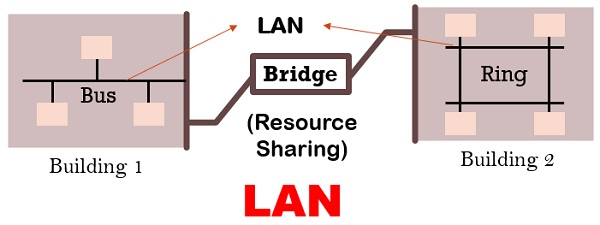
Types of networks

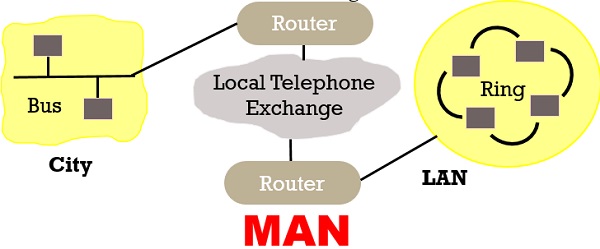
LAN refers to a group of computers that all belong to the same organization and that are linked within a small geographic area using a network and often the same technology (the most widespread being Ethernet).  
  
A local area network is a network in its simplest form. Data transfer speeds over a local area network can reach up to 10 Mbps, such as for an Ethernet network, and 1 Gbps, as with FDDI or Gigabit Ethernet. A local area network can reach as many as 100, or even 1000, users.  
  
By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined: in a "peer-to-peer" network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role; or in a "client/server" environment, in which a central computer provides network services to users.

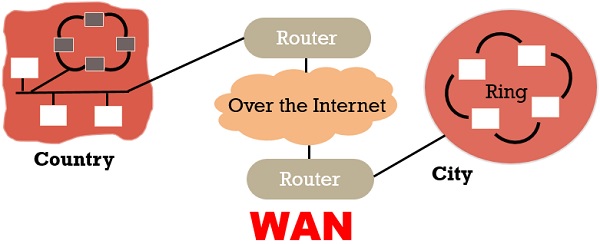
MANs connect multiple geographically close LANs (over an area of up to several dozen miles) to one another at high speeds. Thus, a MAN lets two remote nodes communicate as if they were part of the same local area network.  
  
A MAN is made from switches or routers connected to one another with high-speed links (usually fibre optic cables).

A WAN connects multiple LANs to one another over great geographic distances. The speed available on a WAN varies depending on the cost of the connections, which increases with distance, and may be low.  
  
WANs operate using routers, which can "choose" the most appropriate path for data to take to reach a network node.

| **BASIS OF COMPARISON** | **LAN** | **MAN** | **WAN** |
| --- | --- | --- | --- |
| Expands to | Local Area Network | Metropolitan Area Network | Wide Area Network |
| Meaning | A network that connects a group of computers in a small geographical area. | It covers relatively large region such as cities, towns. | It spans large locality and connects countries together. Example Internet. |
| Ownership of Network | Private | Private or Public | Private or Public |
| Design and maintenance | Easy | Difficult | Difficult |
| Propagation Delay | Short | Moderate | Long |
| Speed | High | Moderate | Low |
| Fault Tolerance | More Tolerant | Less Tolerant | Less Tolerant |
| Congestion | Less | More | More |
| Used for | College, School, Hospital. | Small towns, City. | Country/Continent. |
| Allows | Single pair of devices to communicate. | Multiple computers can simultaneously interact. | A huge group of computers communicate at the same time. |







Types of topology

| **Parameters** | **Bus** | **Ring** | **Star** | **Mesh** |
| --- | --- | --- | --- | --- |
| Network Performance | Small | Small or Large | Small | Small |
| Cable Length Requirement | Less | Neither less nor | More | More |
| Traffic | Less | High | Medium | No |
| Dataflow Efficiency | More | Neither less nor more | More | More |
| Failure | Easy to solve | Difficult to solve | Easy to solve except hub/switch fails | Easy to solve |
| Cost | Low | High | High | High |

 network topology can either be the physical or logical arrangement of devices on a network.

These connected devices can be routers, switches, firewalls, network printers, wireless access points, user computers etc (basically anything that can be assigned an IP address).  Note that end user devices are also part of the network topology.

Bus topology has a network arrangement where nodes make use of a single communication line for data transmission.

Many networks at the beginning of computer networking era made use of this topology due to easy implementation.

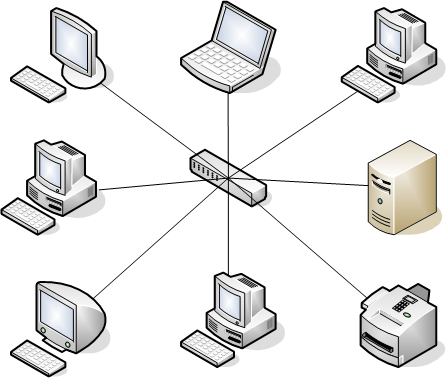
Advantages

* Since there is a single communication line, means the same medium is shared. Therefore, the major advantage of using this topology is its simplicity.
* Easy to setup and extend.
* Less costly. Less cabling needs.

Disadvantages

* On the other hand, having a single communication line for data transmission makes it easier for collision to occur, which is seen as a disadvantage of using this network topology.
* If the single network cable has a problem or disconnection, the whole network breaks.
* Difficult to identify a problem.
* All devices receive all signals from every other host. This is not efficient.

Star Topology – Advantages and Disadvantages



The star network topology is one of the most commonly used topologies today because of its simplicity and efficiency.

In this kind of topology, a centralized node is located at the core of the network topology, in which all the other nodes must communicate through.

This topology is mostly used in homes and offices today. For example, the classic Ethernet LAN networks are using the Star Topology. There is an Ethernet Switch (centralized node) on which all computers and network devices are connected to.

Advantages

* Easy to install and implement with wiring etc.
* Easy to troubleshoot and detect problems in the network.
* If one device fails, it does not affect the other devices in the network.
* You can easily add or remove devices without affecting the rest of the network.
* Centralized management and monitoring through the central switch/hub.

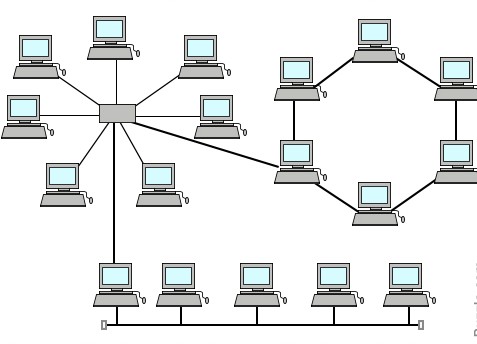
Disadvantages

* The main disadvantage of using this topology is that it has a single point of failure, i.e. when the central switch node is down, there will be a break in communication for all connected devices.
* More cabling is needed since you connect each individual devices to the central node.
* Performance of the whole network depends on the performance of the central node.

Disadvantage

The disadvantage is the point of failure, as a single node can break the transmission of data on the network

Hybrid Topology – Advantages and Disadvantages



This network topology is basically made up of several topologies i.e. a combination of two or more topologies, which could be bus, star, ring, etc.

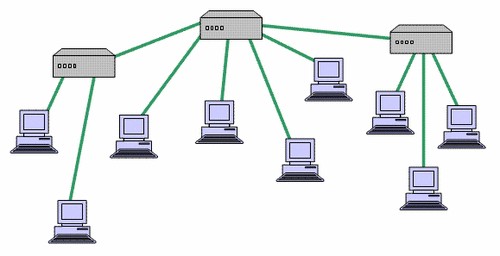
Advantages

* In terms of the advantages of using this kind of topology, we find that it has a high level of fault tolerance, which makes it reliable and flexible.
* Scalable as you can add new nodes easily.
* You can design it in such a way as to use the best features of various other topologies.

Disadvantages

* The disadvantages include things such as high cost and complexity of maintenance. This topology is used in real-life where scalability and high performance is important, for example Internet Service Providers.
* Costly infrastructure.

Tree Topology – Advantages and Disadvantages

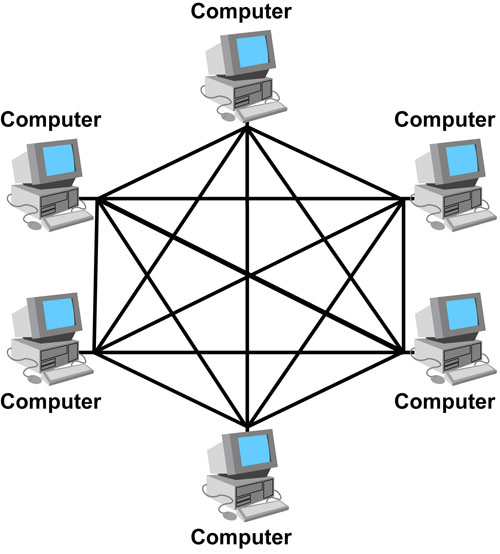


This network topology is ideal for when you have a device acting as the root device on the network.

Note this this topology works with the design of a star and bus topology combined. This has to do with linking star topologies together to form a single network topology, which is linked using a bus topology.

The disadvantage of using this topology is the multiple points of failures that are created, i.e. both the star and bus topology needs to be up at all times.

Mesh Topology – Advantages and Disadvantages



Mesh network topologies create a scenario where there is connection to and from each node that is connected on the network. That is, all network nodes are interconnected between them just like a mesh.

Mesh topologies are used in mission critical network environments such as hospitals or financial institutions, where availability is of utmost importance.

Advantages

* The main advantage of this type is fault tolerance, which is because of the redundant links that are created.
* If one device/node in the network fails, the rest of the devices can work normally without interruption.
* Adding more devices in the network does not affect the rest of the devices.

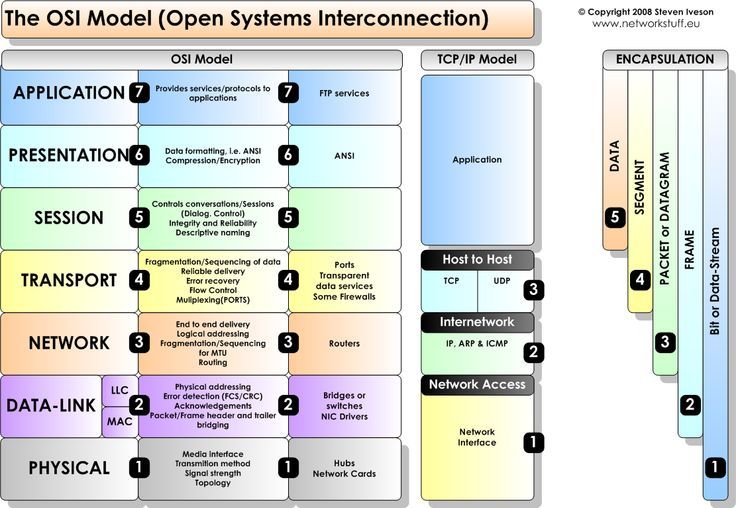
Disadvantages

* The obvious disadvantage of using this type of network is the high cost of implementation.
* Implementation and maintenance of such a topology is time consuming and difficult.
* Cabling cost is high.

Circuit and packet switching

|  |  |
| --- | --- |
| **CIRCUIT SWITCHING** | **PACKET SWITCHING** |
| In circuit switching there are 3 phases i) Connection Establishment. ii) Data Transfer. iii) Connection Released. | In Packet switching directly data transfer takes place . |
| In circuit switching, each data unit know the entire path address which is provided by the source | In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers. |
| In Circuit switching, data is processed at source system only | In Packet switching, data is processed at all intermediate node including source system. |
| Delay between data units in circuit switching is uniform. | Delay between data units in packet switching is not uniform. |
| Resource reservation is the feature of circuit switching because path is fixed for data transmission. | There is no resource reservation because bandwidth is shared among users. |
| Circuit switching is more reliable. | Packet switching is less reliable. |
| Wastage of resources are more in Circuit Switching | Less wastage of resources as compared to Circuit Switching |
| It is not a store and forward technique. | It is a store and forward technique. |
| Transmission of the data is done by the source | Transmission of the data is done not only by the source, but also by the intermediate routers |
| Congestion can occur during connection establishment time, there might be a case will requesting for channel the channel is already occupied. | Congestion can occur during data transfer phase, large number of packets comes in no time |

Osi layer

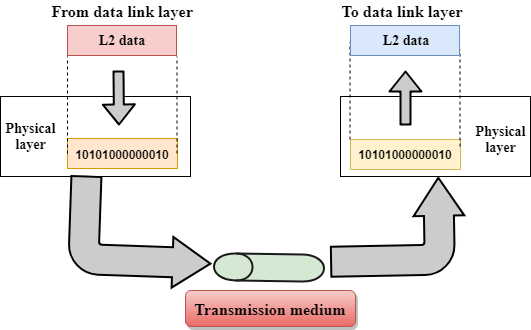


Characteristics of OSI Model:

## Characteristics of OSI Model:

* The OSI model is divided into two layers: upper layers and lower layers.
* The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
* The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium

### Physical layer

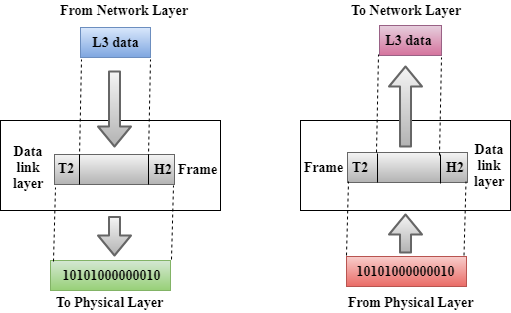


* The main functionality of the physical layer is to transmit the individual bits from one node to another node.
* It is the lowest layer of the OSI model.
* It establishes, maintains and deactivates the physical connection.
* It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

* **Line Configuration:** It defines the way how two or more devices can be connected physically.
* **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
* **Topology:** It defines the way how network devices are arranged.
* **Signals:** It determines the type of the signal used for transmitting the information.

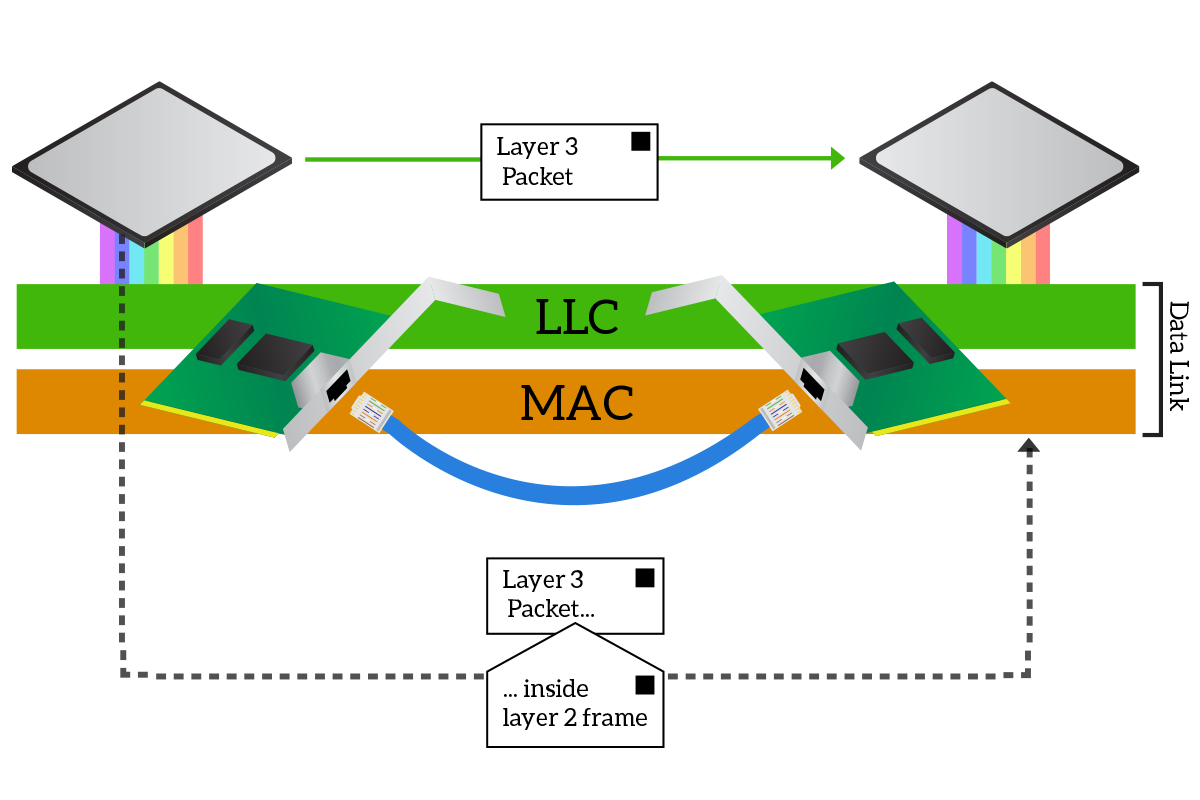
### Data-Link Layer



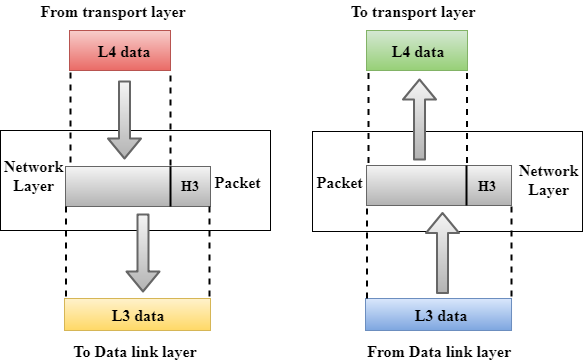
* This layer is responsible for the error-free transfer of data frames.
* It defines the format of the data on the network.
* It provides a reliable and efficient communication between two or more devices.
* It is mainly responsible for the unique identification of each device that resides on a local 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.
* **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:** 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:** 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 3 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.

# Data Link Layer

* In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.
* The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
* The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
* The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.
* The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.
* An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link.

### Following services are provided by the Data Link Layer:

* **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
* **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
* **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
* **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
* **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
* **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

TCP/IP supports the following protocols:

## ARP

* ARP stands for Address Resolution Protocol.
* It is used to associate an IP address with the MAC address.
* Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

#### Note: MAC address: The MAC address is used to identify the actual device. IP address: It is an address used to locate a device on the network.

### How ARP works

If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.

### Steps taken by ARP protocol

If a device wants to communicate with another device, the following steps are taken by the device:

* The device will first look at its internet list, called the ARP cache to check whether an IP address contains a matching MAC address or not. It will check the ARP cache in command prompt by using a command **arp-a**.
* If ARP cache is empty, then device broadcast the message to the entire network asking each device for a matching MAC address.
* The device that has the matching IP address will then respond back to the sender with its MAC address
* Once the MAC address is received by the device, then the communication can take place between two devices.
* If the device receives the MAC address, then the MAC address gets stored in the ARP cache. We can check the ARP cache in command prompt by using a command arp -a.

#### Note: ARP cache is used to make a network more efficient.

In the above screenshot, we observe the association of IP address to the MAC address.

### There are two types of ARP entries:

* **Dynamic entry:** It is an entry which is created automatically when the sender broadcast its message to the entire network. Dynamic entries are not permanent, and they are removed periodically.
* **Static entry:** It is an entry where someone manually enters the IP to MAC address association by using the ARP command utility.

## RARP

* RARP stands for **Reverse Address Resolution Protocol**.
* If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
* The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
* The message format of the RARP protocol is similar to the ARP protocol.
* Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

## ICMP

* ICMP stands for Internet Control Message Protocol.
* The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
* ICMP uses echo test/reply to check whether the destination is reachable and responding.
* ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
* An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
* ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
* ICMP messages are transmitted within IP datagram.
* The first field specifies the type of the message.
* The second field specifies the reason for a particular message type.
* The checksum field covers the entire ICMP message.

### Error Reporting

ICMP protocol reports the error messages to the sender.

**Five types of errors are handled by the ICMP protocol:**

* Destination unreachable
* Source Quench
* Time Exceeded
* Parameter problems
* Redirection
* **Destination unreachable:** The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable.
* **Source Quench:** The purpose of the source quench message is congestion control. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate so that the router will be free from congestion.
* **Time Exceeded:** Time Exceeded is also known as "Time-To-Live". It is a parameter that defines how long a packet should live before it would be discarded.

**There are two ways when Time Exceeded message can be generated:**

Sometimes packet discarded due to some bad routing implementation, and this causes the looping issue and network congestion. Due to the looping issue, the value of TTL keeps on decrementing, and when it reaches zero, the router discards the datagram. However, when the datagram is discarded by the router, the time exceeded message will be sent by the router to the source host.

When destination host does not receive all the fragments in a certain time limit, then the received fragments are also discarded, and the destination host sends time Exceeded message to the source host.

* **Parameter problems:** When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.
* **Redirection:** Redirection message is generated when host consists of a small routing table. When the host consists of a limited number of entries due to which it sends the datagram to a wrong router. The router that receives a datagram will forward a datagram to a correct router and also sends the "Redirection message" to the host to update its routing table.

## IGMP

* IGMP stands for **Internet Group Message Protocol**.
* The IP protocol supports two types of communication:
  + **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.
  + **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.
* The IGMP protocol is used by the hosts and router to support multicasting.
* The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.
* IGMP is a part of the IP layer, and IGMP has a fixed-size message.
* The IGMP message is encapsulated within an IP datagram.

**Where**,

**Type:** It determines the type of IGMP message. There are three types of IGMP message: Membership Query, Membership Report and Leave Report.

**Maximum Response Time:** This field is used only by the Membership Query message. It determines the maximum time the host can send the Membership Report message in response to the Membership Query message.

**Checksum:** It determines the entire payload of the IP datagram in which IGMP message is encapsulated.

**Group Address:** The behavior of this field depends on the type of the message sent.

* **For Membership Query**, the group address is set to zero for General Query and set to multicast group address for a specific query.
* **For Membership Report**, the group address is set to the multicast group address.
* **For Leave Group**, it is set to the multicast group address.

### IGMP Messages

* **Membership Query message**
  + This message is sent by a router to all hosts on a local area network to determine the set of all the multicast groups that have been joined by the host.
  + It also determines whether a specific multicast group has been joined by the hosts on a attached interface.
  + The group address in the query is zero since the router expects one response from a host for every group that contains one or more members on that host.
* **Membership Report message**
  + The host responds to the membership query message with a membership report message.
  + Membership report messages can also be generated by the host when a host wants to join the multicast group without waiting for a membership query message from the router.
  + Membership report messages are received by a router as well as all the hosts on an attached interface.
  + Each membership report message includes the multicast address of a single group that the host wants to join.
  + IGMP protocol does not care which host has joined the group or how many hosts are present in a single group. It only cares whether one or more attached hosts belong to a single multicast group.
  + The membership Query message sent by a router also includes a "**Maximum Response time**". After receiving a membership query message and before sending the membership report message, the host waits for the random amount of time from 0 to the maximum response time. If a host observes that some other attached host has sent the "**Maximum Report message**", then it discards its "**Maximum Report message**" as it knows that the attached router already knows that one or more hosts have joined a single multicast group. This process is known as feedback suppression. It provides the performance optimization, thus avoiding the unnecessary transmission of a "**Membership Report message**".
* **Leave Report**  
  When the host does not send the "Membership Report message", it means that the host has left the group. The host knows that there are no members in the group, so even when it receives the next query, it would not report the group.

# Transport Layer protocols

* The transport layer is represented by two protocols: TCP and UDP.
* The IP protocol in the network layer delivers a datagram from a source host to the destination host.
* Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
* An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
* Each port is defined by a positive integer address, and it is of 16 bits.

## UDP

* UDP stands for **User Datagram Protocol**.
* UDP is a simple protocol and it provides nonsequenced transport functionality.
* UDP is a connectionless protocol.
* This type of protocol is used when reliability and security are less important than speed and size.
* UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
* The packet produced by the UDP protocol is known as a user datagram.

## User Datagram Format

* **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
* **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
* **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
* **Checksum:** The checksum is a 16-bit field which is used in error detection.

### Disadvantages of UDP protocol

* UDP provides basic functions needed for the end-to-end delivery of a transmission.
* It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
* UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

## TCP

* TCP stands for Transmission Control Protocol.
* It provides full transport layer services to applications.
* It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

## Features Of TCP protocol

* **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
* **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.  
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
* **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
* **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
* **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
* **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  + Establish a connection between two TCPs.
  + Data is exchanged in both the directions.
  + The Connection is terminated.

## TCP Segment Format

**Where,**

* **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
* **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
* **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
* **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
* **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
* **Reserved:** It is a six-bit field which is reserved for future use.
* **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

### There are total six types of flags in control field:

* **URG:** The URG field indicates that the data in a segment is urgent.
* **ACK:** When ACK field is set, then it validates the acknowledgement number.
* **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
* **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
* **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation ( with the ACK bit set ), and confirmation acknowledgement.
* **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
  + **Window Size:** The window is a 16-bit field that defines the size of the window.
  + **Checksum:** The checksum is a 16-bit field used in error detection.
  + **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
  + **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

## Differences b/w TCP & UDP

|  |  |  |
| --- | --- | --- |
| **Basis for Comparison** | **TCP** | **UDP** |
| Definition | TCP establishes a virtual circuit before transmitting the data. | UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not. |
| Connection Type | It is a Connection-Oriented protocol | It is a Connectionless protocol |
| Speed | slow | high |
| Reliability | It is a reliable protocol. | It is an unreliable protocol. |
| Header size | 20 bytes | 8 bytes |
| acknowledgement | It waits for the acknowledgement of data and has the ability to resend the lost packets. | It neither takes the acknowledgement, nor it retransmits the damaged frame. |

### TCP/IP Protocol Architecture Model

The OSI model describes idealized network communications with a family of protocols. TCP/IP does not directly correspond to this model. TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all. The following table shows the layers of the Oracle Solaris implementation of TCP/IP. The table lists the layers from the topmost layer (application) to the bottommost layer (physical network).

**Table 1-2 TCP/IP Protocol Stack**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | **OSI Ref. Layer No.** | **OSI Layer Equivalent** | **TCP/IP Layer** | **TCP/IP Protocol Examples** | | 5,6,7 | Application, session, presentation | Application | NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others | | 4 | Transport | Transport | TCP, UDP, SCTP | | 3 | Network | Internet | IPv4, IPv6, ARP, ICMP | | 2 | Data link | Data link | PPP, IEEE 802.2 | | 1 | Physical | Physical network | Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI, and others | |

The table shows the TCP/IP protocol layers and the OSI model equivalents. Also shown are examples of the protocols that are available at each level of the TCP/IP protocol stack. Each system that is involved in a communication transaction runs a unique implementation of the protocol stack.

#### Physical Network Layer

The **physical network layer** specifies the characteristics of the hardware to be used for the network. For example, physical network layer specifies the physical characteristics of the communications media. The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

#### Data-Link Layer

The **data-link layer** identifies the network protocol type of the packet, in this instance TCP/IP. The data-link layer also provides error control and “framing.” Examples of data-link layer protocols are Ethernet IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

#### Internet Layer

The Internet layer, also known as the **network layer** or **IP layer**, accepts and delivers packets for the network. This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP).

##### IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

* **IP addressing** – The IP addressing conventions are part of the IP protocol. [Designing an IPv4 Addressing Scheme](https://docs.oracle.com/cd/E23823_01/html/816-4554/ipplan-5.html#scrolltoc) introduces IPv4 addressing and [IPv6 Addressing Overview](https://docs.oracle.com/cd/E23823_01/html/816-4554/ipv6-overview-10.html#scrolltoc) introduces IPv6 addressing.
* **Host-to-host communications** – IP determines the path a packet must take, based on the receiving system's IP address.
* **Packet formatting** – IP assembles packets into units that are known as **datagrams**. Datagrams are fully described in [Internet Layer: Where Packets Are Prepared for Delivery](https://docs.oracle.com/cd/E23823_01/html/816-4554/ipov-29.html#ipov-38).
* **Fragmentation** – If a packet is too large for transmission over the network media, IP on the sending system breaks the packet into smaller fragments. IP on the receiving system then reconstructs the fragments into the original packet.

Oracle Solaris supports both IPv4 and IPv6 addressing formats, which are described in this book. To avoid confusion when addressing the Internet Protocol, one of the following conventions is used:

* When the term “IP” is used in a description, the description applies to both IPv4 and IPv6.
* When the term “IPv4” is used in a description, the description applies only to IPv4.
* When the term “IPv6” is used in a description, the description applies only to IPv6.

##### ARP Protocol

The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers. ARP assists IP in directing datagrams to the appropriate receiving system by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

##### ICMP Protocol

The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:

* **Dropped packets** – Packets that arrive too fast to be processed
* **Connectivity failure** – A destination system cannot be reached
* **Redirection** – Redirecting a sending system to use another router

#### Transport Layer

The TCP/IP **transport layer** ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets. This type of communication is known as **end-to-end**. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service. UDP provides unreliable datagram service.

##### TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets. This transmission consists of the following:

* Starting point, which opens the connection
* Entire transmission in byte order
* Ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains many parameters that help processes on the sending system connect to peer processes on the receiving system.

TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a “reliable, connection-oriented” protocol.

##### SCTP Protocol

SCTP is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP. Moreover, SCTP can support connections between systems that have more than one address, or **multihomed**. The SCTP connection between sending and receiving system is called an **association**. Data in the association is organized in chunks. Because SCTP supports multihoming, certain applications, particularly applications used by the telecommunications industry, need to run over SCTP, rather than TCP.

##### UDP Protocol

UDP provides datagram delivery service. UDP does not verify connections between receiving and sending hosts. Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use UDP.

#### Application Layer

The **application layer** defines standard Internet services and network applications that anyone can use. These services work with the transport layer to send and receive data. Many application layer protocols exist. The following list shows examples of application layer protocols:

* Standard TCP/IP services such as the ftp, tftp, and telnet commands
* UNIX “r” commands, such as rlogin and rsh
* Name services, such as NIS and the domain name system (DNS)
* Directory services (LDAP)
* File services, such as the NFS service
* Simple Network Management Protocol (SNMP), which enables network management
* Router Discovery Server protocol (RDISC) and Routing Information Protocol (RIP) routing protocols

##### Standard TCP/IP Services

* **FTP and Anonymous FTP** – The File Transfer Protocol (FTP) transfers files to and from a remote network. The protocol includes the ftp command and the in.ftpd daemon. FTP enables a user to specify the name of the remote host and file transfer command options on the local host's command line. The in.ftpd daemon on the remote host then handles the requests from the local host. Unlike rcp, ftp works even when the remote computer does not run a UNIX based operating system. A user must log in to the remote system to make an ftp connection, unless the remote system has been configured to allow anonymous FTP.

You can obtain an enormous amount of material from **anonymous FTP servers** that are connected to the Internet. Universities and other institutions set up these servers to offer software, research papers, and other information to the public domain. When you log in to this type of server, you use the login name anonymous, hence the term “anonymous FTP server.”

Using anonymous FTP and setting up anonymous FTP servers is outside the scope of this manual. However, many books, such as **The Whole Internet User's Guide & Catalog**, discuss anonymous FTP in detail. Instructions for using FTP are in [System Administration Guide: Network Services](https://docs.oracle.com/cd/E23823_01/html/816-4555/index.html). The [ftp(1)](https://docs.oracle.com/cd/E23823_01/html/816-5165/ftp-1.html#REFMAN1ftp-1) man page describes all ftp command options that are invoked through the command interpreter. The [ftpd(1M)](https://docs.oracle.com/cd/E23823_01/html/816-5166/ftpd-1m.html" \l "REFMAN1Mftpd-1m) man page describes the services that are provided by the in.ftpd daemon.

* **Telnet** – The Telnet protocol enables terminals and terminal-oriented processes to communicate on a network that runs TCP/IP. This protocol is implemented as the telnet program on local systems and the in.telnetd daemon on remote machines. Telnet provides a user interface through which two hosts can communicate on a character-by-character or line-by-line basis. Telnet includes a set of commands that are fully documented in the [telnet(1)](https://docs.oracle.com/cd/E23823_01/html/816-5165/telnet-1.html#REFMAN1telnet-1) man page.
* **TFTP** – The Trivial File Transfer Protocol (tftp) provides functions that are similar to ftp, but the protocol does not establish ftp's interactive connection. As a result, users cannot list the contents of a directory or change directories. A user must know the full name of the file to be copied. The [tftp(1)](https://docs.oracle.com/cd/E23823_01/html/816-5165/tftp-1.html" \l "REFMAN1tftp-1)man page describes the tftp command set.

### Comparison Chart

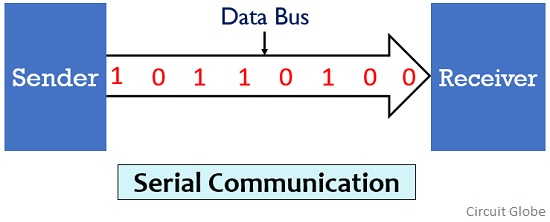
| **Basis for Comparison** | **Serial Communication** | **Parallel Communication** |
| --- | --- | --- |
| Data transmission speed | Slow | Comparatively fast |
| Number of communication link used | Single | Multiple |
| Number of transmitted bit/clock cycle | only one bit. | n number of link will carry n bits. |
| Cost | Low | High |
| Crosstalk | Not present | Present |
| System Up-gradation | Easy | Quite difficult |
| Mode of transmission | Full duplex | Half duplex |
| Suitable for | Long distance | Short distance |
| High frequency operation | More efficient | Less efficient |

### Definition of Serial Communication

In serial communication the data bits are transmitted serially over a common communication link one after the other.

Basically it does not allow simultaneous transmission of data because only a single channel is utilized. Thereby allowing sequential transfer rather than simultaneous transfer.

The figure below shows the serial data transmission:

[](https://circuitglobe.com/wp-content/uploads/2019/07/serial-communication.jpg)

It is highly suitable for long distance signal transmission as only a single wire or bus is used. So, it can be connected between two points that are separated at a large distance with respect to each other.

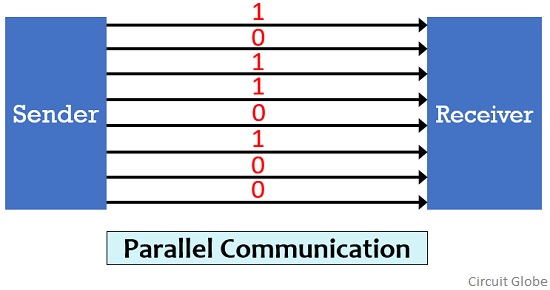
But as only a **single data bit is transmitted per clock pulse** thus the transmission of data is a quiet time taking process.

### Definition of Parallel Communication

In parallel communication the various data bits are simultaneously transmitted using multiple communication links between sender and receiver.

Here, despite using a single channel between sender and receiver, various links are used and each bit of data is transmitted separately over all the communication link.

The figure below shows the transmission of 8 byte data using parallel communication technique:



Here, as we can see that for the transmission of 8-bit of data, 8 separate communication links are utilized. And so rather following a sequential data transmission, simultaneous transmission of data is allowed.

This leads to a faster communication between the sender and receiver. But for connecting multiple lines between sender and receiver multiple connecting unit are to be present between a pair of sender and receiver.

And this is the reason why parallel communication is not suitable for long distance transmission, because connecting multiple lines to large distances is very difficult and expensive.

## Key Differences Between Serial and Parallel Communication

1. Due to the presence of single communication link the speed of data transmission is slow. While multiple links in case of parallel communication allows data transmission at comparatively faster rate.
2. Whenever there exists a need for system up-gradation then upgrading a system that uses serial communication is quite an easy task as compared to upgrading a parallel communication system.
3. In serial communication, the all data bits are transmitted over a common channel thus proper spacing is required to be maintained in order to avoid interference. While in parallel communication, the utilization of multiple link reduces the chances of interference between the transmitted bits.
4. Serial communication supports higher bandwidth while parallel communication supports comparatively lower bandwidth.
5. Serial communication is efficient for high frequency operation. However, parallel communication shows its suitability more in case of low frequency operations.
6. Due to existence of single link, the problem of crosstalk is not present in serial communication. But multiple links increase the chances of crosstalk in parallel communication.
7. Serial communication is suitable for long distance transmission of data as against parallel communication is suitable for short distance transmission of data.