R. C. PATEL
INSTITUTE OF TECHNOLOGY
An Autonomous Institute

Introduction to Networking

Patil Mayur J.
Assistant Professor
Department of Computer Engineering
R. C. Patel Institute of Technology, Shirpur

January 30, 2023

Outline I

1. Introduction to Computer Networks
2. Computer Network Applications
3. Network S/W & H/W Component
3.1 Hardware Component
3.2 Software Component
4. Network Topology
5. Types of Network Topology
5.1 Point to Point Topology
5.2 Star Topology
5.3 Bus Topology
5.4 Ring Topology
5.5 Mesh Topology
5.6 Tree Topology
5.7 Hybrid Topology
6. Design Issues for the Layers
7. Reference Model in Computer Network

Outline II

7.1 TCP/IP Reference Model
7.2 Application Layer
7.3 Transport Layer
7.4 Internet Layer
7.5 Network Interface Layer

8. OSI Reference Model
8.1 Physical Layer
8.2 Data Link Layer
8.3 Network Layer
8.4 Transport Layer
8.5 Session Layer
8.6 Presentation Layer
8.7 Application Layer

- We are living in a connected world.
- Information is being produced, exchanged, and traced across the globe in real time.
- It's possible as almost everyone and everything in the digital world is interconnected through one way or the other.
- A group of two or more similar things or people interconnected with each other is called **network.**

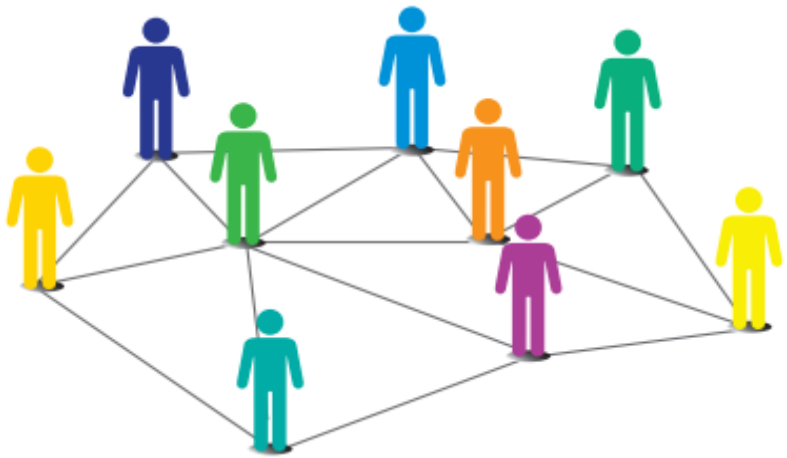


Figure: Interconnection forming a social network

- The term **telecommunication** means communication at a distance.
- The word **data** refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- **Data communications** are the exchange of data between two devices via some form of transmission medium such as a wire cable or wireless.
- The term **Network** means a group, chain or a collection of something that come together for the purpose of communication.

- A **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.

OR

- A **Computer Network** is a system that connects numerous independent computers in order to share information (data) and resources.

OR

- A **Computer Network** is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media.

- A **Computer Network** is a set of **devices (nodes)** connected by communication links.
- A **Node** can be a **computer, printer, or any other device** capable of sending and/or receiving data generated by other nodes on the network.
- **Servers, networking hardware, personal computers, and other specialized or general-purpose hosts** can all be nodes in a computer network.
- The aim of the computer network is the sharing of resources among various devices.
- In the case of computer network technology, there are several types of networks that vary from simple to complex level.

- A group of computers which are connected to each other and follow similar usage protocols for the purpose of sharing information and having communications provided by the networking nodes is called a **Computer Network.**
- A network may be small where it may include just one system or maybe as large as what one may want.
- The nodes may further be classified into various types.
- These includes
  1. Personal Computers
  2. Servers
  3. Networking Hardware
  4. General Hosts

Evolution of Computer Networks

1961 — **The idea of Advanced Research Project Agency Network (ARPANET) is conceptualized**

Evolution of Computer Networks

1961 The idea of Advanced Research Project Agency Network (ARPANET) is conceptualized

1969 ARPANET became functional by connecting University of California, Los Angeles (UCLA) and Stanford Research Institute (SRI)

Evolution of Computer Networks

- **1961** — **The idea of Advanced Research Project Agency Network (ARPANET) is conceptualized**
- **1969** — **ARPANET became functional by connecting University of California, Los Angeles (UCLA) and Stanford Research Institute (SRI)**
- **1971** — Roy Tomlinson develops network messaging or E-mail. Symbol @ comes to mean "at"

Evolution of Computer Networks

- **1961** The idea of Advanced Research Project Agency Network (ARPANET) is conceptualized
- **1969** ARPANET became functional by connecting University of California, Los Angeles (UCLA) and Stanford Research Institute (SRI)
- **1971** Roy Tomlinson develops network messaging or E-mail. Symbol @ comes to mean "at"
- **1974** The term Internet was coined, First commercial use of ARPANET, was started in the name of Telenet

Evolution of Computer Networks

- **1961** The idea of Advanced Research Project Agency Network (ARPANET) is conceptualized
- **1969** ARPANET became functional by connecting University of California, Los Angeles (UCLA) and Stanford Research Institute (SRI)
- **1971** Roy Tomlinson develops network messaging or E-mail. Symbol @ comes to mean "at"
- **1974** The term Internet was coined, First commercial use of ARPANET, was started in the name of Telenet
- **1982** TCP/IP introduced as standard protocol on ARPANET

Evolution of Computer Networks

- **1961** The idea of Advanced Research Project Agency Network (ARPANET) is conceptualized
- **1969** ARPANET became functional by connecting University of California, Los Angeles (UCLA) and Stanford Research Institute (SRI)
- **1971** Roy Tomlinson develops network messaging or E-mail. Symbol @ comes to mean "at"
- **1974** The term Internet was coined, First commercial use of ARPANET, was started in the name of Telenet
- **1982** TCP/IP introduced as standard protocol on ARPANET
- **1983** Domain Name System introduced

Evolution of Computer Networks

- **1961** The idea of Advanced Research Project Agency Network (ARPANET) is conceptualized
- **1969** ARPANET became functional by connecting University of California, Los Angeles (UCLA) and Stanford Research Institute (SRI)
- **1971** Roy Tomlinson develops network messaging or E-mail. Symbol @ comes to mean "at"
- **1974** The term Internet was coined, First commercial use of ARPANET, was started in the name of Telenet
- **1982** TCP/IP introduced as standard protocol on ARPANET
- **1983** Domain Name System introduced
- **1986** National Science Foundation brings connectivity to more people with its NSFNET program

[1] WPA:- Wi-Fi Protected Access

1990 **The Berners-Lee at CERN developed HTML and URL, thus giving birth to World Wide Web (www)**

[1] WPA:- Wi-Fi Protected Access

Evolution of Computer Networks Contd...

1990 **The Berners-Lee at CERN developed HTML and URL, thus giving birth to World Wide Web (www)**

1997 **First version of Wi-fi (802.11) standard was introduced**

[1] WPA:- Wi-Fi Protected Access

- **1990** The Berners-Lee at CERN developed HTML and URL, thus giving birth to World Wide Web (www)
- **1997** First version of Wi-fi (802.11) standard was introduced
- **1999** The 802.11a standard for Wi-Fi was made official in 1999, designed to use the 5 GHz band and provide transmission speeds up to 25 Mbps.

[1] WPA:- Wi-Fi Protected Access

- **1990** The Berners-Lee at CERN developed HTML and URL, thus giving birth to World Wide Web (www)
- **1997** First version of Wi-fi (802.11) standard was introduced
- **1999** The 802.11a standard for Wi-Fi was made official in 1999, designed to use the 5 GHz band and provide transmission speeds up to 25 Mbps.
- **1999** The WEP encryption protocol for Wi-Fi is introduced in September 1999, for use with 802.11b.

[1] WPA:- Wi-Fi Protected Access

Evolution of Computer Networks Contd...

- **1990** The Berners-Lee at CERN developed HTML and URL, thus giving birth to World Wide Web (www)
- **1997** First version of Wi-fi (802.11) standard was introduced
- **1999** The 802.11a standard for Wi-Fi was made official in 1999, designed to use the 5 GHz band and provide transmission speeds up to 25 Mbps.
- **1999** The WEP encryption protocol for Wi-Fi is introduced in September 1999, for use with 802.11b.
- **2003** 802.11g devices were available to the public starting in January 2003, providing transmission speeds up to 20 Mbps.

[1] WPA:- Wi-Fi Protected Access

Evolution of Computer Networks Contd...

- **1990** The Berners-Lee at CERN developed HTML and URL, thus giving birth to World Wide Web (www)
- **1997** First version of Wi-fi (802.11) standard was introduced
- **1999** The 802.11a standard for Wi-Fi was made official in 1999, designed to use the 5 GHz band and provide transmission speeds up to 25 Mbps.
- **1999** The WEP encryption protocol for Wi-Fi is introduced in September 1999, for use with 802.11b.
- **2003** 802.11g devices were available to the public starting in January 2003, providing transmission speeds up to 20 Mbps.
- **2003** The WPA [1] encryption protocol for Wi-Fi is introduced in 2003, for use with 802.11g.

[1] WPA:- Wi-Fi Protected Access

Evolution of Computer Networks Contd...

2003 — **The WPA2 encryption protocol is introduced in 2004, as an improvement over and replacement for WPA. All Wi-Fi devices are required to be WPA2 certified by 2006.**

2003 **The WPA2 encryption protocol is introduced in 2004, as an improvement over and replacement for WPA. All Wi-Fi devices are required to be WPA2 certified by 2006.**

2009 The 802.11n standard for Wi-Fi was made official in 2009. It provides higher transfer speeds over 802.11a and 802.11g, and it can operate on the 2.4 GHz and 5 GHz bandwidths.

- **2003** — **The WPA2 encryption protocol is introduced in 2004, as an improvement over and replacement for WPA. All Wi-Fi devices are required to be WPA2 certified by 2006.**
- **2009** — The 802.11n standard for Wi-Fi was made official in 2009. It provides higher transfer speeds over 802.11a and 802.11g, and it can operate on the 2.4 GHz and 5 GHz bandwidths.
- **2018** — **The Wi-Fi Alliance introduced WPA3 encryption for Wi-Fi in January 2018, which includes security enhancements over WPA2.**

Components of Computer Network

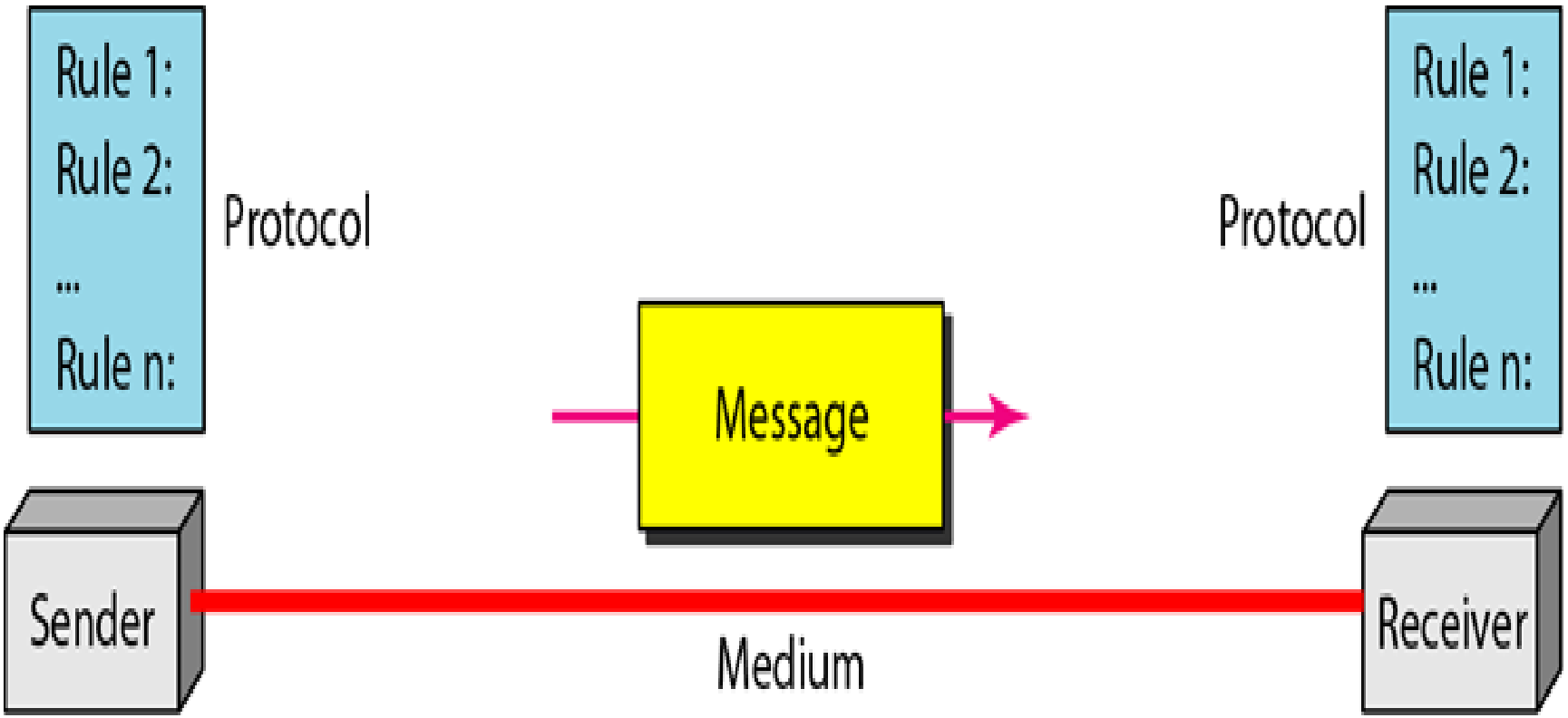


Figure: Components of Computer Network

- There are five basic components of a computer network

1. **Message**: It is the data or information which needs to be transferred from one device to another device over a computer network.
2. **Sender**: Sender is the device that has the data and needs to send the data to other device connected to the network.
3. **Receiver**: A receiver is the device which is expecting the data from other device on the network.
4. **Protocol**: A protocol is a set of rules that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol.
5. **Transmission Media**: In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.

Communication

- People can communicate with each other around the world through Computer Networks.
- They can talk and share information with each other using different network services such as email, social networking, video conferencing, groupware, wikis, blogs, and SMS services.

Data Sharing

- Different users connected to the computer network can share data among them.
- For Example, on the Internet, a large number of users can access the same database in the network.

Software Sharing

- In a computer network, usually, application software is installed on a centralized computer (Server Computer).
- This software can be shared over the network instead of purchasing a separate copy of the software for each other.

Hardware Sharing

- In a Computer Network, Hardware devices such as Printers, Access points, HDD, SATA, SSD, Drivers, etc.
- For example, many users can share a single printer connected to the network.

Internet Sharing

- In a computer network, many users can access the internet through single internet and can use different services.
- For example, our campus internet connectivity.

Centralized Software Management

- All the software is installed or updated on one server computer.
- This saves time for installing/updating the individual computer in the network.
- Users connected to the network can access these software programs.

Data Security and Management

- The computer network provides centralized data storage.
- It means that all the data is stored on a centralized server.
- A system administrator has full control and can read or change critical information.
- A system administrator can take the backup of data very easily.
- Security features can also be implemented on the data very easily.

Entertainment

- Computer Network provides many sources of entertainment to people.
- For example, we can play different types of games, see movies, and listen to music.

Saving Disk Space

- Applications of Computer Networks play a vital In a computer network.
- All computers use the same copy of the application programs and data files.
- These are only stored on the hard disks on the server computer.
- There is no need to store the application programs and data files on an individual's computer on the networks.
- In this way, disk space on each computer is saved.

Remote Access

- A network also provides the facilities to access the data remotely.
- A user can access and update data by connecting to the network from anywhere in the world.

Advantages of Computer Network

- **Increased Storage Capacity**
  - You will be able to access files and multimedia, such as music and images, which are stored remotely on another computer or network-attached storage.
- **Higher Information Security**
  - As a result of granting authorization to computers, computer networks can provide a sense of security.
  - Most of the time, authorization is done using a user ID and password.
  - Thus, it ensures that someone can only log in if their information matches details in the database.
- **Easy sharing of files**
  - The data you store on other devices can be shared with other users and accessed remotely if they are connected.

- **Faster resources sharing**
  - You can also save money by using networked resources like printers, scanners, copiers, etc. or by sharing software among multiple users.
- **Improved communication**
  - Customers, suppliers and the staff can easily share information and contact one another via email, chat or calls made over the network.
- **Better collaboration**
  - Collaboration in the business world is made easier with the use of computers and a computer network.
  - All these tasks can be performed comfortably, whether it's connecting teams, arranging social gatherings, or acquiring personal responses.

Advantages of Computer Network Contd...

- **Higher connectivity**
  - It allows individuals to stay connected no matter where they are.
  - With the advent of video calling apps and Google documents, we can see live examples of how we can connect with our friends and colleagues in these testing times.
- **Enhanced flexibility**
  - Here, flexibility means that different people will be able to explore different things as per their requirements.
  - For this purpose, computer networks provide you a wide array of choices to share a particular piece of information.
  - For example, e-mail or messaging apps like Whatsapp. So, there is flexibility for different users.
- **Reliability**
  - Computer networking ensures information backup for uninterrupted functioning.
  - So, you need not worry about device and equipment crash anymore.

Disadvantages of Computer Network

- **Network Setup Costs**
  - Setting up the network requires hardware like routers, hubs and switches and cabling that can cost significantly.
  - The cost further varies based on the number of systems to be added to the network.
- **Issues with Independent Usage**
  - Because everything is centralized, the network lacks independence.
  - As a result, individual users cannot use the computer as they wish.
- **Malware Infection**
  - Viruses or Malware can propagate easily between the connected computers in a network.
  - It is quite likely that malware will spread to the remaining computers if one of the systems gets infected.
  - However, this can be prevented by running regular malware scans.

Disadvantages of Computer Network Contd..

- **Expert Assistance is Required**
  - Networks must be monitored continuously to ensure their performance and functionality.
  - Therefore, if you want to maintain your computer network, you need a team of experts.
- **Lack of Independence**
  - Since most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever.
  - Centralized decision making can sometimes hinder how a client user wants to use his own computer.
- **Lack of Robustness**
  - If a computer network's main server breaks down, the entire system would become useless.
  - Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill.

Disadvantages of Computer Network Contd..

- **Security of Computer Networks is a Concern**
  - From viruses to hackers, there are many ways in which computer networks can be disrupted.
  - DDoS attacks, viruses, data corruption, and internet outages are just a few examples of disruptions you might see on a day to day basis.
  - Regardless of whether a network is running online or offline, it will not be 100% secure.
- **Health Issues**
  - Since computer networks provide access to a variety of content such as entertainment, games, and movies, this leads to an addictive dependence on the services and overuse.
- **Maintainance**
  - For the proper functioning of a computer network, it requires regular maintenance.
  - The problem is this cannot be done with basic skills.
  - It involves advanced configurations and complicated installations.

Key Terms for Networking

1. **Performance**
   - It is measured in terms of transit time and response time.
     - Transit time is the time for a message to travel from one device to another
     - Response time is the elapsed time between an inquiry and a response.
   - **Performance** is dependent on the following factors:
     - The number of users
     - Type of transmission medium
     - Capability of connected network
     - Efficiency of software
2. **Reliability**
   - It is measured in terms of
     - Frequency of failure
     - Recovery from failures
3. **Security**
   - It means protecting data from unauthorized access.

Computer Network Application

- **Resource Sharing**
  - Resource sharing means you can share one Hardware and Software among multiple users.
  - Hardware includes printers, disks, fax machines, & computing devices.
  - Software includes Oracle VM Virtual Box, Android Studio, etc.
- **Information Sharing**
  - Using a Computer network, we can share Information over the network, and it provides Search capabilities such as **WWW**.
  - Over the network, a single information can be shared among the many users over the internet.
- **Communication**
  - Communication includes email, calls, message broadcast, electronic funds transfer system etc.

- **Entertainment Industry**
  - In Entertainment industry also uses computer networks widely.
  - Some of the Entertainment industries are Video on demand, Multi-person real-time simulation games, movie/TV programs, etc.
- **Access to Remote Databases**
  - Computer networks allow us to access the Remote Database of the various applications by the end-users.
  - Some applications are Reservation for Hotels, Airplane Booking, Net Banking, Automated Library etc.
- **Business Applications**
  - The result of business application here is resource sharing.
  - The purpose of resource sharing is that without moving to the physical location of the resource, all the data, plans, and tools can be shared to any network user.
  - Most of the companies are doing business electronically with other companies and with other clients worldwide with the help of a computer network.

- **Social Media**
  - Social media is also a great example of a computer network application.
  - It helps people to share and receive any information related to political, ethical, and social issues.
- **E-Commerce**
  - A goal that is starting to become more important in businesses is doing business with consumers over the Internet.
  - Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home.
  - This sector is expected to grow quickly in the future.
- **Groupware**
  - These applications are used to automate the administrative functions of a modern office for video conferencing and chatting.
  - They facilitate the work of groups for increased productivity; they can be used to communicate, co-operate, coordinate, solve problems, compete, and negotiate.

Network S/W & H/W Component

- Computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home.
- A **hardware** component is any physical component of a network.
- This includes things like cables, servers, switches, and routers.
- A **software** components are the programs or applications that run on these devices.
- Software includes things like operating systems, antivirus software, and networking tools.
- Computer networks use nodes to transfer information.
- **Nodes** are typically devices like servers, routers, and switches.
- The figure (next slide) shows a network along with its components.

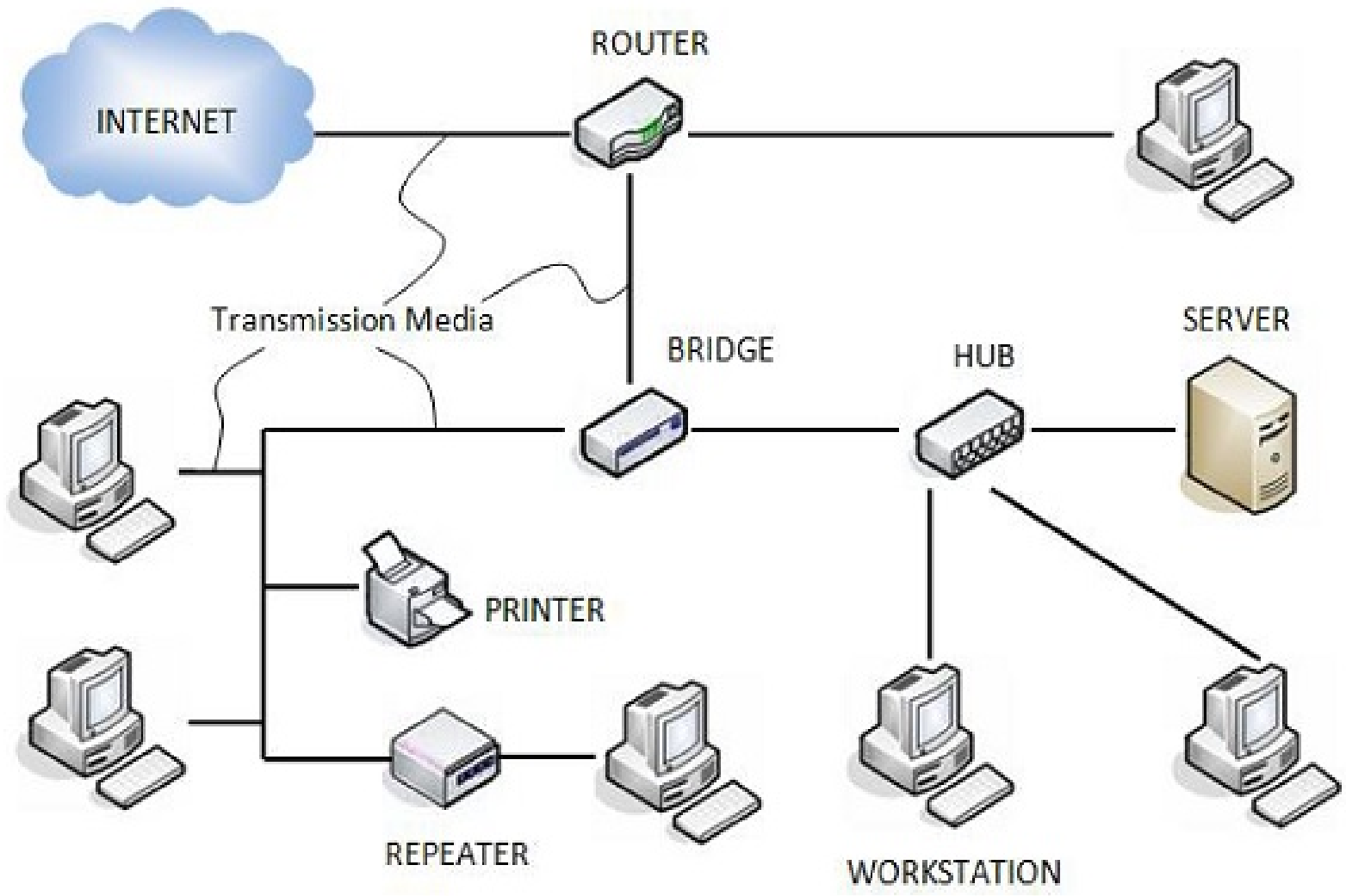


Figure: Network Component

Hardware Component

- **Servers**
  - Servers are high-configuration computers that manage the resources of the network.
  - The network operating system is typically installed in the server and so they give user accesses to the network resources.
  - Servers can be of various kinds:
    1. File Server
    2. Database Server
    3. Print Server
    4. Mail Server
- **Clients**
  - Clients are computers that request and receive service from the servers to access and use the network resources.
- **Peers**
  - Peers are computers that provide as well as receive services from other peers in a workgroup network.

- **Transmission Media**
  - Transmission media are the channels through which data is transferred from one device to another in a network.
  - Transmission media may be guided media like **coaxial cable, fibre optic cables** etc; or maybe unguided media like **microwaves, infra-red waves** etc.
- **Connecting Devices**
  - Connecting devices act as middleware between networks or computers, by binding the network media together.
  - Some of the common connecting devices are:
    1. Router
    2. Switch
    3. Bridge
    4. Hub
    5. Repeater
    6. Gateway

- **Network Operating System**
  - Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
- **Protocol Suite**
  - A **protocol** is a rule or guideline followed by each computer for data communication.
  - Protocol suite is a set of related protocols that are laid down for computer networks.
  - The two popular protocol suites are
    1. OSI Model (Open System Interconnections)
    2. TCP/IP Model

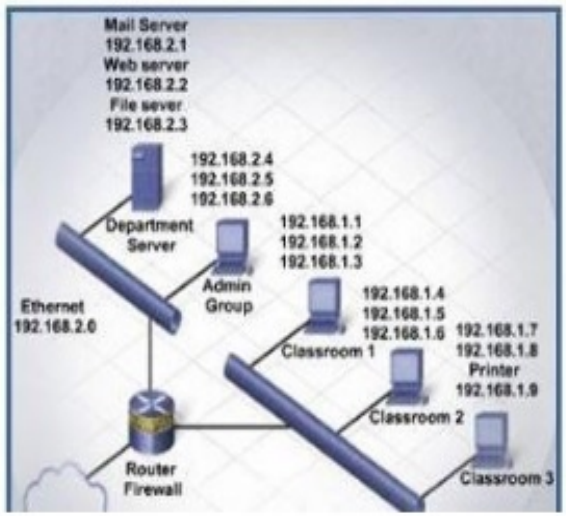
Network Topology

- The configuration, or topology, of a network is key to determining its performance.
- Network topology is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other.
- **Network Topology** refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other.
- Think of your network as a city, and the topology as the road map.
- Topologies may define both physical and logical aspect of the network.
- Both logical and physical topologies could be same or different in a same network.

Network Topology Contd...

- **Physical Topology**
  - The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged.
  - Setup, maintenance, and provisioning tasks require insight into the physical network.
- **Logical Topology**
  - The logical network topology is a higher-level idea of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network.
  - Logical network topology includes any virtual and cloud resources.
- Effective network management and monitoring require a strong grasp of both the physical and logical topology of a network to ensure your network is efficient and healthy.

Network Topology Contd...



Physical topology is the physical layout of the components on the network.

Logical topology determines how the hosts access the medium to communicate across the network.

Figure: Physical & Logical Topology

Physical vs Logical Topology

Physical Topology	Logical Topology
Physical Topology means the physical layout of the network.	Logical topology means how the network device layout will be shown and how the data will be transferred.
In this topology, we are concerned with how data will be transferred from the actual path.	This topology is concerned with the high-level representation of the data transfer.
As per the requirement, we can modify the layout of the network.	There is no change accepted.
It can affect cost, bandwidth, scalability etc.	It can affect data delivery.

Physical vs Logical Topology Contd...

Physical Topology	Logical Topology
Types of physical topologies are star, mesh, bus, and ring.	Types of logical topologies are logical bus, and logical ring.
It is an actual route concerned with transmission.	It is a high level representation of data flow.
Physical connection of the network.	Data path followed on the network.
For example Ring, Bus, Star, and Mesh.	For example Ring and Bus.

Types of Network Topology

- Network topology plays a major role in how a network functions.
- The topology has a direct effect on network functionality.
- Choosing the right topology can help increase performance, as a properly chosen and maintained network topology increases energy efficiency and data transfer rates.
- A well-defined network topology makes it easier for network admins to locate faults, troubleshoot issues and to allocate network resources.
- Following are the types of network topology,
  1. **Point to Point**
  2. **Star Topology**
  3. **Bus Topology**
  4. **Ring Topology**
  5. **Mesh Topology**
  6. **Tree Topology**
  7. **Hybrid Topology**

Point to Point Topology

- Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable.
- The receiving end of one host is connected to sending end of the other and vice-versa.
- Point to Point topology is the simplest topology that connects two nodes directly together with a common link.
- The entire bandwidth of the common link is reserved for transmission between those two nodes.
- The point-to-point connections use an actual length of wire or cable to connect the two ends.
- When you change TV channels by remote, you are establishing a point-to-point connection between the remote control and the TV's control system.

Figure: Point to Point Topology

- This simplistic topology is very easy to install and maintain, and it is designed for very small networks.
- This type of network has a major disadvantage that it can only handle two nodes in a network.
- One common example of this point-to-point topology is that a PC connected to a printer.

Advantages of Point to Point Topology

- Highest Bandwidth because there is only two nodes having entire bandwidth of a link.
- Very fast compared to other network topologies because it can access only two nodes.
- Very simple connectivity.
- It provides low Latency.
- Easy to handle and maintain.
- Node Can be Replaced in few seconds.

Disadvantages of Point to Point Topology

- This topology is only used for small areas where nodes are closely located.
- The entire network depends on the common channel in case of link broken entire network will become dead.
- There is another major drawback of this topology there are only two nodes if any of the node stops working, data cannot be transfer across the network.
- For example, if there are two PCs in the network and one of them breaks, you cannot transfer or receive information from a broken PC.

Star Topology

- All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection.
- That is, there exists a point to point connection between hosts and hub.
- The hub device can be any of the following:
  1. Layer-1 device such as hub or repeater
  2. Layer-2 device such as switch or bridge
  3. Layer-3 device such as router or gateway
- As in Star topology, hub acts as single point of failure.
- If hub fails, connectivity of all hosts to all other hosts fails.
- Every communication between hosts, takes place through only the hub.
- Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Star Topology Contd...

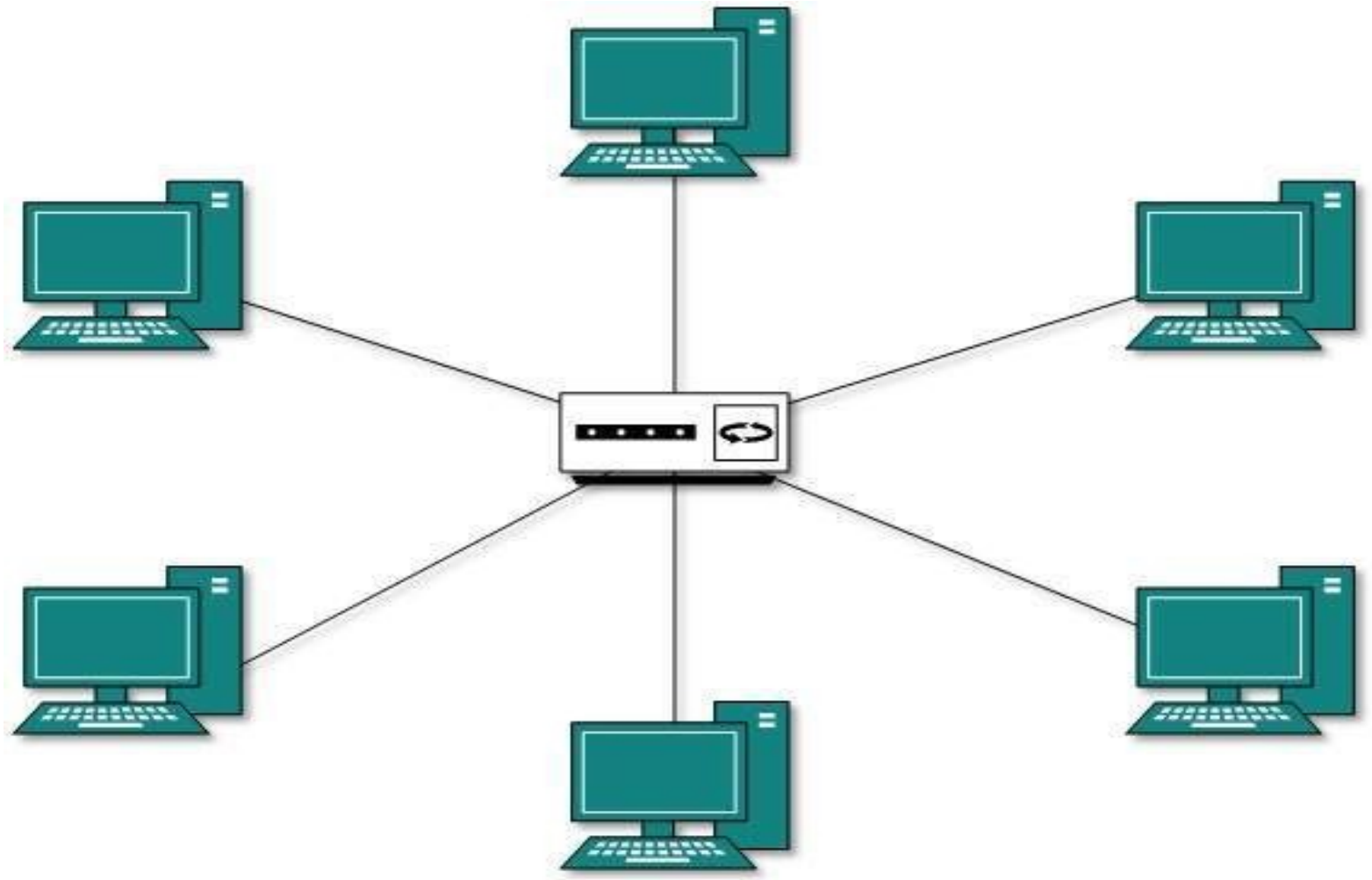


Figure: Star Topology

Advantages of Star Topology

- **Efficient troubleshooting**
  - Troubleshooting is quite efficient in a star topology as compared to bus topology.
  - In a star topology, all the stations are connected to the centralized network.
  - Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **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.

Advantages of Star Topology Contd...

- **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 or RJ-45 cables are used to connect the computers.
- **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.

Bus Topology

- In case of Bus topology, all devices share single communication line or cable.
- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the 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.

Bus Topology Contd...

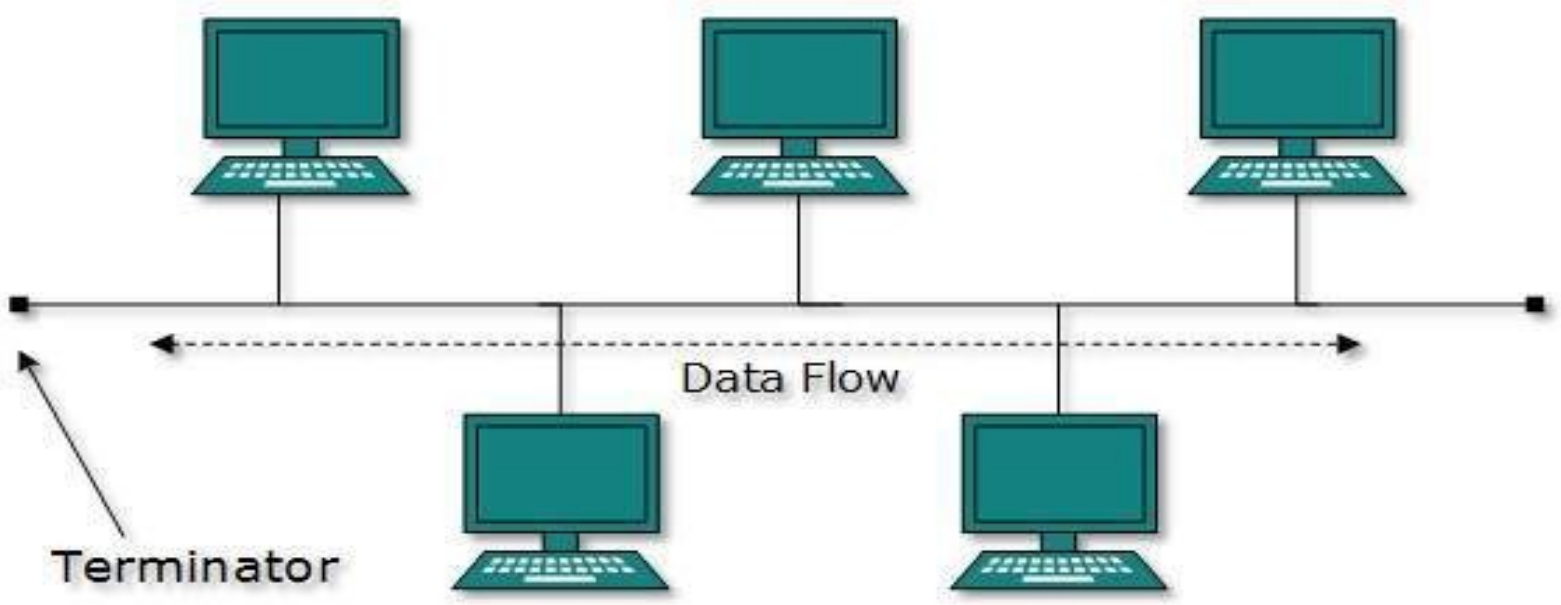


Figure: Bus Topology

- The backbone cable is considered as a "single lane" through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA (Carrier Sense Multiple Access)**.

- **CSMA**
  - It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost.
  - There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

1. **CSMA/CD**
   - **CSMA/CD (Collision Detection)** is an access method used to detect the collision.
   - Once the collision is detected, the sender will stop transmitting the data.
   - Therefore, it works on **"recovery after the collision".**
2. **CSMA/CA**
   - **CSMA/CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not.
   - If busy, then the sender waits until the media becomes idle.
   - This technique effectively reduces the possibility of the collision.
   - Therefore, it does not works on **"recovery after the collision".**

Advantages 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 upto **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.

Disadvantages 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

- In ring topology, each host machine connects to exactly two other machines, creating a circular network structure.
- The node that receives the message from the previous computer will re-transmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing.**

Ring Topology Contd...

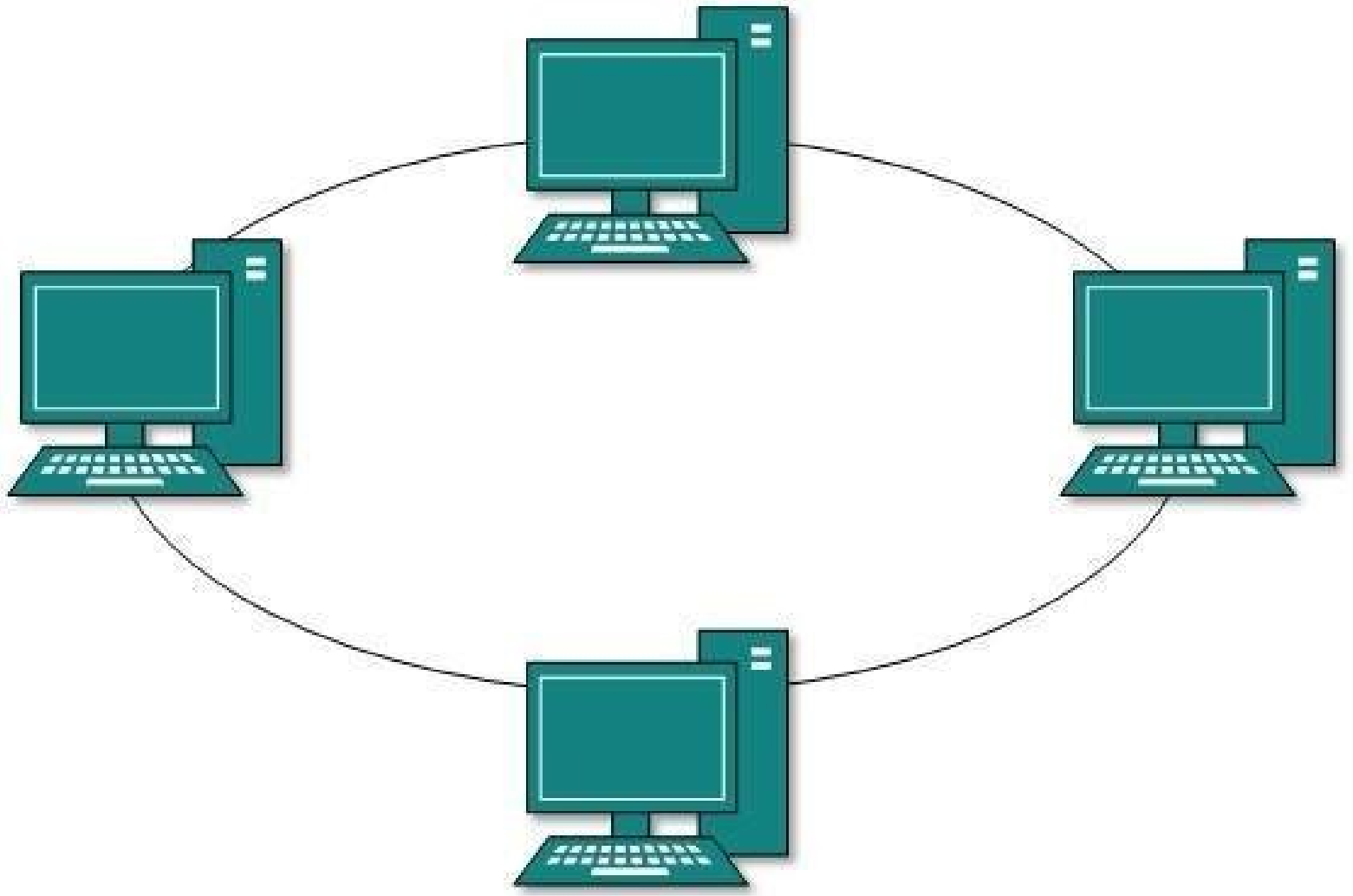


Figure: Ring Topology

Ring Topology Contd...

- **Token Passing** is a network access method in which token is passed from one node to another node.
- **Token** is a frame that circulates around the network.
- **Working of Token Passing**
  - A token moves around the network, and it is passed from computer to computer until it reaches the destination.
  - The sender modifies the token by putting the address along with the data.
  - The data is passed from one device to another device until the destination address matches.
  - Once the token received by the destination device, then it sends the acknowledgment to the sender.
  - In a ring topology, a token is used as a carrier.

Advantages 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.
- **Delay**
  - Communication delay is directly proportional to the number of nodes.
  - Adding new devices increases the communication delay.
- **Reconfiguration difficult**
  - Adding new devices to the network would slow down the network.

Mesh Topology

- In this type of topology, a host is connected to one or multiple hosts.
- 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:

$$Number\ \ of\ \ Cables\ \ = \ \ \frac{n \times (n-1)}{2}$$

- Where **n** is the number of nodes that represents the network.

Mesh Topology Contd...

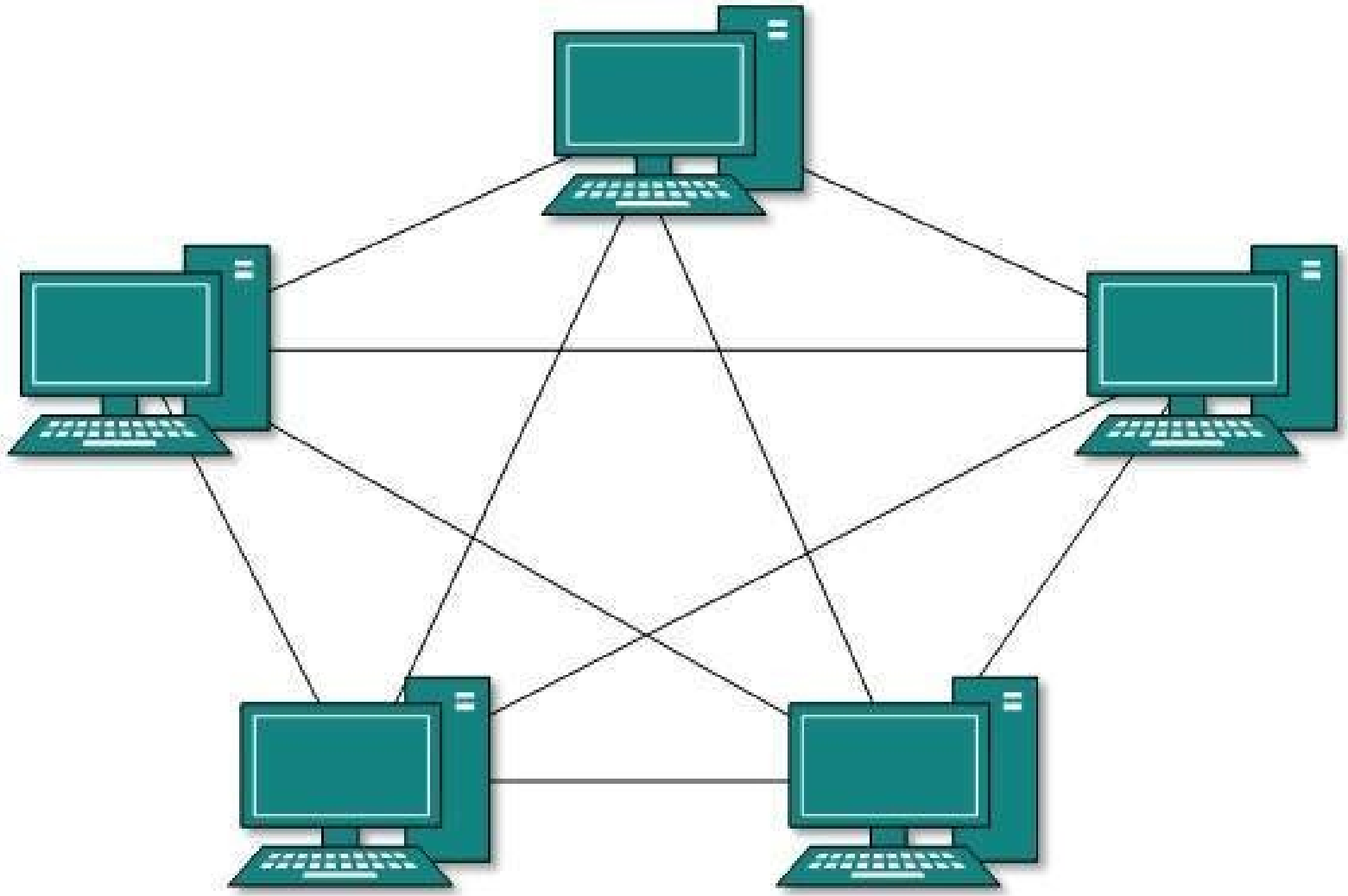


Figure: Mesh Topology

Mesh Topology Contd...

- Mesh topology is divided into two categories:
  1. **Fully Connected Mesh Topology**
  2. **Partially Connected Mesh Topology**
- **Fully Connected Mesh Topology**
  - In a full mesh topology, each computer is connected to all the computers available in the network.
  - All hosts have a point-to-point connection to every other host in the network.
  - It provides the most reliable network structure among all network topologies.
- **Partially Connected Mesh Topology**
  - In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.
  - This topology exists where we need to provide reliability to some hosts out of all.

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.

Disadvantages 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.

Tree Topology

- Also known as Hierarchical Topology.
- This is the most common form of network topology in use presently.
- This topology imitates as extended Star topology and inherits properties of bus topology.
- This topology divides the network in to multiple levels/layers of network.
- In this topology, a network is bifurcated into three types of network devices.
  1. The lowermost is access-layer where computers are attached.
  2. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer.
  3. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.

Tree Topology Contd...

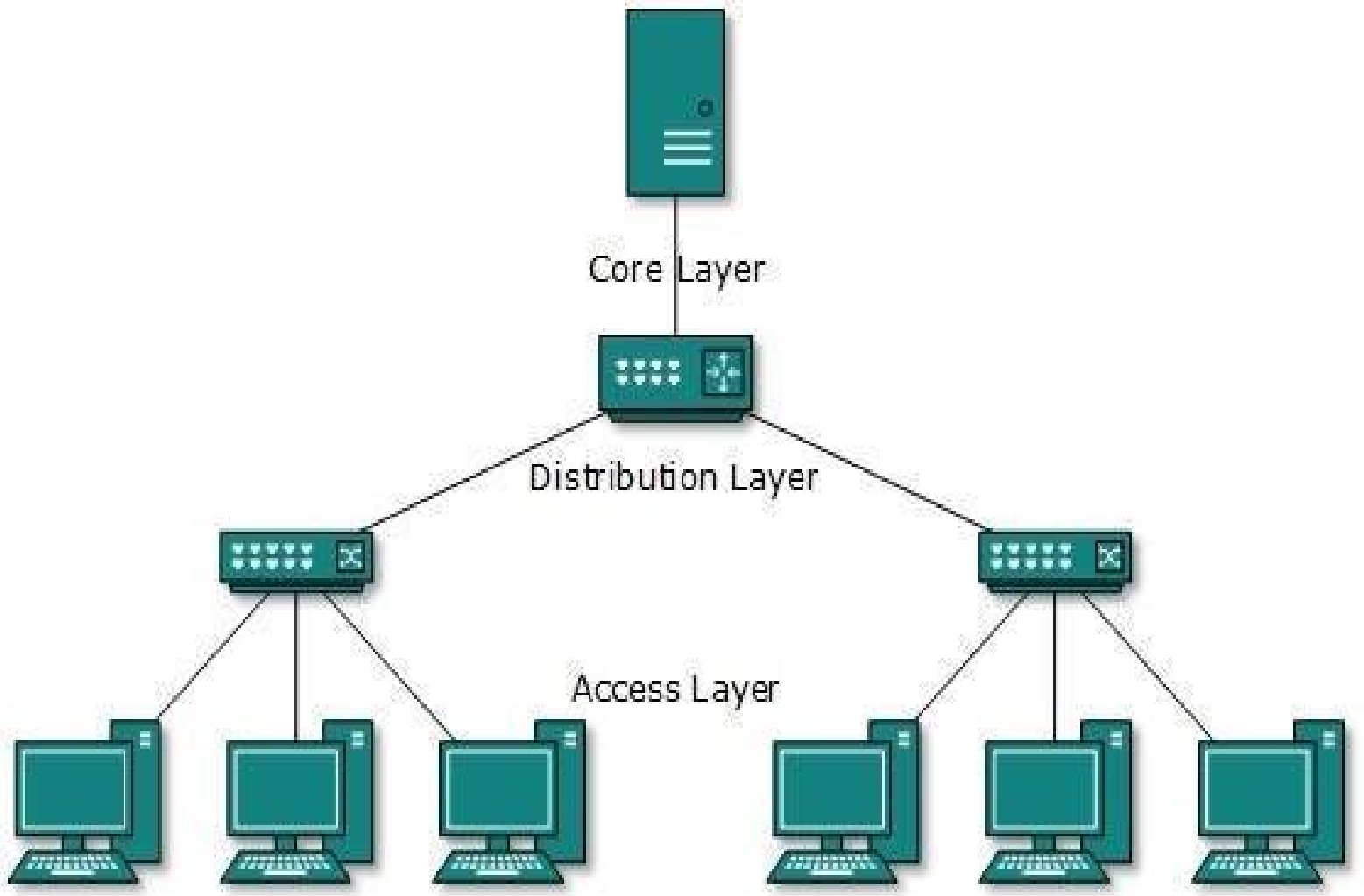


Figure: Tree Topology

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.

Hybrid Topology

- A network structure whose design contains more than one topology is said to be 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.
- Hybrid topology inherits merits and demerits of all the incorporating topologies.
- The combining topologies may contain attributes of Star, Ring, Bus topologies.

Hybrid Topology Contd...

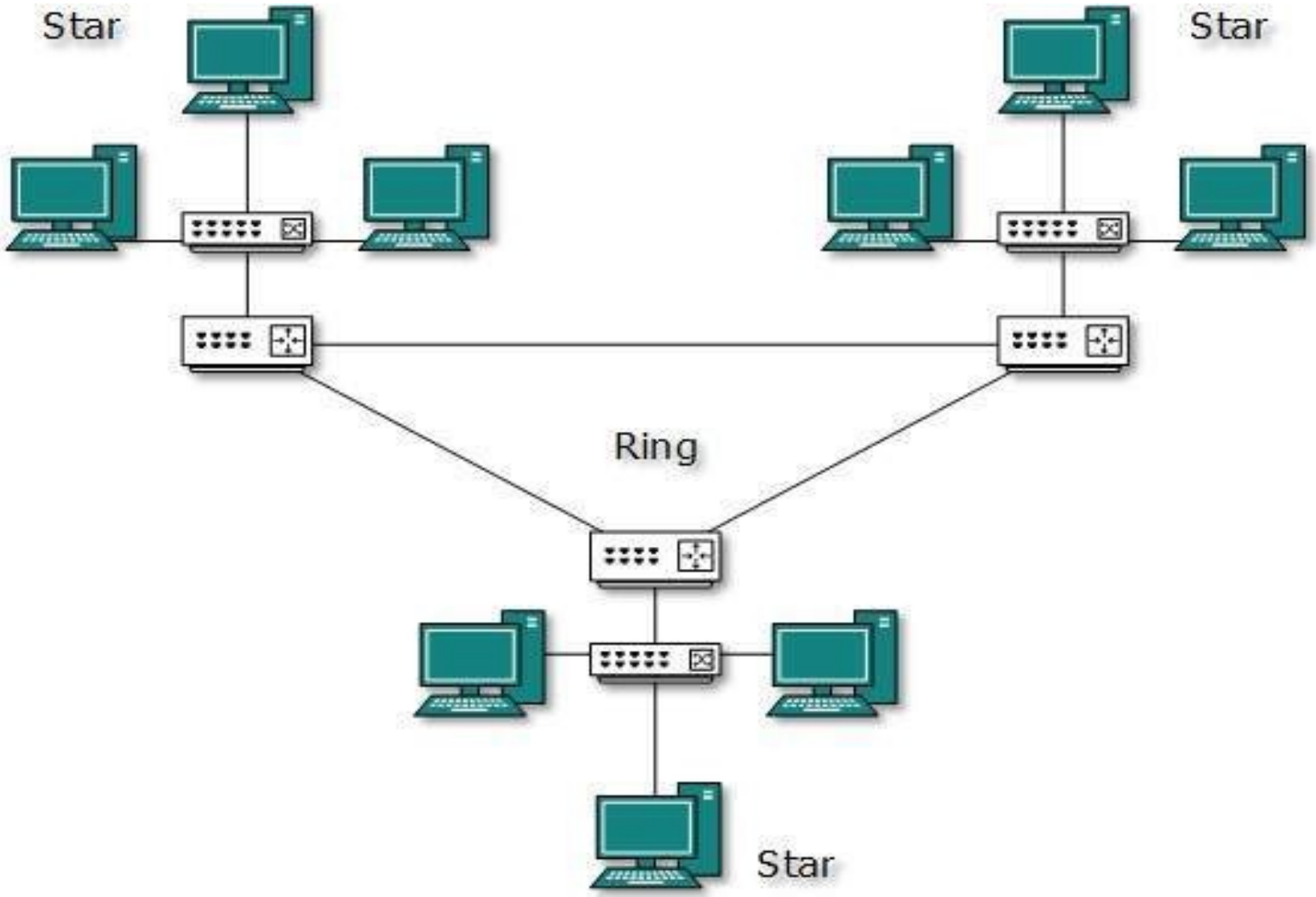


Figure: Hybrid Topology

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.

Design Issues for the Layers

- A number of design issues exist for the layer to layer approach of computer networks.
- Some of the main design issues are as follows
  1. **Reliability**
  2. **Scalability**
  3. **Addressing**
  4. **Error Control**
  5. **Flow Control**
  6. **Resource Allocation**
  7. **Multiplexing & De-multiplexing**
  8. **Routing**
  9. **Security**

- **Reliability**
  - Network channels and components may be unreliable, resulting in loss of bits while data transfer.
  - So, an important design issue is to make sure that the information transferred is not distorted.
  - It is a design issue of making a network that operates correctly.
- **Scalability**
  - Networks are continuously evolving.
  - The sizes are continually increasing leading to congestion.
  - Also, when new technologies are applied to the added components, it may lead to incompatibility issues.
  - Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.
  - When network gets large, new problem arises.
  - Thus scalability is important so that network can continue to work well when it gets large.

- **Addressing**
  - At a particular time, innumerable messages are being transferred between large numbers of computers.
  - So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.
  - There are multiple processes running on one machine.
  - Every layer needs a mechanism to identify senders and receivers.
- **Error Control**
  - Unreliable channels introduce a number of errors in the data streams that are communicated.
  - So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.
  - It is an important issue because physical communication circuits are not perfect.
  - Many error detecting and error correcting codes are available.
  - Both sending and receiving ends must agree to use any one code.

- **Flow Control**
  - If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver.
  - So, a proper flow control mechanism needs to be implemented.
  - If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers.
- **Resource Allocation**
  - Computer networks provide services in the form of network resources to the end users.
  - The main design issue is to allocate and deallocate resources to processes.
  - The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

- **Multiplexing & De-multiplexing**
  - It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination.
  - So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.
  - Multiplexing is needed in the physical layer at sender end and de-multiplexing is need at the receiver end.
- **Routing**
  - There may be multiple paths from the source to the destination.
  - Routing involves choosing an optimal path among all possible paths, in terms of cost and time.
  - There are several routing algorithms that are used in network systems.
- **Security**
  - A major factor of data communication is to defend it against threats like eavesdropping and alteration of messages.
  - So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

Reference Model in Computer Network

- The term **Reference Model** defined a standard means of communication architecture which is accepted worldwide.
- As users are using the network of a system and are situated over a broad physical range.
- The network devices users are using might have different architecture.
- So, for providing a standard communication between these heterogeneous devices, a standardized model (also termed as a **Reference Model**) is necessary for providing us the way how different devices have to communicate despite their diverse architecture.
- For this reason, two models were designed,
  1. **OSI Reference Model (Based on Hypothetical Communication)**
  2. **TCP/IP Reference Model (Based on Fully Practical Model)**

TCP/IP Reference Model

- TCP/IP Reference Model is a four-layered suite of communication protocols.
- It was developed by the DoD (Department of Defence) in the 1960s.
- It is named after the two main protocols that are used in the model, namely, TCP and IP.
- TCP stands for **Transmission Control Protocol** and IP stands for **Internet Protocol.**
- TCP/IP Model helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them.
- The purpose of TCP/IP model is to allow communication over large distances.

TCP/IP Reference Model Contd...

- It provides end-to-end data communication.
- It specifies all the processes involved in end-to-end data communication which includes packetizing, addressing, routing, transmission.
- It contains four layers and all the functionalities are organized in these four layers.
- Support for a flexible architecture.
- Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.
- The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

TCP/IP Reference Model Contd...

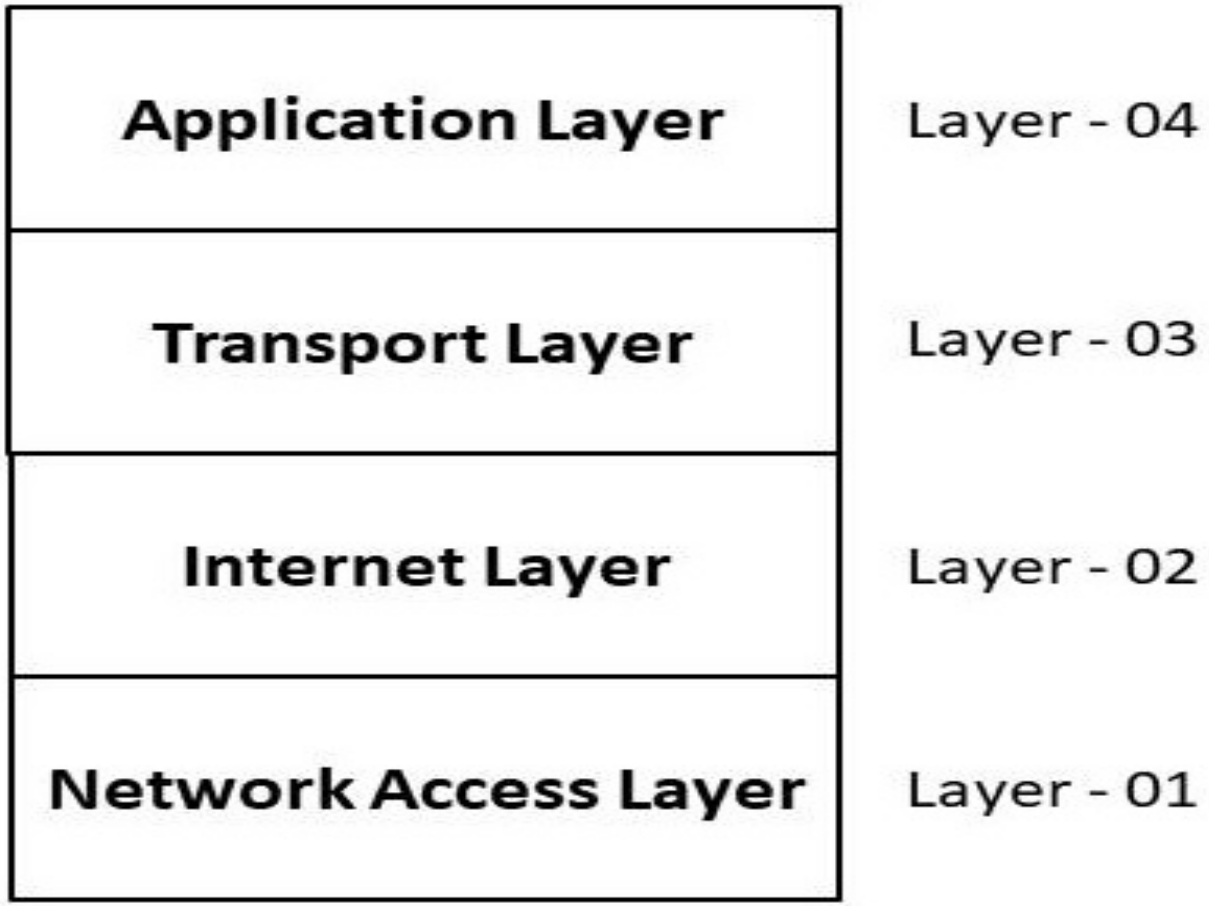


Figure: TCP/IP Layers

TCP/IP Reference Model Contd...

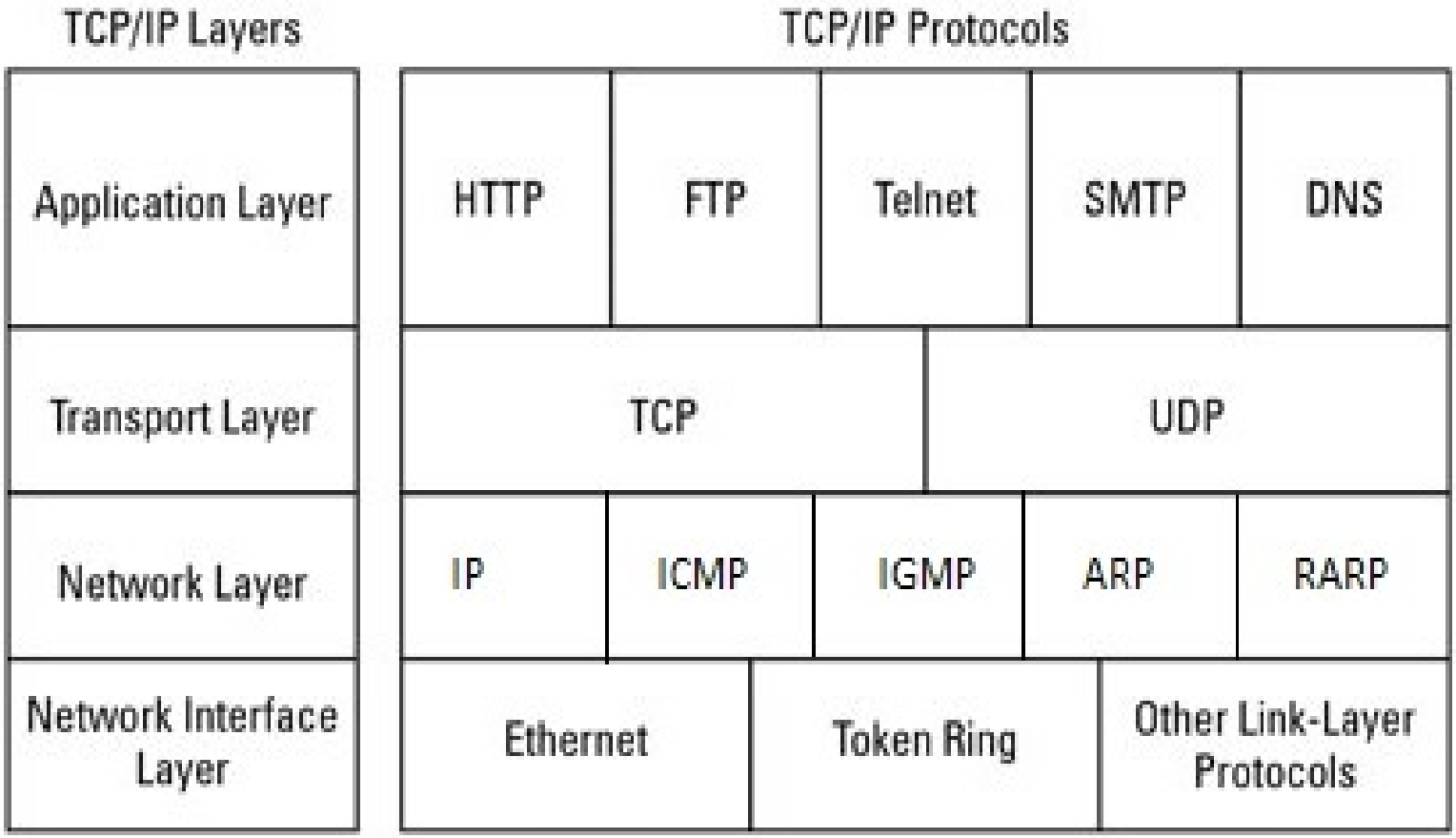
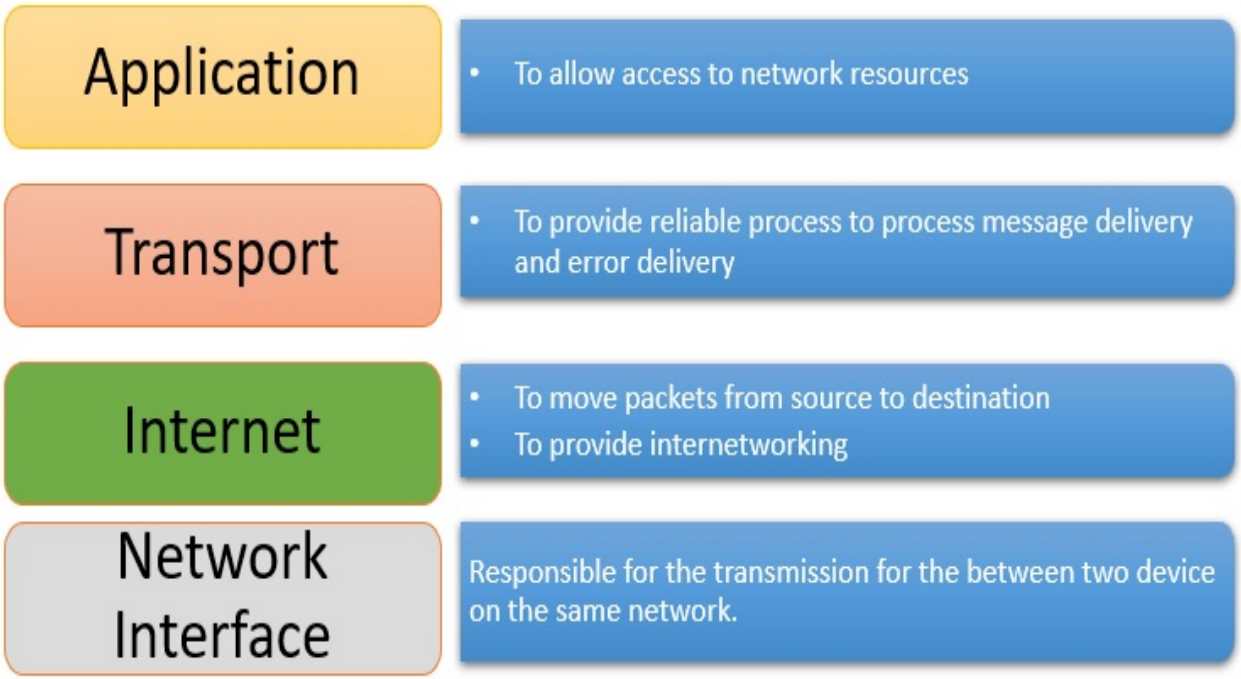


Figure: TCP/IP Protocol Suite

TCP/IP Reference Model Contd...

- The functionality of the TCP/IP model is divided into four layers, and each includes specific protocols.
- TCP/IP is a layered server architecture system in which each layer is defined according to a specific function to perform.
- All these four TCP/IP layers work collaboratively to transmit the data from one layer to another.



Application Layer

- Application layer interacts with an application program, which is the highest level of TCP/IP model.
- The application layer is closest to the end-user.
- It means the application layer allows users to interact with other software application.
- Application layer interacts with software applications to implement a communicating component.
- Example of the application layer is an application such as file transfer, email, remote login, etc.
- Node-to-node communication based on the user-interface occurs at this layer.
- Multiple protocols are present in this layer, such as **Hypertext Transfer Protocol (HTTP)**, **File Transfer Protocol (FTP)**, **Network Time Protocol (NTP)**, **Telecommunication Network (TELNET)**, **NFS**, **SSH**, **SMTP**, **TFTP**.

Application Layer Contd...

- An application layer is the topmost layer in the TCP/IP model.
- It It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer.
- Every application cannot be placed inside the application layer except those who interact with the communication system.
- **For Example:**
  - **Text Editor** cannot be considered in application layer.
  - While web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Hypertext Transfer Protocol (HTTP)

- Hypertext Transfer Protocol is used to manage the communication between the server and web browsers.
- This protocol allows us to access the data over the WWW.
- It transfers the data in the form of plain text, audio, video.

Network Time Protocol (NTP)

- Network Time Protocol can set one standard time source in our computer, which enables sync between the server and the user.

File Transfer Protocol (FTP)

- FTP stands for File Transfer Protocol.
- FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Telecommunication Network (TELNET)

- It is an abbreviation for Terminal Network.
- It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

Simple Mail Transfer Protocol (SMTP)

- The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol.
- This protocol is used to send the data to another e-mail address.

Simple Network Management Protocol (SNMP)

- It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

Transport Layer

- The transport layer is responsible for the end-to-end communication and delivery of the error-free data.
- It provides services that include connection-oriented communication, flow control, reliability.
- It decides if data transmission should be on parallel path or single path.
- Transport layer adds header information to the data.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer also arrange the packets to be sent, in sequence.
- The transport layer also offers an acknowledgment of the successful data transmission.
- Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system.

Transport Layer Contd...

- It divides the message received from the application layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be re-transmitted.
- Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.
- It determines how much data should be sent where and at what rate.
- It helps ensure that data units are delivered error-free and in sequence.
- There are two main protocols present in this layer,
  1. **Transmission Control Protocol (TCP)**
  2. **User Datagram Protocol (UDP)**

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and re-transmits the damaged frames.
- It ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- It is a connection-oriented protocol and provides reliable communication and error-free delivery of data from the source to the destination host.
- It is used by many internet applications including World Wide Web(WWW), email.

User Datagram Protocol (UDP)

- It provides connection-less service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user data-gram has been damaged.
- It prioritizes speed over the accuracy of delivery.
- UDP does not specify which packet is lost.
- It provides simple, cost-effective but unreliable service.

Internet Layer

- An internet layer is a second layer of TCP/IP layes of the TCP/IP model.
- It is also known as a network layer.
- The main responsibility of the network layer is to transport data packets from the source to the destination host across the entire network.
- It helps the packet to travel independently to the destination.
- Order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer.
- Sending the data packets to their destination network is the main function of the Internet layer.

Internet Layer Contd...

- This layer mainly performs the logical addressing of the data packets by adding the IP(Internet Protocol) address to it.
- The IP addressing can be done either by using the Internet Protocol Version 4(IPv4) or Internet Protocol Version 6(IPv6).
- The Internet layer also performs routing of data packets using the IP addresses.
- The data packets can be sent from one network to another using the routers in this layer.
- This layer also performs the sequencing of the data packets at the receiver's end.
- The protocols that are used in the Internet layer are,
  1. **IP(Internet Protocol)**
  2. **ICMP(Internet Control Message Protocol)**
  3. **IGMP(Internet Group Management Protocol)**
  4. **ARP(Address Resolution Protocol)**
  5. **RARP(Reverse Address Resolution Protocol)**

Internet Protocol (IP)

- This protocol implements logical host addresses known as IP addresses.
- The IP addresses are used by the internet and higher layers to identify the device and to provide inter-network routing.
- It determines the path through which the data is to be transmitted.
- An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- When IP datagram is sent over the same local network such as LAN, MAN, WAN & it is known as direct delivery.
- When source and destination are on the distant network, then the IP datagram is sent indirectly.

Internet Control Message Protocol (ICMP)

- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination.
- If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- The core responsibility of the ICMP protocol is to report the problems, not correct them.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Address Resolution Protocol (ARP)

- Its job is to find the hardware address of a host from a known IP address.
- The two terms are mainly associated with the ARP Protocol
  1. **ARP Request**
     - When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  2. **ARP Reply**
     - Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply.
     - The recipient adds the physical address both to its cache memory and to the datagram header.

Network Interface Layer

- This layer is also called a network access layer.
- It helps you to defines details of how data should be sent using the network.
- It deals with data in the form of bits.
- This layer mainly handles the host to host communication in the network.
- It defines the transmission medium and mode of communication between two devices.
- The medium can be wired or wireless, and the mode can be simplex, half-duplex, or full-duplex.
- This layer is the group of communication protocols that acts as a link to which the host is connected physically.

Network Interface Layer Contd...

- It also specifies the line configuration(point-to-point or multi-port), data rate(number of bits sent each second), and topology in the network.
- The functionality of the physical layer varies from network-to-network.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used in this layer are:
  1. **Ethernet**
  2. **FDDI(Fiber Distributed Data Interface)**
  3. **Token Ring**
  4. **Frame Relay**

OSI Reference Model

- **Open System Interconnection (OSI)** is a reference model developed in 1984 by the **International Organization for Standardization**.
- It specifies how information from one computer's software application passes through physical media to another computer's software application.
- The OSI model is also known as the ISO-OSI model.
- It is a conceptual reference model that describes the entire flow of information from one computer to the other computer.
- The OSI model is a 7-layered model, so it is also known as a 7-layered architecture model.
- The basic idea behind layered architecture is to divide the design into smaller pieces.
- Most networks are organized in a series of layers to reduce the design complexity.

OSI Reference Model Contd...

- The OSI model is made up of seven layers.
- These layers are involved when a message is sent from one computer to other computer.
- When the message travels from source to destination, it pass through many intermediate nodes.
- These intermediate nodes involve the first three layers of the OSI model.
- Each layer defines particular network functions.

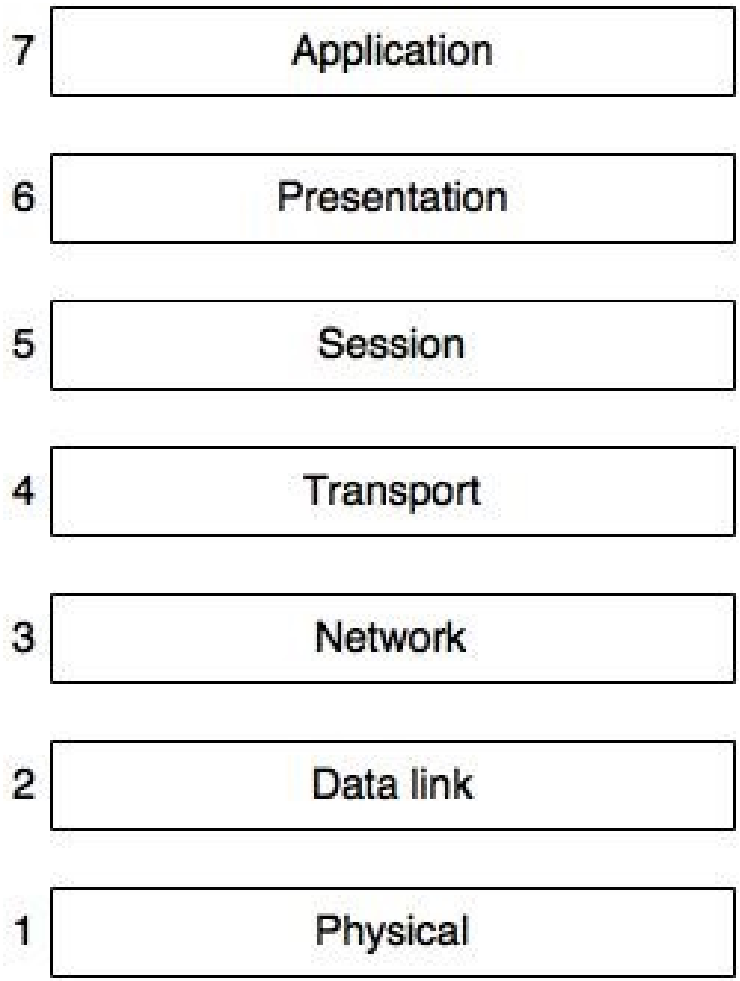
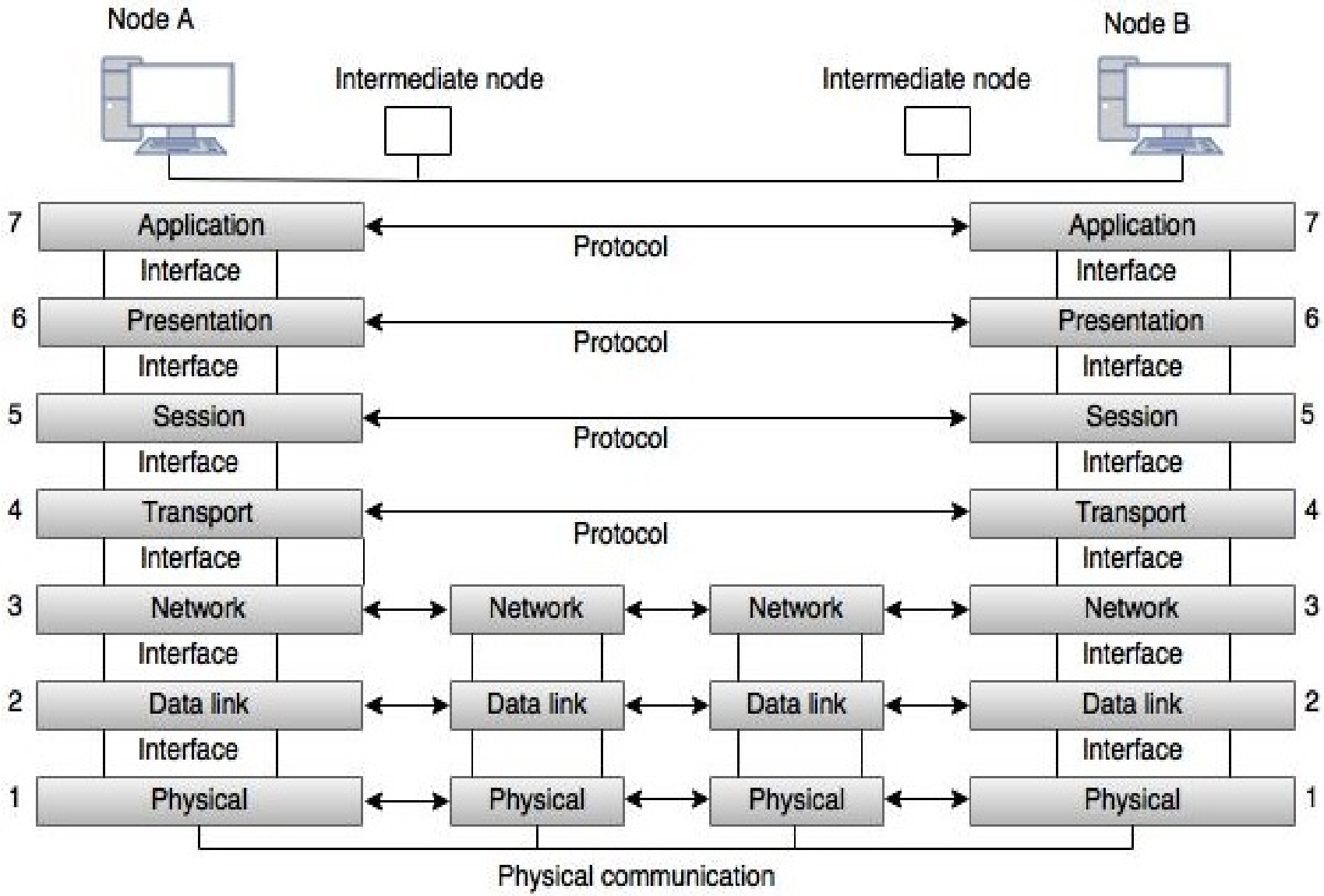


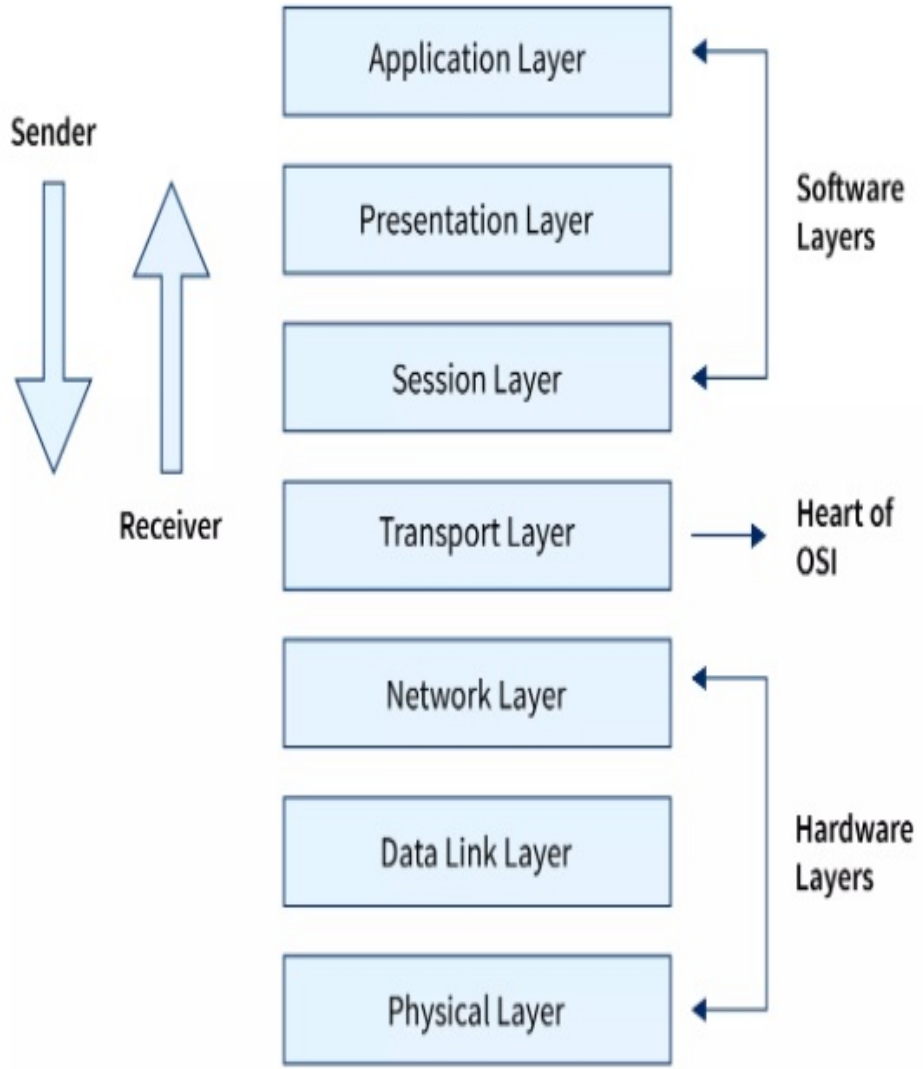
Fig: Seven layers of the OSI model

OSI Reference Model Contd...



OSI Reference Model Contd...

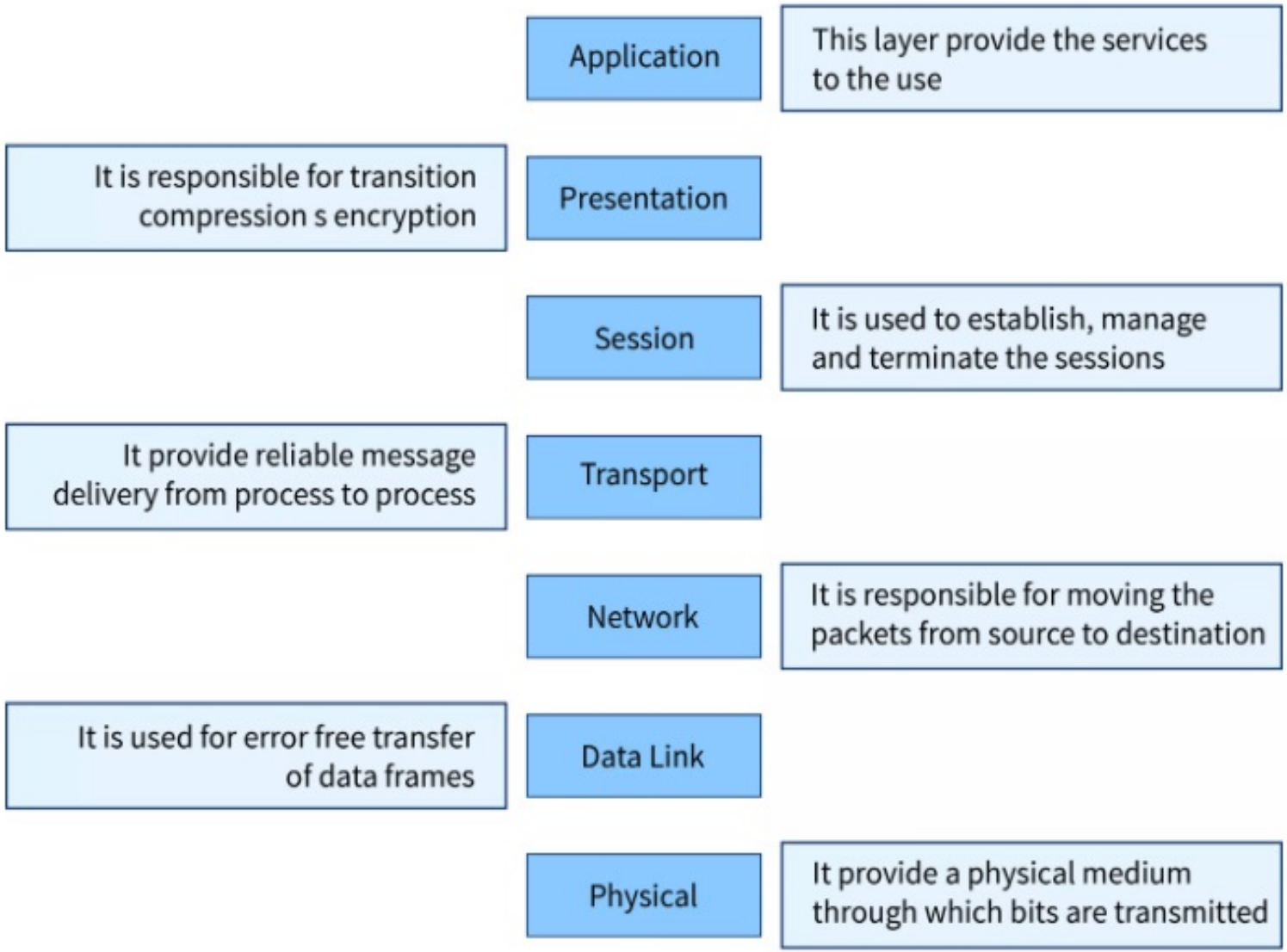
- The first three layers are known as the **software layer.**
- The last three layers are known as the **hardware layer.**
- The **transport layer** is the heart of the OSI model.
- The data is sent through the physical layer to the application layer (at the sender's end).
- The data is received through the application layer to the physical layer (at the receiver's end).



OSI Reference Model Contd...

- The basic idea behind layered architecture is to divide the design into smaller pieces.
- Most networks are organized in a series of layers to reduce the design complexity.
- The benefits of this layered division of the OSI model is discussed below
  1. The change in one layer does not affect the other layers.
  2. The layered architecture reduces the complexity by dividing the task in a manageable way.
  3. The layered architecture provides abstraction from other layers.
  4. Due to the abstraction, any layer can be changed independently.
  5. Each layer can be changed, tested, and analyzed independently.
- **Open systems** are the systems that are open to communicating and exchanging information over the networks.

Basic Overview of OSI Layers



- The lower layer is responsible for all the data transfer issues and is also known as the Hardware Layer.
- The layers present in the lower layer of the OSI Model are
  1. Network Layer
  2. Data Link Layer
  3. Physical Layer
- The upper layer is responsible for all the application-related issues and is also known as Software Layer.
- The layers present in the upper layer of the OSI Model are
  1. Application Layer
  2. Presentation Layer
  3. Session Layer
  4. Transport Layer

Physical Layer

- The physical layer coordinates the functions required to transmit the bitstream of data over the physical medium.
- The physical layer is the lowest layer of the OSI model.
- The main work of the physical layer of the OSI model is to **activate, maintain,** and **deactivate** the physical connection.
- The physical layer is also responsible for the transmission and reception of the unstructured raw data over the network.
- The data in the physical layer consists of a stream of bits.
- The bits of data must be encoded into the form of signals for transmission.
- For the transmission, the physical layer sets the **voltages, light speed(in the case of fiber optics cable),** and **data rates (numbers of bits to be transmitted per second)**.

Functions of Physical Layer

- The physical layer encodes the signals at the sender's end and decodes the signals at the receiver's end.
- It also defines the type of encoding scheme to be used (how 0's and 1's are to be changed into signals).
- It deals with the synchronization of the sender and the receiver so that the receiver and the sender are at the same bit level.
- The physical layer deals with the line configuration i.e. how the devices are connected through a dedicated link.
- It deals with the type of topology to be used for example ring, mesh, bus, star, hybrid, etc.
- Network topology is the physical and logical arrangement of nodes and connections in a computer network.
- The physical layer also deals with the direction and type of transmission between two or more devices.
- The mode of transmission can be **Simplex, Half Duplex,** and **Full Duplex**.

Working of Physical Layer

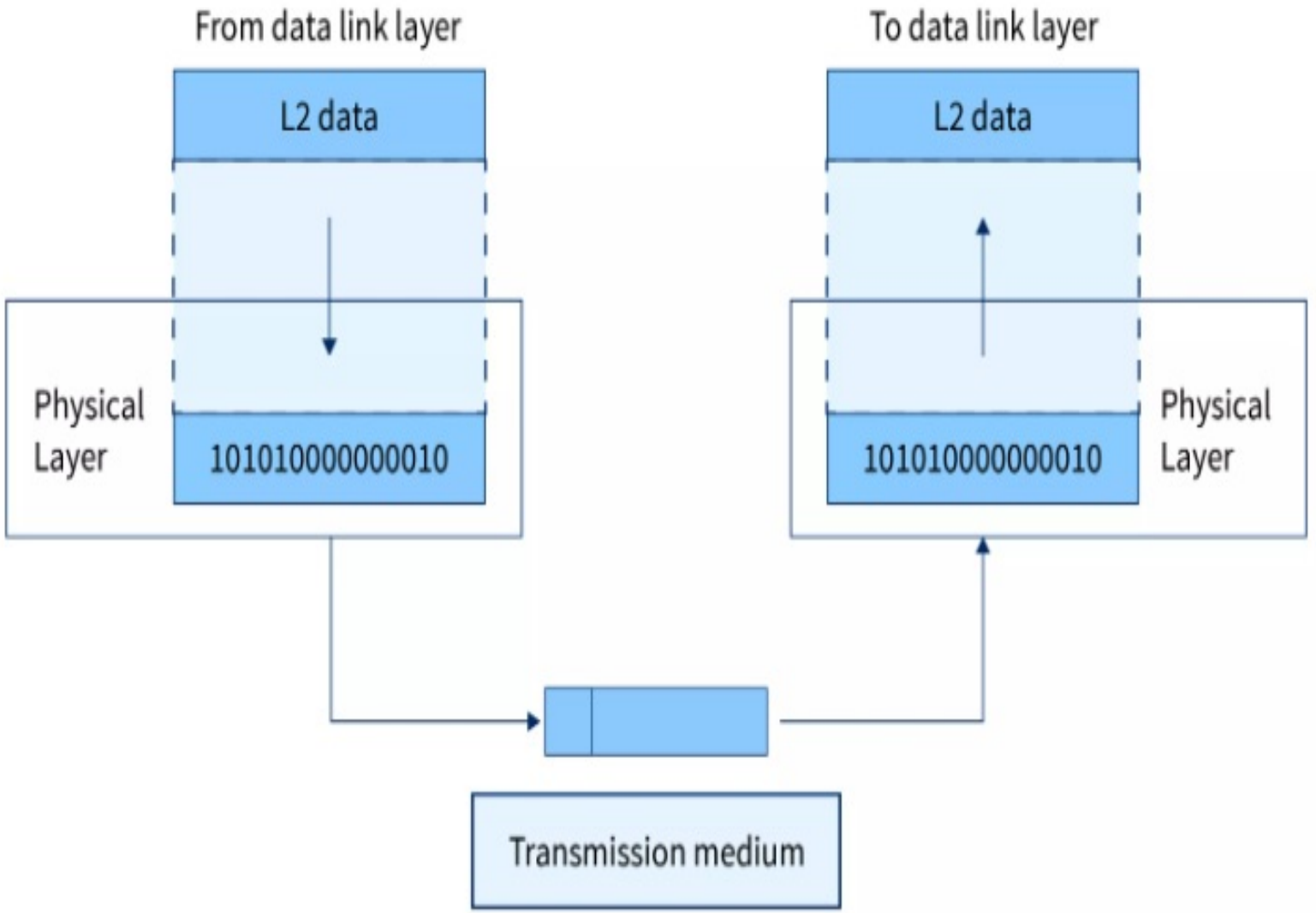


Figure: Transmission of data and working of the physical layer

Protocols & Devices used on Physical Layer

- The various protocols used in the physical layer are
  1. Digital Subscriber Line (DSL)
  2. Integrated Services Digital Network (ISDN)
  3. Ethernet
  4. FDDI
  5. Token Ring
- The various devices used in the physical layer are
  1. Network adapters
  2. Hubs
  3. Cables
  4. Repeaters
  5. Modem

Data Link Layer

- The data link is the second layer of the OSI model, which is used to transmit the error-free frames from one node to the other.
- If the two computer nodes are on the same networks, then the data link layer provides a connection between the two nodes.
- The main work of the data link layer is to convert the data into the form of frames.
- It adds a header to the frame to define the sender and receiver of the frame.
- Data link layer detects and corrects the transmission errors using the correction method.
- It contains two sub-layers
  1. Logical Link Control Layer
  2. Media Access Control Layer

1. **Logical Link Control Layer**
   - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
   - It identifies the address of the network layer protocol from the header.
   - It also provides flow control.
2. **Media Access Control Layer**
   - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
   - It is used for transferring the packets over the network.

- **Framing**
  - Framing is the technique in which the data is divided into streams of bits (called frames) received from the network layer.
  - Along with the conversion of data into frames, the data link layer adds a header and trailer to the frames.
  - The header (present at the starting of the frame) contains the hardware's physical address of source and destination.
  - The trailer (present at the end of the frame) contains the error detection and correction bits.

Figure: Frame Structure on Data Link Layer

- **Flow Control**
  - The data link layer also maintains the flow control of data during transmission.
  - Suppose that the rate of data transmission and data absorption varies then there is data loss, so the data link layer maintains the flow control.
  - It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted.
- **Error Control**
  - The data link layer adds the error detection and correction bits at the end of the frames in the form of trailers.
  - These bits are used to detect the errors and then re-transmit the damaged or lost data to prevent any kind of duplication.
  - Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the trailer.
  - CRC is added to the message frame before it is sent to the physical layer. If any error seems to occurs, then the receiver sends the acknowledgment for the re-transmission of the corrupted frames.

- **Access Control**
  - It also maintains access control.
  - In situations where two or more devices are connected to the same communication medium then the data link layer protocols determine the device that can transmit the data.

Note

- The physical address is also known as the MAC (Media Access Control) address.
- The MAC address is a unique address of each computer present on the NIC card.

Working of Data Link Layer

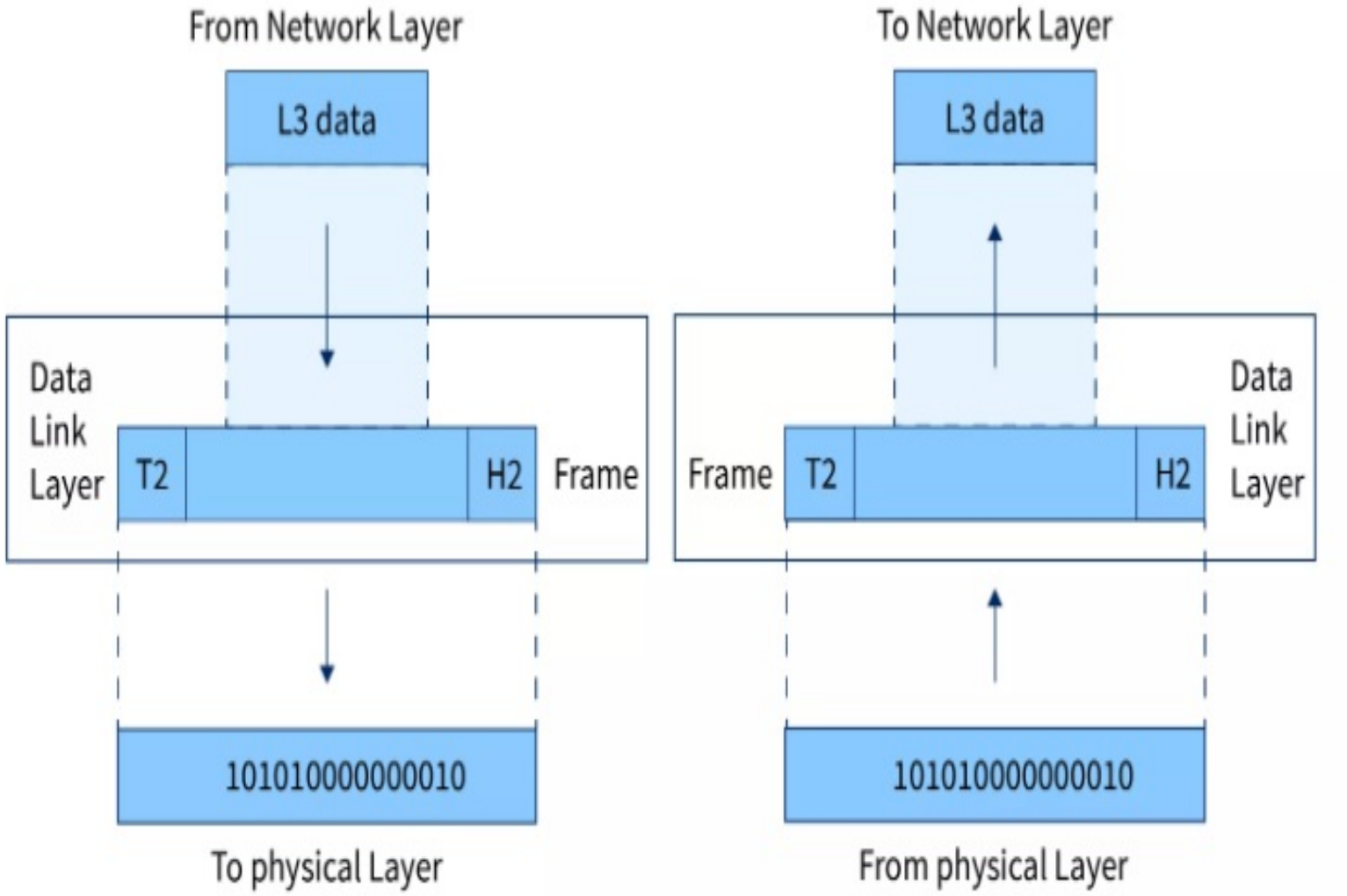


Figure: Transmission of data and working of the data link layer

Protocols & Devices used on DLL

- The various protocols used in the data link layer are
  1. PPP (Point-to-Point Protocol)
  2. Frame Relay
  3. ATM (The Asynchronous Transfer Mode protocol)
- The various devices used in the data link layer are
  1. Bridges
  2. Switches
  3. NIC cards (Network Interface Cards)

Network Layer

- The network layer is the third layer of the OSI model which provides communication between hosts of different networks.
- The network layer divides the data received from the transport layer in the form of **packets.**
- The network layer provides two ways of communication namely

1. **Connection-Oriented**
   - In **connection-oriented** communication, a communication session is established before any useful data can be transferred.
2. **Connection-Less.**
   - In **connection-less** communication, the data can be transferred without establishing any connection.

- This layer manages device addressing, tracks the location of devices on the network.

Network Layer Contd...

- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The network layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an inter-network.
- The protocols used to route the network traffic are known as Network layer protocols.
- Examples of protocols are IPv4 and IPv6.

Functions of Network Layer

- **Inter-networking**
  - An inter-networking is the main responsibility of the network layer.
  - It provides a logical connection between different devices.
- **Logical Addressing**
  - A Network layer adds the source and destination address to the header of the frame.
  - It helps in the proper identification of devices on the network.
- **Routing**
  - Routing simply means determining the best (optimal) path out of multiple paths from the source to the destination.
  - So the network layer must choose the best routing path for the data to travel.
- **Packetizing**
  - A Network Layer receives the segments from the upper layer and converts them into packets.
  - This process is known as Packetizing.
  - It is achieved by Internet Protocol (IP).

Working of Network Link Layer

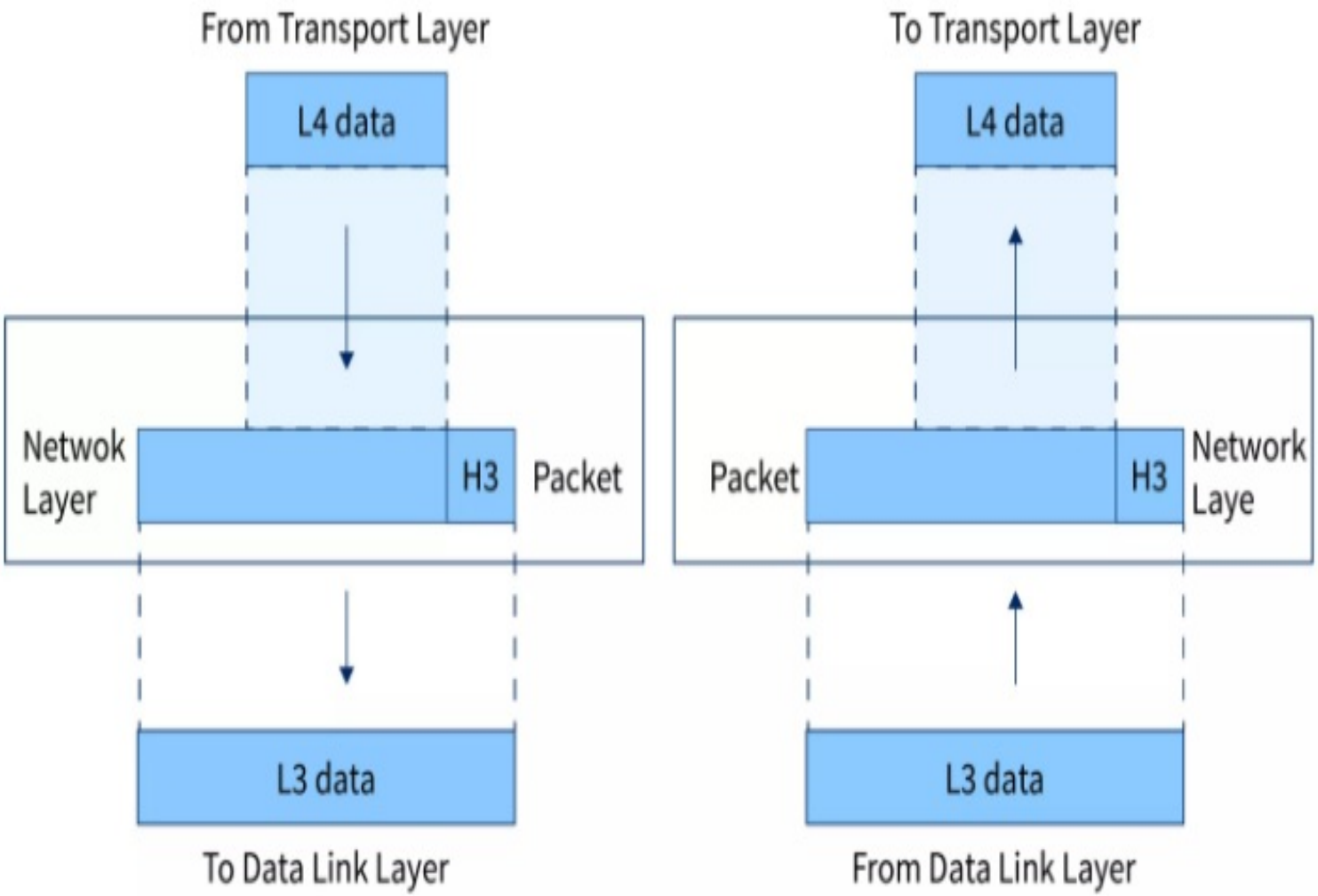


Figure: Transmission of data and working of the network layer

Protocols & Devices used on Network Layer

- The various protocols used in the network layer are
  1. IPv4 (Internet Protocol version 4)
  2. IPv6 (Internet Protocol version 6)
  3. ICMP (Internet Control Message Protocol)
  4. ARP (Address Resolution Protocol)
  5. RARP (Reverse Address Resolution Protocol)
- The various devices used in the network layer are
  1. Routers
  2. Brouters

Note

- The network layer does not guarantee the delivery of packets to the destination.
- There is no reliability guarantee as well.

Transport Layer

- The transport layer is the fourth layer of the OSI model which is responsible for the process to process delivery of data.
- The main aim of the transport layer is to maintain the order so that the data must be received in the same sequence as it was sent by the sender.
- The network layer provides two ways of communication namely **Connection-Oriented** & **Connection-Less.**
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

- The two protocols used in this layer are
  1. **Transmission Control Protocol (TCP)**
     - It is a standard protocol that allows the systems to communicate over the internet.
     - It establishes and maintains a connection between hosts.
     - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments.
     - Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination.
     - The transmission control protocol reorders the packets in the correct order at the receiving end.
  2. **User Datagram Protocol (UDP)**
     - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received.
     - The sender does not wait for any acknowledgment.
     - Therefore, this makes a protocol unreliable.

- **Service-Point Addressing**
  - The transmission of data from source to the destination not only from one computer to another computer but also from one process to another process.
  - The transport layer adds the header that contains the address known as a service-point address or port address.
  - The responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and Reassembly**
  - When the transport layer receives the message from the upper layer, it divides the message into multiple segments.
  - Each segment is assigned with a sequence number that uniquely identifies each segment.
  - When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- **Connection Control**
  - Transport layer provides **Connection-Oriented** service & **Connection-Less** service.
  - A connection-less service treats each segment as an individual packet, and they all travel in different routes to reach the destination.
  - A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets.
  - In connection-oriented service, all the packets travel in the single route.
- **Flow Control**
  - The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control**
  - Error control is performed end-to-end rather than across the single link.
  - The sender transport layer ensures that message reach at the destination without any error.

Working of Transport Layer

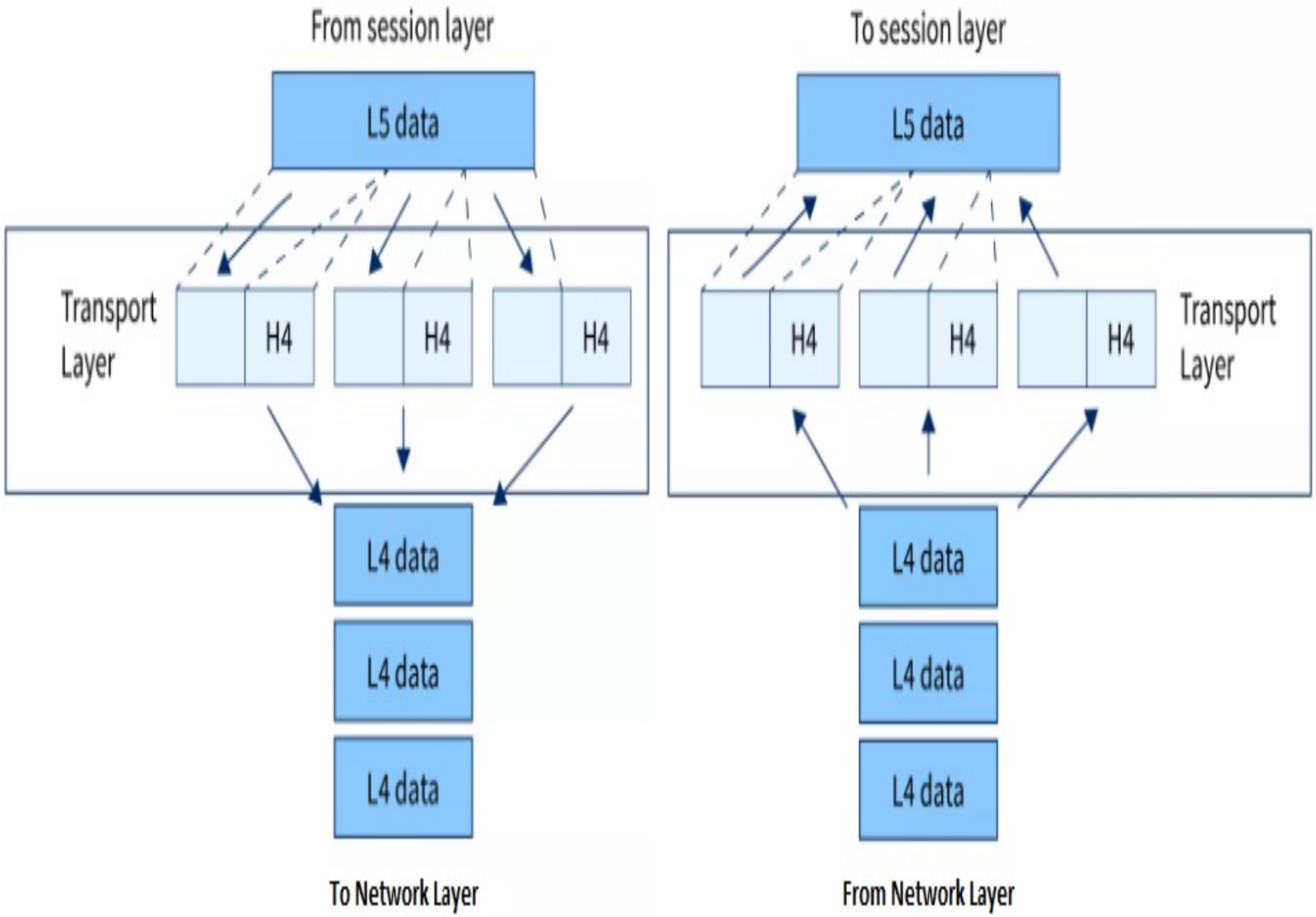


Figure: Transmission of data and working of the transport layer

Protocols & Devices used on Transport Layer

- The various protocols used in the transport layer are
  1. TCP (Transmission Control Protocol)
  2. UDP (User Datagram Protocol)
- The various devices used in the transport layer are
  1. Load Balancers/Firewalls

Session Layer

- The session layer is the fifth layer of the OSI model.
- Whose main aim is to establish, manage, and terminate the connection between applications.
- Session layer is the network dialog controller.
- Specific responsibility of session layer is dialog control.
- The Session Layer allows users on different machines to establish active communication sessions between them.
- Session layer manages and synchronize the conversation between two different applications.
- In Session layer, streams of data are marked and are re-synchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

- **Dialog control**
  - Session layer acts as a dialog controller that creates a dialog between two processes.
  - In other words we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization**
  - Session layer adds some checkpoints when transmitting the data in a sequence.
  - If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint.
  - This process is known as Synchronization and recovery.

Note

- Half-duplex allows the transmission of signals in both directions but not simultaneously.
- Full-duplex allows the transmission of signals in both directions at the same time.

Working of Session Layer

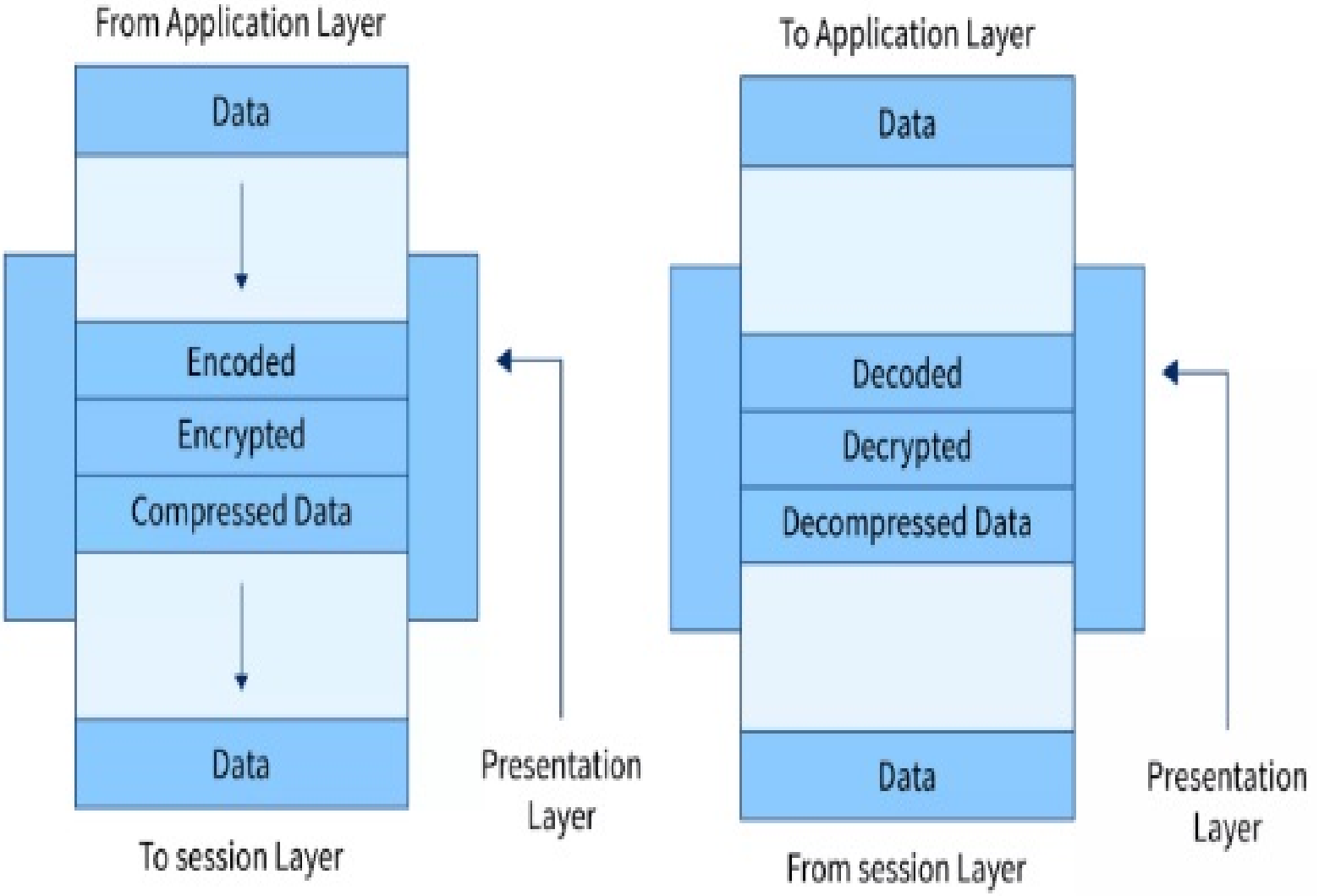


Figure: Transmission of data and working of the session layer

Protocols & Devices used on Session Layer

- The various protocols used in the session layer are
  1. PAP (Password Authentication Protocol)
  2. PPTP (Point-to-Point Tunneling Protocol)
  3. RPC (Remote Procedure Call Protocol)
- The various devices used in the session layer are
  1. Gateways

Presentation Layer

- The presentation layer is the sixth layer of the OSI model.
- This layer mainly concentrates on the syntax and semantics of the information exchanged between the systems.
- The main aim of the presentation layer is to convert the data from one presentation format to the other format as different applications may use different applications.
- It acts as a data translator for a network.
- The Presentation layer is also known as the syntax layer.
- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information(data) and will be able to use the data.
- Languages(syntax) can be different of the two communicating systems.
- Under this condition presentation layer plays a role translator.

Functions of Presentation Layer

- **Translation**
  - The processes in two systems exchange the information in the form of character strings, numbers and so on.
  - Different computers use different encoding methods.
  - The presentation layer handles the interoperability between the different encoding methods.
  - It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption**
  - Encryption is needed to maintain privacy.
  - Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression**
  - Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted.
  - Data compression is very important in multimedia such as text, audio, video.

Working of Presentation Layer

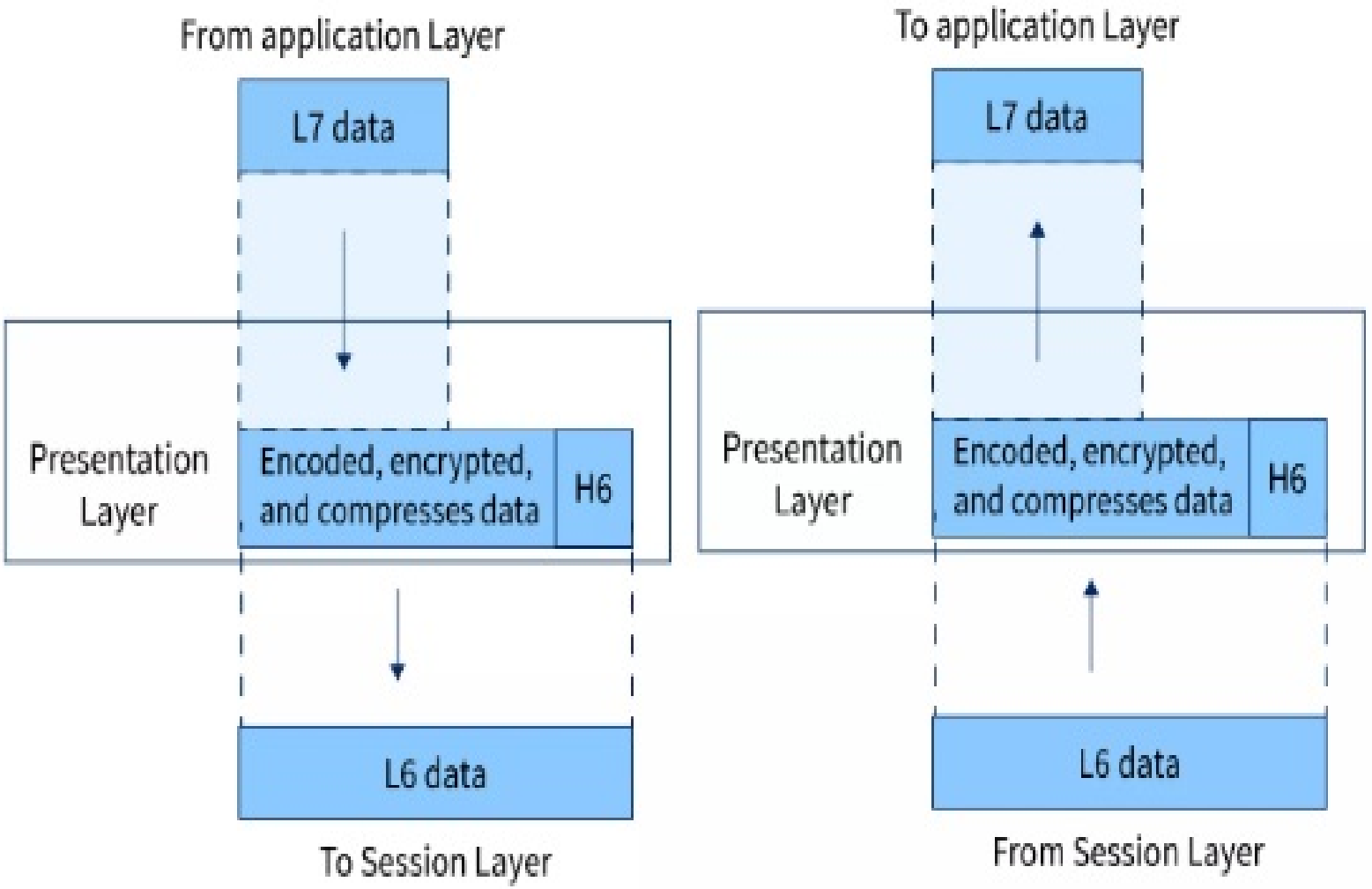


Figure: Transmission of data and working of the presentation layer

Protocols used on Presentation Layer

- The various protocols used in the presentation layer are
  1. AFP (Apple Filing Protocol)
     - AFP protocol is designed by Apple company for sharing all files over the entire network.
  2. FTP (File Transfer Protocol)
     - FTP is a internet protocol, and its main goal is to transmit all files in between one host to other hosts over the internet.
  3. LPP (Lightweight Presentation Protocol)
     - This protocol is used to offer ISO presentation services on top of TCP/IP based protocol stacks.
  4. NCP (NetWare Core Protocol)
     - NCP is a Novell client server model protocol that is designed especially for Local Area Network(LAN).
     - It is capable to perform several functions like as file/print-sharing, clock synchronization, remote processing and messaging.
  5. NDR (Network Data Representation)
     - NDR is an data encoding standard, and it is implement in the Distributed Computing Environment (DCE).

Application Layer

- The application layer is the seventh and the last layer of the OSI model, which mainly concentrates on providing services to the users.
- The application layer contains numerous protocols that are used by users for different purposes.
- Application layers allow users to access and share files, access and send emails, access web pages (via the world wide web), etc.
- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- This layer provides the network services to the end-users.

- **File transfer, access, and management (FTAM)**
  - An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services**
  - An application layer provides the facility for email forwarding and storage.
- **Addressing**
  - To achieve communication between client and server system, there is a need for addressing.
  - When a request is sent from the client side to the server side, this request contains the server address and its own address.
  - The server answered to the client request, this request contains the destination address, i.e., client address.
  - DNS is used to achieve this type of addressing.

Working of Application Layer

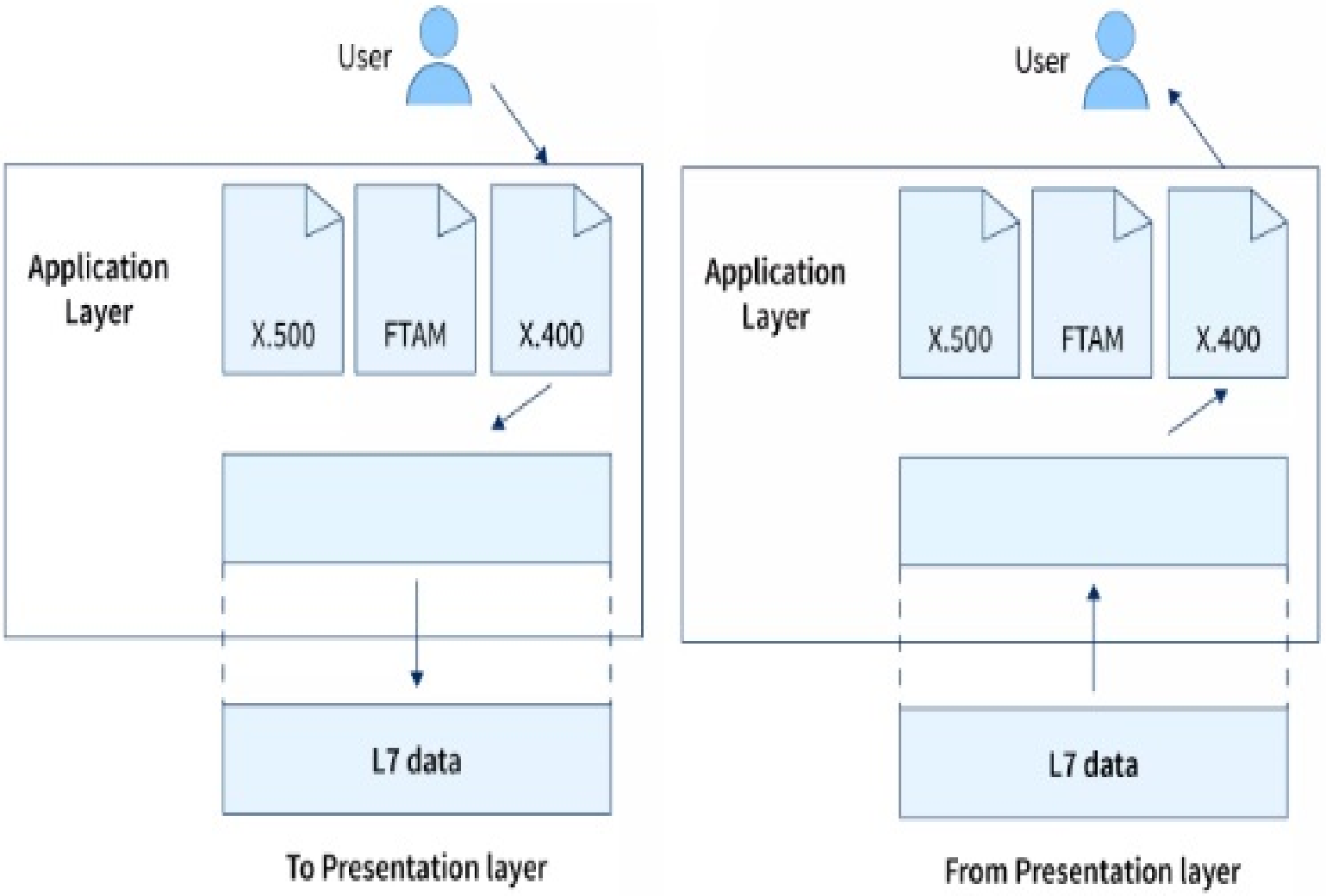


Figure: Transmission of data and working of the application layer

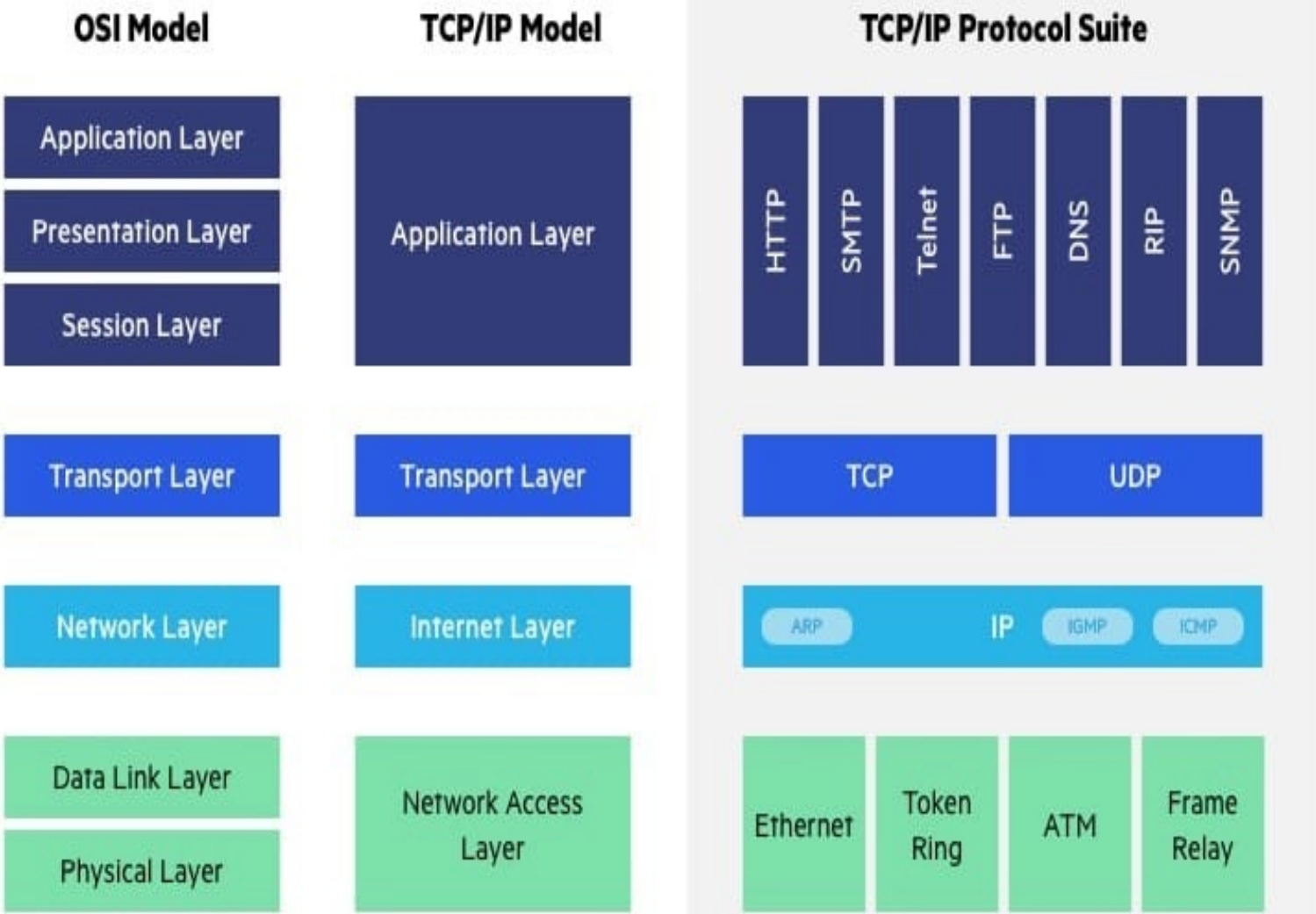
Protocols & Devices on Application Layer

- The various protocols used in the application layer are
  1. DNS (Domain Name System)
  2. SMTP (Simple Mail Transfer Protocol)
  3. FTP (File Transfer Protocol)
  4. POP (Post Office Protocol)
  5. HTTP (HyperText Transfer Protocol)
- The various devices used in the application layer are
  1. PC's (Personal Computer)
  2. Phones
  3. Servers
  4. Firewalls

Summary of OSI Model

No.	Layer Name	Responsibility	Information Form (Data Unit)	Device
7	**Application Layer**	Helps in identifying the client and synchronize communication	Message	-
6	**Presentation Layer (Translation Layer)**	Data from application layer is extracted and manipulated as required format for transmission	Message	-
5	**Session Layer**	Establishes connection, maintenance, authentication and ensure security	Message	Gateway
4	**Transport Layer (HEART of OSI)**	Take service from network layer and provide it to application layer	Segment	Firewall
3	**Network Layer**	Transmission of data from one host to other. Located in different network	Packet	Router
2	**Data Link Layer**	Node to node delivery of messages	Frame	Switch, Bridge
1	**Physical Layer**	Establishing physical connection between devices	Bits	Hub, Repeater, Modem, Cables

Summary - OSI Model vs TCP/IP Model



OSI Model vs TCP/IP Model

OSI Model	TCP/IP Model
OSI stands for Open System Interconnection	TCP/IP stands for Transmission Control Protocol/Internet Protocol
OSI model has been developed by ISO (International Standard Organization).	It was developed by ARPANET (Advanced Research Project Agency Network).
This model is based on a vertical approach.	This model is based on a horizontal approach.
An OSI Model is a reference model, based on which a network is created.	The TCP/IP is the implementation of the OSI Model.
It consists of 7 layers.	It consists of 4 layers.
Protocols in the OSI model are hidden & can be easily replaced when the technology changes.	In this model, the protocol cannot be easily replaced.

OSI Model vs TCP/IP Model Contd...

OSI Model	TCP/IP Model
It is an independent standard and generic protocol used as a communication gateway between the network and the end user.	It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts.
It is also known as a reference model through which various networks are built. It is also referred to as a guidance tool.	It is an implemented model of an OSI model.
In this model, the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
It is protocol independent.	It is protocol dependent.

OSI Model vs TCP/IP Model Contd...

OSI Model	TCP/IP Model
In this model, the network layer provides both connection-oriented and connectionless service.	The network layer provides only connectionless service.
OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them.	In the TCP/IP model, services, protocols, and interfaces are not properly separated.
It provides standardization to the devices like router, motherboard, switches, and other hardware devices.	It does not provide the standardization to the devices. It provides a connection between various computers.
In the OSI model, the data link layer and physical are separate layers.	In TCP/IP, physical and data link are both combined as a single host-to-network layer.

References I

This study material is only for internal circulation & it has been completed with the help of following books, internet sources, articles, & blogs.

1. Andrew S. Tanenbaum, David J. Wetherall, "Computer Network", 5^{th} Edition, Pearson Education.
2. Behrouz A. Forozaun, "Data Communications & Networking", 5^{th} Edition, TMH.
3. S. Keshav, "An Engineering Approach to Computer Networking", 3^{rd} Edition, Pearson Education.
4. Oliver C. Ibe, "Fundamentals of Data Communication Networks", 1^{st} Edition, Willey Publications.
5. https://beginnersbook.com/2019/03/introduction-to-computer-network/
6. https://www.javatpoint.com/computer-network-introduction

References II

7. https://www.geeksforgeeks.org/what-is-computer-networking/
8. https://www.studytonight.com/computer-networks/overview-of-computer-networks
9. https://conceptsall.com/applications-of-computer-networks/
10. https://turbofuture.com/computers/Network-Application
11. https://www.tutorialspoint.com/Computer-Network-Components
12. https://www.javatpoint.com/computer-network-topologies
13. https://www.tutorialspoint.com/The-TCP-IP-Reference-Model
14. https://www.geeksforgeeks.org/tcp-ip-model/
15. https://www.javatpoint.com/computer-network-tcp-ip-model
16. https://www.studytonight.com/computer-networks/tcp-ip-reference-model

17. https://workat.tech/core-cs/tutorial/tcp-ip-reference-model-in-computer-networks
18. https://www.guru99.com/tcp-ip-model.html
19. https://docs.oracle.com/cd/E19683-01/806-4075/ipov-10/index.html
20. https://www.techtarget.com/searchnetworking/definition/ TCP-IP
21. https://byjus.com/govt-exams/tcp-ip-model/
22. https://afteracademy.com/blog/what-is-the-tcp-ip-model-and-how-it-works/

23. https://www.dummies.com/article/technology/information-technology/networking/general-networking/network-basics-tcpip-protocol-suite-185407/
24. https://www.scaler.com/topics/computer-network/osi-model/
25. https://www.tutorialride.com/computer-network/protocol-layers-and-reference-models-in-computer-network.htm
26. https://www.javatpoint.com/osi-model
27. https://www.studytonight.com/computer-networks/osi-model-session-layer
28. https://www.studytonight.com/computer-networks/osi-model-presentation-layer

29. https://digitalthinkerhelp.com/presentation-layer-in-osi-model-functions-protocols-examples-services/
30. https://www.includehelp.com/computer-networks/functions-of-application-layer-in-the-osi-model.aspx
31. https://www.geeksforgeeks.org/layers-of-osi-model/
32. https://www.imperva.com/learn/application-security/osi-model/
33. https://www.javatpoint.com/osi-vs-tcp-ip
34. https://byjus.com/free-ias-prep/difference-between-tcp-ip-and-osi-model/
35. https://www.guru99.com/difference-tcp-ip-vs-osi-model.html

R. C. PATEL
INSTITUTE OF TECHNOLOGY
An Autonomous Institute

Thank You

for your attention.

Do you have any question?