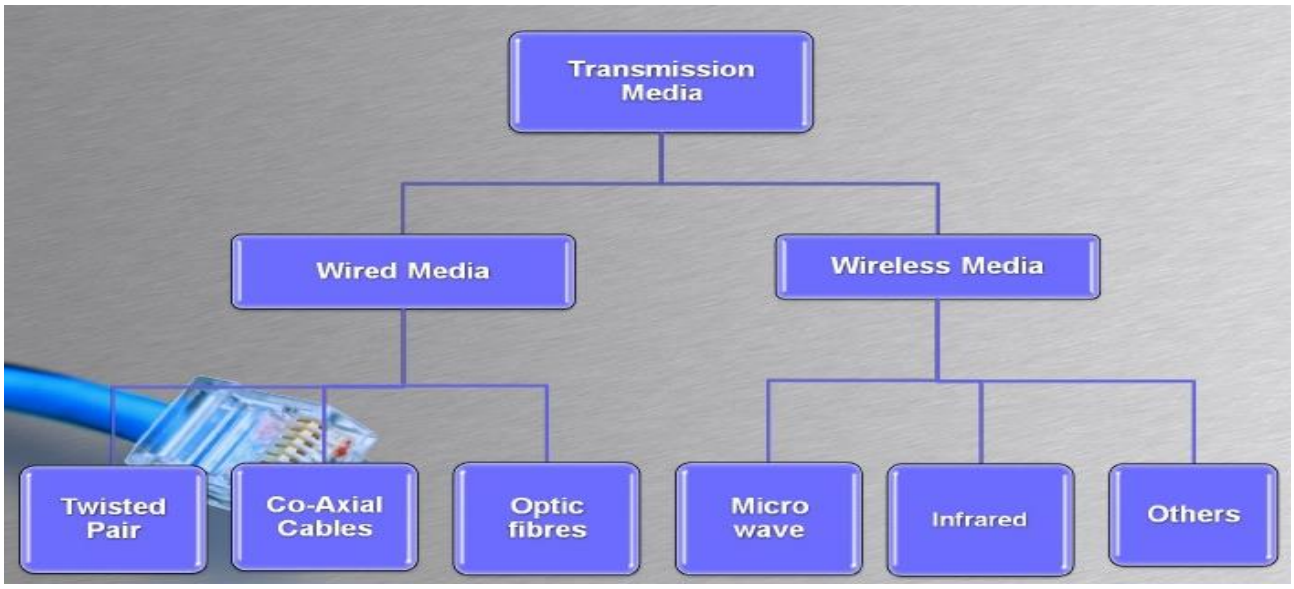
UNIT-1
INTRODUCTION

Syllabus:
Introduction: OSI overview, TCP/IP and other networks models, Examples of Networks: Novell Networks, Arpanet, Internet, Network Topologies WAN, LAN, MAN.

Introduction:

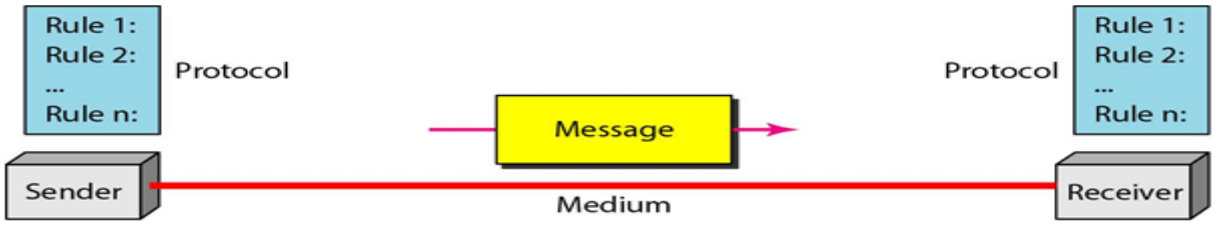
- A **network** is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

- **Computer Networks:** A collection of autonomous computers interconnected by a single technology to facilitate data communication.
- Two computers are said to be interconnected if they are able to exchange information. Here the connection may be Wired or Wire-less.
- A **wired network** is a common type of wired configuration. Most wired networks use Ethernet cables to transfer data between connected PCs.
- Examples include telephone networks, cable television or internet access, and fiber-optic communication.
- A **wireless network** is a computer network that uses wireless data connections between network nodes.
- Examples of wireless networks include cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks.



Components of Data-communication:

- The five components that make up a data communication are the message, sender, receiver, medium, and protocol.



1. **Message:** The message is the information (data) to be communicated. The Popular forms of information include text, numbers, pictures, audio, and video.

2. **Sender**: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

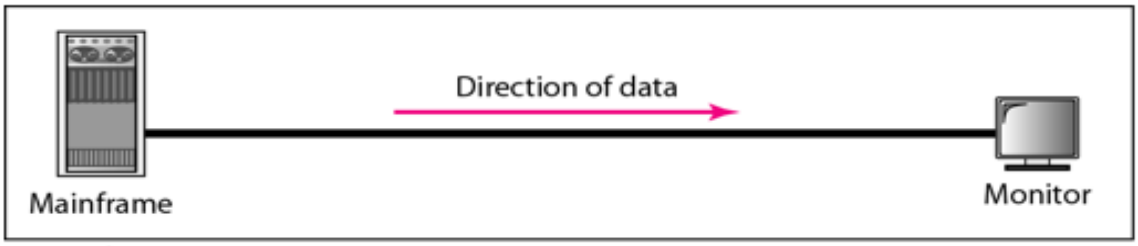
3. **Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. **Transmission medium.** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

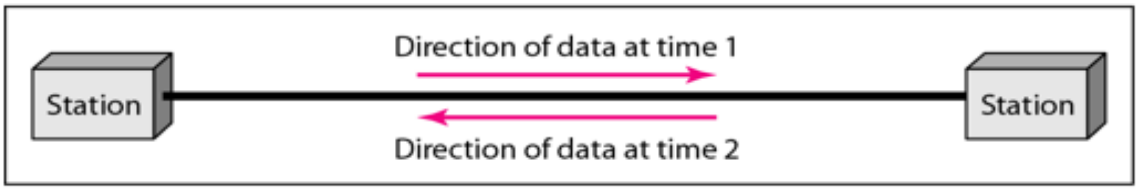
5. **Protocol.** A protocol is a set of rules that maintain data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just like a person speaking French cannot be understood by a person who speaks only Japanese.

Data-flow in communication network:

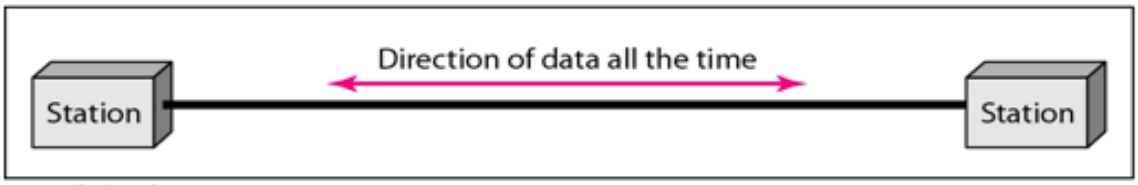
- Communication between two devices can be simplex, half-duplex, or full-duplex as shown in following figure.



a. Simplex



b. Half-duplex



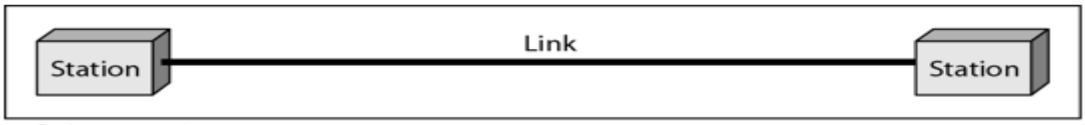
c. Full-duplex

- **Simplex :**
  - In simplex mode, the communication is unidirectional, as on a one-way road. Only one of the two devices on a link can transmit; the other can only receive (see Figure a).
  - **Keyboards and traditional monitors** are examples of simplex devices. The keyboard can only give input; the monitor can only accept output.
  - The simplex mode can use the entire capacity of the communication channel to send data in one direction only.

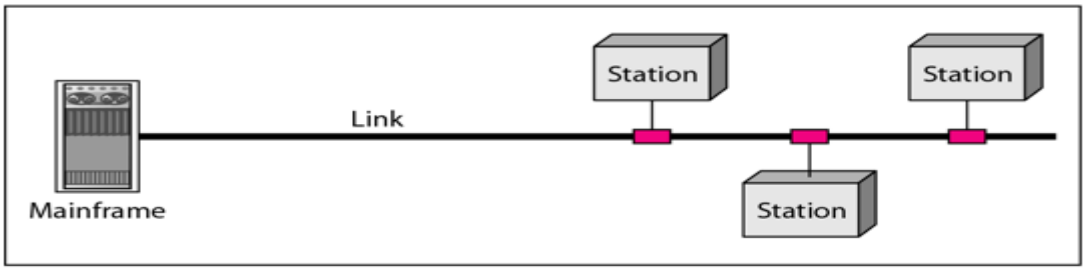
- **Half-Duplex :**
  - In half-duplex mode, each system can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (see Figure b).
  - The half-duplex mode is like a one-lane street with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. **Walkie-talkies** are half-duplex system.
  - The half-duplex mode is used in cases where there is no need for communication in both directions at the same time.
- **Full-Duplex :**
  - In full-duplex mode (also called duplex), both systems can transmit and receive simultaneously (see Figure c).
  - The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time.
  - In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction.
  - This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.
  - One common example of full-duplex communication is **the telephone network**. When two people are communicating by a telephone line, both can talk and listen at the same time.
  - The full-duplex mode is used when communication in both directions is required all the time.

Type of Connection:

- There are two possible types of connections: **point-to-point and multipoint**.



a. Point-to-point



b. Multipoint

- **Point-to-Point:** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, (see Figure a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.
- **Multipoint:** A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure b). In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a ***spatially*** *shared* connection. If users must take turns, it is a ***timeshared*** connection.

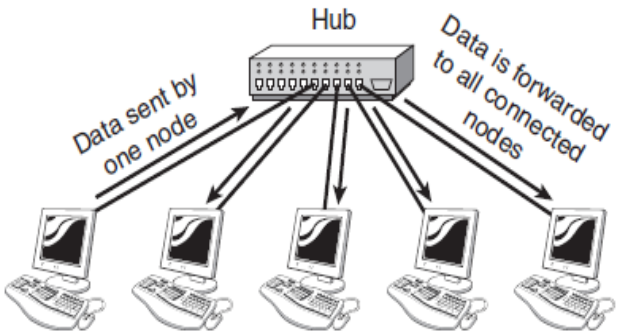
Basic Networking-Devices:

- **NIC(Network Interface Card:**

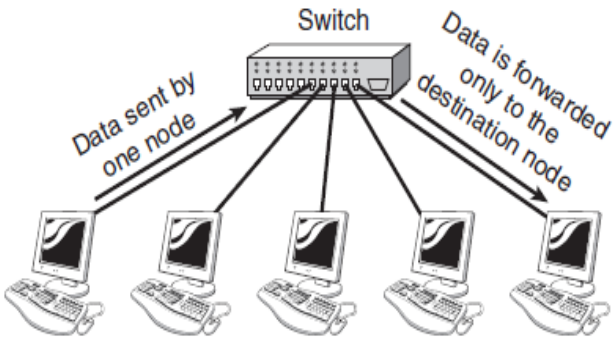
  - A network interface card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network.
  - Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology

- **Connecting Cables:**

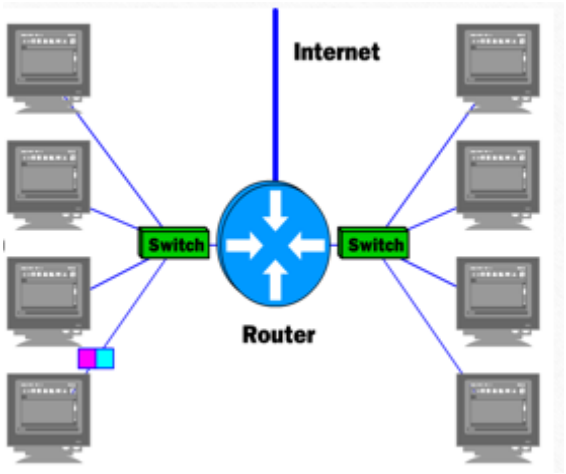
- **Hub**:
  - A hub, also called a network hub, is a common connection point for devices in a network.
  - Hubs are devices commonly used to connect segments of a LAN. Hub contains multiple ports.
  - When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.



- **Switch**
  - A **network switch** is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device.
  - A network switch forwards data only to the devices that need to receive it, rather than broadcasting the same data out of each of its ports.

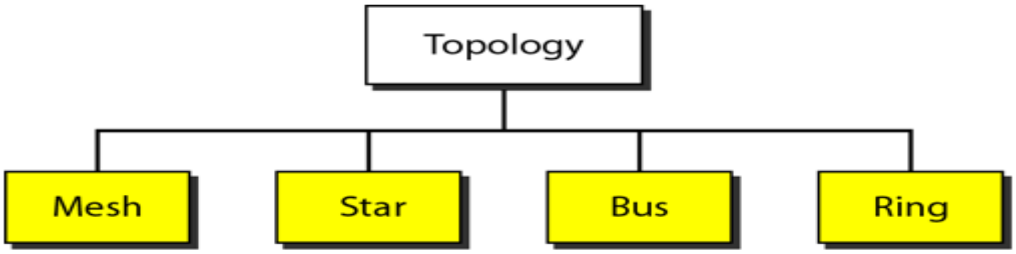


- **Routers**
  - **Routers** are small electronic devices that join multiple computer networks together via either wired or wireless connections.
  - A router is connected to two or more data lines from different networks.
  - When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination.
  - Using information in its routing table or routing policy, it directs the packet to the next network.



Network Topologies:

- A **network topology** is the arrangement of a **network**, including its nodes and connecting lines.



Mesh Topology:

- In a mesh topology, every device has a dedicated **point-to-point link** to every other device. The term *dedicated* means that the link carries data only between the two devices it connects.
- One practical example of a mesh topology is the connection of **telephone regional offices** in which each regional office needs to be connected to every other regional office.
- To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node.
- Node 1 must be connected to *n* - 1 nodes, node 2 must be connected to *n* – 1 nodes, and finally node *n* must be connected to n-1 nodes.
- However each physical link allows communication in both directions (duplex mode).

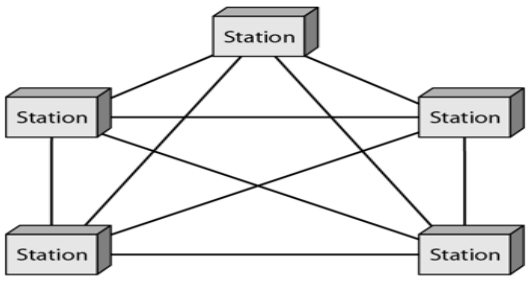


Fig: ***A fully connected mesh topology (five devices)***

Advantages of mesh-topology:

- Dedicated links guarantees that each connection can carry its own data load.
- Mesh topology is robust. If one link becomes unusable, it does not fail the entire system.
- There is the advantage of privacy or security.
- Point-to-Point links make fault identification and fault correction easy.

Disadvantages of mesh-topology:

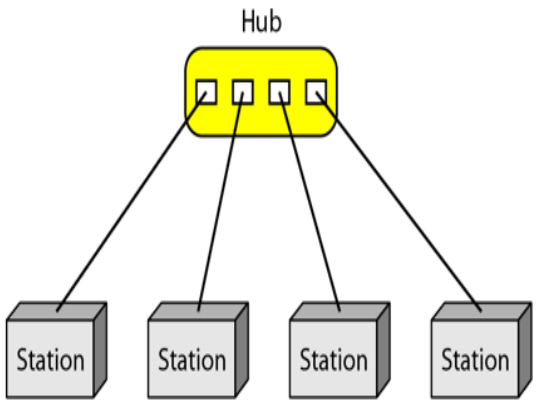
- The amount of cabling and the number of I/O ports required are high.
- Every device must be connected to every other device, installation and reconnection are difficult.
- The bulk wiring can be greater than the available space (in walls, ceilings, or floors).
- The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

Star-Topology:

- In a star topology, each device has a dedicated **point-to-point link** only to a central controller, usually called a **hub**.
- The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then transfers the data to the other connected device.
- The star topology is used in **local-area networks (LANs**),

Advantages of star topology:

- A star topology is less expensive than a mesh topology.
- In a star, each device needs only one link and one I/O port to connect it to any number of others.
- Any additions, moves, and deletions involve only one connection: between that device and the hub.
- If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault correction.

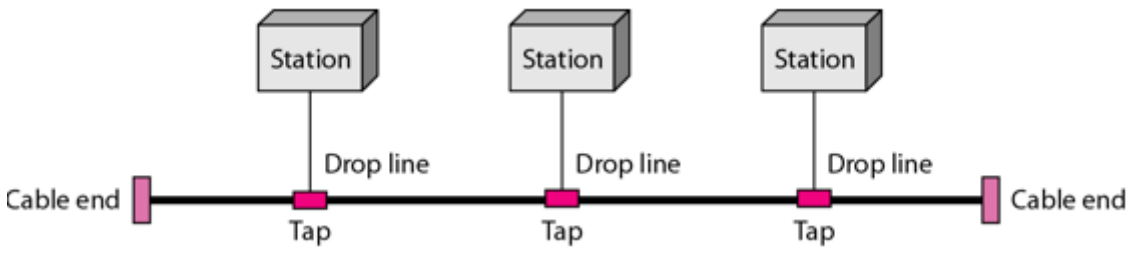


Disadvantages of star topology:

- Star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. This reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

Bus-Topology:

- A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network
- Nodes are connected to the bus cable by **drop lines** and **taps**.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.



- As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther.
- For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.
- Bus topology was the one of the first topologies used in the design of early **local area networks**. Ethernet LANs can use a bus topology, but they are less popular now

Advantages of bus topology

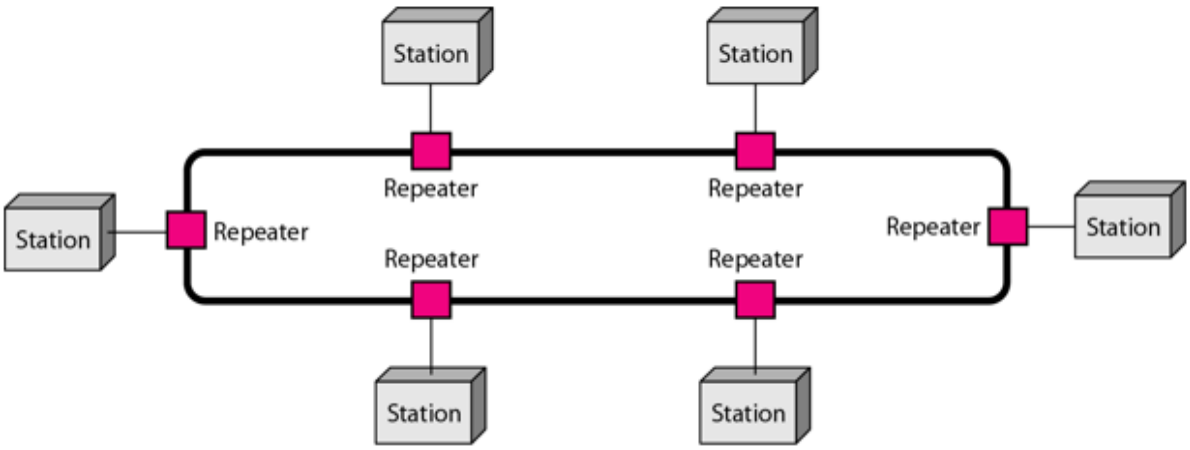
- Ease of installation.
- In a bus, this redundancy is eliminated.

Disadvantages of bus topology

- Difficult reconnection and fault isolation
- A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- A fault or break in the bus cable stops all transmission. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring-Topology:

- In a ring topology, each device has a dedicated **point-to-point** connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- **Each device in the ring incorporates a repeater**. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages of ring topology:

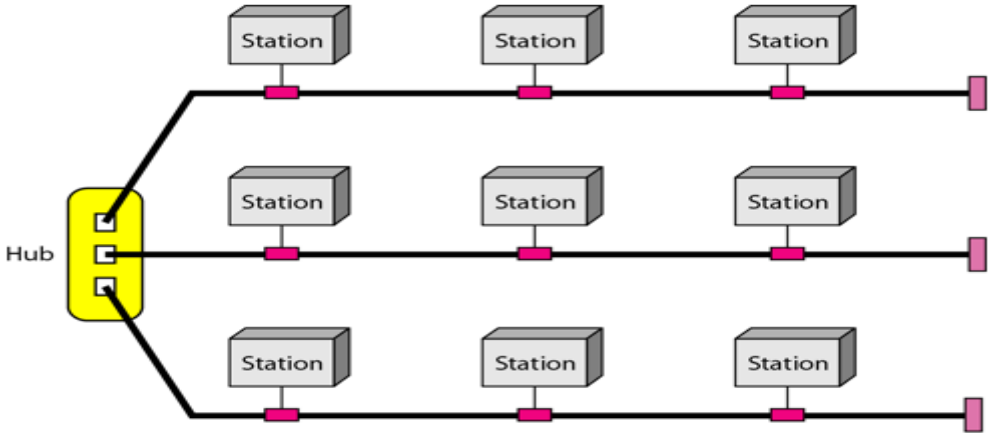
- easy to install and reconfigure
- Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections

Disadvantages of ring topology:

- Unidirectional traffic, In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

Hybrid-Topology:

- A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure



A hybrid topology: a star backbone with three bus networks

Categories of Networks:

- Based on the **size** (geographical area) network fall into 3 categories:
  - **LAN (Local Area Networks)**
  - **MAN (Metropolitan Area Networks)**
  - **WAN (Wide Area Networks)**

LAN (Local Area Networks):

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus.
- Currently, LAN size is limited to a few kilometres.
- LANs are designed to allow resources to be shared between personal computers or workstations.
- The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.
- LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.
- In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are ***bus, ring,*** *and* ***star.***

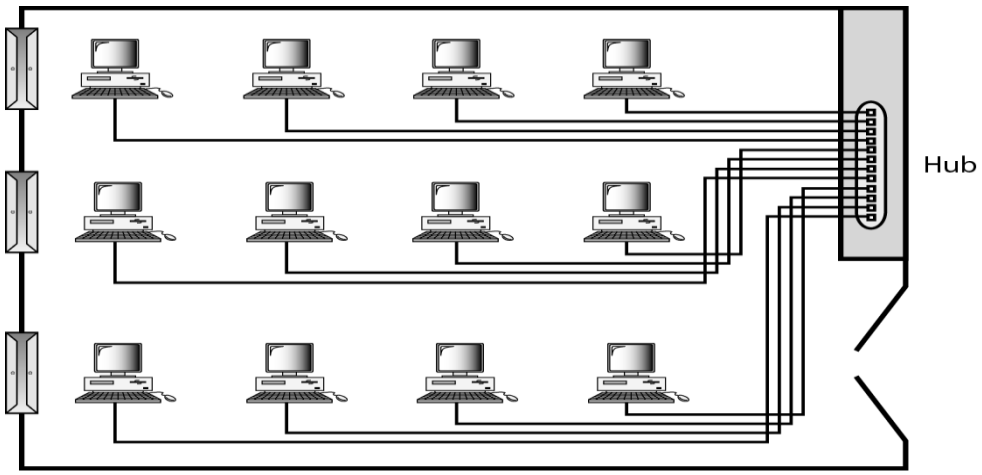


Figure: An isolated LAN connecting 12 computers to a hub in a closet

MAN (Metropolitan Area Networks)

- A metropolitan area network (MAN) is a network with a size between a LAN and a WAN.
- It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.
- MANs are widely used in Television Broadcasting.

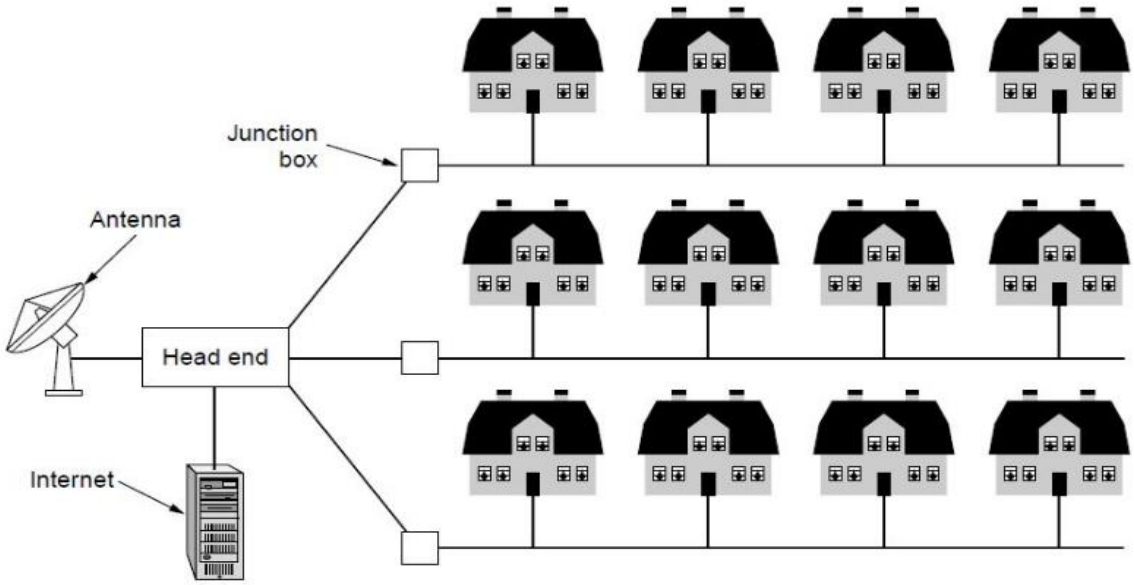


Figure: Metropolitan area network based cable TV.

- A MAN is implemented by a standard called **DQDB (Distributed Queue Dual Bus)** or IEEE 802.16.

WAN (Wide Area Networks):

- A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.
- A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet.
- The WAN can be designed in two ways:
- **The switched WAN** connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.

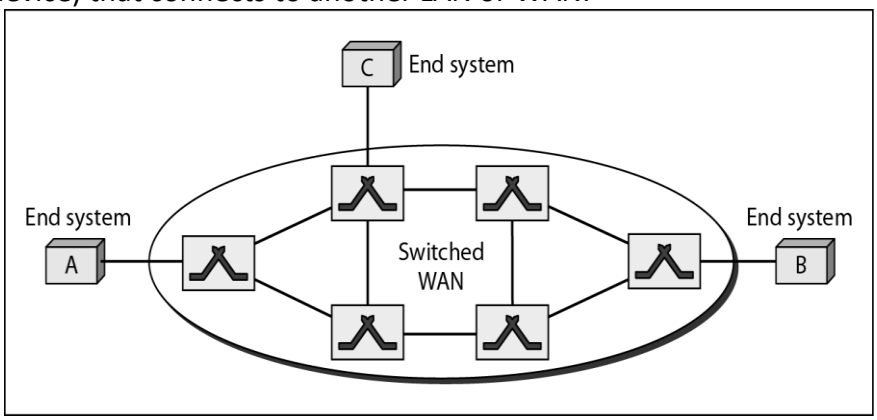


Figure: Switched WAN

- **The point-to-point WAN** is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP).
- This type of WAN is often used to provide Internet access.

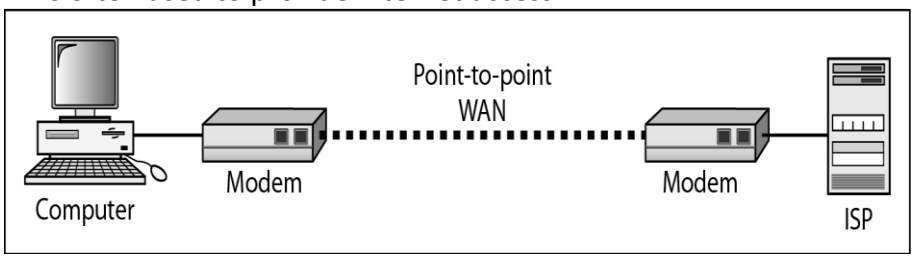
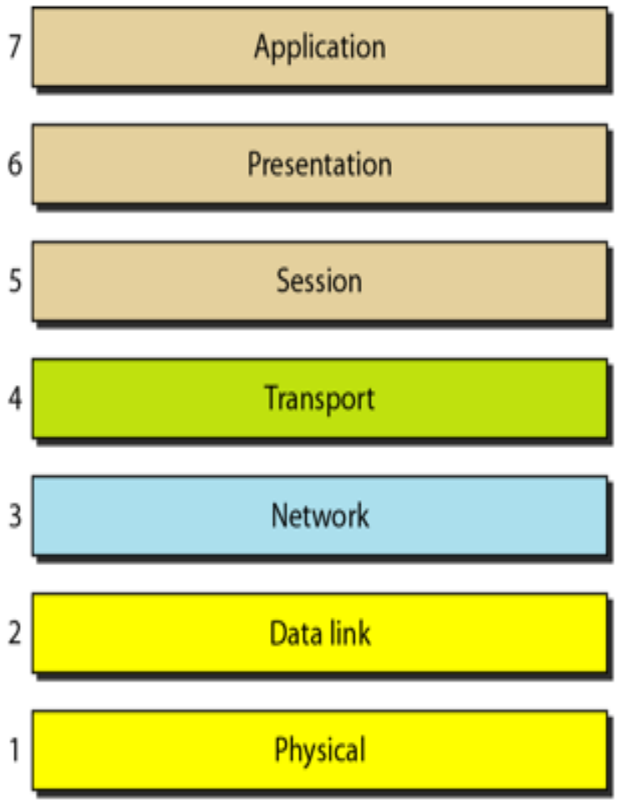
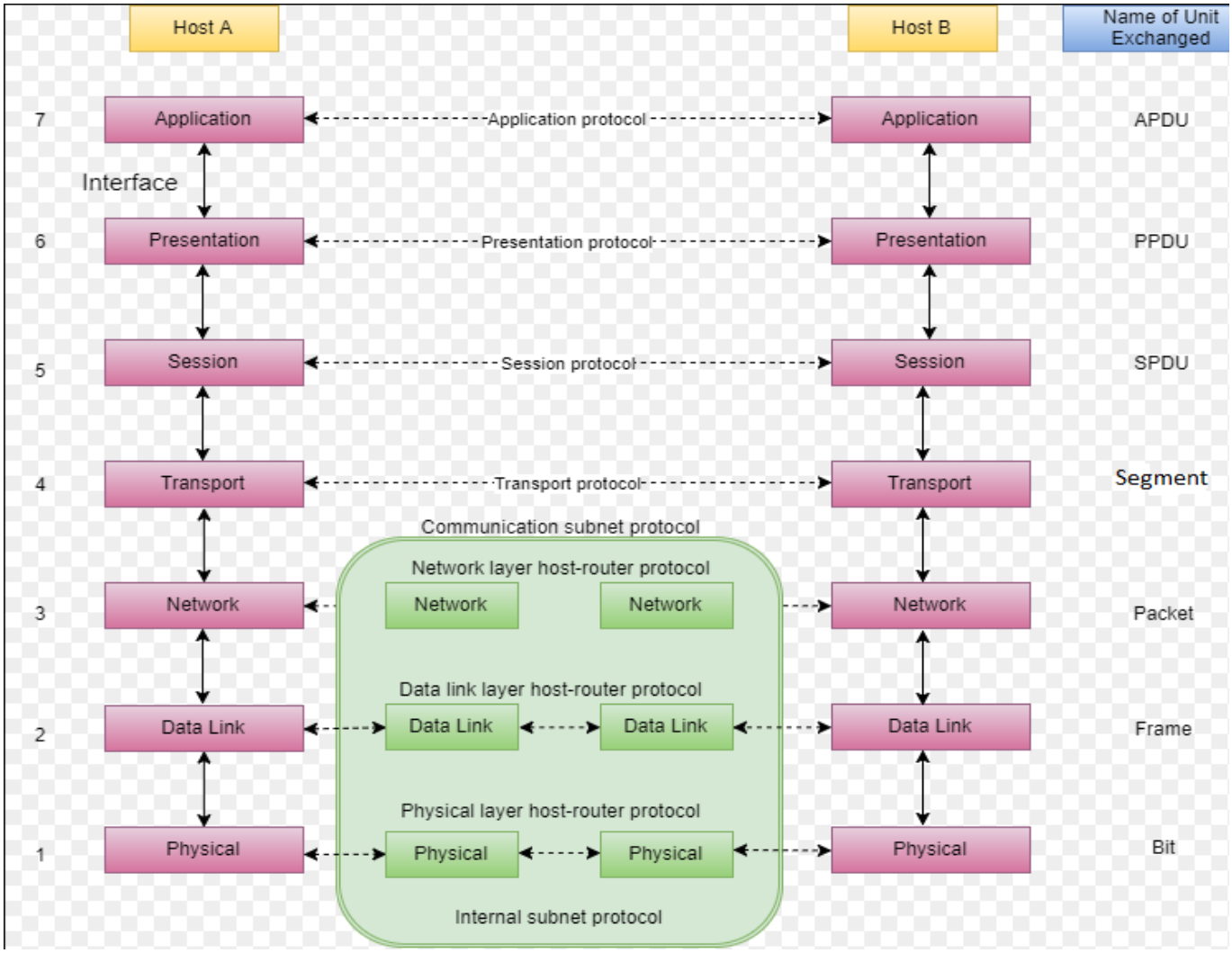


Figure: Point-to-Point WAN

OSI-Reference model:

- The OSI model is based on the proposal developed by International Standards Organization (ISO) this model is called as ISO-OSI (Open Systems Interconnection) Reference Model because it is used for connecting the open systems.
- That is the systems which are open for communication with other systems.
- It was a first step towards the International standardization of the protocols used in various layers by Day and Zimmermann in 1983.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of **seven** separate but related layers, each of which defines a part of the process of moving information across a network.





Physical Layer(Layer-1):

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

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

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

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

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

Data Link Layer (Layer 2)

- The data link layer is responsible for the node to node delivery of the message.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
- Data Link Layer is divided into two sub layers:
    - Logical Link Control (LLC)
    - Media Access Control (MAC)
- Packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). Datalink Layer also encapsulates Sender and Receiver's MAC address in the header.
- **The functions of the data Link layer are**:

    Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

    Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.

    Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

    Flow Control: The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.

    Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.
- Switch & Bridge are Data Link Layer devices.

Network Layer (Layer 3):

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

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

    Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.
- Network layer is implemented by networking devices such as routers.

Transport Layer (Layer 4):

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

  Segmentation and Reassembly: This layer accepts the message from the (session) layer, breaks the message into smaller units. Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.

  Service Point Addressing: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.
- **The services provided by transport layer:**

  Connection Oriented Service (TCP):

  In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

  Connection less service(UDP):

  In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.
- Data in the Transport Layer is called as Segments.
- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls. Transport Layer is called as Heart of OSI model.

Session Layer (Layer 5):

- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
- **The functions of the session layer are:**

  Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.

  Synchronization: This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

  Dialog Controller: The session layer determines which device will communicate first and the amount of data that will be sent.

Presentation Layer (Layer 6):

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

  Translation: For example, ASCII to EBCDIC.

  Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

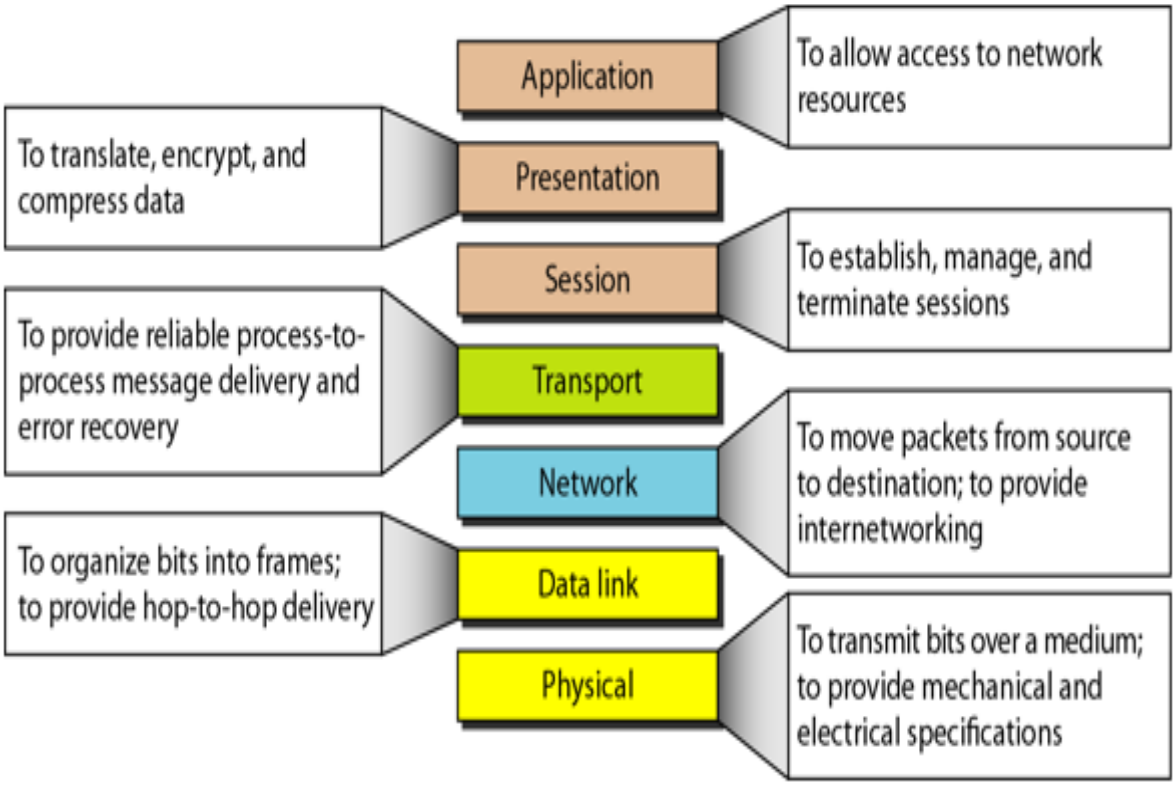
  Compression: Reduces the number of bits that need to be transmitted on the network.

Application Layer (Layer 7):

- At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications.
- These applications produce the data, which has to be transferred over the network.
- This layer also serves as window for the application services to access the network and for displaying the received information to the user.
  Ex: Application – Browsers, Skype Messenger etc.
- *Application Layer is also called as Desktop Layer.*
- **The functions of the Application layer are:**
  - * Network Virtual Terminal
  - * File transfer access and management
  - * Mail Services
  - * Directory Services

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

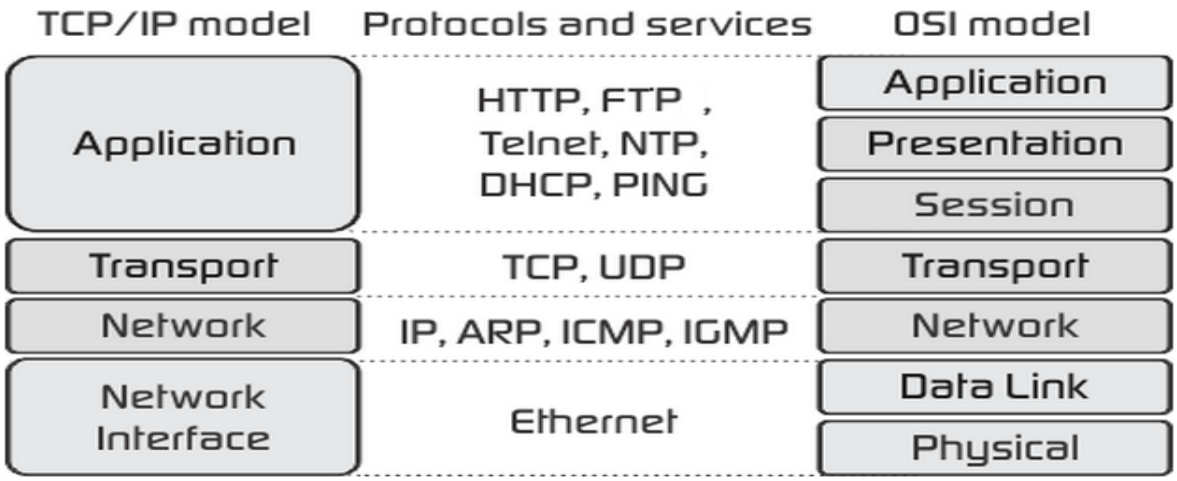
Summary of Layers:



TCP/IP Model:

- The **OSI Model** we just looked at is just a reference/logical model.
- It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model.
- It contains four layers, unlike seven layers in the OSI model. The layers are:

  Application Layer/Process Layer
  Transport Layer/Host-to-Host Layer
  Network/Internet Layer
  Network interface Layer



Network interface Layer:

- This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model.
- It looks out for hardware addressing and the protocols present in this layer allows for physical transmission of data.
- We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

Network or Internet Layer:

- This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network.
- **The main protocols residing at this layer are:**

  IP: stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.

  ICMP: Stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.

  ARP: stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

Transport Layer:

- This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data.
- It shields the upper-layer applications from the complexities of data.
- The two main protocols present in this layer are:

Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgement feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

User Datagram Protocol (UDP) – On the other hand does not provide any such features. It is the go to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

Application Layer:

- This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer.
- It is responsible for node-to-node communication and controls user-interface specifications.
- Some of the protocols present in this layer are: HTTP, FTP, Telnet, SMTP, NTP, DNS, DHCP.

HTTP: Hyper Text Transfer Protocol, used by the World Wide Web to manage communications between web browsers and server.

FTP: File Transfer Protocol, the standard network protocol used for the transfer of computer files between a client and server on a computer network.

TELNET: Used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.

NTP: Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source.

SMTP: Simple Mail Transfer Protocol is a TCP/IP protocol used in sending and receiving e-mail.

DNS: The domain name system (**DNS**) is the way that internet domain names are located and translated into internet protocol (IP) addresses.

DHCP: The **Dynamic Host Configuration Protocol** (**DHCP**) is a network management protocol used on TCP/IP networks whereby a **DHCP** server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

Comparison between OSI and TCP/IP Model:

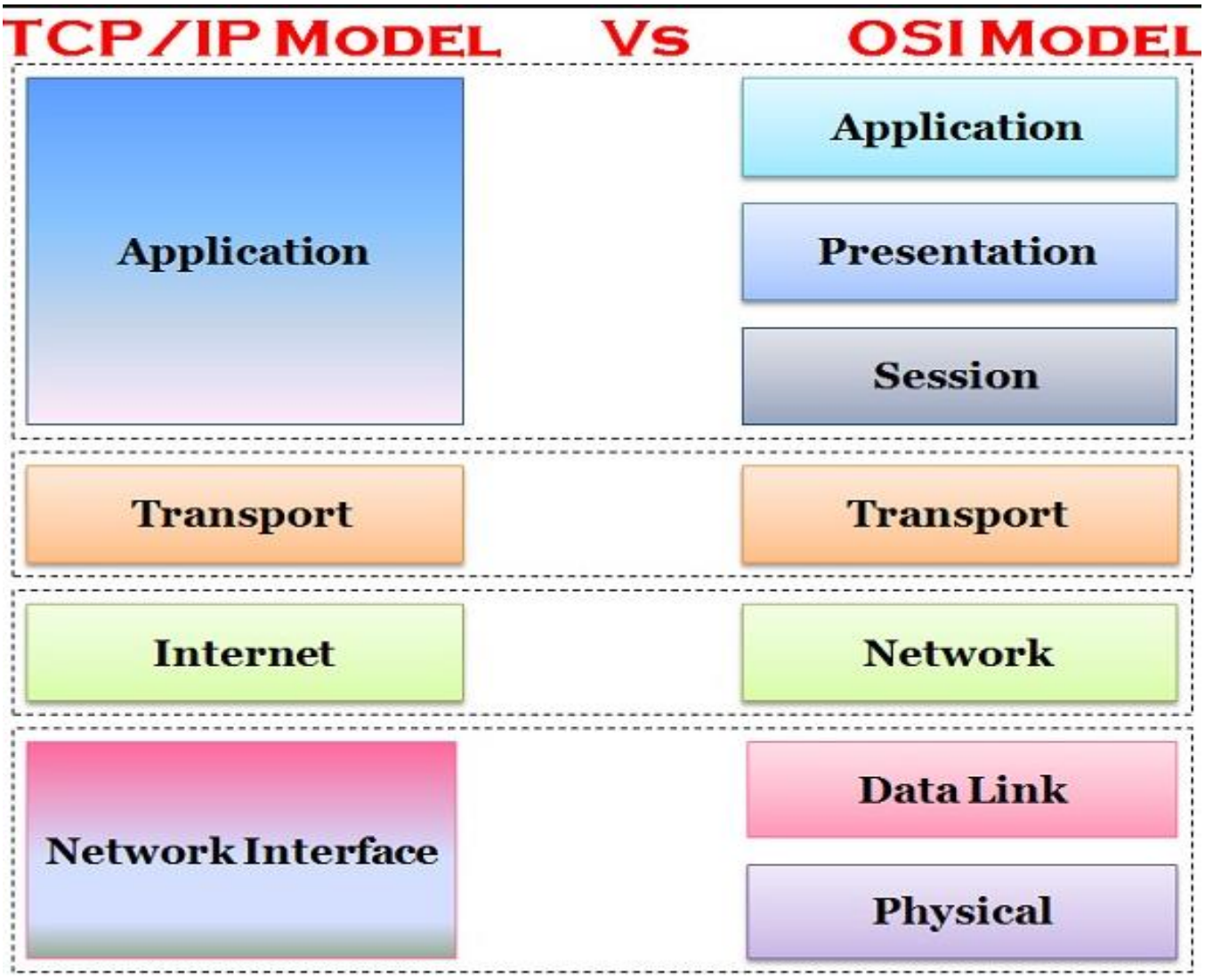
Following are some similarities between OSI Reference Model and TCP/IP Reference Model.

- Both are layered architecture.
- Layers provide similar functionalities.
- Both are protocol stack.
- Both are reference models.

Comparison:

OSI(Open System Interconnection)	**TCP/IP (Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.

9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers



Novell Networks (or) NetWare:

- **NetWare** is a discontinued computer network operating system developed by Novell, Inc.
- It initially used cooperative multitasking to run various services on a personal computer, using the IPX network protocol.
- The original NetWare product in 1983, supported clients running both CP/M and MS-DOS, ran over a proprietary star network topology and was based on a Novell-built file server using the Motorola 68000 processor, but the company soon moved away from building its own hardware.
- NetWare became hardware-independent, running on any suitable Intel-based IBM PC compatible system, and a wide range of network cards.
- From the beginning NetWare implemented a number of features inspired by mainframe and minicomputer systems that were not available in its competitors.
- In the early 1990s, Novell introduced separate cheaper networking products, unrelated to classic NetWare. These were NetWare Lite 1.0 (NWL), and later Personal NetWare 1.0 (PNW) in 1993.
- In 1993, the main product line took a dramatic turn when Version 4 introduced NetWare Directory Services (NDS), a global directory service similar to the Active Directory that Microsoft would release seven years later. This, along with a new e-mail system, GroupWise, application configuration suite, ZENworks, and security product BorderManager were all targeted at the needs of large enterprises.
- By 2000, however, Microsoft was taking more of Novell's customer base and Novell increasingly looked to a future based on a Linux kernel.
- The successor to NetWare, *Open Enterprise Server* (OES), released in March 2005, offered all the services previously hosted by NetWare v6.5, but on a SUSE Linux Enterprise Server; the NetWare kernel remained an option until OES 11 in late 2011.
- The final update release was version 6.5SP8 of May 2009; Netware is no longer on Novell's product list. NetWare 6.5SP8 General Support ended in 2010, with Extended Support until the end of 2015, and Self Support until the end of 2017. The replacement is *Open Enterprise Server*.

ARPANET:

In the mid-1960s, mainframe computers in research organizations were stand-alone devices. Computers from different manufacturers were unable to communicate with one another. The **Advanced Research Projects Agency (ARPA)** in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for **ARPANET,** a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *interface message processor* (IMP). The IMPs, in turn, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the *Network Control Protocol* (NCP) provided communication between the hosts.

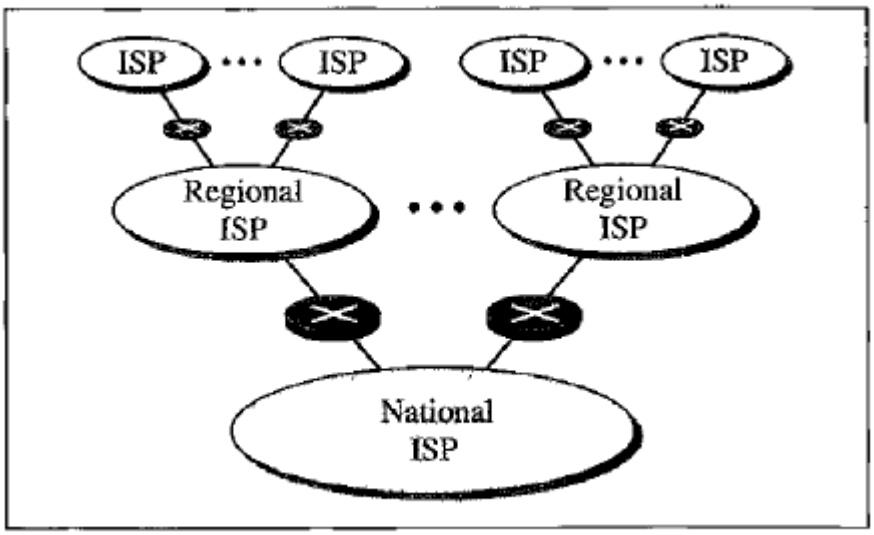
In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetting Project*. Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

Shortly thereafter, authorities made a decision to split TCP into two protocols: **Transmission Control Protocol (TCP)** and **Internetworking Protocol (IP).** IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCP/IP.

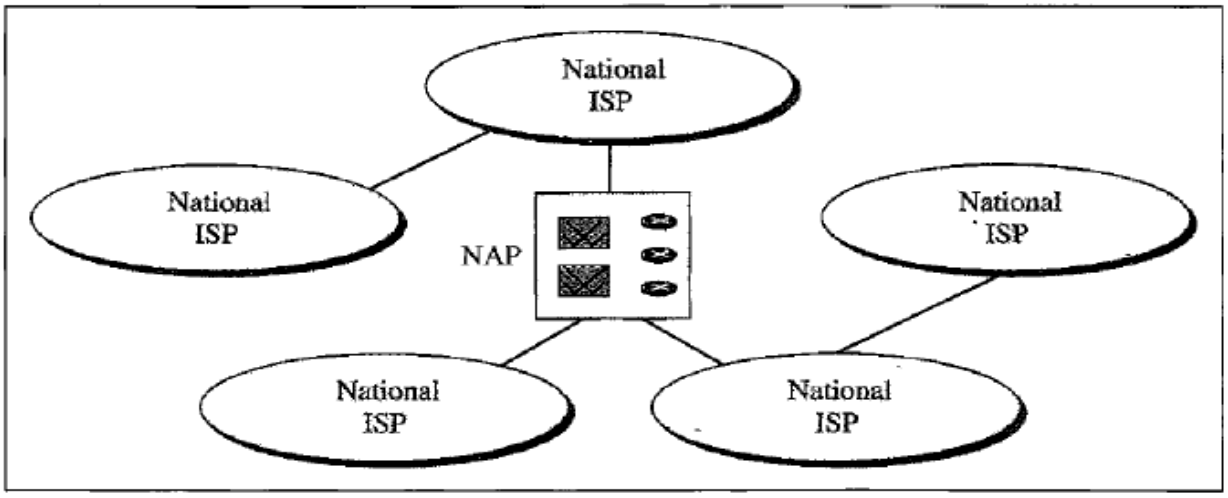
Internet:

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing—new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of **Internet service providers (ISPs).** There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure 1.13 shows a conceptual (not geographic) view of the Internet.

Hierarchical organization of the Internet



a. Structure of a national ISP



b. Interconnection of national ISPs

International Internet Service Providers

At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers

The **national Internet service providers** are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet MCI. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called **network access points (NAPs).** Some national ISP networks are also connected to one another by private switching stations called *peering points*. These normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers

Regional internet service providers or **regional ISPs** are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

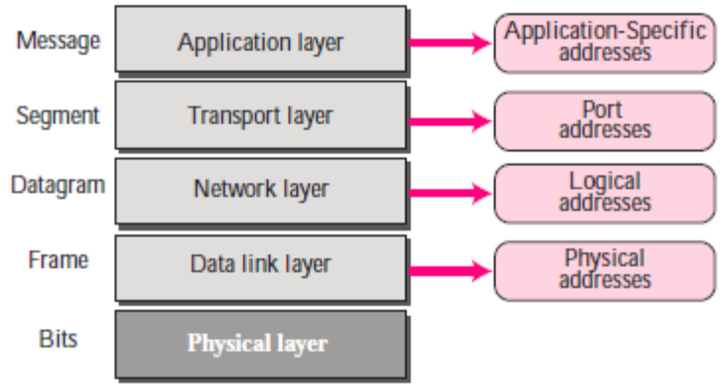
Local Internet Service Providers

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

****

ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical address, logical address, port address, and application-specific address. Each address is related to a one layer in the TCP/IP architecture, as shown in the following Figure.



Physical Addresses

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

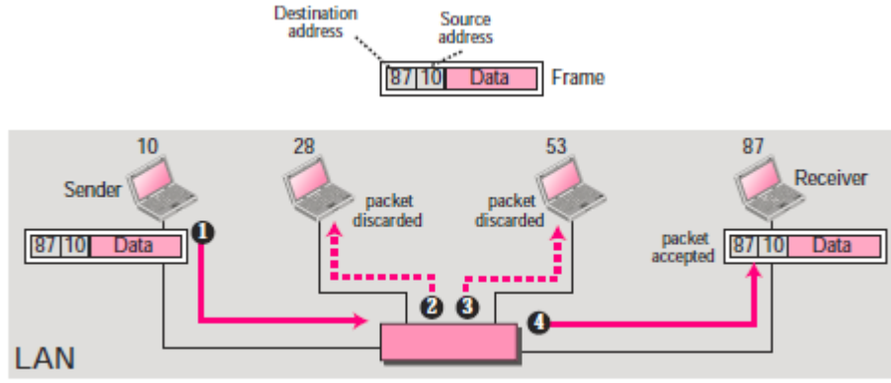
Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below.

07:01:02:01:2C:4B
A 6-byte (12 hexadecimal digits) physical address

Example (1)

In Figure below a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (a LAN). At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.

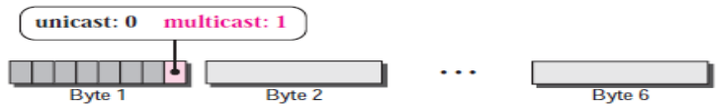
Note that in most data link protocols, the destination address 87 in this case, comes before the source address (10 in this case). The frame is propagated through the LAN. Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.



Unicast, Multicast, and Broadcast Physical Addresses

Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network). Some networks support all three addresses.

A source address is always a unicast address—the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. The least significant bit of the first byte defines the type of address.



Q: Define the type of the following destination addresses:

1. 4A:30:10:21:10:1A
2. 47:20:1B:2E:08:EE
3. FF:FF:FF:FF:FF:FF

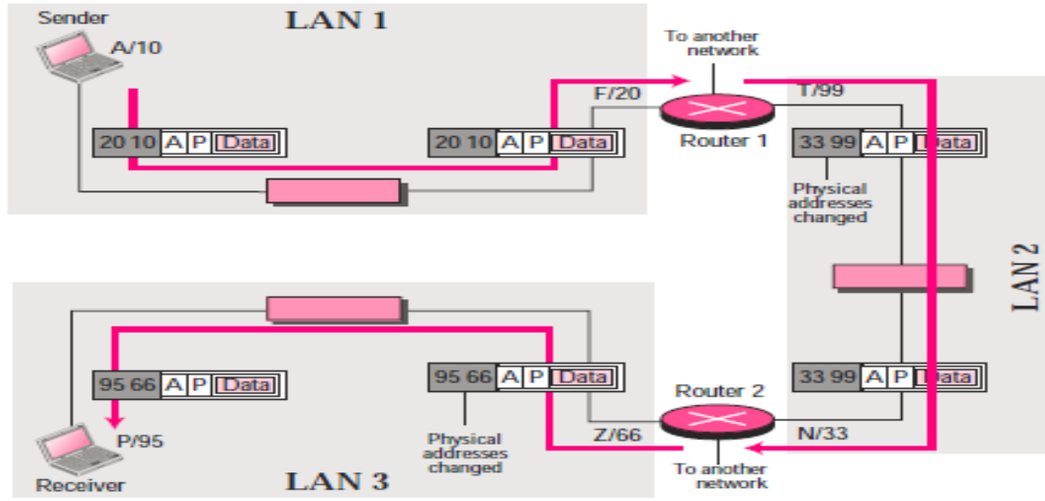
Logical Addresses

Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example (2)

The Figure below shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection. Although it may be obvious that each router must have a separate physical address for each connection, it may. The computer with logical address

A and physical address **10** needs to send a packet to the computer with logical address **P** and physical address **95**. The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). Note that in most protocols, the logical source address comes before the logical destination address (contrary to the order of physical addresses). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its routing table and finds the logical address of the next hop (router 1) to be F.



Another protocol, Address Resolution Protocol (ARP) finds the physical address of router 1 that corresponds to its logical address (20). Now the network layer passes this address to the data link layer, which in turn, encapsulates the packet with physical destination address 20 and physical source address 10. The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2.

Note the physical addresses in the frame. The source physical address changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost. At router 2 we have a similar scenario. The physical addresses are changed, and a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination logical address P matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer. Note that although physical addresses will change from hop to hop, logical addresses remain the same from the source to destination.

The physical addresses will change from hop to hop, but the logical addresses remain the same.

Unicast, Multicast, and Broadcast Addresses

The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network).

Port Addresses

The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. Computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes.

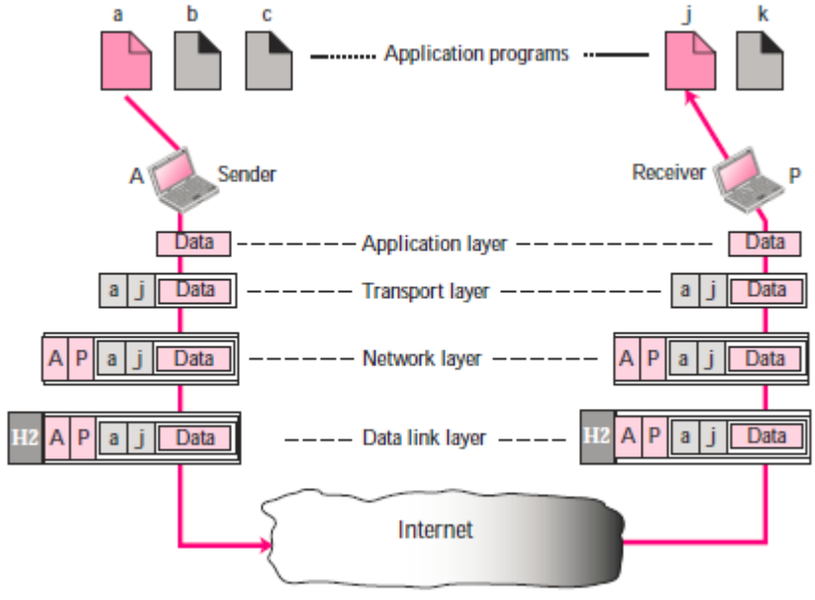
In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

A port address is a 16-bit address represented by one decimal number as shown.

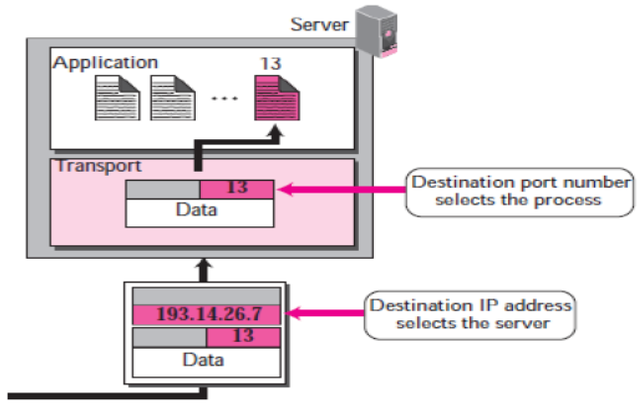
753
A 16-bit port address represented as one single number

Example (3)

The following Figure shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses **a**, **b**, and **c**. The receiving computer is running two processes at this time with port addresses **j** and **k**. Process **a** in the sending computer needs to communicate with process **j** in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a client program and the other is a server program.



To show that data from process **a** need to be delivered to process **j**, and not **k**, the transport layer encapsulates data from the application layer in a packet and adds two port addresses (**a** and **j**), source and destination. The packet from the transport layer is then encapsulated in another packet at the network layer with logical source and destination addresses (**A** and **P**). Finally, this packet is encapsulated in a frame with the physical source and destination addresses of the next hop. We have not shown the physical addresses because they change from hop to hop inside the cloud designated as the Internet. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.



- In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535.
- The client program defines itself with a port number, called the **ephemeral port number** (chosen randomly). The word ephemeral means *short lived*.
- The server process must also define itself with a port number (called well-known port numbers). This port number, however, cannot be chosen randomly.

*ICANN Ranges (*Internet Corporation for Assigned Names and Numbers)

ICANN has divided the port numbers into three ranges: well-known, registered, and dynamic (or private)

- **Well-known ports:** The ports ranging from 0 to 1,023 are assigned and controlled by ICANN..
- **Registered ports:** The ports ranging from 1,024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.
- **Dynamic ports:** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers. The original recommendation was that the ephemeral port numbers for clients be chosen from this range. However, most systems do not follow this recommendation.

Application-Specific Addresses

Some applications have user-friendly addresses that are designed for that specific application. Examples include the e-mail address (for example, co_sci@yahoo.com) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.