COMPUTER NETWORKS

UNIT-1

NETWORK FUNDAMENTALS

Uses of Networks – Categories of Networks -Communication model –Data transmission concepts and terminology – Protocols – OSI– LAN Topology - Transmission media.

COMPUTER NETWORK

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

USES OF COMPUTER NETWORK

Computer networks have become invaluable to organizations as well as individuals. Some of its main uses are as follows −

- **Information and Resource Sharing** − Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.

- **Retrieving Remote Information** − Through computer networks, users can retrieve remote information on a variety of topics. The information is stored in remote databases to which the user gains access through information systems like the World Wide Web.

- **Speedy Interpersonal Communication** − Computer networks have increased the speed and volume of communication like never before. Electronic Mail (email) is extensively used for sending texts, documents, images, and videos across the globe. Online communications have increased by manifold times through social networking services.

- **E-Commerce** − Computer networks have paved way for a variety of

business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.

- **Highly Reliable Systems** − Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.

- **Cost–Effective Systems** − Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.

- **VoIP** − VoIP or Voice over Internet protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

Categories of Network

One way to categorize the different types of computer network designs is by their scope or scale. For historical reasons, the networking industry refers to nearly every type of design as some kind of *area network*. Common examples of area network types are:

- LAN - Local Area Network
- WLAN - Wireless Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network

Local Area Network

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet. In addition to operating in a limited

space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

Wireless Local Area Network

As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

Wide Area Network

A WAN is a network that spans more than one geographical location often connecting separated LANs. WANs are slower than LANs and often require additional and costly hardware such as routers, dedicated leased lines, and complicated implementation procedures.

Metropolitan Area Network

A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned an operated by a single entity such as a government body or large corporation.

COMMUNICATION MODEL

Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork.

A set of devices often mentioned as nodes connected by media link is called a Network.

A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called **Communication channels**.

Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same

network. It is also called Data Network. The best example of computer network is Internet.

Computer network does not mean a system with one Control Unit connected to multiple other systems as its slave. That is Distributed system, not Computer Network.

A network must be able to meet certain criteria, these are mentioned below:

1. Performance
2. Reliability
3. Scalability

Computer Networks: Performance

It can be measured in the following ways:

- **Transit time :** It is the time taken to travel a message from one device to another.
- **Response time :** It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are :

1. Efficiency of software
2. Number of users
3. Capability of connected hardware

Computer Networks: Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

Computer Networks: Security

It refers to the protection of data from any unauthorised user or access. While travelling through network, data passes many layers of

network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Properties of a Good Network

1. **Interpersonal Communication:** We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc, all of these are possible because of computer networks.

2. **Resources can be shared:** We can share physical resources by making them available on a network such as printers, scanners etc.

3. **Sharing files, data:** Authorised users are allowed to share the files on the network.

Basic Communication Model

A Communication model is used to exchange data between two parties. For example: communication between a computer, server and telephone (through modem).

Communication Model: Source

Data to be transmitted is generated by this device, example: telephones, personal computers etc.

Communication Model: Transmitter

The data generated by the source system is not directly transmitted in the form its generated. The transmitter transforms and encodes the data in such a form to produce electromagnetic waves or signals.

Communication Model: Transmission System

A transmission system can be a single transmission line or a complex network connecting source and destination.

Communication Model: Receiver

Receiver accepts the signal from the transmission system and converts it into a form which is easily managed by the destination device.

Communication Model: Destination

Destination receives the incoming data from the receiver.

Data Communication

The exchange of data between two devices through a transmission medium is called **Data Communication**. The data is exchanged in the form of **0's** and **1's**. The transmission medium used is wire cable. For data communication to occur, the communication device must be a part of a communication system. Data Communication has two types - **Local** and **Remote** which are discussed below:

Data Communication: Local

Local communication takes place when the communicating devices are in the same geographical area, same building, or face-to-face etc.

Data Communication: Remote

Remote communication takes place over a distance i.e. the devices are farther. The effectiveness of a data communication can be measured through the following features :

1. **Delivery**: Delivery should be done to the correct destination.
2. **Timeliness**: Delivery should be on time.
3. **Accuracy**: Data delivered should be accurate.

Components of Data Communication

1. **Message:** It is the information to be delivered.
2. **Sender:** Sender is the person who is sending the message.

3. **Receiver:** Receiver is the person to whom the message is being sent to.

4. **Medium:** It is the medium through which the message is sent. For example: A Modem.

5. **Protocol:** These are some set of rules which govern data communication.

Data transmission concepts and terminology

Before we dive into details of networking, let us discuss some common terms associated with data communication.

Channel

Physical medium like cables over which information is exchanged is called **channel**. Transmission channel may be **analog** or **digital**. As the name suggests, analog channels transmit data using **analog signals** while digital channels transmit data using **digital signals**.

In popular network terminology, path over which data is sent or received is called **data channel**. This data channel may be a tangible medium like copper wire cables or broadcast medium like **radio waves**.

Data Transfer Rate

The speed of data transferred or received over transmission channel, measured per unit time, is called data transfer rate. The smallest unit of measurement is bits per second (bps). 1 bps means 1 bit (0 or 1) of data is transferred in 1 second.

Here are some commonly used data transfer rates −

- 1 Bps = 1 Byte per second = 8 bits per second
- 1 kbps = 1 kilobit per second = 1024 bits per second
- 1 Mbps = 1 Megabit per second = 1024 Kbps
- 1 Gbps = 1 Gigabit per second = 1024 Mbps

Bandwidth

Data transfer rates that can be supported by a network is called its bandwidth. It is measured in bits per second (bps). Modern day

networks provide bandwidth in Kbps, Mbps and Gbps. Some of the factors affecting a network's bandwidth include −

- Network devices used
- Protocols used
- Number of users connected
- Network overheads like collision, errors, etc.

Throughput

Throughput is the actual speed with which data gets transferred over the network. Besides transmitting the actual data, network bandwidth is used for transmitting error messages, acknowledgement frames, etc.

Throughput is a better measurement of network speed, efficiency and capacity utilization rather than bandwidth.

Protocol

Protocol is a set of rules and regulations used by devices to communicate over the network. Just like humans, computers also need rules to ensure successful communication. If two people start speaking at the same time or in different languages when no interpreter is present, no meaningful exchange of information can occur.

Similarly, devices connected on the network need to follow rules defining situations like when and how to transmit data, when to receive data, how to give error-free message, etc.

Some common protocols used over the Internet are −

- Transmission Control Protocol
- Internet Protocol
- Point to Point Protocol
- File Transfer Protocol
- Hypertext Transfer Protocol
- Internet Message Access Protocol

PROTOCOLS

There are various types of protocols that support a major and compassionate role in communicating with different devices across the network. These are:

1. Transmission Control Protocol (TCP)
2. Internet Protocol (IP)
3. User Datagram Protocol (UDP)
4. Post office Protocol (POP)
5. Simple mail transport Protocol (SMTP)
6. File Transfer Protocol (FTP)
7. Hyper Text Transfer Protocol (HTTP)
8. Hyper Text Transfer Protocol Secure (HTTPS)
9. Telnet
10. Gopher

Transmission Control Protocol (TCP): TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.

Internet Protocol (IP): IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.

User Datagram Protocol (UDP): UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.

Post office Protocol (POP): POP3 is designed for receiving incoming E-mails.

Simple mail transport Protocol (SMTP): SMTP is designed to send and distribute outgoing E-Mail.

File Transfer Protocol (FTP): FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.

Hyper Text Transfer Protocol (HTTP): HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.

Hyper Text Transfer Protocol Secure (HTTPS): HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. HTTP is used for transferring data between the client browser (request) and the web server (response) in the hypertext format, same in case of HTTPS except that the transferring of data is done in an encrypted format. So it can be said that https thwart hackers from interpretation or modification of data throughout the transfer of packets.

Telnet: Telnet is a set of rules designed for connecting one system with another. The connecting process here is termed as remote login. The system which requests for connection is the local computer, and the system which accepts the connection is the remote computer.

Gopher: Gopher is a collection of rules implemented for searching, retrieving as well as displaying documents from isolated sites. Gopher also works on the client/server principle.

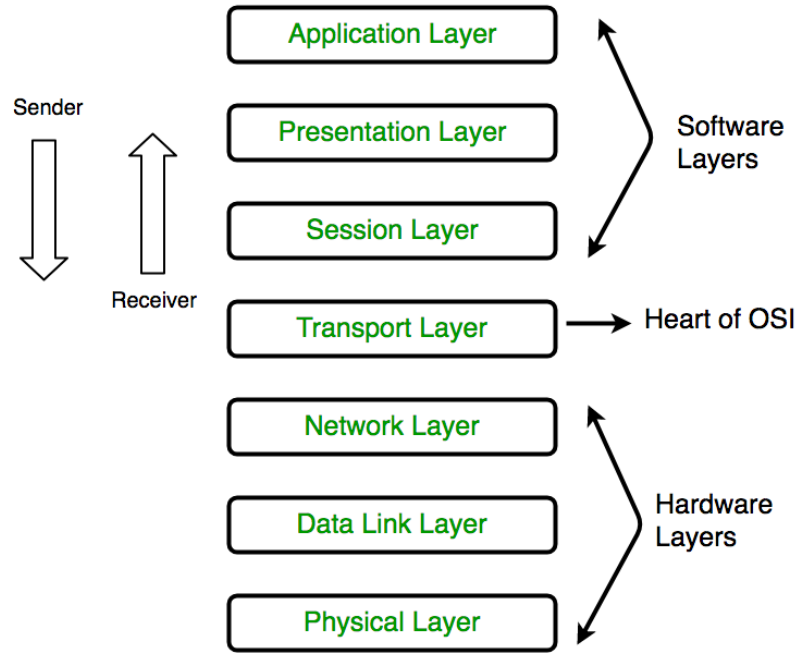
Some other popular protocols act as co-functioning protocols associated with these primary protocols for core functioning. These are:

- ARP (Address Resolution Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- IMAP4 (Internet Message Access Protocol)
- SIP (Session Initiation Protocol)

- RTP (Real-Time Transport Protocol)
- RLP (Resource Location Protocol)
- RAP (Route Access Protocol)
- L2TP (Layer Two Tunnelling Protocol)
- PPTP (Point To Point Tunnelling Protocol)
- SNMP (Simple Network Management Protocol)
- TFTP (Trivial File Transfer Protocol)

OSI MODEL

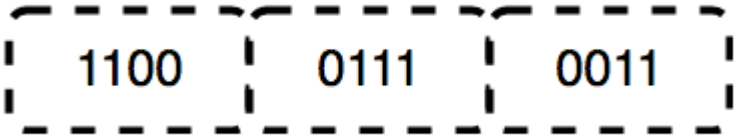
OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is

responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

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

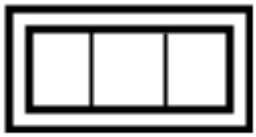
2. Data Link Layer (DLL) (Layer 2) :

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

- Logical Link Control (LLC)
- Media Access Control (MAC)

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

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



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, the Data link layer adds physical addresses (MAC address) of the 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 the amount of data that can be sent before receiving acknowledgement.

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

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

3. Network Layer (Layer 3) :

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

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

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

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

4. Transport Layer (Layer 4) :

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

the data if an error is found.

• **At sender's side:**

Transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.
Note: The sender needs to know the port number associated with the receiver's application.

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

• **At receiver's side:**

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

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 segments 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 the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

Connection-Oriented Service: It is a three-phase process that includes
– Connection Establishment
– Data Transfer
– Termination / disconnection
In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

* Data in the Transport Layer is called as **Segments**.
** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
Transport Layer is called as **Heart of OSI** model.

5. Session Layer (Layer 5) :

This layer is responsible for the 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 synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

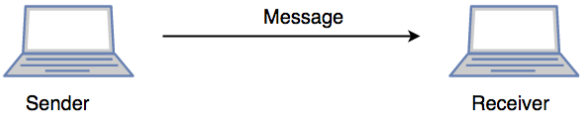
Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as “Application Layer”.
**Implementation of these 3 layers is done by the network application

itself. These are also known as **Upper Layers** or **Software Layers**.

SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0's and 1's) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

The 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 ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

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

7. Application Layer (Layer 7) :

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

Ex: Application – Browsers, Skype Messenger, etc.
**Application Layer is also called Desktop Layer.

The functions of the Application layer are :

Network Virtual Terminal

FTAM-File transfer access and management

Mail Services

Directory Services

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

LAN NETWORK TOPOLOGIES

Network topologies can take a bit of time to understand when you're all new to this kind of cool stuff, but it's very important to fully understand them as they are key elements to understanding and troubleshooting networks and will help you decide what actions to take when you're faced with network problems.

PHYSICAL AND LOGICAL TOPOLOGIES

There are two types of topologies: Physical and Logical. The physical topology of a network refers to the layout of cables, computers and other peripherals. Try to imagine yourself in a room with a small network, you can see network cables coming out of every computer that is part of the network, then those cables plug into a hub or switch. What you're looking at is the physical topology of that network !

Logical topology is the method used to pass the information between the computers. In other words, looking at that same room, if you were to try to see how the network works with all the computers

talking (think of the computers generating traffic and packets of data going everywhere on the network) you would be looking at the logical part of the network. The way the computers will be talking to each other and the direction of the traffic is controlled by the various protocols (like Ethernet) or, if you like, rules.

If we used token ring, then the physical topology would have to change to meet the requirements of the way the token ring protocol works (logically).

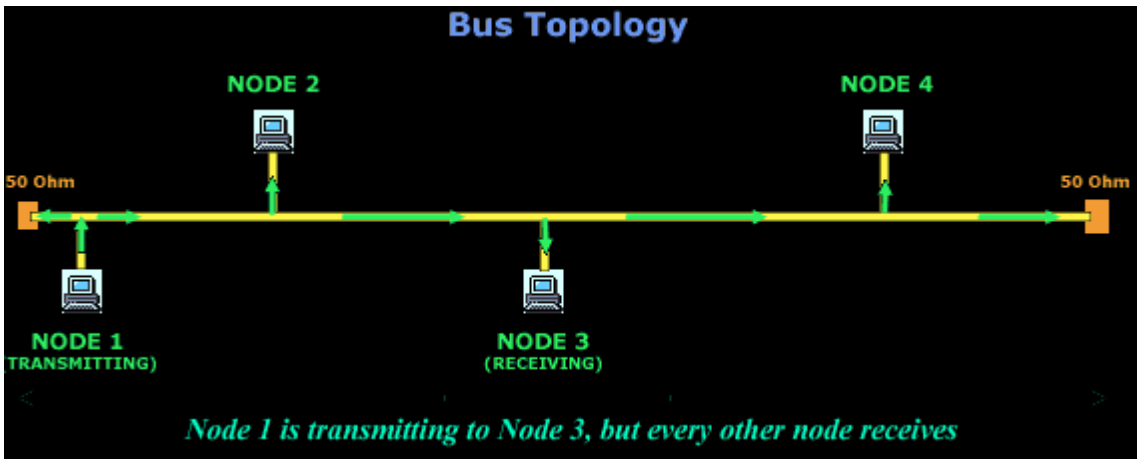
If it's all still confusing, consider this: The physical topology describes the layout of the network, just like a map shows the layout of various roads, and the logical topology describes how the data is sent accross the network or how the cars are able to travel (the direction and speed) at every road on the map.

The most common types of physical topologies, which we are going to analyse, are: Bus, Hub/Star and Ring

THE PHYSICAL BUS TOPOLOGY

Bus topology is fairly old news and you probably won't be seeing much of these around in any modern office or home.

With the Bus topology, all workstations are connect directly to the main backbone that carries the data. Traffic generated by any computer will travel across the backbone and be received by all workstations. This works well in a small network of 2-5 computers, but as the number of computers increases so will the network traffic and this can greatly decrease the performance and available bandwidth of your network.



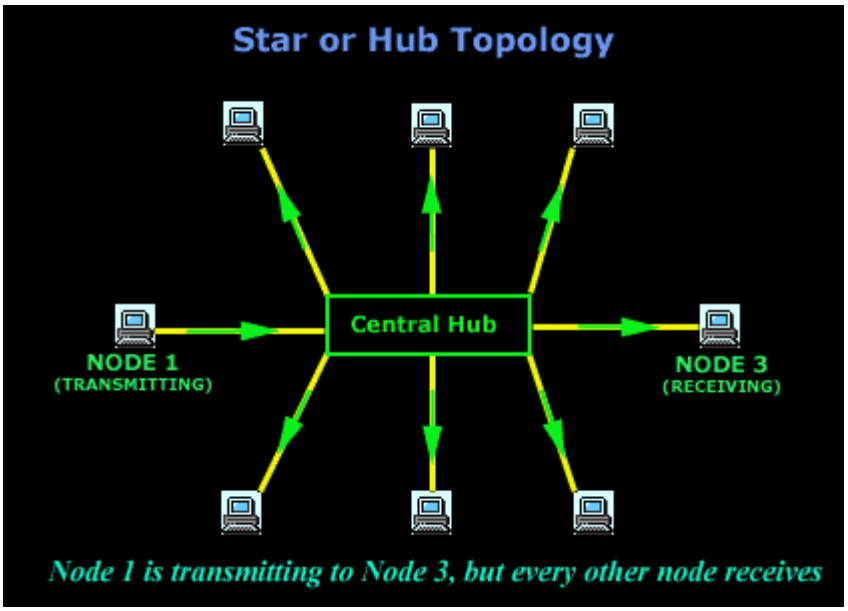
As you can see in the above example, all computers are attached to a continuous cable which connects them in a straight line. The arrows clearly indicate that the packet generated by Node 1 is transmitted to all computers on the network, regardless the destination of this packet.

Also, because of the way the electrical signals are transmitted over this cable, its ends must be terminated by special terminators that work as "shock absorbers", absorbing the signal so it won't reflect back to where it came from. The value of 50Ohms has been selected after carefully taking in consideration all the electrical characteristics of the cable used, the voltage that the signal which runs through the cables, the maximum and minimum length of the bus and a few more.

If the bus (the long yellow cable) is damaged anywhere in its path, then it will most certainly cause the network to stop working or, at the very least, cause big communication problems between the workstations.

Thinnet - 10 Base2, also known as coax cable (Black in colour) and Thicknet - 10 Base 5 (Yellow in colour) is used in these type of topologies.

THE PHYSICAL HUB OR STAR TOPOLOGY



The Star or Hub topology is one of the most common network topologies found in most offices and home networks. It has become very popular in contrast to the bus type (which we just spoke about),

because of the cost and the ease of troubleshooting.

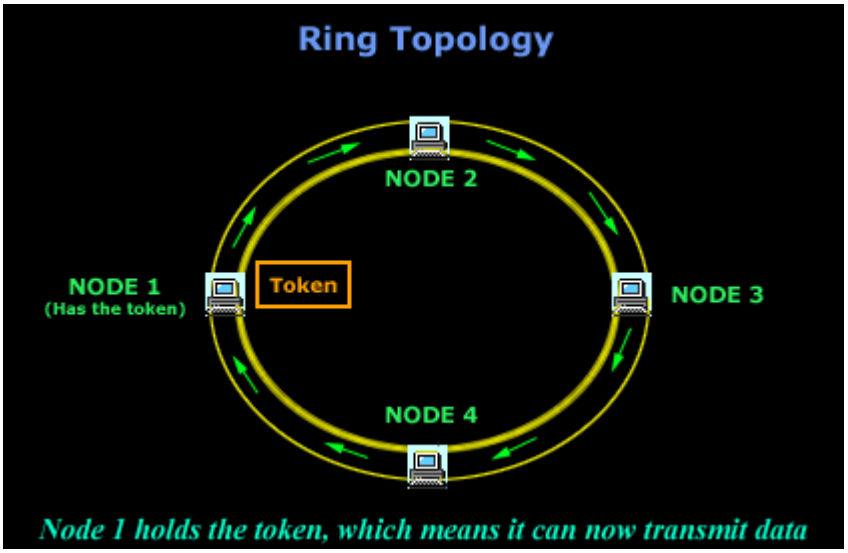
The advantage of the star topology is that if one computer on the star topology fails, then only the failed computer is unable to send or receive data. The remainder of the network functions normally.

The disadvantage of using this topology is that because each computer is connected to a central hub or switch, if this device fails, the entire network fails!

A classic example of this type of topology is the UTP (10 base T), which normaly has a blue colour. Personally I find it boring, so I decided to go out and get myself green, red and yellow colours :)

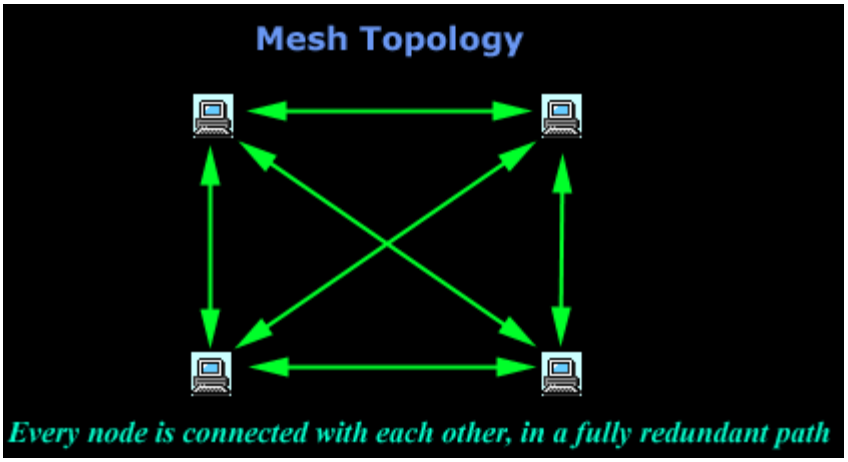
THE PHYSICAL RING TOPOLOGY

In the ring topology, computers are connected on a single circle of cable. Unlike the bus topology, there are no terminated ends. The signals travel around the loop in one direction and pass through each computer, which acts as a repeater to boost the signal and send it to the next computer. On a larger scale, multiple LANs can be connected to each other in a ring topology by using Thicknet coaxial or fiber-optic cable.



The method by which the data is transmitted around the ring is called token passing. IBM's token ring uses this method. A *token* is a special series of bits that contains control information. Possession of the token allows a network device to transmit data to the network. Each network has only one token.

THE PHYSICAL MESH TOPOLOGY



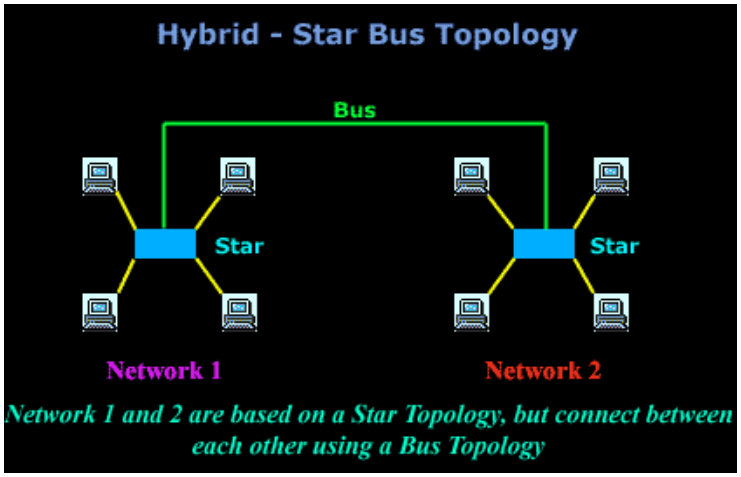
In a mesh topology, each computer is connected to every other computer by a separate cable. This configuration provides redundant paths through the new work, so if one computer blows up, you don't lose the network :) On a large scale, you can connect multiple LANs using mesh topology with leased telephone lines, Thicknet coaxial cable or fiber optic cable.

Again, the big advantage of this topology is its backup capabilities by providing multiple paths through the network.

THE PHYSICAL HYBRID TOPOLOGY

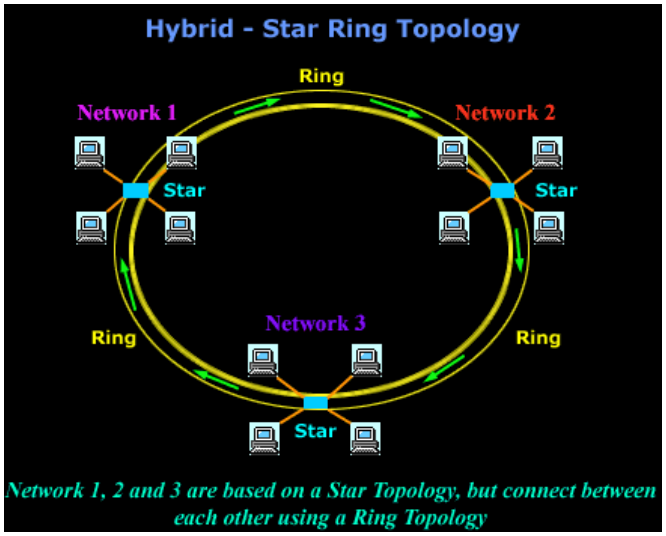
With the hybrid topology, two or more topologies are combined to form a complete network. For example, a hybrid topology could be the combination of a star and bus topology. These are also the most common in use.

STAR-BUS



In a star-bus topology, several star topology networks are linked to a bus connection. In this topology, if a computer fails, it will not affect the rest of the network. However, if the central component, or hub, that attaches all computers in a star, fails, then you have big problems since no computer will be able to communicate.

STAR-RING



In the Star-Ring topology, the computers are connected to a central component as in a star network. These components, however, are wired to form a ring network.

Like the star-bus topology, if a single computer fails, it will not affect the rest of the network. By using token passing, each computer in a star-ring topology has an equal chance of communicating. This allows for greater network traffic between segments than in a star-bus topology.

TRANSMISSION MEDIA

The transmission media is nothing but the physical media over which communication takes place in computer networks.

Magnetic Media

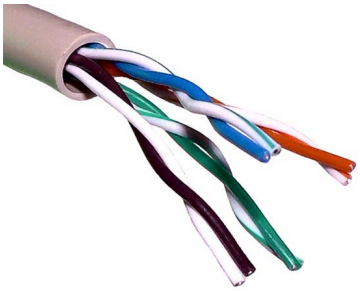
One of the most convenient way to transfer data from one computer to another, even before the birth of networking, was to save it on some storage media and transfer physical from one station to another. Though it may seem old-fashion way in today's world of high speed internet, but when the size of data is huge, the magnetic media comes into play.

For example, a bank has to handle and transfer huge data of its customer, which stores a backup of it at some geographically far-away place for security reasons and to keep it from uncertain calamities. If the bank needs to store its huge backup data then its,transfer through internet is not feasible.The WAN links may not support such high speed.Even if they do; the cost too high to afford.

In these cases, data backup is stored onto magnetic tapes or magnetic discs, and then shifted physically at remote places.

Twisted Pair Cable

A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires, only one carries actual signal and another is used for ground reference. The twists between wires are helpful in reducing noise (electro-magnetic interference) and crosstalk.



There are two types of twisted pair cables:

- Shielded Twisted Pair (STP) Cable
- Unshielded Twisted Pair (UTP) Cable

STP cables comes with twisted wire pair covered in metal foil. This

makes it more indifferent to noise and crosstalk.

UTP has seven categories, each suitable for specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.

Coaxial Cable

Coaxial cable has two wires of copper. The core wire lies in the center and it is made of solid conductor.The core is enclosed in an insulating sheath.The second wire is wrapped around over the sheath and that too in turn encased by insulator sheath.This all is covered by plastic cover.

Because of its structure,the coax cable is capable of carrying high frequency signals than that of twisted pair cable.The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.

There are three categories of coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet), and RG-11 (Thick Ethernet). RG stands for Radio Government.

Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.

Power Lines

Power Line communication (PLC) is Layer-1 (Physical Layer) technology which uses power cables to transmit data signals.In PLC, modulated data is sent over the cables. The receiver on the other end de-modulates and interprets the data.

Because power lines are widely deployed, PLC can make all powered devices controlled and monitored. PLC works in half-duplex.

There are two types of PLC:

- Narrow band PLC
- Broad band PLC

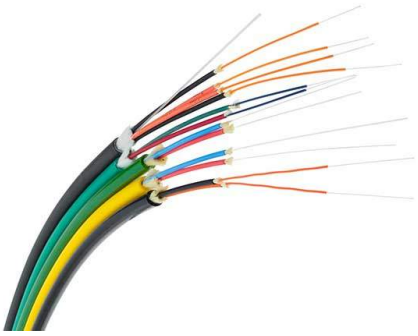
Narrow band PLC provides lower data rates up to 100s of kbps, as they work at lower frequencies (3-5000 kHz).They can be spread over several kilometers.

Broadband PLC provides higher data rates up to 100s of Mbps and works at higher frequencies (1.8 – 250 MHz).They cannot be as much extended as Narrowband PLC.

Fiber Optics

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.

Fiber Optic provides the highest mode of speed. It comes in two modes, one is single mode fiber and second is multimode fiber. Single mode fiber can carry a single ray of light whereas multimode is capable of carrying multiple beams of light.



Fiber Optic also comes in unidirectional and bidirectional capabilities. To connect and access fiber optic special type of connectors are used. These can be Subscriber Channel (SC), Straight Tip (ST), or MT-RJ.