**Computer Network Notes**

**CST-102**

**By Dr. Ramamani Tripathy**

**Associate Professor (CSE, Chitkara University)**

Q. What is Computer Network?

A **computer network** is a **digital telecommunications network** which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections (data links) between nodes. These data links are established over cable media such as wires or optic cables, or wireless media such as Wi-Fi.

Other Definition

A **computer 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 or receiving data from the other node/device through the network.

Characteristics of computer network

**1. Reliable**

Computer networks are very reliable tools, and by using this, users can easily interconnect the devices. Even if they need to print, check the mails, attend the meeting, and access data from another computer, their networking experience stays stable. There are only a few chances that any error or problem can occur. But mostly, these networking systems allow for getting a smooth and stable network connectivity experience.

**2. Flow of Data**

It enables the flow of data from one computing device to another, making it a crucial feature of a computer network. With the help of computer networking, users can get access to transmit the data such as files, documents, and other types of information. These two devices allow each other to share the data without any stoppage.

**3. High Performance**

The performance of the networking can be analyzed with the help of time taken by a command. In simple terms, it can be calculated in terms of time and response. If the response is fast and it also takes less time to transmit the data. Then it is a great way users can share their files and utilize multiple resources.

And with computer networking, users get this fast experience. Hence, computer networking also provides high performance by taking less time in sending or receiving the data.

**4. Secure**

Security is one of the significant aspects, especially in technical terms. Nowadays, most businesses are dependent on computers and access these devices using networking. Thus, if computer network technology is not robust and secure, it can allow unauthorized access to the company’s crucial data. But now, mainly computer networking tools provide the highest level of security, and they prevent any unwanted access.

Thus, security is another feature of a computer network that ensures there is no leakage of data. Because of this, the data sent by one node is directly reached to the second or receiving node without any data or information loss.

**5. Data Fault Tolerance**

Fault tolerance is another fantastic feature offered by computer networks. They can keep working even if there is any fault or damage with the networking. The device can be connected with wires or wireless mediums. So when the sending device sends the information, the receiving device has blockage at its wireless medium.

Components of Computer Network

Any data communication system is bound to have these five major components; sender, receiver, message, transmission medium and protocol.

# Computer Network Types

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

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



* LAN(Local Area Network)
* PAN(Personal Area Network)
* MAN(Metropolitan Area Network)
* WAN(Wide Area Network)

## LAN (Local Area Network)

* Local Area Network is a group of computers connected to each other in a small area such as building, office.
* LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
* It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
* The data is transferred at an extremely faster rate in Local Area Network.
* Local Area Network provides higher security.



## PAN (Personal Area Network)

* Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
* Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
* **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
* Personal Area Network covers an area of **30 feet**.
* Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.



**There are two types of Personal Area Network:**



* Wired Personal Area Network
* Wireless Personal Area Network

**Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

**Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

### Examples of Personal Area Network:

* **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
* **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
* **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

## MAN (Metropolitan Area Network)

* A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
* Government agencies use MAN to connect to the citizens and private industries.
* In MAN, various LANs are connected to each other through a telephone exchange line.
* The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
* It has a higher range than Local Area Network (LAN).



### Uses of Metropolitan Area Network:

* MAN is used in communication between the banks in a city.
* It can be used in an Airline Reservation.
* It can be used in a college within a city.
* It can also be used for communication in the military.

## WAN (Wide Area Network)

* A Wide Area Network is a network that extends over a large geographical area such as states or countries.
* A Wide Area Network is quite bigger network than the LAN.
* A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
* The internet is one of the biggest WAN in the world.
* A Wide Area Network is widely used in the field of Business, government, and education.



### Examples Of Wide Area Network:

* **Mobile Broadband:** A 4G network is widely used across a region or country.
* **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
* **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

### Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

* **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
* **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
* **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
* **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
* **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
* **Global business:** We can do the business over the internet globally.
* **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

### Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

* **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
* **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
* **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
* **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

## Internetwork

* An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
* An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
* An internetworking uses the **internet protocol**.
* The reference model used for internetworking is **Open System Interconnection (OSI)**.

## Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

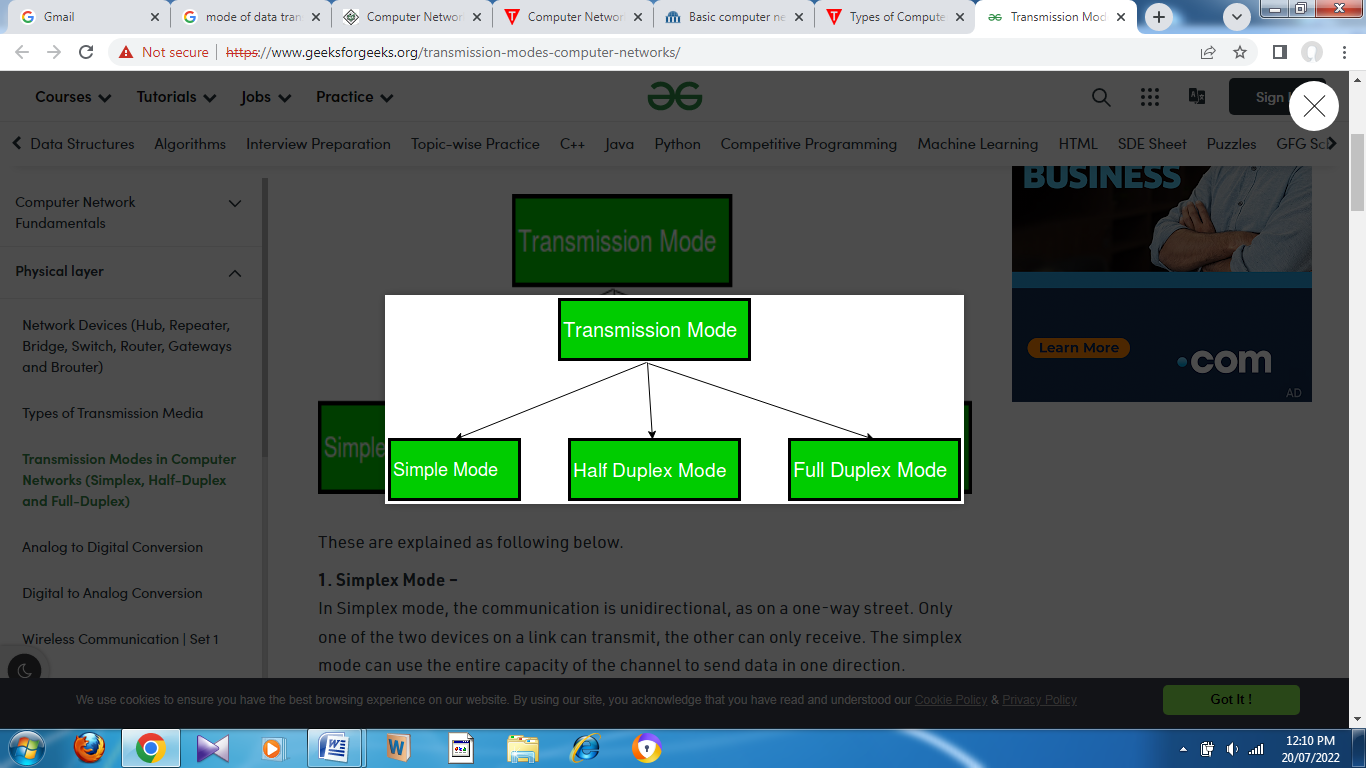
2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

## Intranet advantages:

* **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
* **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
* **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
* **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
* **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

# Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

Transmission mode means transferring data between two devices. It is also known as a communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. There are three types of transmission mode:-



**1.SimplexMode** **–**  
In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.   
Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



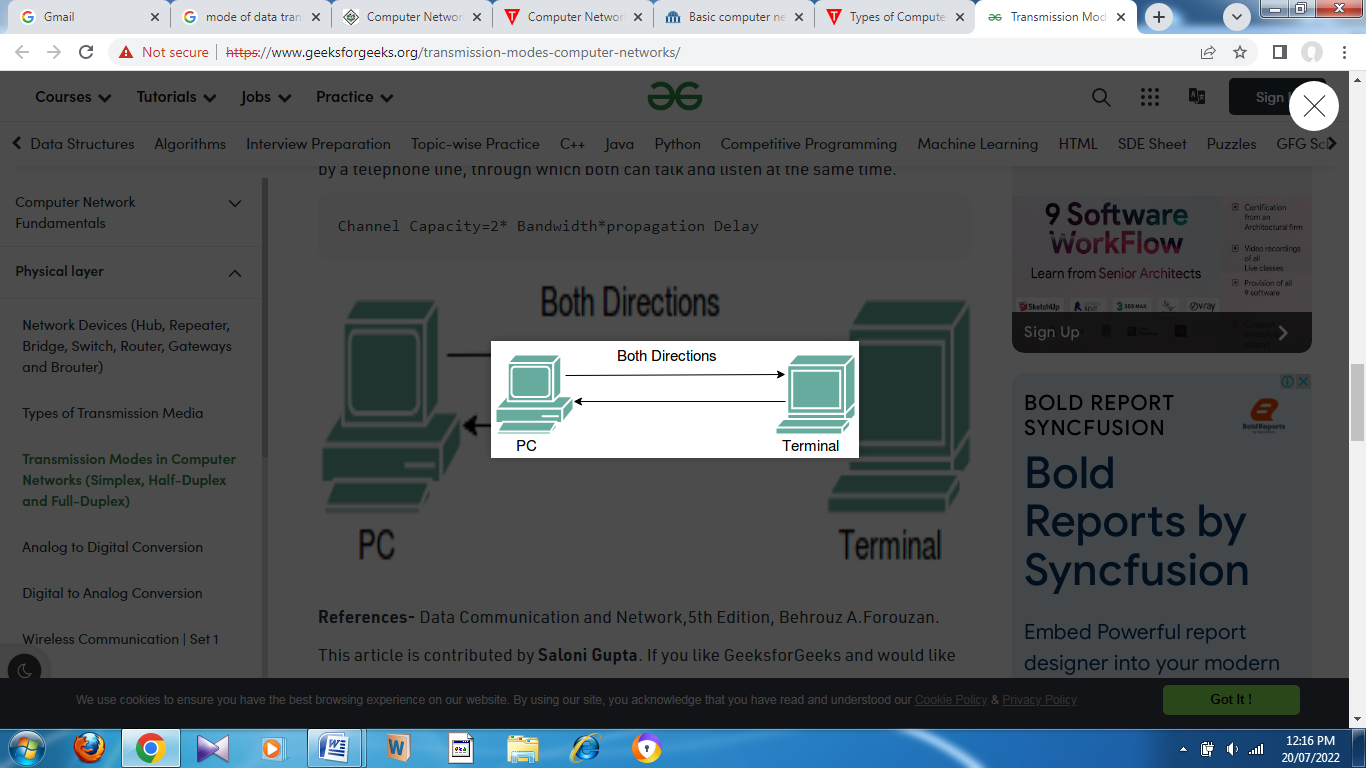
**2.Half-DuplexMode** **–**  
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.   
Example: Walkie-talkie in which message is sent one at a time and messages are sent in both directions.



**3.Full-DuplexMode** **–**  
In full-duplex mode, both stations can transmit and receive simultaneously. In full\_duplex mode, signals going in one direction share the capacity of the link with signals going in another 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 is divided between signals traveling in both directions.

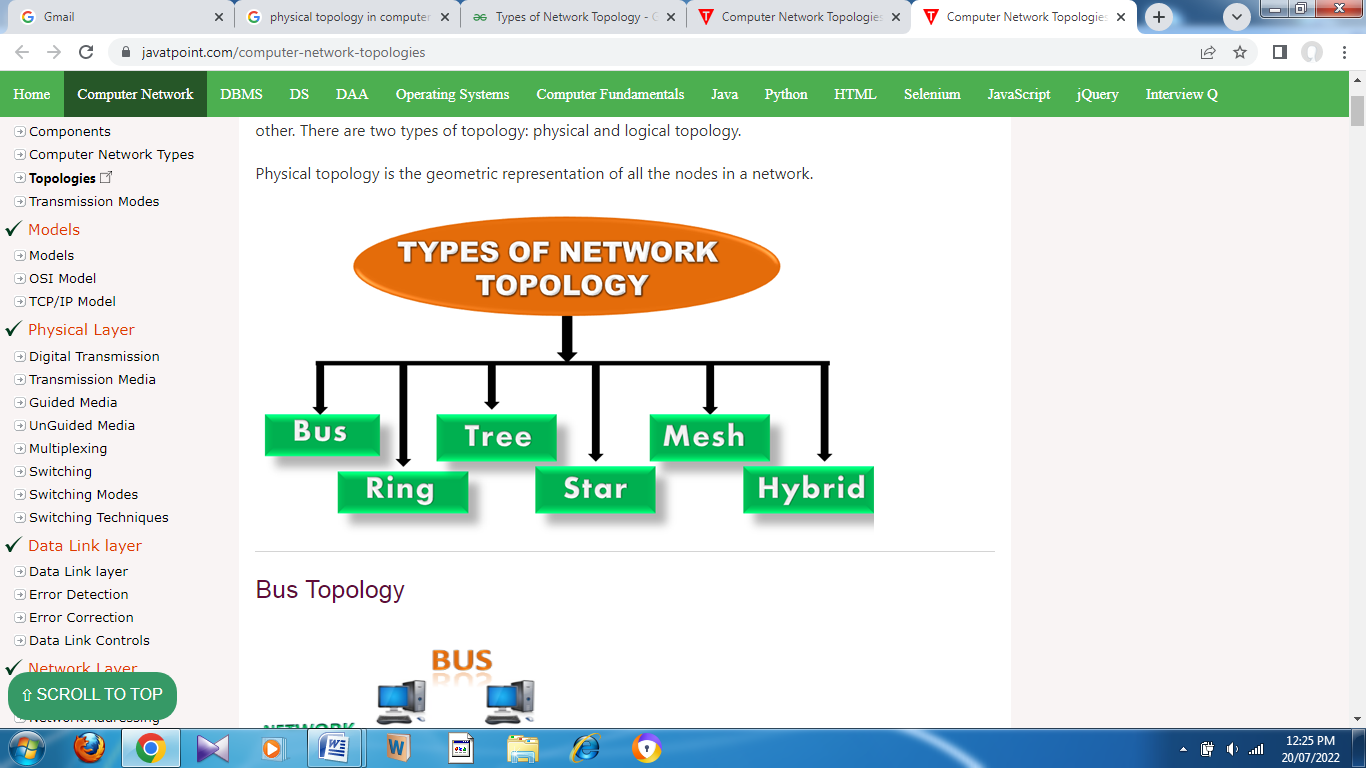
Full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.   
Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



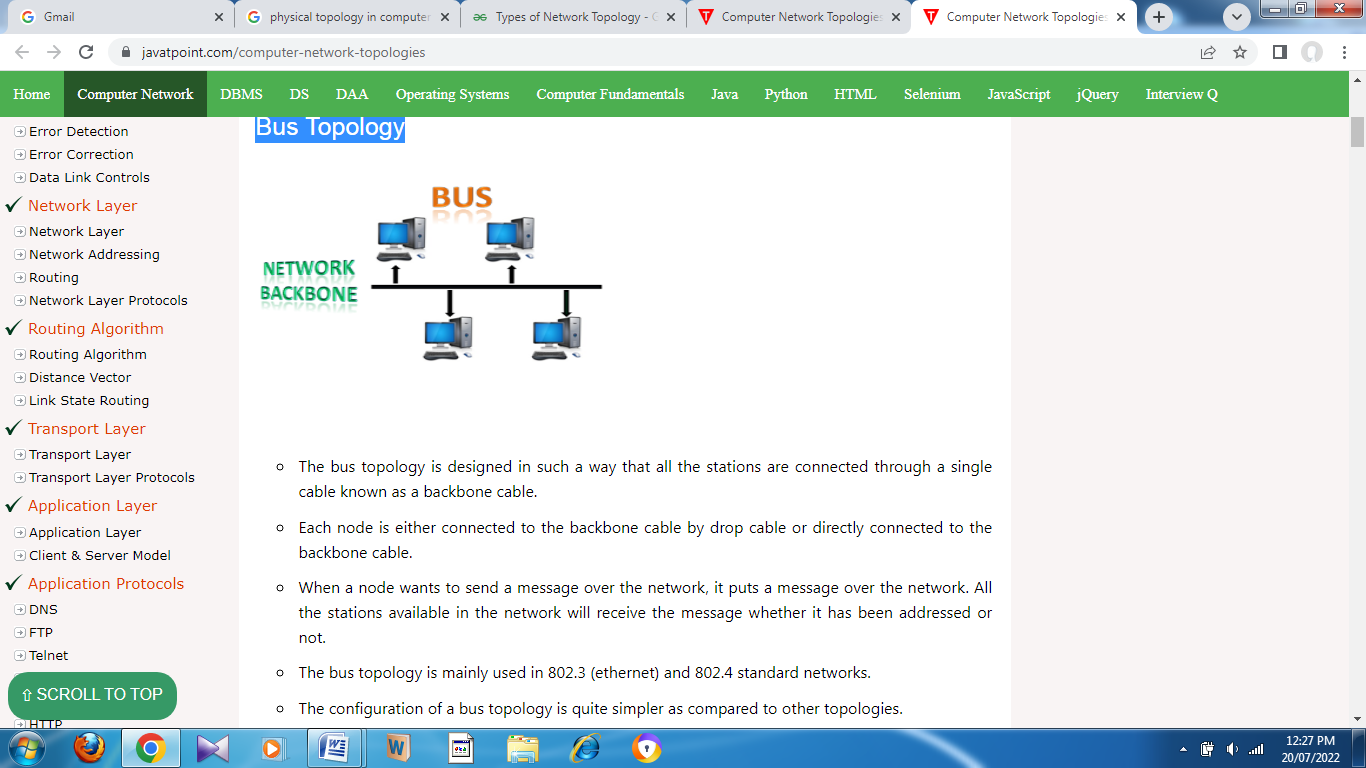
# What is Topology?

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

Physical topology is the geometric representation of all the nodes in a network.



## Bus Topology



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

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

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

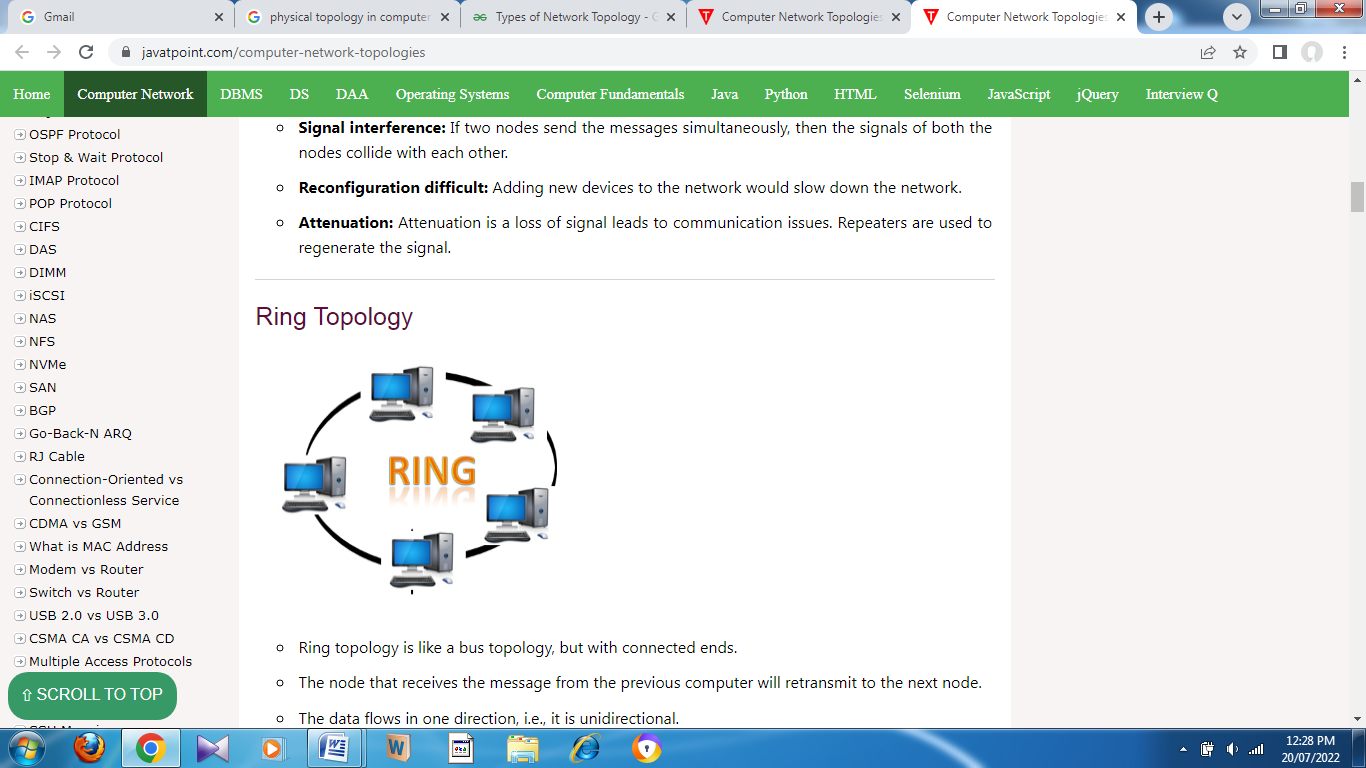
Advantages of Bus topology:

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

Disadvantages of Bus topology:

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

## Ring Topology



* Ring topology is like a bus topology, but with connected ends.
* The node that receives the message from the previous computer will retransmit to the next node.
* The data flows in one direction, i.e., it is unidirectional.
* The data flows in a single loop continuously known as an endless loop.
* It has no terminated ends, i.e., each node is connected to other node and having no termination point.
* The data in a ring topology flow in a clockwise direction.
* The most common access method of the ring topology is **token passing**.
  + **Token passing:** It is a network access method in which token is passed from one node to another node.
  + **Token:** It is a frame that circulates around the network.

Working of Token passing

* A token moves around the network, and it is passed from computer to computer until it reaches the destination.
* The sender modifies the token by putting the address along with the data.
* The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
* In a ring topology, a token is used as a carrier.

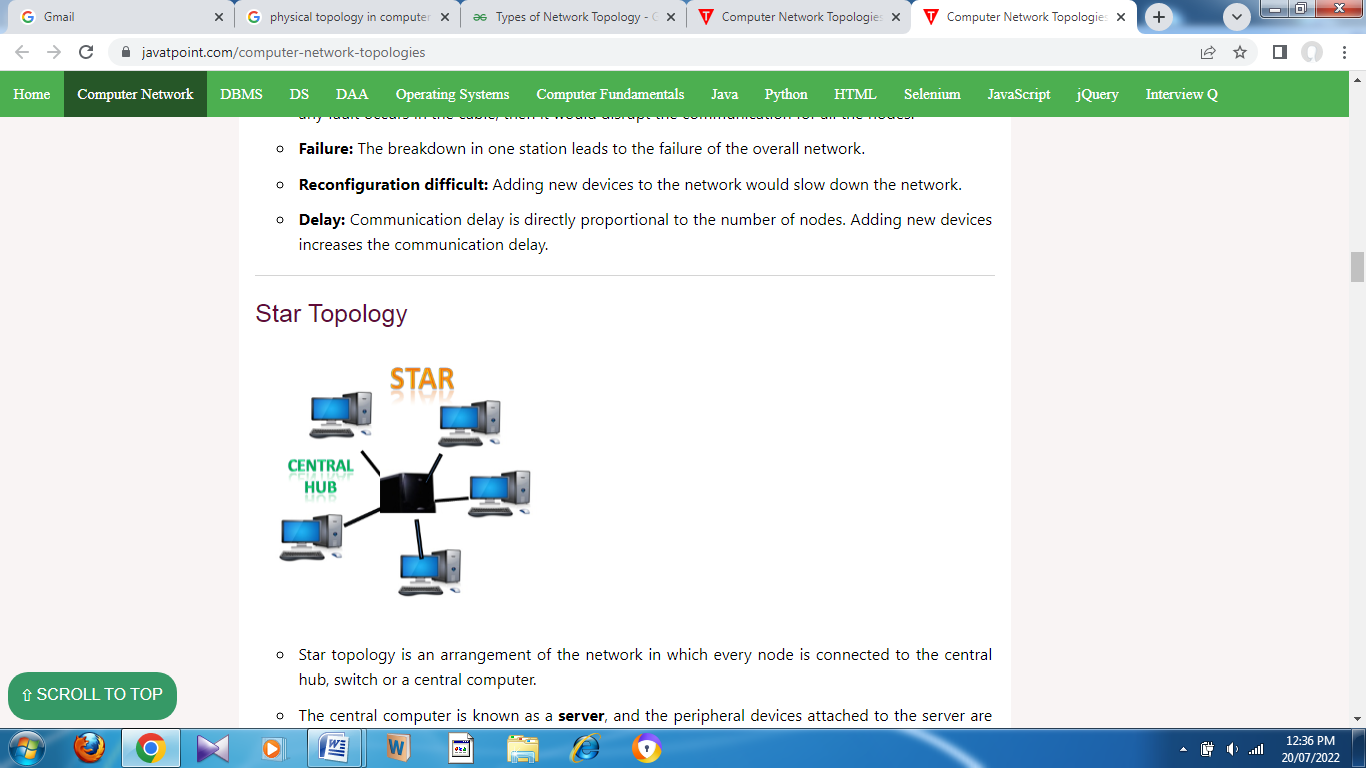
Advantages of Ring topology:

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

Disadvantages of Ring topology:

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

## Star Topology



* Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
* The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
* Coaxial cable or RJ-45 cables are used to connect the computers.
* Hubs or Switches are mainly used as connection devices in a **physical star topology**.
* Star topology is the most popular topology in network implementation.

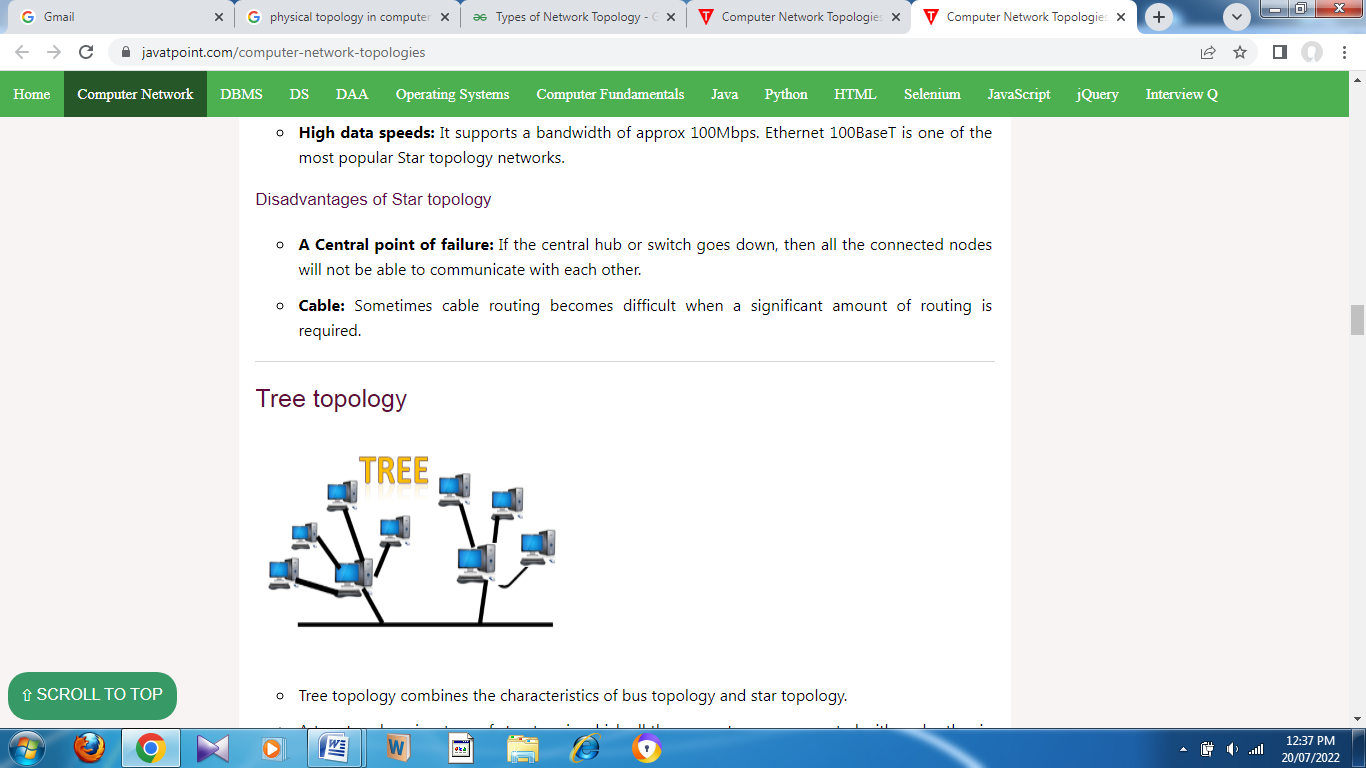
Advantages of Star topology

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

Disadvantages of Star topology

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

## Tree topology



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

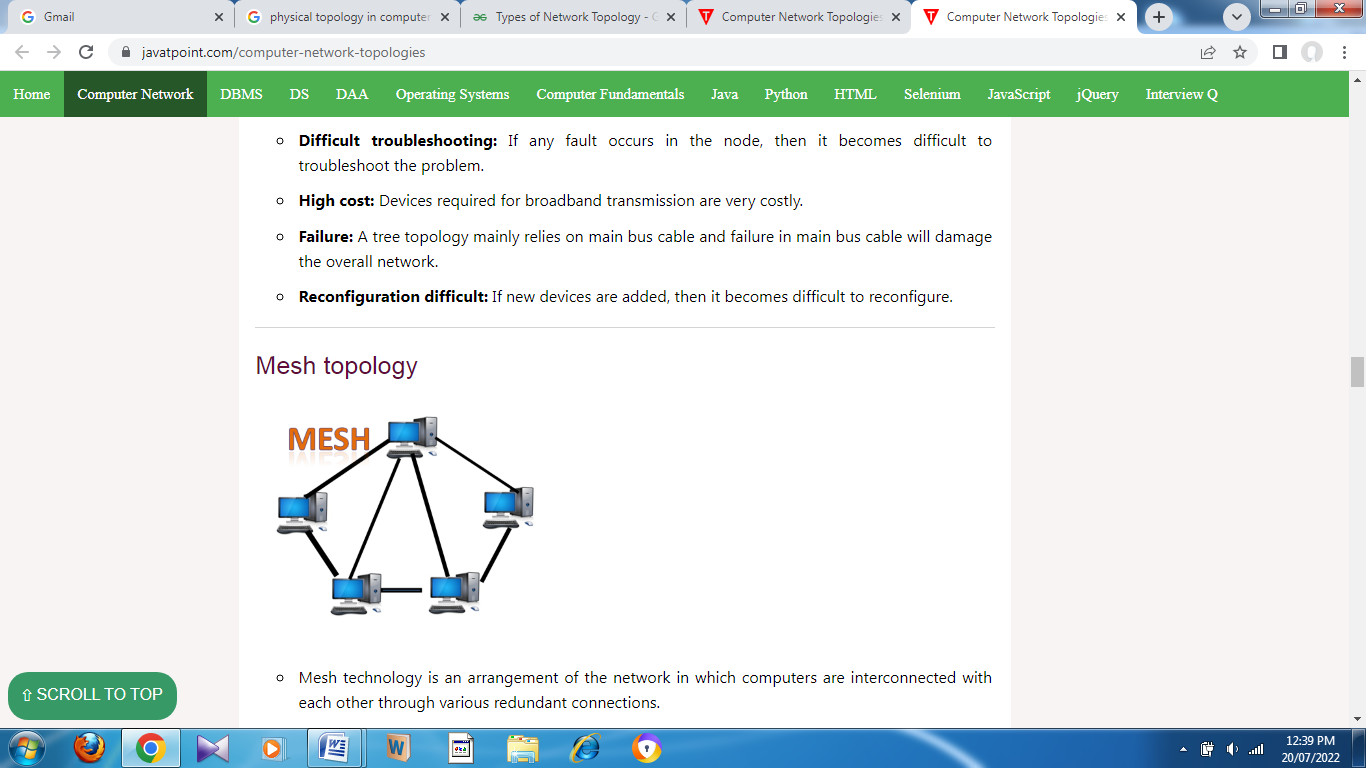
Advantages of Tree topology

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

Disadvantages of Tree topology

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

Mesh topology

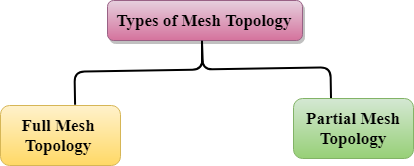


* Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.
* It does not contain the switch, hub or any central computer which acts as a central point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

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

**Mesh topology is divided into two categories:**

* Fully connected mesh topology
* Partially connected mesh topology



* **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
* **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

**Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

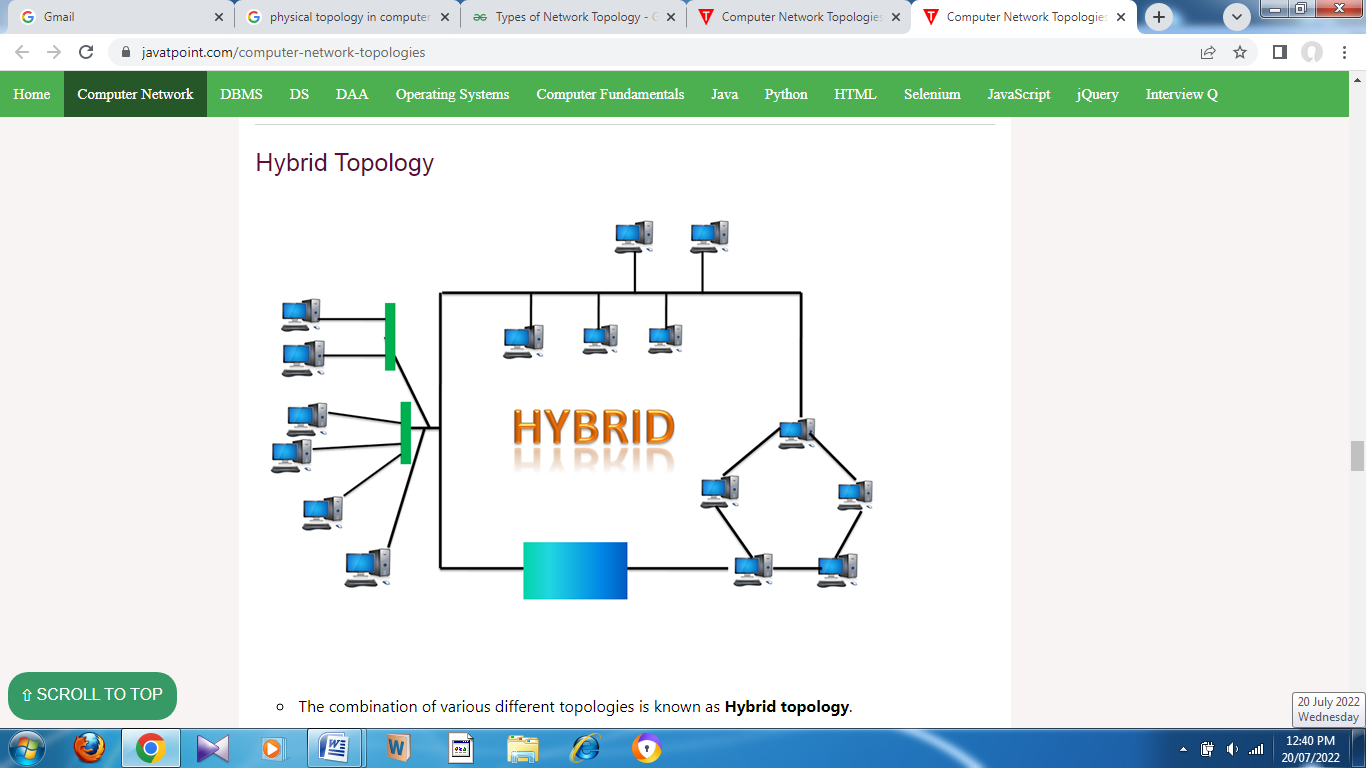
**Fast Communication:** Communication is very fast between the nodes.

**Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

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

Hybrid Topology



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

Advantages of Hybrid Topology

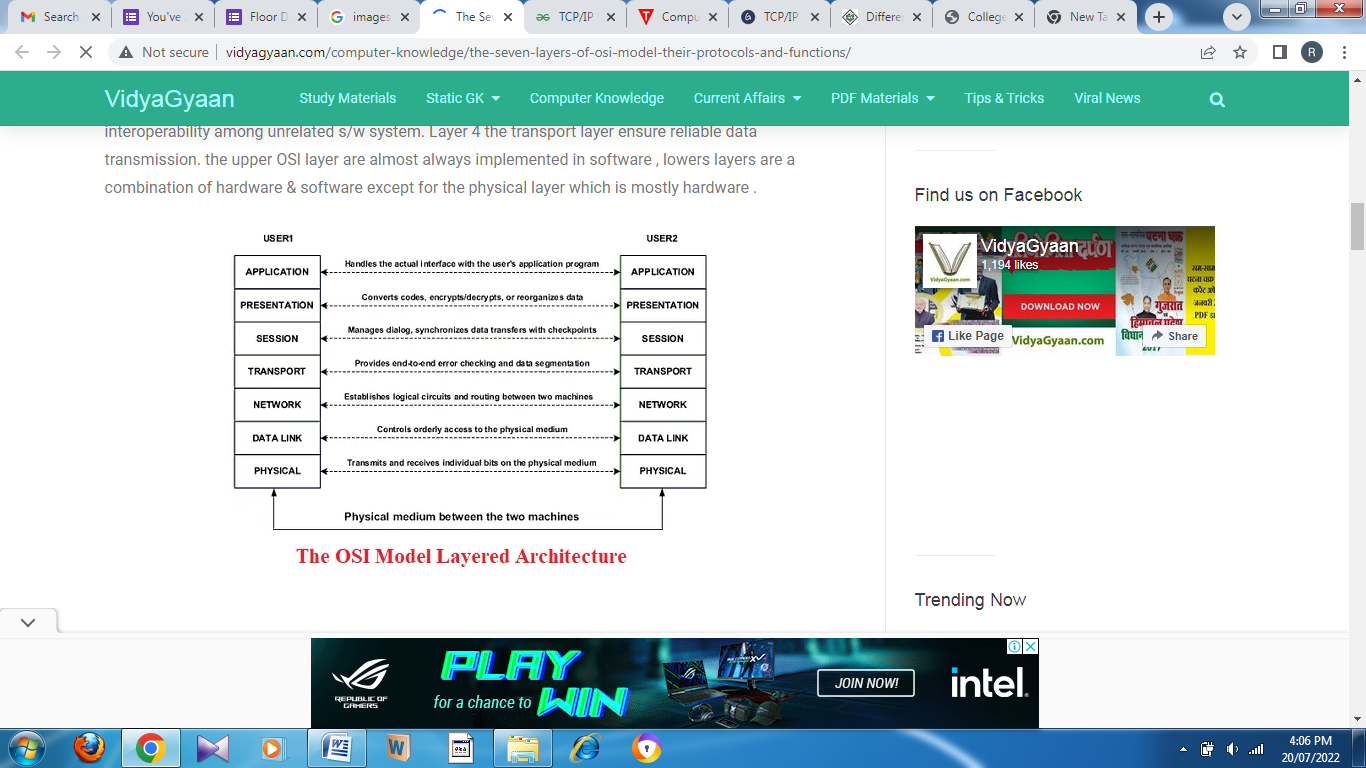
* **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
* **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
* **Flexible:** This topology is very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

Disadvantages of Hybrid topology

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

OSI Model

* OSI stands for **Open System Interconnection** is a reference model that describes how information from a [software](https://www.javatpoint.com/software) application in one [computer](https://www.javatpoint.com/what-is-computer) moves through a physical medium to the software application in another computer.
* OSI consists of seven layers, and each layer performs a particular network function.
* OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
* OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
* Each layer is self-contained, so that task assigned to each layer can be performed independently.



Functions of the OSI Layers

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

* The main functionality of the physical layer is to transmit the individual bits from one node to another node.
* It is the lowest layer of the OSI model.
* It establishes, maintains and deactivates the physical connection.
* It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

* **Line Configuration:** It defines the way how two or more devices can be connected physically.
* [**Data Transmission**](https://www.javatpoint.com/computer-network-transmission-modes)**:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
* [**Topology**](https://www.javatpoint.com/computer-network-topologies)**:** It defines the way how network devices are arranged.
* **Signals:** It determines the type of the signal used for transmitting the information.

Data-Link Layer

* This layer is responsible for the error-free transfer of data frames.
* It defines the format of the data on the network.
* It provides a reliable and efficient communication between two or more devices.
* It is mainly responsible for the unique identification of each device that resides on a local network.
* It contains two sub-layers:
  + **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  + **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

Functions of the Data-link layer

* **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

OSI Model

* **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
* **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
* **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
* **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer

* It is a layer 3 that manages device addressing, tracks the location of devices on the network.
* It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
* The Data link layer is responsible for routing and forwarding the packets.
* Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
* The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

* **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
* [**Addressing**](https://www.javatpoint.com/network-addressing)**:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
* [**Routing**](https://www.javatpoint.com/computer-network-routing)**:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
* **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer

* The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
* The main responsibility of the transport layer is to transfer the data completely.
* It receives the data from the upper layer and converts them into smaller units known as segments.
* This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

**The two protocols used in this layer are:**

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

Functions of Transport Layer:

* **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
* **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
* **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
* **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
* **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer

* It is a layer 5 in the OSI model.
* The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

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

Presentation Layer

* A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
* It acts as a data translator for a network.
* This layer is a part of the operating system that converts the data from one presentation format to another format.
* The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

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

Application Layer

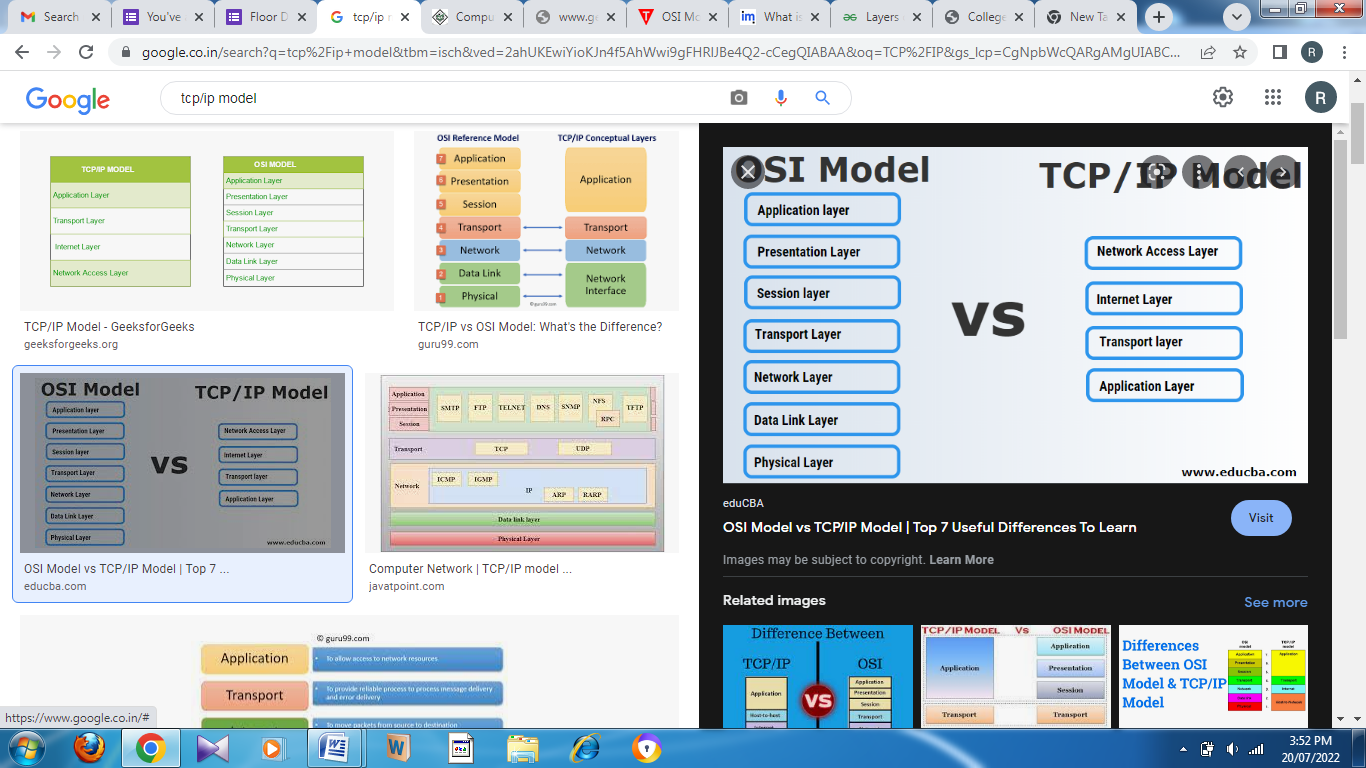
* An application layer serves as a window for users and application processes to access network service.
* It handles issues such as network transparency, resource allocation, etc.
* An application layer is not an application, but it performs the application layer functions.
* This layer provides the network services to the end-users.

Functions of Application layer:

* **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
* **Mail services:** An application layer provides the facility for email forwarding and storage.
* Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

The application layer uses HTTP, FTP, POP, SMTP, and DNS protocols that allow the software to send and receive information and present meaningful data to users.

# 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:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

**1. Network Access 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 the 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.

**2. 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 :

1. **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.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **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.

**3. Host-to-Host 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 :

1. **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 acknowledgment 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.
2. **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.

**4. 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, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at [Protocols in Application Layer](https://www.geeksforgeeks.org/protocols-application-layer/) for some information about these protocols. Protocols other than those present in the linked article are :

* + 1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
    2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
    3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

|  |  |
| --- | --- |
| **OSI Model** | **TCP/IP model** |
| It is developed by ISO (International Standard Organization) | It is developed by ARPANET (Advanced Research Project Agency Network). |
| OSI model provides a clear distinction between interfaces, services, and protocols. | TCP/IP doesn’t have any clear distinguishing points between services, interfaces, and protocols. |
| OSI refers to Open Systems Interconnection. | TCP refers to Transmission Control Protocol. |
| OSI uses the network layer to define routing standards and protocols. | TCP/IP uses only the Internet layer. |
| OSI follows a vertical approach. | TCP/IP follows a horizontal approach. |
| [OSI model](https://www.guru99.com/layers-of-osi-model.html) use two separate layers physical and data link to define the functionality of the bottom layers. | TCP/IP uses only one layer (link). |
| OSI layers have seven layers. | TCP/IP has four layers. |
| OSI model, the transport layer is only connection-oriented. | A layer of the TCP/IP model is both connection-oriented and connectionless. |
| In the OSI model, the data link layer and physical are separate layers. | In TCP, physical and data link are both combined as a single host-to-network layer. |
| Session and presentation layers are not a part of the TCP model. | There is no session and presentation layer in TCP model. |
| It is defined after the advent of the Internet. | It is defined before the advent of the internet. |
| The minimum size of the OSI header is 5 bytes. | Minimum header size is 20 bytes. |