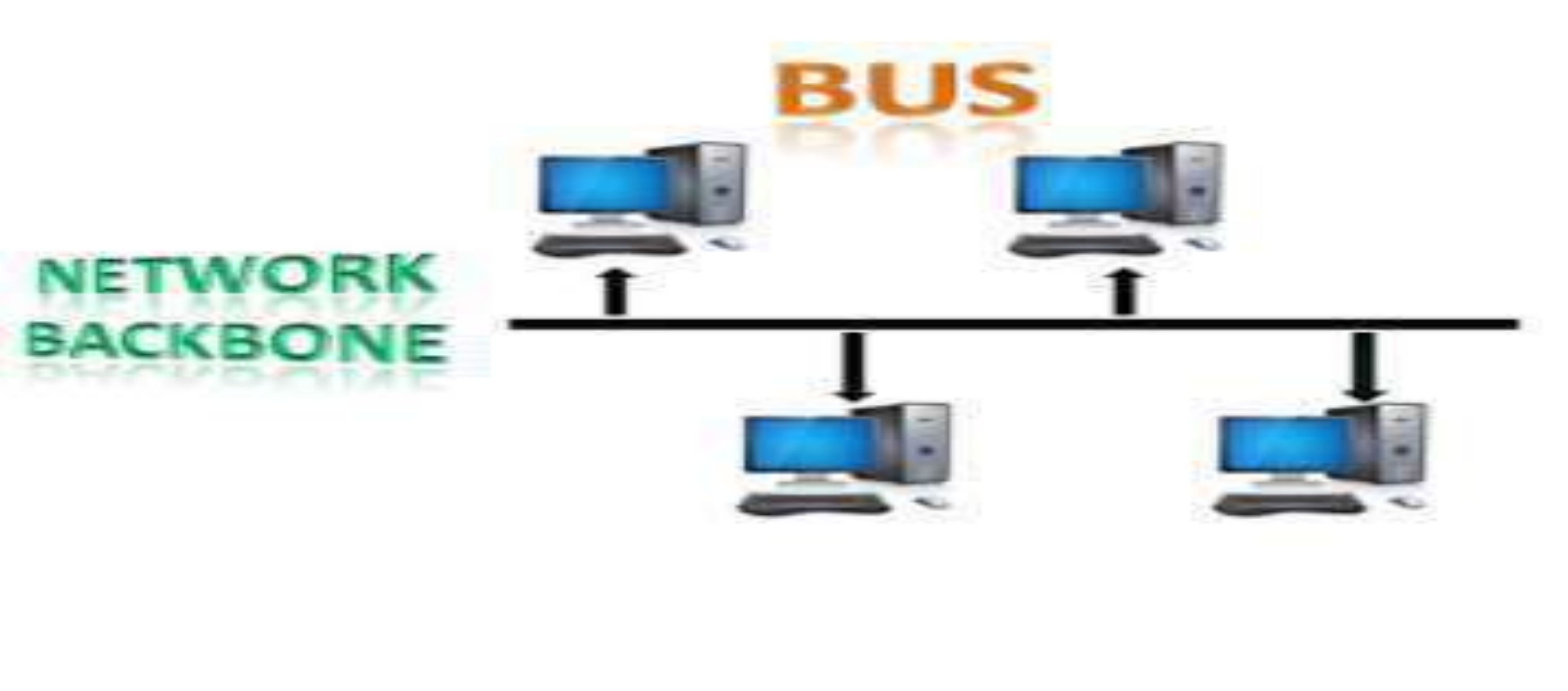
- Resource Sharing
- Server-Client Model
- Communication Medium
- eCommerce
- Access to remote information
- Person-to-Person communication
- Interactive entertainment

WHAT IS TOPOLOGY?

- Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.



BUS TOPOLOGY



BUS TOPOLOGY

- The bus topology is designed in such a way that all the stations are connected through a Each node is either connected to the bsingle cable known as a backbone cable.
- backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (Ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.

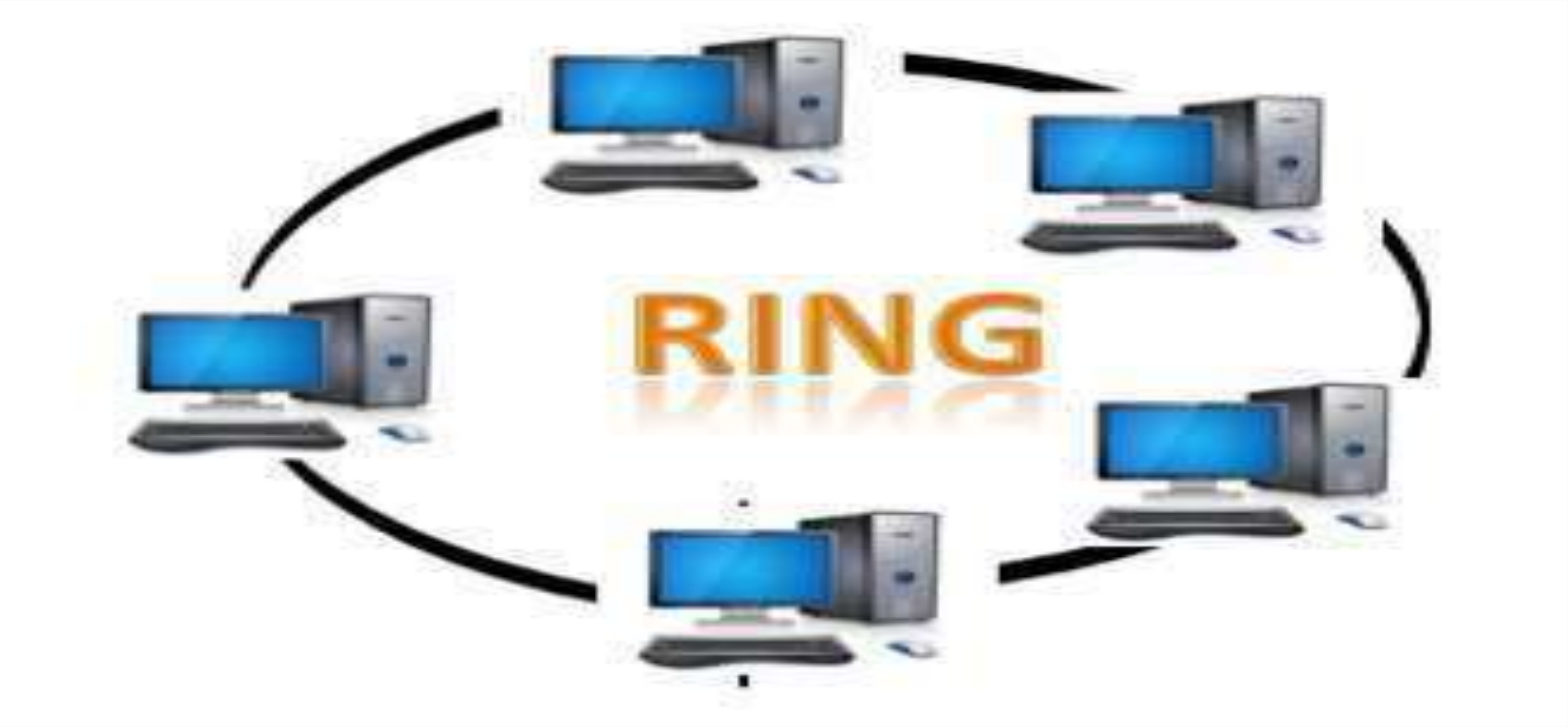
ADVANTAGE OF BUS TOPOLOGY

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

DISADVANTAGE OF BUS TOPOLOGY

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

RING TOPOLOGY



RING TOPOLOGY

- In this topology, it forms a ring connecting devices with its exactly two neighboring devices.
- A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network
- The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

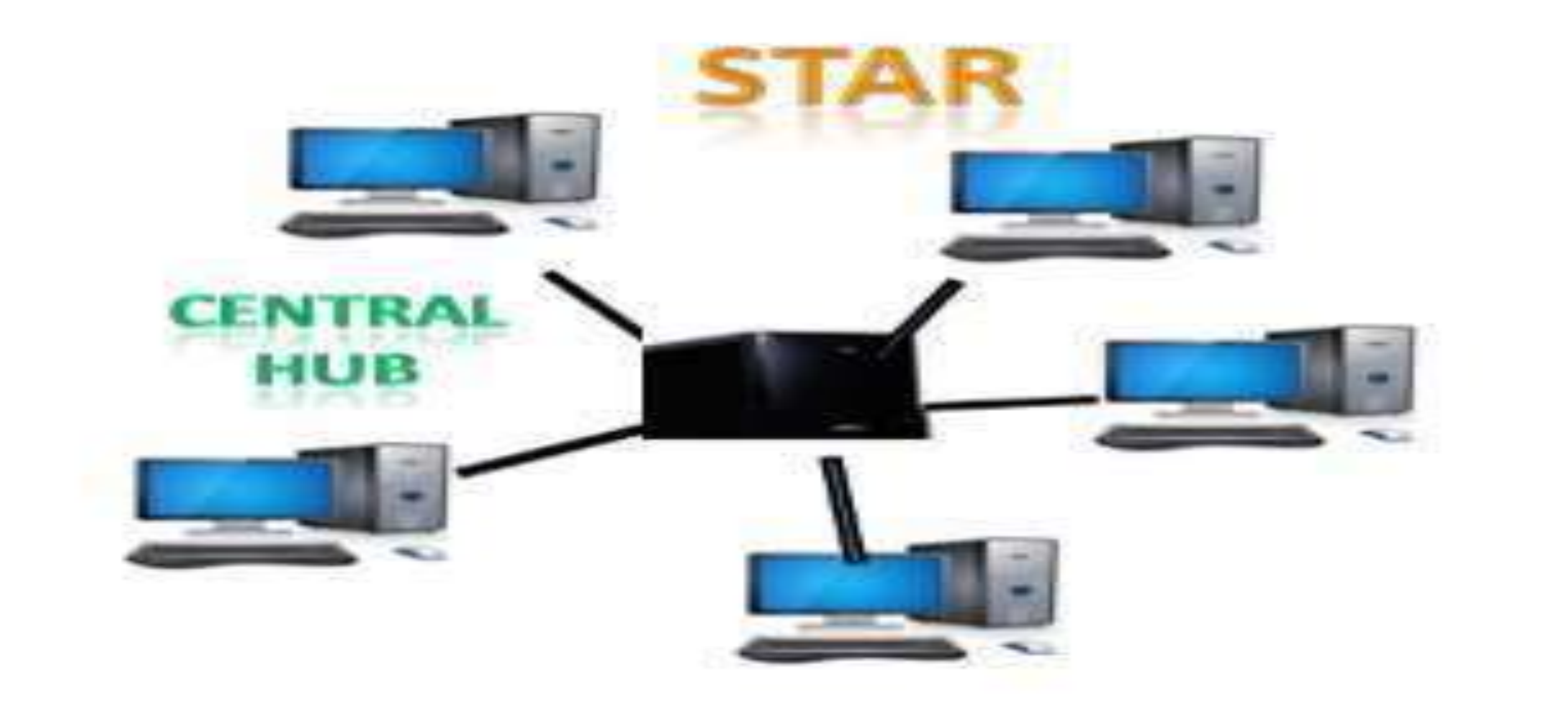
ADVANTAGE OF RING TOPOLOGY

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

DISADVANTAGES OF RING TOPOLOGY

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

STAR TOPLOGY



STAR TOPOLOGY

- In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them.
- A star topology having four systems connected to a single point of connection i.e. hub.

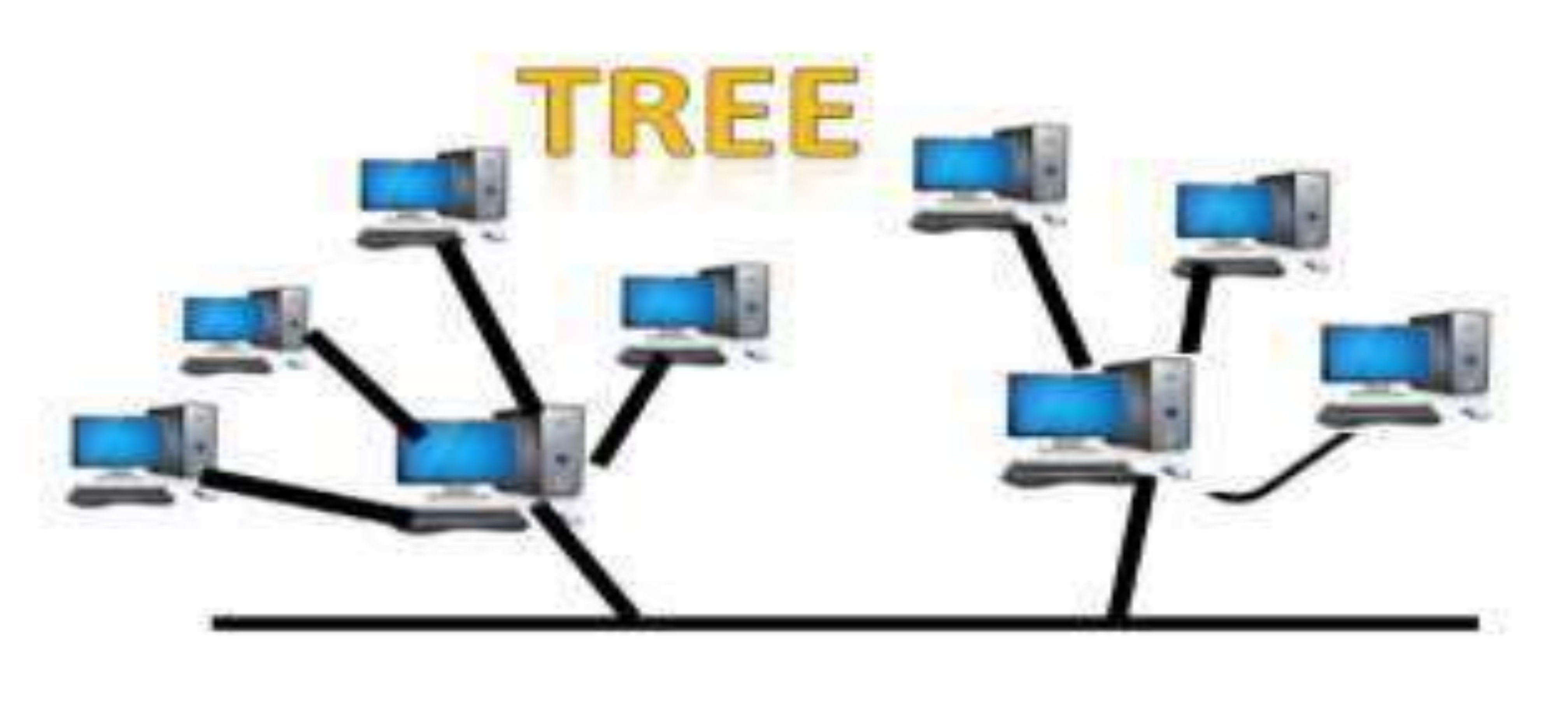
ADVANTAGE OF STAR TOPOLOGY

- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

DISADVANTAGES OF STAR TOPOLOGY

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

TREE TOPOLOGY



TREE TOPOLOGY

- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- Tree topology combines the characteristics of bus topology and star topology.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

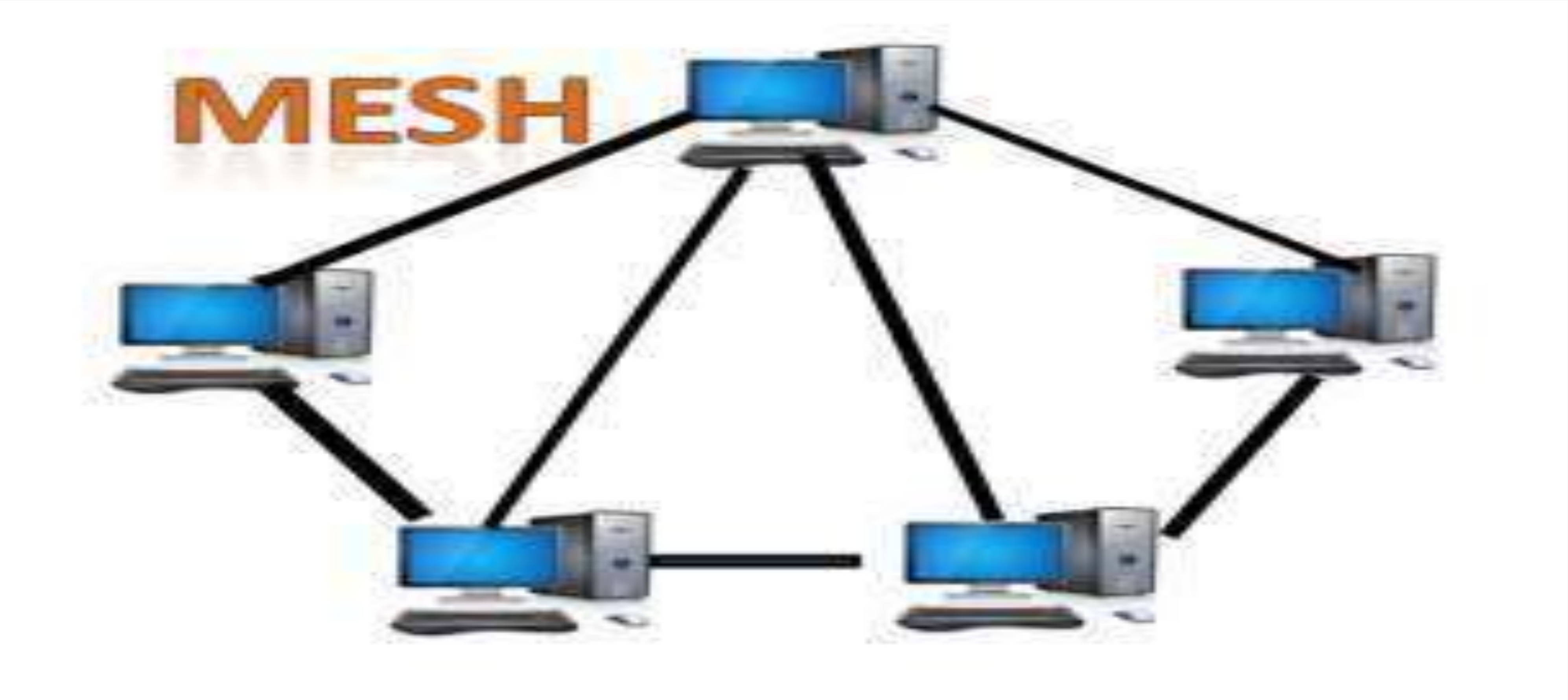
ADVANTAGES OF TREE TOPOLOGY

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

DISADVANTAGES OF TREE TOPOLOGY

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

MESH TOPOLOGY



MESH TOPOLOGY

- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula:
  Number of cables = (n*(n-1))/2;

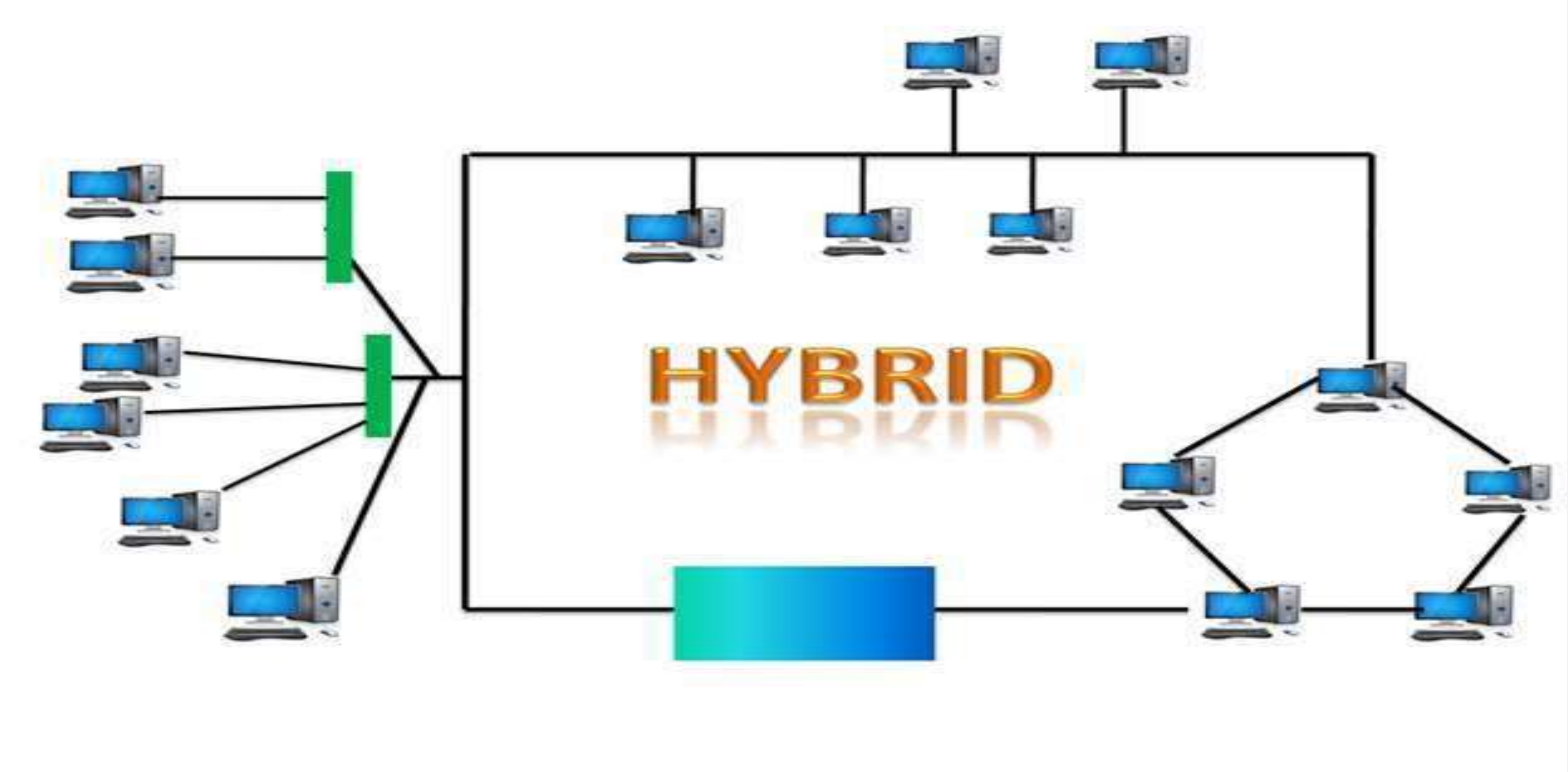
ADVANTAGES OF MESH TOPOLOGY

- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

DISADVANTAGE OF MESH TOPOLOGY

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

HYBRID TOPOLOGY



HYBRID TOPOLOGY

- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

ADVANTAGES OF HYBRID TOPOLOGY

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without
- affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the
- requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

DISADVANTAGES OF HYBRID TOPOLOGY

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

OPEN SYSTEMS INTERCONNECTION (OSI) MODEL

- International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.
- Open Systems Interconnection (OSI) reference model is the result of this effort.
- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- Term "open" denotes the ability to connect any two systems which conform to the reference model and associated standards.

OSI REFERENCE MODEL

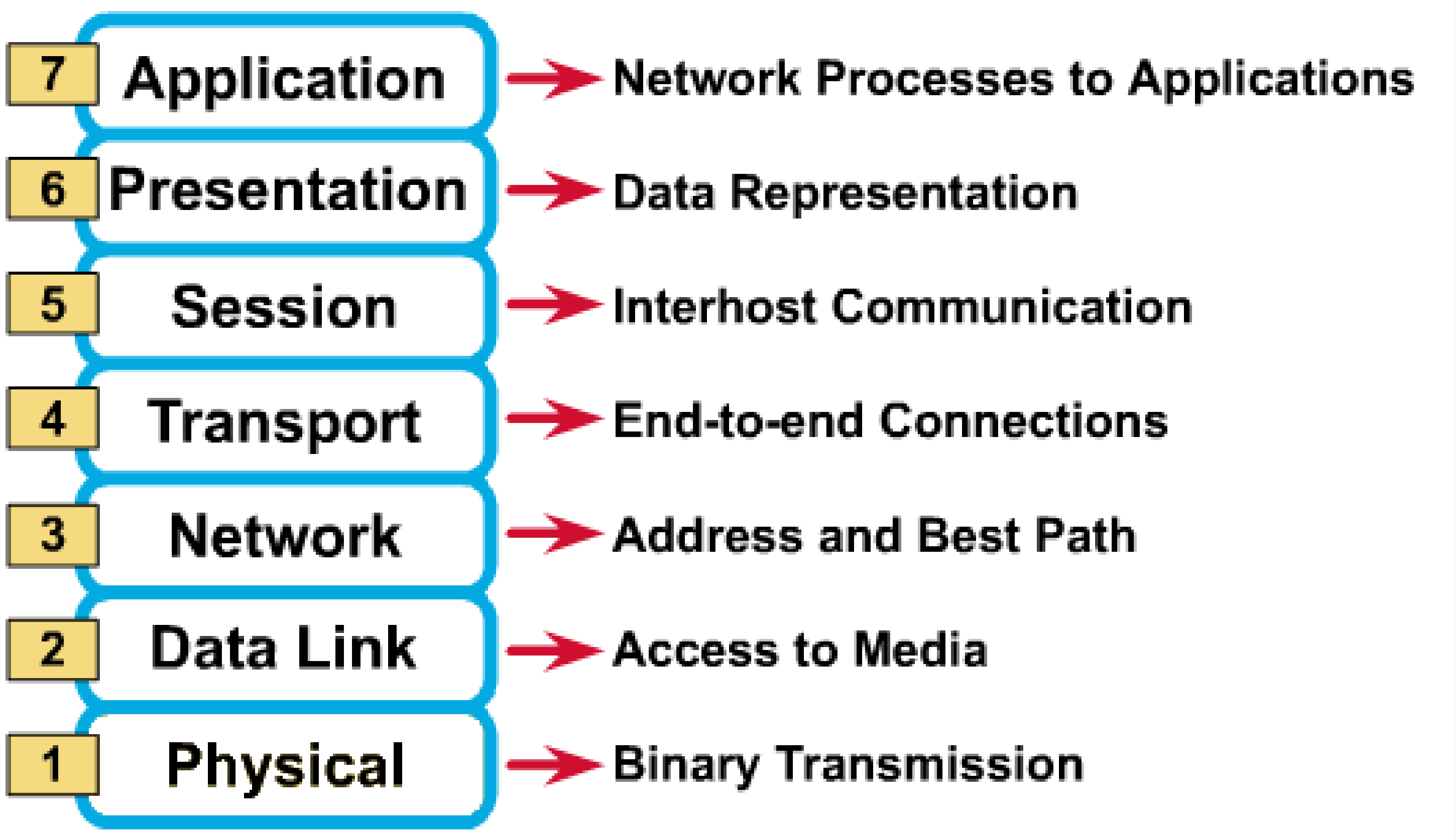
- The OSI model is now considered the primary Architectural model for inter-computer communications.

- The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.

- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems .

- This separation into smaller more manageable functions is known as layering.

OSI REFERENCE MODEL: 7 LAYERS



7	Application	Network Processes to Applications
6	Presentation	Data Representation
5	Session	Interhost Communication
4	Transport	End-to-end Connections
3	Network	Address and Best Path
2	Data Link	Access to Media
1	Physical	Binary Transmission

OSI: A LAYERED NETWORK MODEL

- The process of breaking up the functions or tasks of networking into layers reduces complexity.
- Each layer provides a service to the layer above it in the protocol specification.
- Each layer communicates with the same layer’s software or hardware on other computers.
- The lower 4 layers (transport, network, data link and physical —Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- The upper four layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.
- Data is Encapsulated with the necessary protocol information as it moves down the layers before network transit.

PHYSICAL LAYER

- Provides physical interface for transmission of information.
- Defines rules by which bits are passed from one system to another on a physical communication medium.
- Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.
- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

DATA LINK LAYER

- Data link layer attempts to provide reliable communication over the physical layer interface.
- Breaks the outgoing data into frames and reassemble the received frames.
- Create and detect frame boundaries.
- Handle errors by implementing an acknowledgement and retransmission scheme.
- Implement flow control.
- Supports points-to-point as well as broadcast communication.
- Supports simplex, half-duplex or full-duplex communication.

NETWORK LAYER

- Implements routing of frames (packets) through the network.
- Defines the most optimum path the packet should take from the source to the destination
- Defines logical addressing so that any endpoint can be identified.
- Handles congestion in the network.
- Facilitates interconnection between heterogeneous networks (Internetworking).
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

TRANSPORT LAYER

- Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.
- Ensures that the data units are delivered error free.
- Ensures that data units are delivered in sequence.
- Ensures that there is no loss or duplication of data units.
- Provides connectionless or connection oriented service.
- Provides for the connection management.
- Multiplex multiple connection over a single channel.

SESSION LAYER

- Session layer provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.

- This layer requests for a logical connection to be established on an end-user's request.
- Any necessary log-on or password validation is also handled by this layer.
- Session layer is also responsible for terminating the connection.
- This layer provides services like dialogue discipline which can be full duplex or half duplex.
- Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.

PRESENTATION LAYER

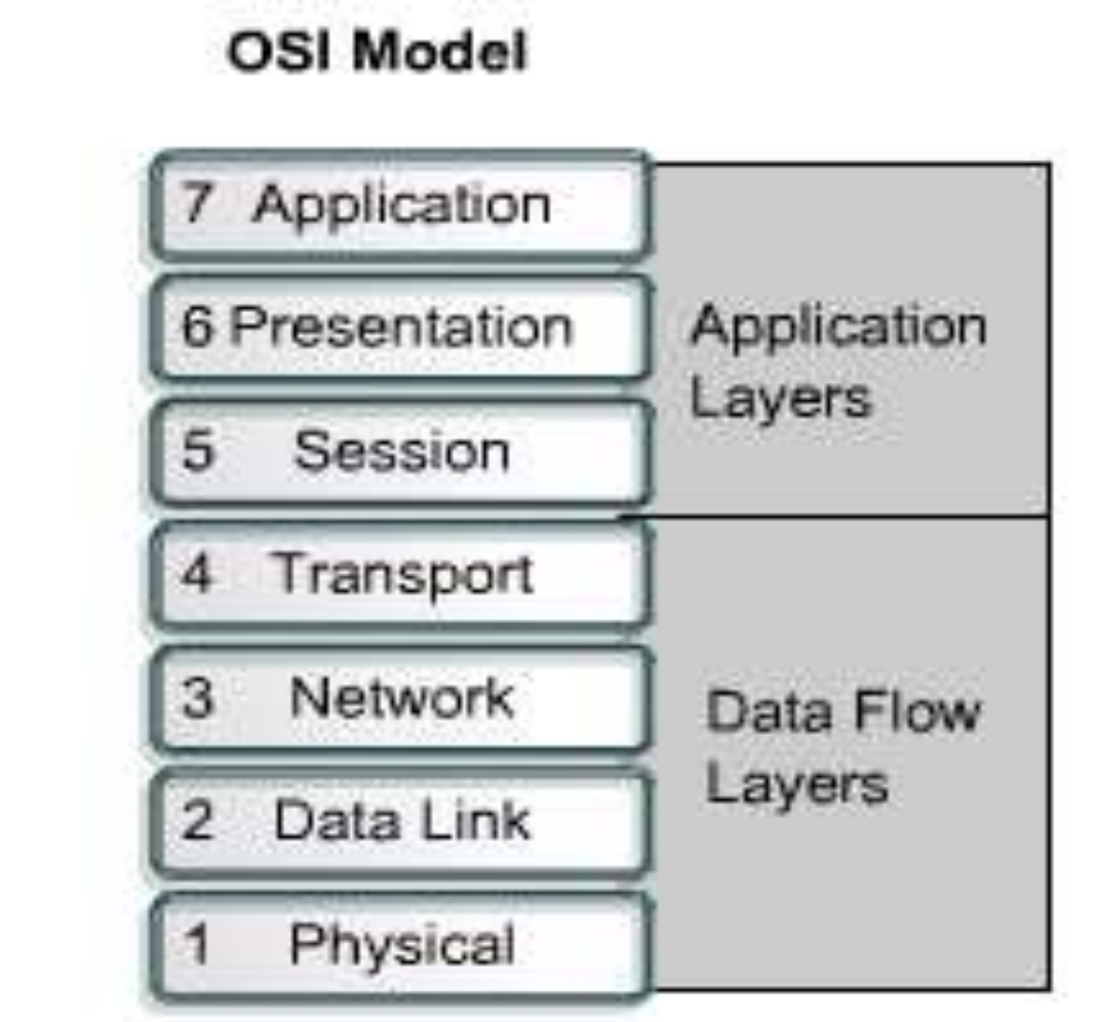
- Presentation layer defines the format in which the data is to be exchanged between the two communicating entities.
- Also handles data compression and data encryption (cryptography).

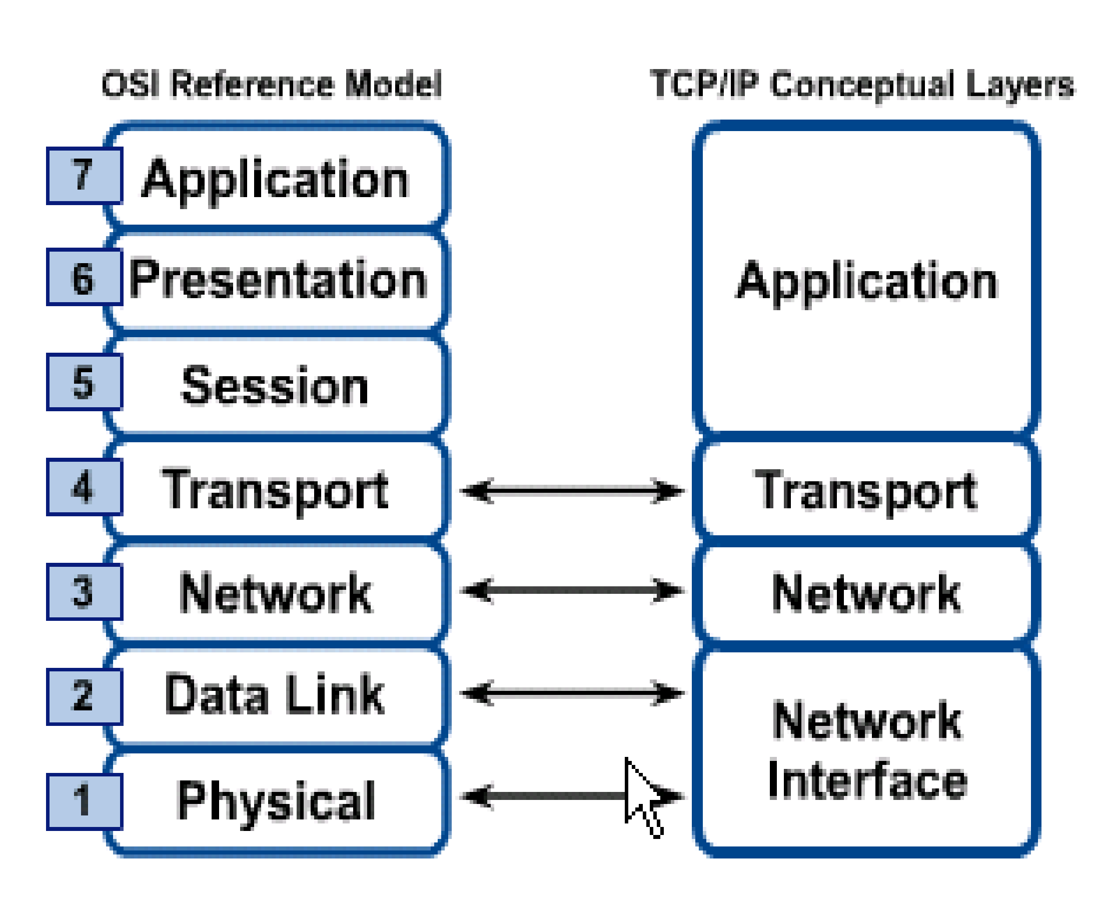
APPLICATION LAYER

- Application layer interacts with application programs and is the highest level of OSI model.
- Application layer contains management functions to support distributed applications.
- Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

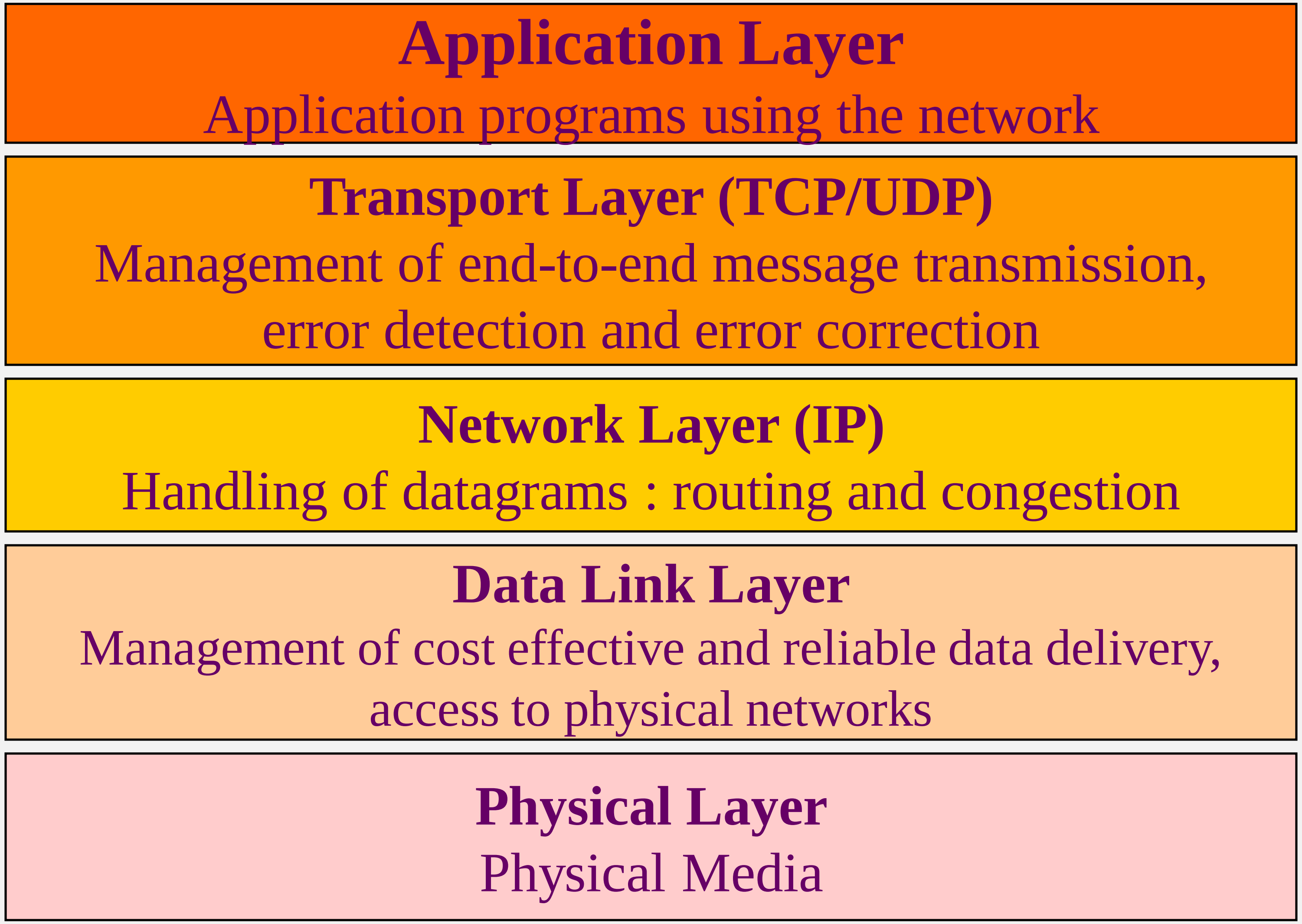
TCP/IP MODEL

OSI & TCP/IP MODELS





TCP/IP MODEL



Application Layer

Application programs using the network

Transport Layer (TCP/UDP)

Management of end-to-end message transmission, error detection and error correction

Network Layer (IP)

Handling of datagrams : routing and congestion

Data Link Layer

Management of cost effective and reliable data delivery, access to physical networks

Physical Layer

Physical Media

Networking Devices:

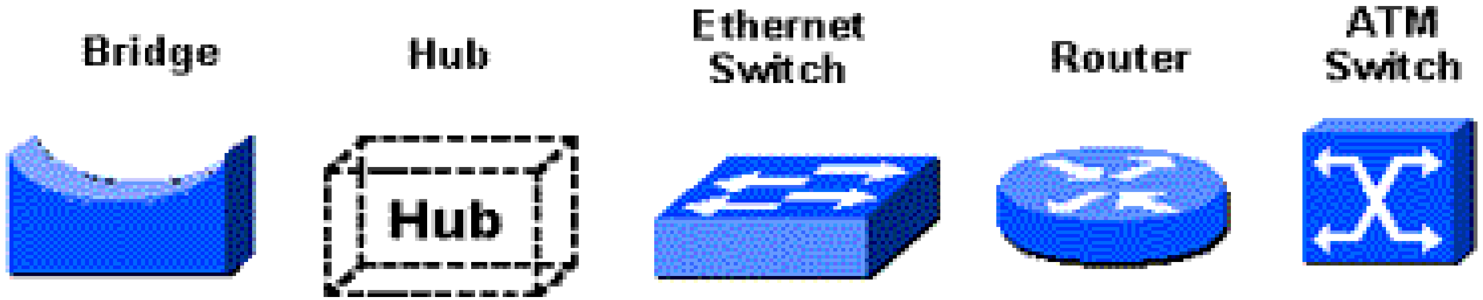
Networking devices are components used to connect computers or other electronic devices Together so that they can share files or resources like printers or fax machines.
These are also called communicating devices.
The following are the various networking devices.

- Repeater
- Hub
- Bridge
- Switch
- Router
- Gateway
- Brouter
- Modem
- Network Interface Card (NIC)

Local Area Networks and Devices

LANs are designed to:

- Operate within a limited geographic area
- Allow multiaccess to high-bandwidth media
- Control the network privately under local administration
- Provide full-time connectivity to local services
- Connect physically adjacent devices

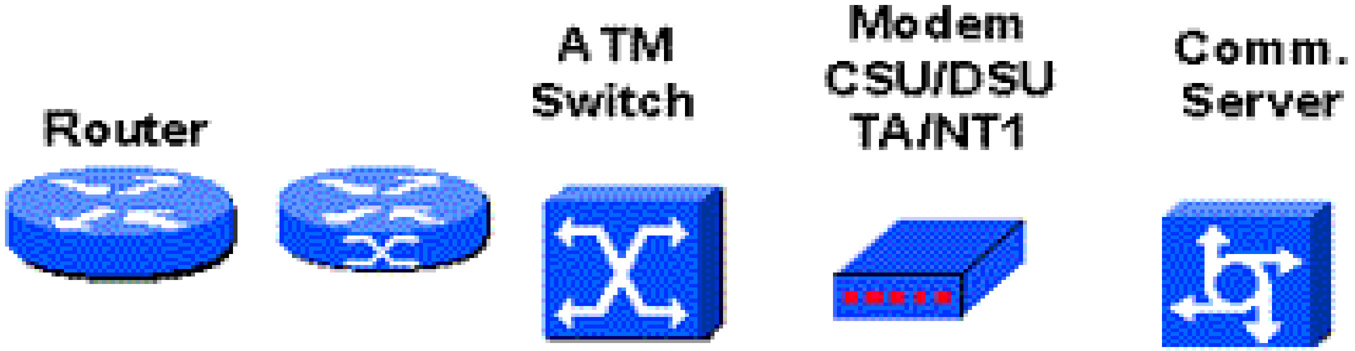


Next

Wide Area Networks and Devices

WANs are designed to:

- Operate over geography of telecommunications carriers
- Allow access over serial interfaces operating at lower speeds
- Control the network subject to regulated public services
- Provide full-time and part-time connectivity
- Connect devices separated over wide, even global areas



Router

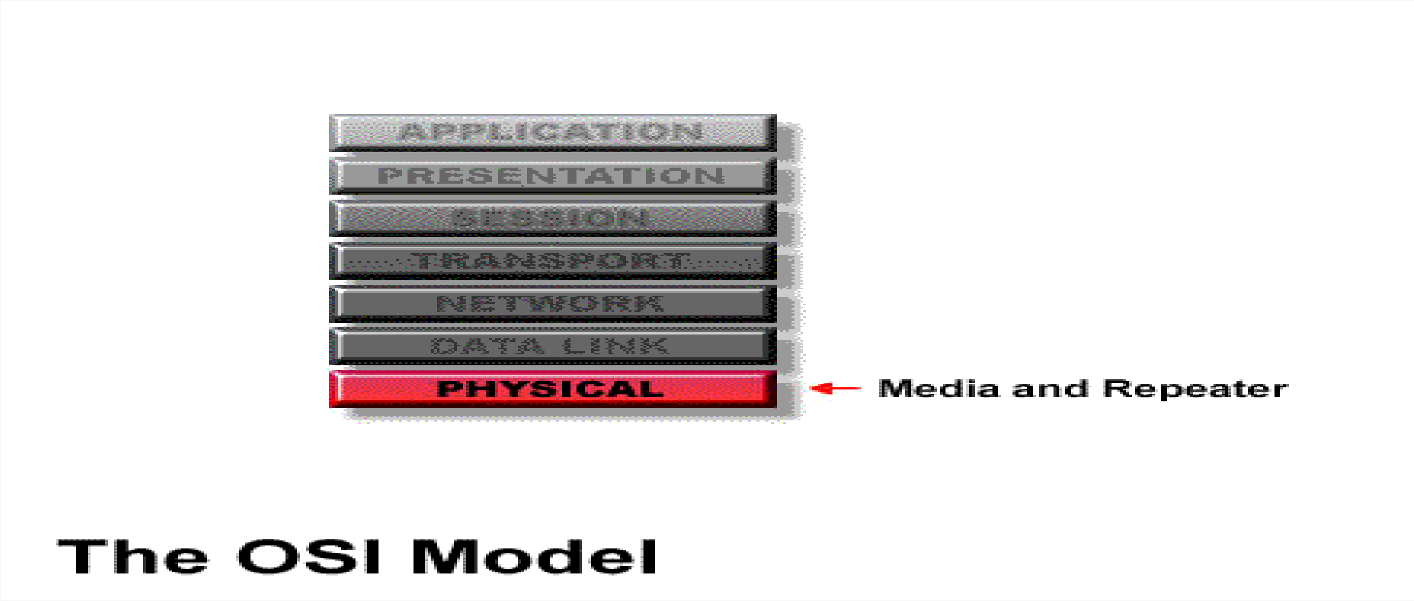
ATM Switch

Modem CSU/DSU TA/NT1

Comm. Server

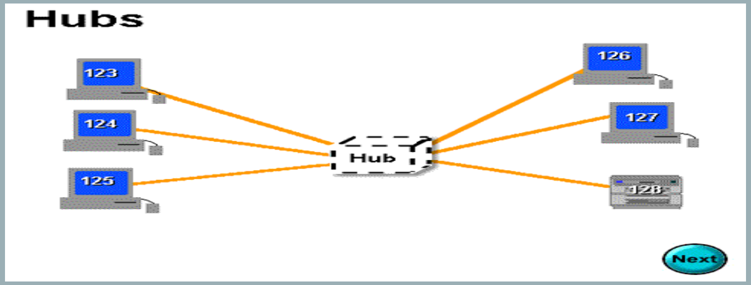
1. Repeater :

- A repeater operates at the physical layer. Its task is to regenerate the signal over the same network before the signal becomes too weak or corrupted.
- A repeater is a regenerator, not an amplifier.
- When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is 2 port device.



Hub :

- A hub is device used to connect several computers together.
- Hubs cannot filter data, so data packets are sent to all connected devices.
- Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.



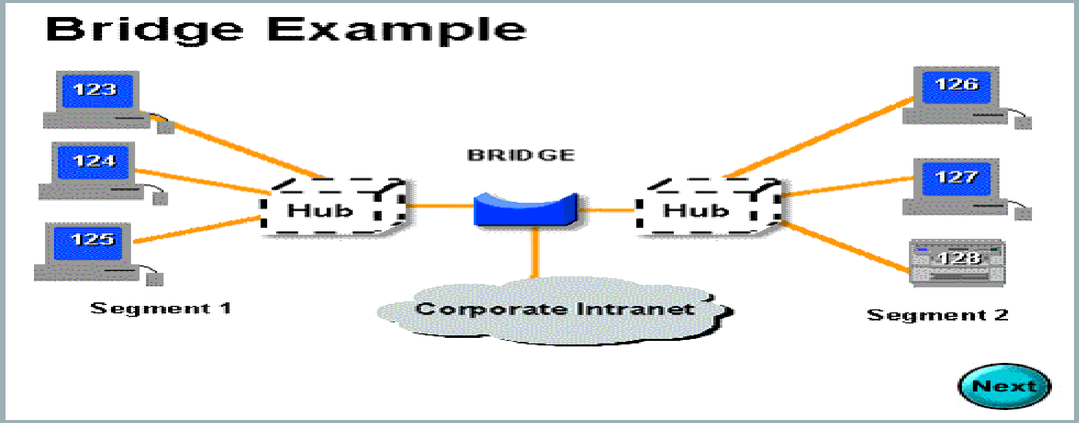
Types of Hub

Active Hub :- Active hubs use electronics to amplify and clean up the signal before it is broadcast to the other ports.

Passive Hub :- Passive hubs simply connect all ports together electrically and they are not powered.

3.Bridge:

- A bridge operates at data link layer.
- A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- Bridges can filter out noise.



4. Switch:

- A network switch is a computer networking device that connects network segments.
- Switch is data link layer device.
- Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

5. Routers:

- A router is a device like a switch that routes data packets based on their IP addresses.
- Router is mainly a Network Layer device.
- Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.

6. Gateway :

- A gateway is a passage to connect two networks together that may work upon different networking models.
- They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer.

7. Brouter:

- It is also known as bridging router is a device which combines features of both bridge and router.
- It can work either at data link layer or at network layer.
- Working as router, it is capable of routing packets across networks; working as bridge, it is capable of filtering local area network traffic.

8. Modem :

- Modem means Modulator- Demodulator.
- Modulation : digital information to analog signals.
- Demodulation: Analog signal back into digital information.

9. Network Interface Card (NIC):

- NIC provides physical interface between computer and cabling.
- NIC prepares data, sends data, and controls the flow of data.
- It can also receive and translate data into bytes for the CPU to understand.
- It has specific MAC address.

NETWORKS PROTOCOL AND STANDARD

Overview of Protocols and Standards in Computer Networks

INTRODUCTION

- Protocols and standards are rules for communication in networks.
- Protocols define how data is sent, received, and processed.
- Standards ensure compatibility between technologies.
- They ensure smooth and efficient network operations.

WHAT IS A PROTOCOL?

- Set of rules for data transmission.
- Like a language for devices.
- Covers data formatting, transmission, error handling, and security.

KEY ELEMENTS OF A PROTOCOL

- Syntax – Data format and structure.
- Semantics – Meaning of each message part.
- Timing – When and how fast data is sent.
- Sequence Control – Correct data order.
- Flow Control – Prevents congestion.
- Error Control – Detects/corrects errors.
- Security – Uses encryption/authentication.

TYPES OF PROTOCOLS

- Network Layer – IP, ICMP: Routing and addressing.
- Transport Layer – TCP, UDP: End-to-end delivery.
- Application Layer – HTTP, FTP, SMTP: App communication.
- Wireless – Wi-Fi, Bluetooth, LTE: Wireless transfer.
- Routing – RIP, OSPF, BGP: Path selection.
- Security – SSL, TLS: Secure communication.
- Internet Protocols – IP (v4/v6): Unique addressing.

IMPORTANT PROTOCOLS

- TCP – Reliable delivery with error checking.
- IP – Packet addressing and routing.
- HTTP/HTTPS – Web data transfer (secure with HTTPS).
- FTP – File sharing.
- SMTP – Email sending.
- DNS – Converts URLs to IP addresses.
- DHCP – Auto-assigns IP addresses.
- SSH – Secure remote access.
- SNMP – Network device monitoring.

PROTOCOLS IN CYBER ATTACKS

- Hackers exploit protocols (e.g., SYN flood attack on TCP).
- Security tools like Cloudflare filter and manage traffic.

WHAT IS A STANDARD?

- Set of accepted design rules for compatibility.
- Helps systems and devices work together.

TYPES OF STANDARDS

- De Facto – Widely used, not officially approved (e.g., Apple ecosystem).
- De Jure – Officially approved (e.g., by ISO, IEEE).
- Examples: TCP, IP, HTTP.

IMPORTANCE IN SECURITY

- Interoperability – Systems/devices can work together.
- Security Baseline – Implements best practices.
- Vulnerability Management – Identifies and fixes issues.

BEST PRACTICES FOR COMPLIANCE

- Use strong encryption tools.
- Perform regular security checks.
- Limit access to sensitive data zones.

CONCLUSION

- Protocols and standards enable secure, efficient communication.
- Ensure compatibility and protection from cyber threats.