Unit-1: Networks Basics

A **computer network** or **data network** is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along network links (data connections). Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. The best- known computer network is the Internet.

To build a computer network is defining what a network is and understanding how it is used to help a business meet its objectives. A network is a connected collection of devices and end systems, such as computers and servers, which can communicate with each other.

In the simplest form, data transfer can take place between two devices which are directly connected by some form of communication medium. But it is not practical for two devices to be directly point to point connected. This is due to the following reasons:

i) The devices are situated at remote places.

ii) There is a set of devices, each of whom may require connecting to others at various times.

iii) Solution to this problem is to connect each device to a communication network. Computer Networks means interconnected set of autonomous systems that permit distributed processing of information.

These are the four major categories of physical components in a computer network:

- **Personal computers (PCs):** The PCs serve as endpoints in the network, sending and receiving data.
- **Interconnections:** The interconnections consist of components that provide a means for data to travel from one point to another point in the network. This category includes components such as the following:
  - Network interface cards (NICs) that translate the data produced by the computer into a format that can be transmitted over the local network
  - Network media, such as cables or wireless media, that provide the means by which the signals are transmitted from one networked device to another
  - Connectors that provide the connection points for the media
- **Switches:** Switches are devices that provide network attachment to the end systems and intelligent switching of the data within the local network.
- **Routers:** Routers interconnect networks and choose the best paths between networks.

Computer Network

- A computer network is a system in which multiple computers are connected to each other to share information and resources.
- The physical connection between networked computing devices is established using either cable media or wireless media.
- The best-known computer network is the Internet.

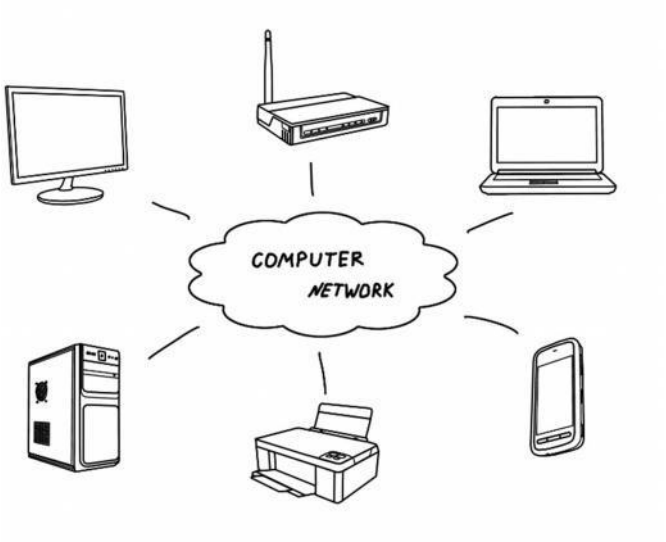


Figure 1 : Computer Network

Advantages of Computer Networks

- **File sharing**
  The major advantage of a computer network is that is allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he is authorized to do so.
- **Resource sharing**
  All computers in the network can share resources such as printers, fax machines, modems, and scanners.
- **Better connectivity and communications**
  It allows users to connect and communicate with each other easily. Various communication applications included e-mail and groupware are used. Through e-mail, members of a network can send message and ensure safe delivery of data to other members, even in their absence.
- **Internet access**
  Computer networks provide internet service over the entire network. Every single computer attached to the network can experience the high speed internet.
- **Entertainment**
  Many games and other means of entertainment are easily available on the internet. Furthermore, Local Area Networks (LANs) offers and facilitates other ways of enjoyments, such as many players are connected through LAN and play a particular game with each other from remote location.

- **Inexpensive system**
  Shared resources mean reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means reduction in file storage expenses. A particular software can be installed only once on the server and made available across all connected computers at once. This saves the expense of buying and installing the same software as many times for as many users.
- **Flexible access**
  A user can log on to a computer anywhere on the network and access his files. This offers flexibility to the user as to where he should be during the course of his routine.
- **Instant and multiple access**
  Computer networks are multiply processed .many of users can access the same information at the same time. Immediate commands such as printing commands can be made with the help of computer networks.

Disadvantages of Computer Networks

- **Lack of data security and privacy**
  Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.
- **Presence of computer viruses and malwares**
  If even one computer on a network gets affected by a virus, there is a possible threat for the other systems getting affected too. Viruses can spread on a network easily, because of the inter- connectivity of workstations. Moreover, multiple systems with common resources are the perfect breeding ground for viruses that multiply.
- **Lack of Independence**
  Since most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use his own computer.
- **Lack of Robustness**
  As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill.
- **Need an efficient handler**
  For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

Use (Applications) of Computer Networks

The key to utilizing multiple resources on a data network is having applications that are aware of these communication mechanisms. Although many applications are available for users in a network environment, some applications are common to nearly all users.

- **Financial services**
  Nowadays, almost all the financial services depend on the computer network. You can access the financial services across the world. For example, a user can transfer money from one place to another by using the electronic fund transfer feature. You can use networking in various financial areas such as ATM, foreign exchange and credit history search.

- **Business**

  Nowadays, most of the works of businesses are done over the computers. To exchange the data and ideas, you need an effective data and resources sharing features. To do this, you need to connect the computer with each other through a network. For example, a person of one department of an organization can share or access the electronic data of other department through network.
- **Email services**

  A computer network provides you the facility to send or receive mails across the globe in few seconds.
- **Mobile applications**

  By using the mobile applications, such as cellular or wireless phones, you can communicate (exchange your views and ideas) with one other.
- **Directory services**

  It provides you the facility to store files on a centralized location to increase the speed of search operation worldwide.
- **Teleconferencing**

  It contains voice conferencing and video conferencing which are based in networking. In teleconferencing the participants need not to be presented at the same location.

Types of Computer Networks

LAN (Local Area Network)

- It is privately-owned networks within a single building or campus of up to a few kilometres in size.
- They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.
- LANs are easy to design and troubleshoot
- In LAN, all the machines are connected to a single cable.
- Different types of topologies such as Bus, Ring, Star and Tree are used.
- The data transfer rates for LAN is up to 10 Gbits/s.
- They transfer data at high speeds. High transmission rate are possible in LAN because of the short distance between various computer networks.
- They exist in a limited geographical area.
- **Advantages**
  - LAN transfers data at high speed.
  - LAN technology is generally less expensive.

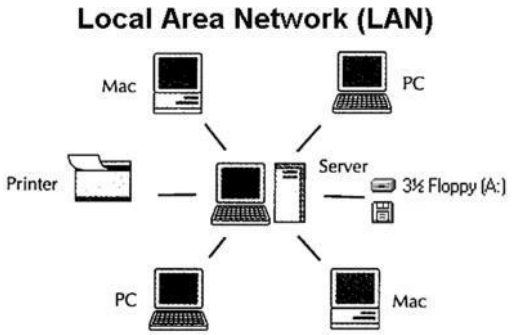


Figure 2: Local Area Network

MAN (Metropolitan Area Network)

- MAN is a larger version of LAN which covers an area that is larger than the covered by LAN but smaller than the area covered by WAN.
- A metropolitan area network or MAN covers a city. The best-known example of a MAN is the cable television network available in many cities.
- MAN connects two or more LANs.
- At first, the companies began jumping into the business, getting contracts from city governments to wire up an entire city.
- The next step was television programming and even entire channels designed for cable only.

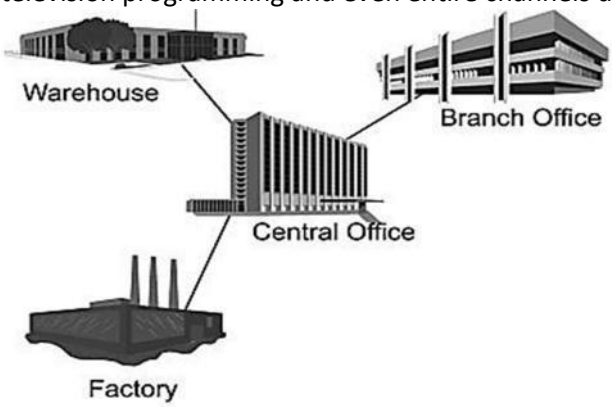


Figure 3: Metropolitan Area Network

WAN (Wide Area Network)

- WAN spans a large geographical area, often a country or region.
- WAN links different metropolitan's countries and national boundaries there by enabling easy communication.
- It may be located entirely with in a state or a country or it may be interconnected around the world.
- It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts.
- The communication between different users of WAN is established using leased telephone lines or satellite links and similar channels.

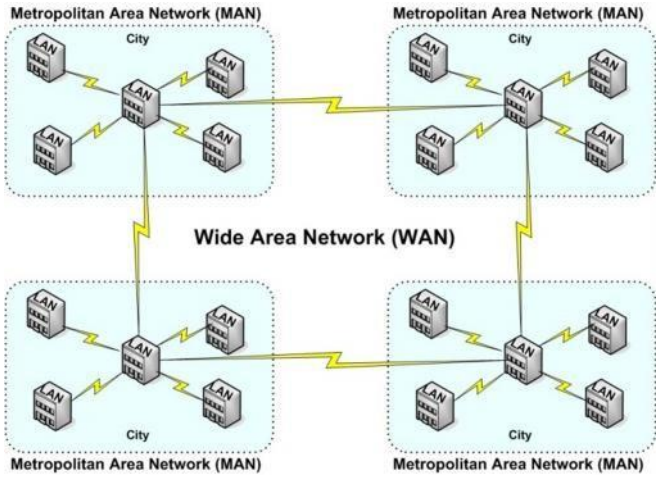


Figure 4: Wide Area Network

Difference between LAN, MAN and WAN.

Parameter	LAN	MAN	WAN
Area covered	Covers small area. i.e. within building	Covers larger than LAN & smaller than WAN	Covers large area
Error rates	Lowest	Moderate	Highest
Transmission speed	High speed	Moderate speed	Low speed
Equipment cost	Inexpensive	Moderate expensive	Most expensive
Design & maintenance	Easy	Moderate	Difficult

Internet

- The internet is a type of world-wide computer network.
- The internet is the collection of infinite numbers of connected computers that are spread across the world.
- We can also say that, the Internet is a computer network that interconnects hundreds of millions of computing devices throughout the world.
- It is established as the largest network and sometimes called network of network that consists of numerous academic, business and government networks, which together carry various information.
- Internet is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
- When two computers are connected over the Internet, they can send and receive all kinds of information such as text, graphics, voice, video, and computer programs.

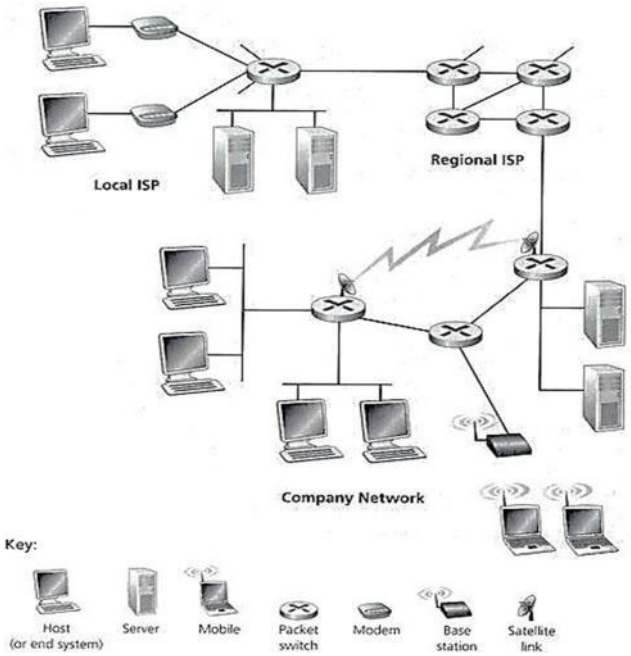


Figure 5: Some pieces of the Internet

Protocol

- A protocol is a set of rules that governs (manages) data communications.
- Protocols defines methods of communication, how to communicate, when to communicate etc.
- A protocol is an agreement between the communicating parties on how communication is to proceed.
- Important elements of protocols are
    1. Syntax
    2. Semantics
    3. Timing
- **Syntax**:- Syntax means format of data or the structure how it is presented e.g. first eight bits are for sender address, next eight bits are for receiver address and rest of the bits for message data.
- **Semantics**:- Semantics is the meaning of each section of bits e.g. the address bit means the route of transmission or final destination of message.
- **Timing**:- Timing means, at what time data can be sent and how fast data can be sent.
- Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication.
- Example: HTTP, IP, FTP etc…

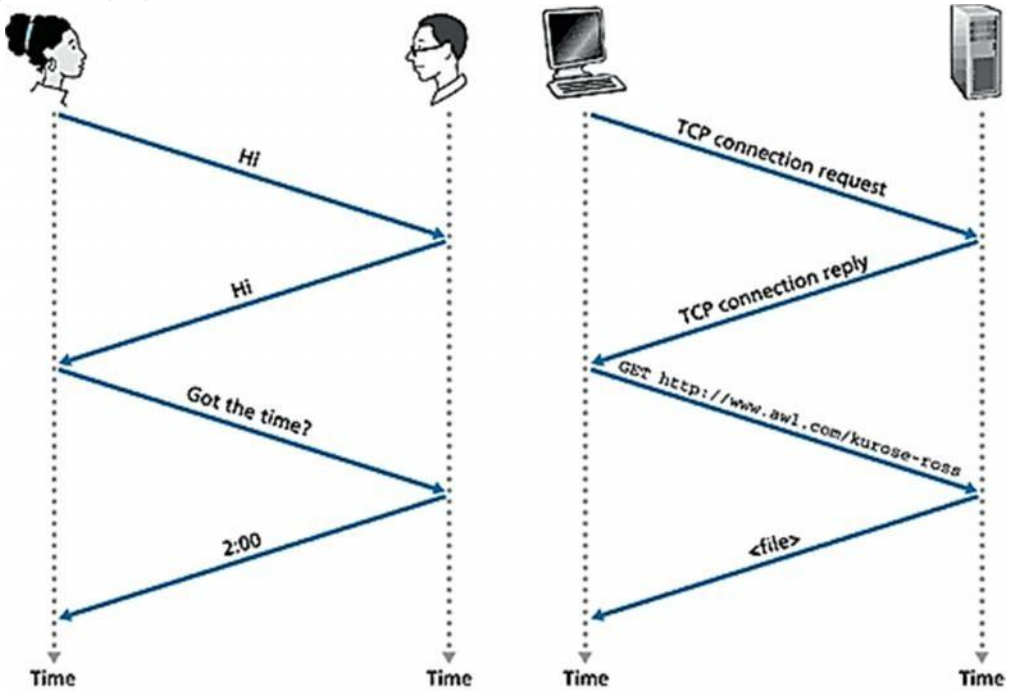


Figure 6: A human protocol and a computer network protocol

The Network Edge

- It defines those computers of the network used at the edge (end) of the network. These computers are known as hosts or end system.
- Host can be classified into the following two types:
    - **Clients**: Refer to the computer systems that request servers for the completion of a task. The clients are generally called desktop PCs or workstations.

- **Servers**: Refer to the computer systems that receive requests from the clients and process them. After the processing is complete, the servers send a reply to the clients who sent the request.

- The concept of clients and servers is essential in the network design. The various networks design models are as follows:
  1. Peer to Peer network
  2. Client Server network

Peer to Peer network

- In this network group of computers is connected together so that users can share resources and information.
- There is no central location (server) for authenticating users, storing files, or accessing resources and each of them works as both client and server.
- This means that users must remember which computers in the workgroup have the shared resource or information that they want to access.
- **Advantage**:
  - It is easy to setup.
  - There is no need of any committed server as each peer acts as both server and client.
  - The network implementation is quite cheap.
  - The resources of a peer can be shared with other peers very easily in the network.
- **Disadvantage:**
  - The speed of the network decreases due to heavy usage.
  - It is not easy to keep track of information on each computer.
  - There is no central backup of files and folders.
  - Network and data security are weak.

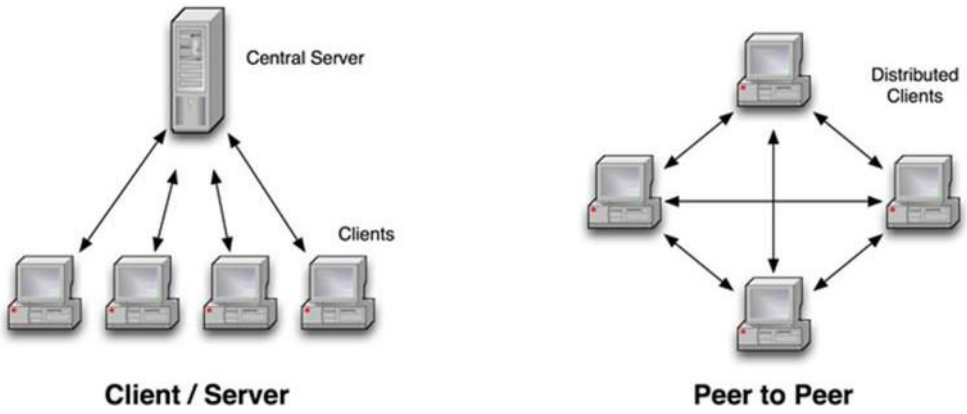


Figure 7: Network Edge - Client/Server Network and Peer to Peer

Client/Server network

- A client/server network is a system where one or more computers called clients connect to a central computer named as server to share or use resources.
  - The client requests a service from server, which may include running an application, querying database, printing a document, performing a backup or recovery procedure. The request made by the client is handled by server.
  - A client/server network is that in which the files and resources are centralized. This means that the server can hold them and other computers (Client) can access them.

- **Advantage**:
  - The server system holds the shared files.
  - The server system can be scheduled to take the file backups automatically.
  - Network access is provided only to authorize users through user security at the server.
  - The server system is a kind of central repository for sharing printer with clients.
  - Internet access, e-mail routing and such other networking tasks are quite easily managed by the server.
  - The software applications shared by the server are accessible to the clients.
- **Disadvantage:**
  - The implementation of the network is quite expensive.
  - An NOS (Network Operating System) is essential.
  - If server fails, the entire network crashes.
  - There may be congestion if more than one client requests for a service at the same time.

Techniques used in data communications to transfer data

1. Connection-oriented method
2. Connectionless method

Connection-oriented method

- Connection-oriented communication includes the steps of setting up a call from one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call.
- However, the network connecting the computers is a packet switched network, unlike the phone system's circuit switched network.
- Connection-oriented communication is done in one of two ways over a packet switched network:
  1. Without virtual circuits
  2. With virtual circuits.

Without virtual circuits:

- This is what TCP does in the Internet.
- The only two machines in the Internet are aware about connection which is established between the two computers at the endpoints.
- The Internet itself, its routers and links have no information about the presence of a connection between the two computers.
- This means that all of the packets flowing between the two computers can follow different routes.
- One benefit of establishing the connection is that the flow of packets from the source to the destination can be slowed down if the Internet is congested and speeded up when congestion disappears.
- Another benefit is that the endpoints can anticipate traffic between them, and agree to cooperate to ensure the integrity and continuity of the data transfers. This allows the network to be treated as a "stream" of data.

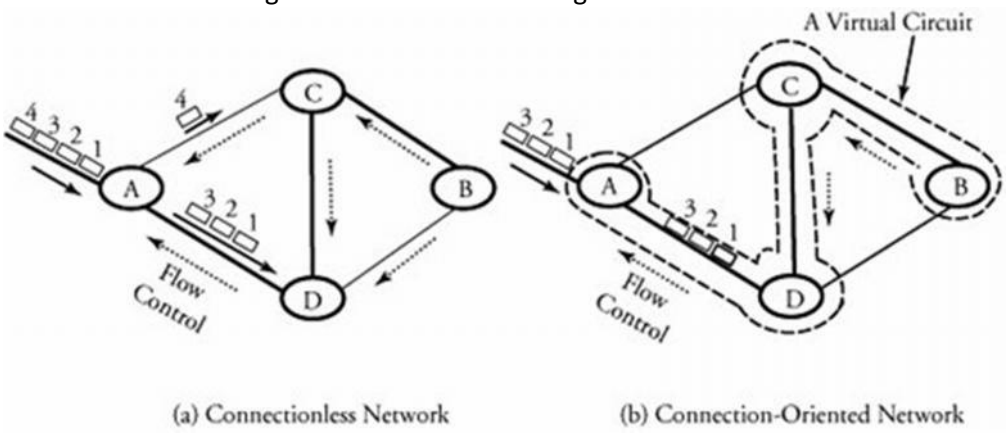
With virtual circuit:

- This is not used in the Internet, but is used in other types of networks (eg. the "X.25" protocol, still popular in Europe).

- The routers within the network route all packets in one connection over the same route. The advantage is that video and voice traffic are easier to carry, because routers can reserve memory space to buffer the transmission.

Connectionless method

- Connectionless communication is just packet switching where no call establishment and release occur.
- A message is broken into packets, and each packet is transferred separately. Moreover, the packets can travel different route to the destination since there is no connection.
- Connectionless service is typically provided by the UDP (User Datagram Protocol). The packets transferred using UDP are also called datagrams.



Feature	Connectionless	Connection-oriented
How is data sent?	one packet at a time	as continuous stream of packets
Do packets follow same route?	no	virtual circuit: yes without virtual circuit: no
Are resources reserved in network?	no	virtual circuit: yes without virtual circuit: no
Are resources reserved in communicating hosts?	no	yes
Is connection establishment done?	no	yes
Is state information stored at network nodes?	no	virtual circuit: yes without virtual circuit: no
What is impact of node/switch crash?	only packets at node are lost	all virtual circuits through node fail
What addressing information is needed on each packet?	full source and destination address	virtual circuit: a virtual circuit number without virtual circuit: full source and destination address

Transmission Media

- A transmission media can be defined as anything that can carry information from a source to a destination.
- On the basis of transmission of data, the transmission media can be classified in to two categories:
    1. Guided (Physical) transmission media
    2. Unguided (Wireless) transmission media

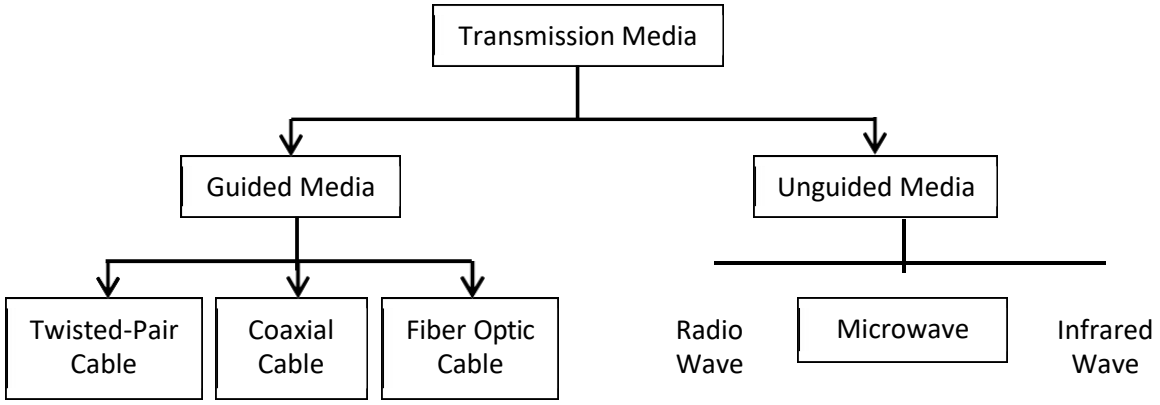


Figure 8: Classification Transmission Media

Guided Transmission Media

- Guided media are those that provide a channel from one device to another.
- The three Guided (Physical) media commonly used for data transmission are:
    1. Twisted-Pair
    2. Coaxial
    3. Fiber Optics

1. Twisted Pair

- A twisted pair consists of two insulated copper wires, typically about 1 mm thick.
- The wires are twisted together in a helical form, just like a DNA molecule.
- Twisting is done because two parallel wires constitute a fine antenna.
- When the wires are twisted, the waves from different twists cancel out, so the wire radiates less effectively.

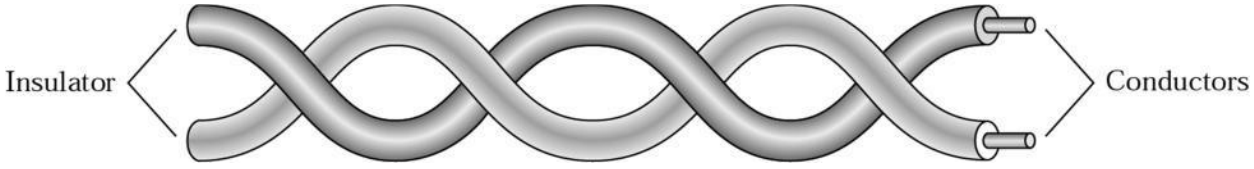


Figure 9: Twisted Pair Cable

Why cable is twisted?

- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relatives to the noise or crosstalk sources.
- This results in a difference at the receiver.
- By twisting the pair, a balance is maintained.

Types of Twisted-Pair Cable

1) Unshielded twisted-pair (UTP)

- Twisted pair cabling comes in several varieties, two of which are important for computer networks.
- **Category 3** twisted pairs consist of two insulated wires gently twisted together.
- Most office buildings had one category 3 cable running from a central wiring closet on each floor into each office.
- **Category 5** is the more advanced twisted pairs were introduced.
- They are similar to category 3 pairs, but with more twists per centimetre, which results in less crosstalk and a better-quality signal over longer distances, making them more suitable for high- speed computer communication.
- Up-and-coming categories are 6 and 7, which are capable of handling signals with bandwidths of 250 MHz and 600 MHz, respectively (versus a mere 16 MHz and 100 MHz for categories 3 and 5 respectively).

Figure 10: Unshielded twisted-pair

2) Shielded twisted-pair (STP).

- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
- Metal casing improves the quality of cable by preventing the penetration of noise or crosstalk.
- It is bulkier and more expensive.
- **Applications:**
  - Used in telephone lines to provide voice and data channels.
  - The DSL lines uses by telephone companies use the high-bandwidth capability of UTP cables.
  - LANs, such as 10Base-T, 100Base-T also uses twisted-pair cables.

2. Coaxial Cable

- It has better shielding than twisted pairs, so it can span longer distances at higher speeds.
- Two kinds of coaxial cable are widely used. One kind is 50-ohm cable which is commonly used when it is intended for digital transmission from the start.
- The other kind is 75-ohm cable which is commonly used for analog transmission and cable television but is becoming more important with the advent of Internet over cable.
- A coaxial cable consists of a stiff copper wire as the core surrounded by an insulating material.
- The insulator is encased by a cylindrical conductor, often as a closely-woven braided mesh.
- The outer conductor is covered in a protective plastic sheath.
- The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity.
- The bandwidth possible depends on the cable quality, length and signal-to-noise ratio of the data signal. Modern cables have a bandwidth of close to 1 GHz.

- Coaxial cables used is widely used within the telephone system for long-distance lines but have now largely been replaced by fiber optics on long-haul routes.

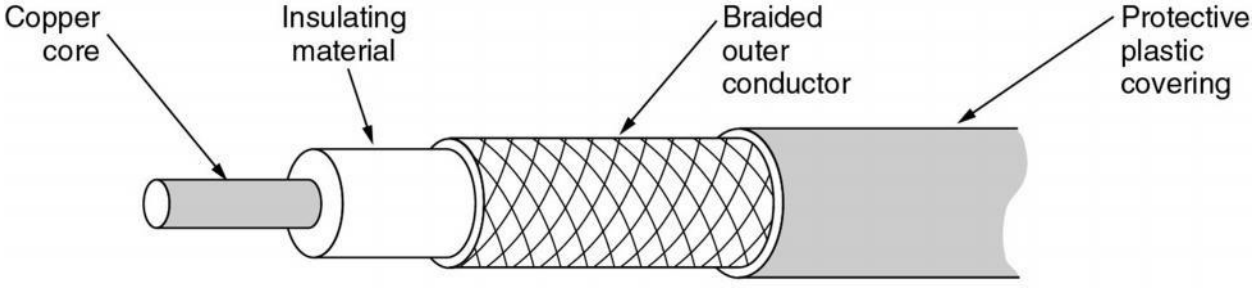


Figure 11: Coaxial Cable

3. Fiber Optics

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through a core is reflected off the cladding instead of being refracted into it.

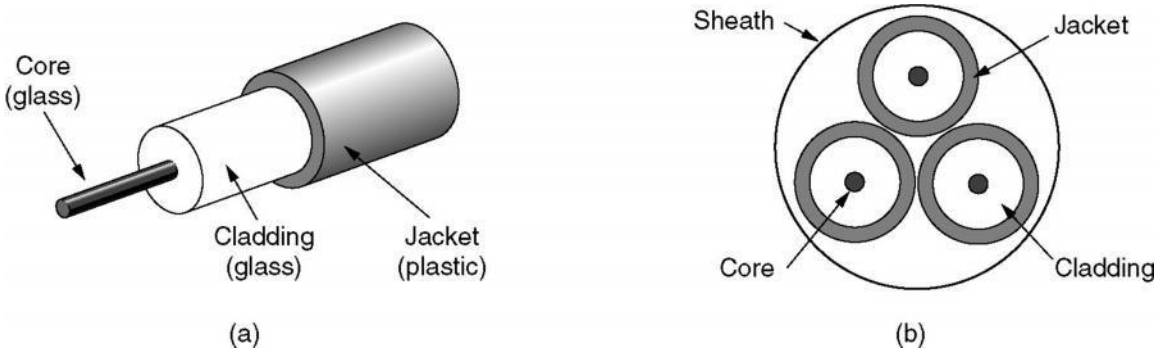


Figure 12: Fiber Optic Cable

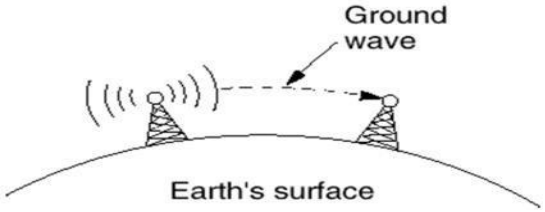
- Fiber optic cables are similar to coax, except without the braid.
- Figure shows a single fiber viewed from the side. At the centre is the glass core through which the light propagates.
- The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core.
- Next comes a thin plastic jacket to protect the cladding. Fibers are typically grouped in bundles, protected by an outer sheath. Figure shows a sheath with three fibers.

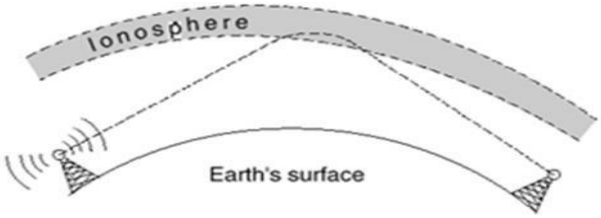
Unguided (Wireless) transmission media

- Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.
  1. Radio Transmission
  2. Microwave Transmission
  3. Infrared
  4. Light wave Transmission

1. Radio Transmission

- Radio waves are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.
- Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.
- The properties of radio waves are frequency dependent.
- At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source, roughly as $1/r^2$ in air.
- At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles. They are also absorbed by rain.
- At all frequencies, radio waves are subject to interference from motors and other electrical equipment.





- In the VLF, LF, and MF bands, radio waves follow the curvature of the earth.
- In the HF they bounce off the ionosphere

2. Microwave Transmission

- Since the microwaves travel in a straight line, if the towers are too far apart, the earth will get in the way. Consequently, repeaters are needed periodically.
- Unlike radio waves at lower frequencies, microwaves do not pass through buildings well. In addition, even though the beam may be well focused at the transmitter, there is still some divergence in space.
- Above 100 MHz, the waves **travel in straight lines** and can therefore be narrowly focused. Concentrating all the energy into a small beam using a **parabolic antenna** gives a much higher signal to noise ratio.
- **Advantages:**
  - No right way is needed (compared to wired media).
  - Relatively inexpensive.
  - Simple to install.
- **Disadvantages:**
  - Do not pass through buildings well.
  - Multipath fading problem (the delayed waves cancel the signal).
  - Absorption by rain above 8 GHz.
  - Severe shortage of spectrum.

3. Infrared

- Unguided infrared and millimetre waves are widely used for short-range communication.
- The remote controls used on televisions, VCRs, and stereos all use infrared communication.
- They are relatively directional, cheap, and easy to build but have a major drawback: they do not pass through solid objects (try standing between your remote control and your television and see if it still works).
- In general, as we go from long-wave radio toward visible light, the waves behave more and more like light and less and less like radio.
- On the other hand, the fact that infrared waves do not pass through solid walls well is also a plus.
- It means that an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings.
- Furthermore, security of infrared systems against eavesdropping is better than that of radio systems precisely for this reason.
- Therefore, no government license is needed to operate an infrared system, in contrast to radio systems, which must be licensed outside the ISM bands.

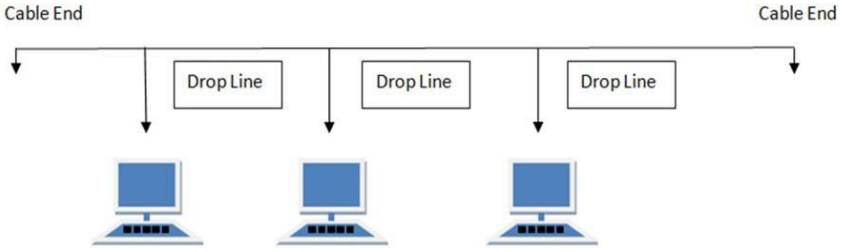
Topologies (Network Topologies)

- Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.
- A Network Topology is the arrangement with which computer systems or network devices are connected to each other.
- Types of network topologies :

1. Bus
2. Ring
3. Star
4. Mesh
5. Tree
6. Hybrid

Bus Topology

- Bus topology is a network type in which every computer and network device is connected to single cable.



Features:

- It transmits data only in one direction.
- Every device is connected to a single cable.

Advantages:

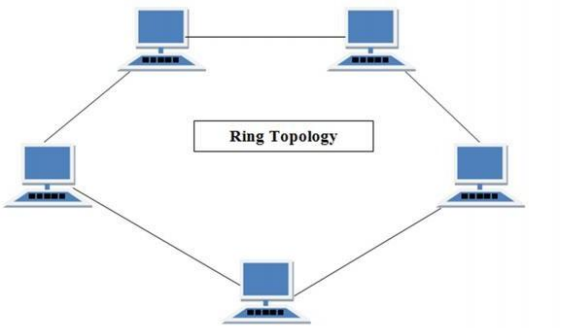
- It is cost effective (cheaper).
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages:

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.

Ring Topology

- It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features:

- A number of repeaters are used and the transmission is unidirectional.
- Date is transferred in a sequential manner that is bit by bit.

Advantages:

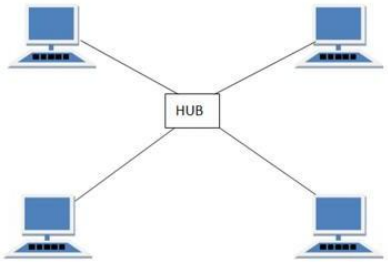
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand.

Disadvantages:

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

Star Topology

- In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features:

- Every node has its own dedicated connection to the hub.
- Acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages:

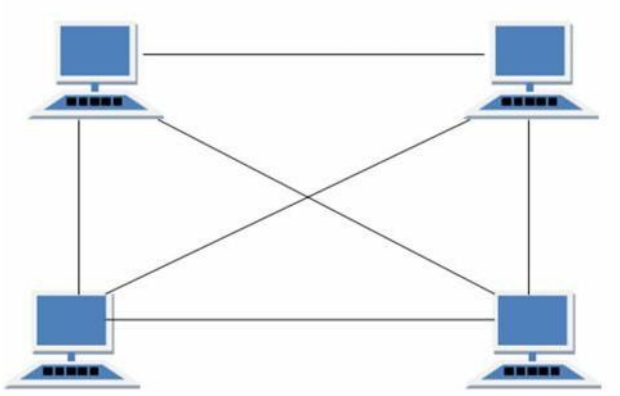
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed rest of the nodes can work smoothly.

Disadvantages:

- Cost of installation is high.
- Expensive to use.
- If the hub is affected then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the .

Mesh Topology

- It is a point-to-point connection to other nodes or devices.
- Traffic is carried only between two devices or nodes to which it is connected.



Features:

- Fully connected.
- Robust.
- Not flexible.

Advantages:

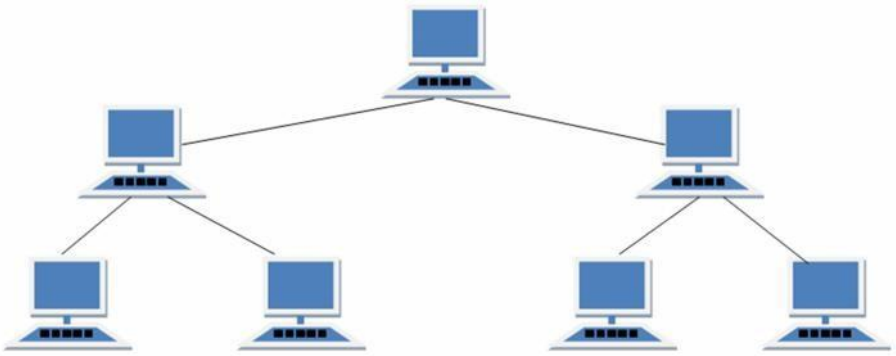
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages:

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

Tree Topology

- It has a root node and all other nodes are connected to it forming a hierarchy.
- It is also called hierarchical topology.
- It should at least have three levels to the hierarchy.



Features:

- Ideal if workstations are located in groups.
- Used in Wide Area Network.

Advantages:

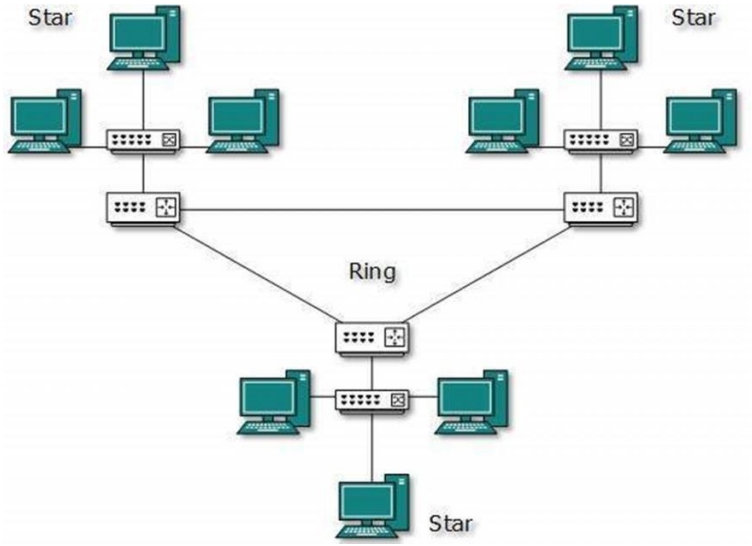
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages:

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails then network fails.

Hybrid Topology

- A network structure whose design contains more than one topology is said to be hybrid topology.
- For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features:

- It is a combination of two or more topologies
- Inherits the advantages and disadvantages of the topologies included

Advantages:

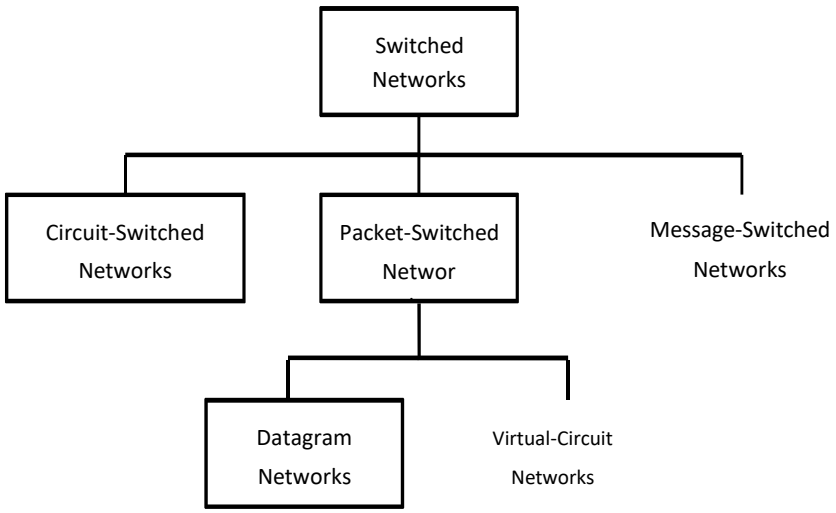
- Reliable as error detecting and trouble shooting is easy.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages:

- Complex in design.
- Costly.

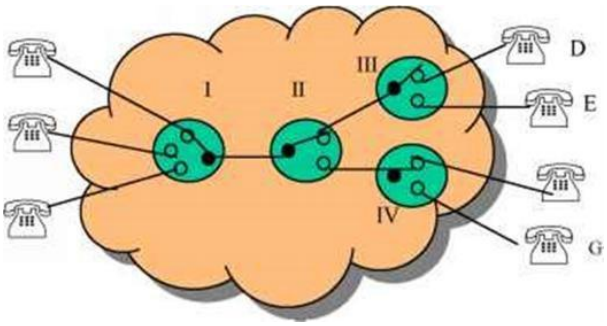
The Network Core

- Network core defines the connection of different network segments together and the process to transmit the data packets across the network.
- The network core is implemented through the use of switching techniques.
- The classification of switching network is shown below:

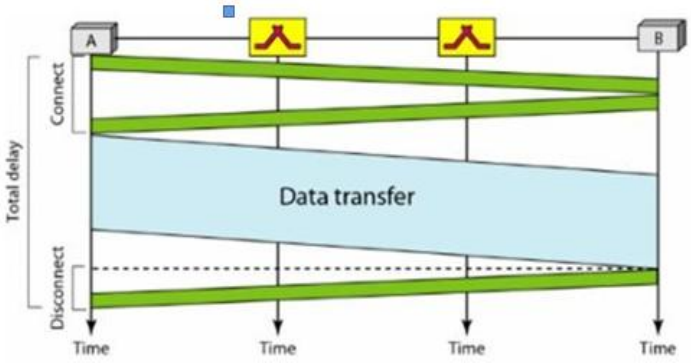


Circuit Switching

- Circuit switching is used in public telephone networks and is the basis for private networks built on leased-lines.
- Circuit switching was developed to handle voice traffic but also digital data (although inefficient)
- With circuit switching a dedicated path is established between two stations for communication.



- Switching and transmission resources within the network are reserved for the exclusive use of the circuit for the duration of the connection.
- The connection is transparent: once it is established, it appears to attach devices as if there were a direct connection.
- Communication via circuit switching involves three phases:
    1. Circuit Establishment
    2. Data Transfer
    3. Circuit Disconnect



- Connection path must be established before data transmission begins. Nodes must have switching capacity and channel capacity to establish connection.
- Circuit switching is inefficient
    1. Channel capacity dedicated for duration of connection
    2. If no data, capacity wasted
- Set up (connection) takes time
- Once connected, transfer is transparent to the users
    1. Data is transmitted at a fixed data rate with no delay (except for the propagation delay)
- Developed for voice traffic (phone)
    1. May also be used for data traffic via modem
- Interconnection of telephones within a building or office.
- In circuit switching, a direct physical connection between two devices is created by space-division switches, time-division switches, or both OR Circuit switching use any of below two technologies:

Space Division Switching

- Developed for analog environment.
- In a space-division switch, the path from one device to another is spatially separate from other paths.
- A crossbar is the most common space-division switch. It connects n inputs to m outputs via n × m cross points.
- Crossbar switch.

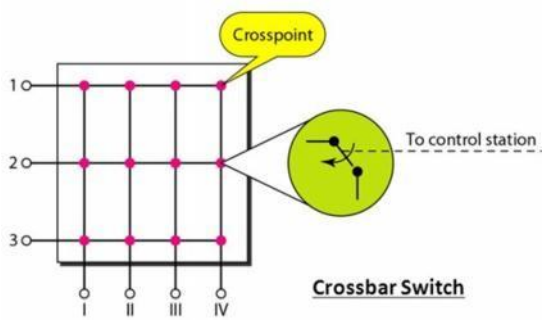


Figure 13: Space Division Switching

Time Division Switching

- In a time-division switch, the inputs are divided in time, using TDM. A control unit sends the input to the correct output device.
- Use digital time division techniques to set up and maintain virtual circuits.

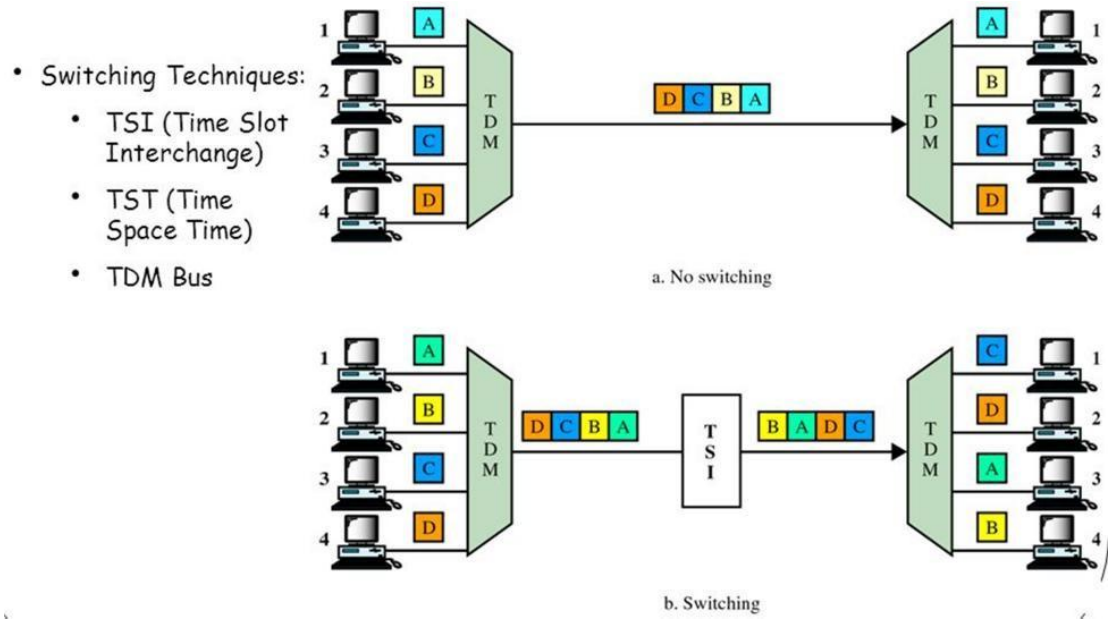


Figure 14: Time Division Switching

Packet Switching

- Packet switching was designed to provide a more efficient facility than circuit-switching for bursty data traffic.
- With packet switching, a station transmits data in small blocks, called packets.
- At each node packets are received, stored briefly (buffered) and passed on to the next node.
    1. Store and forward mechanism
- Each packet contains some portion of the user data plus control info needed for proper functioning of the network.
- A key element of packet-switching networks is whether the internal operation is datagram or virtual circuit (VC).
    1. With internal VCs, a route is defined between two endpoints and all packets for that VC follow the same route.
    2. With internal diagrams, each packet is treated independently, and packets intended for the same destination may follow different routes.
- Examples of packet switching networks are X.25, Frame Relay, ATM and IP.
- Station breaks long message into packets. Packets sent one at a time to the network.
- Packets handled in two ways:

    1. Datagram
        - Each packet treated independently
        - Packets can take any practical route
        - Packets may arrive out of order
        - Packets may go missing
        - Up to receiver to re-order packets and recover from missing packets

2. **Virtual Circuit**
    - Preplanned route established before any packets sent.
    - Once route is established, all the packets between the two communicating parties follow the same route through the network
    - Call request and call accept packets establish connection (handshake)
    - Each packet contains a Virtual Circuit Identifier (VCI) instead of destination address
    - No routing decisions required for each packet
    - Clear request to drop circuit
    - Not a dedicated path

Message Switching

- This technique was somewhere in middle of circuit switching and packet switching.
- In message switching, the whole message is treated as a data unit and is transferred in its entirety.
- A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

UNIT-2: OSI REFERNCE MODEL

In 1983, the International Standards Organization (ISO) developed a model called Open Systems Interconnection (OSI) which is a standard reference model for communication between two end users in a network. The model is used in developing products and understanding networks. It is a prescription of characterizing and standardizing the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it.

Layers in the OSI Model

OSI divides Telecommunications into Seven Layers as shown below in the Figure 1 given below. Each layer is responsible for a particular aspect of data communication. For example, one layer may be responsible for establishing connections between devices, while another layer may be responsible for error checking during transfer.

The layers of the OSI model are divided into two groups: the upper layers and lower layers. The upper layers (Host layers) focus on user applications and how files are represented on the computers prior to transport. The lower layers (Media Layers) concentrate on how the communication across a network actually occurs. Each layer has a set of functions that are to be performed by a specific protocol(s). The OSI reference model has a protocol suit for all of its layers.

In computing, a protocol is a convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication.

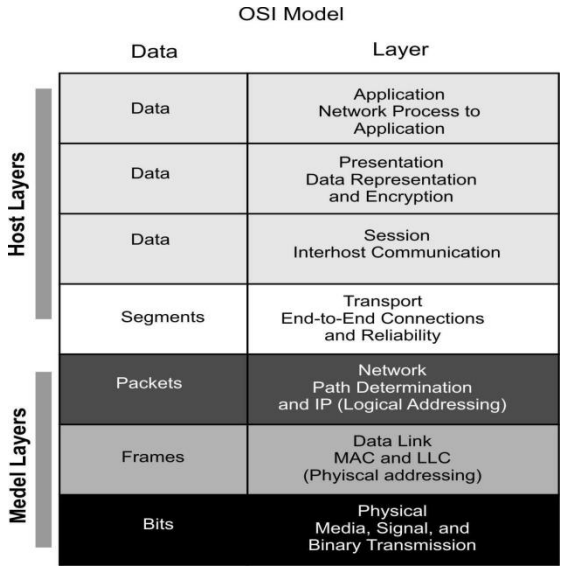


Figure 1: The OSI Model

Layer 1: The Physical Layer

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides :

- **Data encoding:** modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization.
- **Transmission technique:** determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- **Physical medium transmission:** transmits bits as electrical or optical signals appropriate for the physical medium, and determines: What physical medium options can be used? And How many volts/db should be used to represent a given signal state, using a given physical medium?
- **Layer 2: The data-link layer:** The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:
- **Frame Traffic Control:** tells the transmitting node to "stop" when no frame buffers are available.
- **Frame Sequencing:** transmits/receives frames sequentially.
- **Frame Acknowledgment:** provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- **Frame Delimiting:** creates and recognizes frame boundaries.
- **Link Establishment and Termination:** establishes and terminates the logical link between two nodes.
- **Frame Error Checking:** checks received frames for integrity.
- **Media access management:** determines when the node "has the right" to use the physical medium.

Data Link Sub layers

- The Data Link Layer is described in more detail with Media Access Control (MAC) and Logical Link Control (LLC) sub layers; where LLC is consider as upper data link layer and MAC as lower data link layer as shown below in the Figure 2.
- Logical Link Control (LLC): The LLC is concerned with managing traffic (flow and error control) over the physical medium and may also assign sequence numbers to frames and track acknowledgements. LLC is defined in the IEEE
- 802.2 specification and supports both connectionless and connection-oriented services used by higher-layer protocols.
- Media Access Control (MAC): The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it.

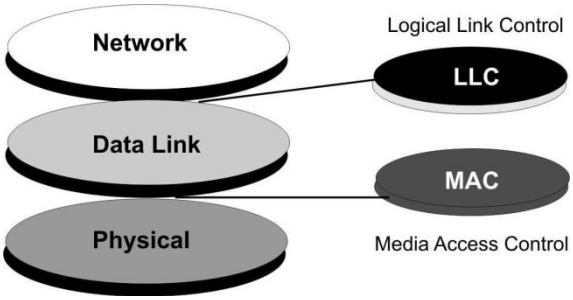


Figure 2: Data Link Sub-Layers

Layer 3: The Network Layer

The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network. The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer, sending data throughout the extended network and making the Internet possible.

Functions of the network layer include:

- Connection setup
- Addressing
- Routing
- Security
- Quality of Service
- Fragmentation

The Network Layer identifies computers on a network. Two types of packets are used at the Network layer; Data packets and Route update packets. Data packets are used to transport user data through the Internet work. Protocols used to support data traffic are called routed protocols. Route update packets are used to update neighboring routers about the network connected to all routers within the internet work. Protocols that send route updates are called routing protocols. This layer is concerned with two functions Routing and Fragmentation / Reassembly:

Routing: It is the process of selecting the best paths in a network along which to send data on physical traffic as shown in Figure 3.

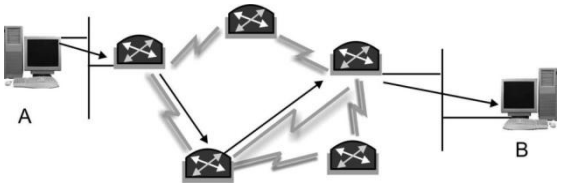


Figure 3: Routing at Network Layer

Fragmentation / Reassembly: if the network layer determines that a next router's maximum transmission unit (MTU) size is less than the current frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Layer 4: The Transport Layer

The transport layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/de-segmentation, and error control. This layer manages the end-to-end control (for example, determining whether all packets have arrived). It ensures complete data transfer. The Basic Transport Layer Services are:

- **Resource Utilization (multiplexing):** Multiple applications run on the same machine but use different ports.
- **Connection Management (establishing & terminating):** The second major task of Transport Layer is establishing connection between sender & the receiver before data transmission starts & terminating the connection once the data transmission is finished
- **Flow Control (Buffering / Windowing):** Once the connection has occurred and transfer is in progress, congestion of the data flow can occur at a destination for a variety of reasons. Possible options include:

  - The destination can become overwhelmed if multiple devices are trying to send it data at the same time.
  - The destination can become overwhelmed if the source is sending faster than it can physically receive.

The Transport Layer is responsible for providing flow control to alleviate the issue of congestion in the data transfer. Two main methods for flow control include:

Buffering: Buffering is a form of data flow control regulated by the Transport Layer as depicted in Figure 4. It is responsible for ensuring that sufficient buffers (Temporary Memory) are available at the destination for the processing of data and that the data is transmitted at a rate that does not exceed what the buffer can handle.

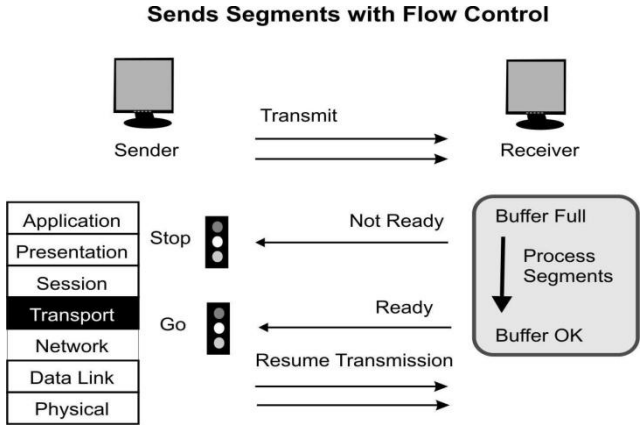


Figure 4: Buffering at Work

Windowing: Windowing is a flow control scheme in which the source computer will monitor and make adjustments to the amount of information sent based on successful, reliable receipt of data segments by the destination computer as shown in Figure 5. The size of the data transmission, called the "window size", is negotiated at the time of connection establishment, which is determined by the amount of memory or buffer that is available.

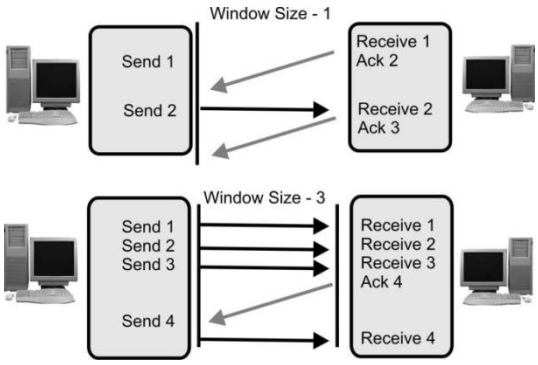


Figure 5: Flow Control & Reliability through Windowing

Reliable Transport (positive acknowledgment): Transport layer provides reliable transport of data by sending positive acknowledgements back to the sender once the data has reached the receiving side, if the data is lost or is corrupted, a negative acknowledgement is sent.

Layer 5: The Session Layer

The session Layer establishes, manages, and terminates sessions (different from connections) between applications as they interact on different hosts on a network. Its main job is to coordinate the service requests and responses between different hosts for applications.

The session established between hosts can be Simplex, half duplex and full duplex:

- **Simplex:** Simplex transmission is like a one-way street where traffic moves in only one direction. Simplex mode is a one-way-only transmission, which means that data can flow only in one direction from the sending device to the receiving device.
- **Half Duplex:** Half Duplex is like the center lane on some three-lane roads. It is a single lane in which traffic can move in one direction or the other, but not in both directions at the same time. Half-duplex mode limits data transmission because each device must take turns using the line. Therefore, data can flow from A to B and from B to A, but not at the same time.
- **Full Duplex:** is like a major highway with two lanes of traffic, each lane accommodating traffic going in opposite directions. Full-duplex mode accommodates two-way simultaneous transmission, which means that both sides can send and receive at the same time. In full-duplex mode, data can flow from A to B and B to A at the same time.

Note: *Full-duplex transmission is, in fact, two simplex connections: One connection has traffic flowing in only one direction; the other connection has traffic flowing in the opposite direction of the first connection.*

Layer 6: The Presentation Layer

The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. This layer, usually part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). This layer is sometimes called the syntax layer. The Presentation Layer is responsible for the following services:

- **Data representation:**

The presentation layer of the OSI model at the receiving computer is also responsible for the conversion of "the external format" with which data is received from the sending computer to one accepted by the other
layers in the host computer. Data formats include postscript, ASCII, or BINARY such as EBCDIC (fully Extended Binary Coded Decimal Interchange Code).

- **Data security:** Some types of encryption (and decryption) are performed at the presentation layer. This ensures the security of the data as it travels down the protocol stack.
- **Data compression:** Compression (and decompression) may be done at the presentation layer to improve the throughput of data.

Layer 7: The Application Layer

The application layer is closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component.

The Application Layer is the highest layer in the protocol stack and the layer responsible for introducing data into the OSI stack. The functions of Application Layer are:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Network management
- Directory services
- Electronic messaging (such as mail) etc

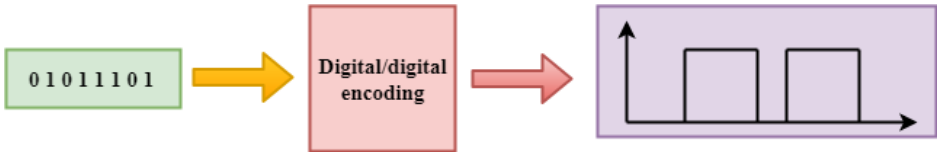
Physical Layer in Detail

Digital Transmission

Data can be represented either in analog or digital form. The computers used the digital form to store the information. Therefore, the data needs to be converted in digital form so that it can be used by a computer.

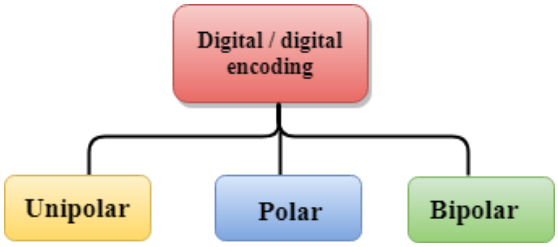
DIGITAL-TO-DIGITAL CONVERSION

Digital-to-digital encoding is the representation of digital information by a digital signal. When binary 1s and 0s generated by the computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process is known as digital-to-digital encoding.



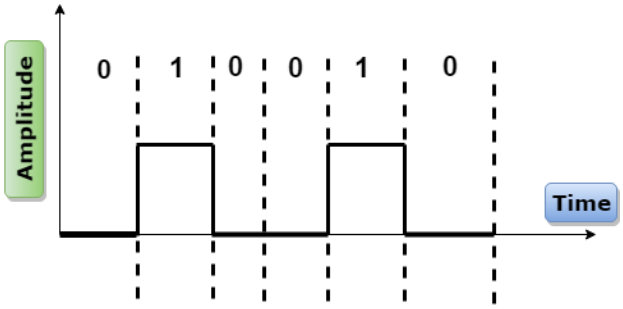
Digital-to-digital encoding is divided into three categories:

- Unipolar Encoding
- Polar Encoding
- Bipolar Encoding



Unipolar

- Digital transmission system sends the voltage pulses over the medium link such as wire or cable.
- In most types of encoding, one voltage level represents 0, and another voltage level represents 1.
- The polarity of each pulse determines whether it is positive or negative.
- This type of encoding is known as Unipolar encoding as it uses only one polarity.
- In Unipolar encoding, the polarity is assigned to the 1 binary state.
- In this, 1s are represented as a positive value and 0s are represented as a zero value.
- In Unipolar Encoding, '1' is considered as a high voltage and '0' is considered as a zero voltage.
- Unipolar encoding is simpler and inexpensive to implement.

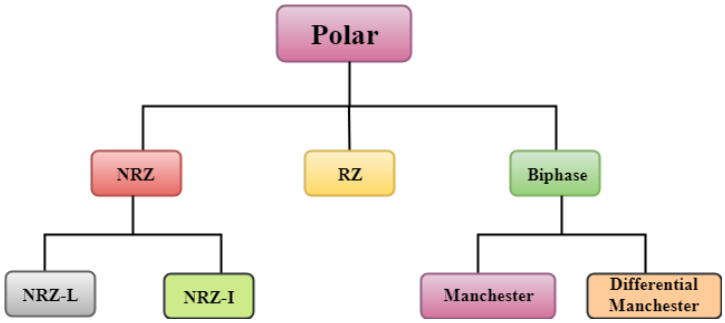


Unipolar encoding has two problems that make this scheme less desirable:

- DC Component
- Synchronization

Polar

- Polar encoding is an encoding scheme that uses two voltage levels: one is positive, and another is negative.
- By using two voltage levels, an average voltage level is reduced, and the DC component problem of unipolar encoding scheme is alleviated.



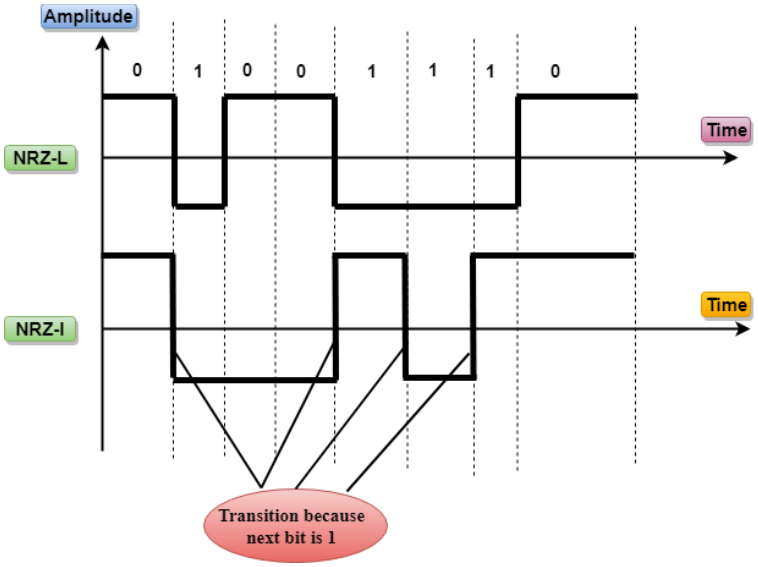
NRZ

- NRZ stands for Non-return zero.
- In NRZ encoding, the level of the signal can be represented either positive or negative.

The two most common methods used in NRZ are:

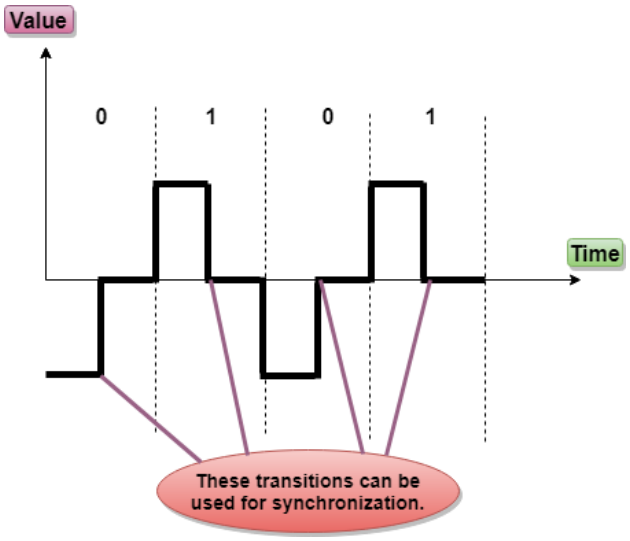
NRZ-L: In NRZ-L encoding, the level of the signal depends on the type of the bit that it represents. If a bit is 0 or 1, then their voltages will be positive and negative respectively. Therefore, we can say that the level of the signal is dependent on the state of the bit.

NRZ-I: NRZ-I is an inversion of the voltage level that represents 1 bit. In the NRZ-I encoding scheme, a transition occurs between the positive and negative voltage that represents 1 bit. In this scheme, 0 bit represents no change and 1 bit represents a change in voltage level.



RZ

- RZ stands for Return to zero.
- There must be a signal change for each bit to achieve synchronization. However, to change with every bit, we need to have three values: positive, negative and zero.
- RZ is an encoding scheme that provides three values, positive voltage represents 1, the negative voltage represents 0, and zero voltage represents none.
- In the RZ scheme, halfway through each interval, the signal returns to zero.
- In RZ scheme, 1 bit is represented by positive-to-zero and 0 bit is represented by negative-to-zero.



Disadvantage of RZ:

It performs two signal changes to encode one bit that acquires more bandwidth.

Biphase

- Biphase is an encoding scheme in which signal changes at the middle of the bit interval but does not return to zero.

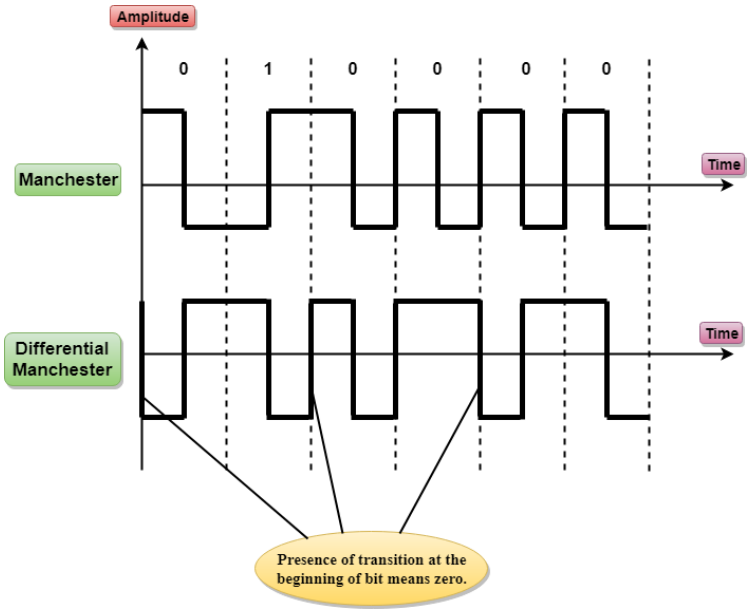
Biphase encoding is implemented in two different ways:

Manchester

- It changes the signal at the middle of the bit interval but does not return to zero for synchronization.
- In Manchester encoding, a negative-to-positive transition represents binary 1, and positive-to-negative transition represents 0.
- Manchester has the same level of synchronization as RZ scheme except that it has two levels of amplitude.

Differential Manchester

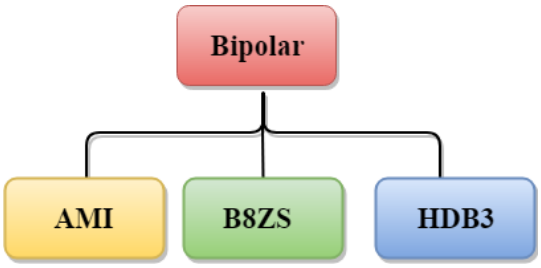
- It changes the signal at the middle of the bit interval for synchronization, but the presence or absence of the transition at the beginning of the interval determines the bit. A transition means binary 0 and no transition means binary 1.
- In Manchester Encoding scheme, two signal changes represent 0 and one signal change represent 1.



Bipolar

- Bipolar encoding scheme represents three voltage levels: positive, negative, and zero.
- In Bipolar encoding scheme, zero level represents binary 0, and binary 1 is represented by alternating positive and negative voltages.
- If the first 1 bit is represented by positive amplitude, then the second 1 bit is represented by negative voltage, third 1 bit is represented by the positive amplitude and so on. This alternation can also occur even when the 1bits are not consecutive.

Bipolar can be classified as:



AMI

- AMI stands for ***alternate mark inversion*** where mark work comes from telegraphy which means 1. So, it can be redefined as **alternate 1 inversion**.
- In Bipolar AMI encoding scheme, 0 bit is represented by zero level and 1 bit is represented by alternating positive and negative voltages.

Advantage:

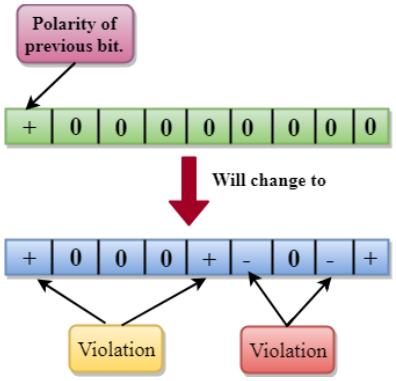
- DC component is zero.
- Sequence of 1s bits are synchronized.

Disadvantage:

- This encoding scheme does not ensure the synchronization of a long string of 0s bits.

B8ZS

- B8ZS stands for **Bipolar 8-Zero Substitution**.
- This technique is adopted in North America to provide synchronization of a long sequence of 0s bits.
- In most of the cases, the functionality of B8ZS is similar to the bipolar AMI, but the only difference is that it provides the synchronization when a long sequence of 0s bits occur.
- B8ZS ensures synchronization of a long string of 0s by providing force artificial signal changes called violations, within 0 string pattern.
- When eight 0 occurs, then B8ZS implements some changes in 0s string pattern based on the polarity of the previous 1 bit.
- If the polarity of the previous 1 bit is positive, the eight 0s will be encoded as zero, zero, zero, positive, negative, zero, negative, positive.

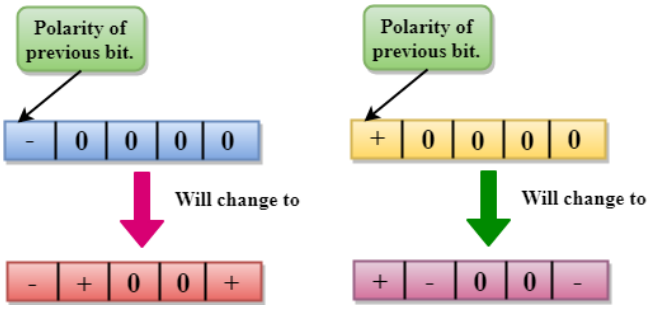


- If the polarity of previous 1 bit is negative, then the eight 0s will be encoded as zero, zero, zero, negative, positive, zero, positive, negative.

HDB3

- HDB3 stands for **High-Density Bipolar 3**.
- HDB3 technique was first adopted in Europe and Japan.
- HDB3 technique is designed to provide the synchronization of a long sequence of 0s bits.
- In the HDB3 technique, the pattern of violation is based on the polarity of the previous bit.
- When four 0s occur, HDB3 looks at the number of 1s bits occurred since the last substitution.
- If the number of 1s bits is odd, then the violation is made on the fourth consecutive of 0. If the polarity of the previous bit is positive, then the violation is positive. If the polarity of the previous bit is negative, then the violation is negative.

If the number of 1s bits since the last substitution is odd.



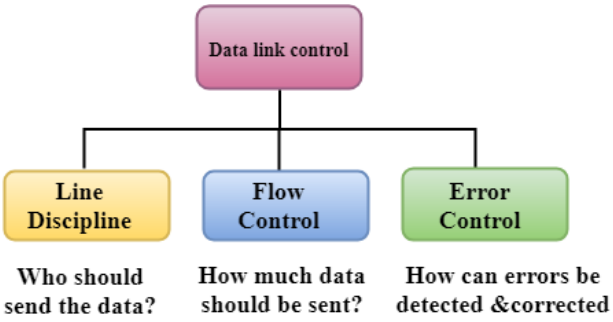
Data Link Layer

Data Link Controls

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control



Line Discipline

- Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

- ENQ/ACK
- Poll/select

END/ACK

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.

END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

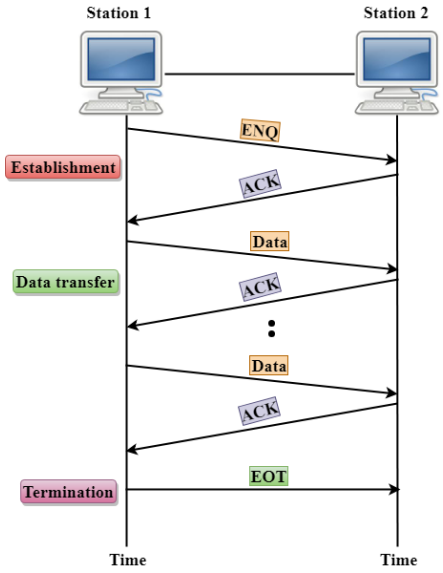
Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.
- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.



Poll/Select

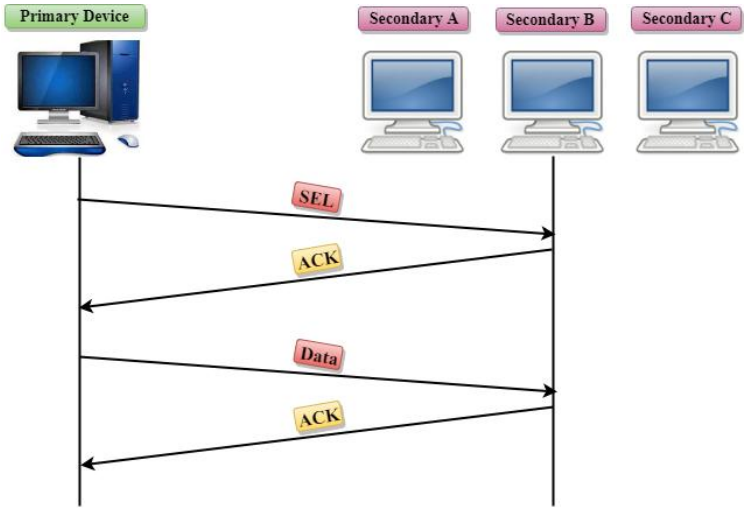
The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.
- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.
- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.
- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

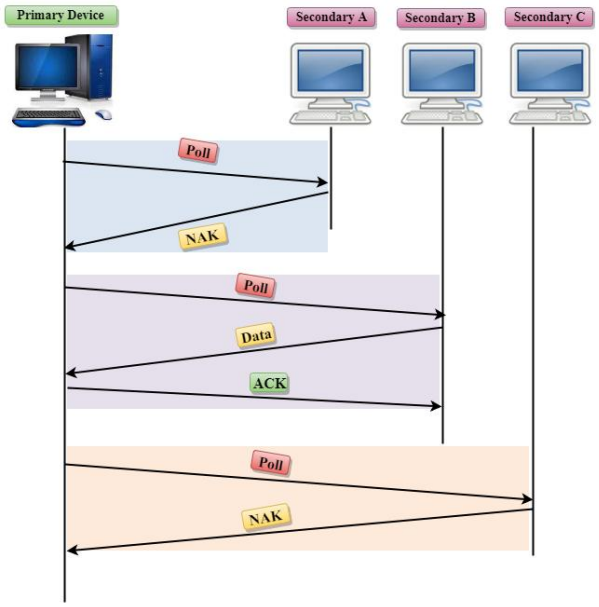
Select

- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.



Poll

- The Poll mode is used when the primary device wants to receive some data from the secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send.
- Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

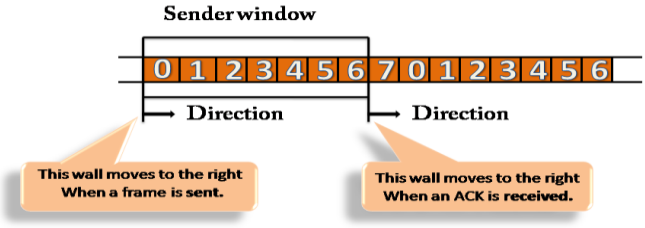
Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.
- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

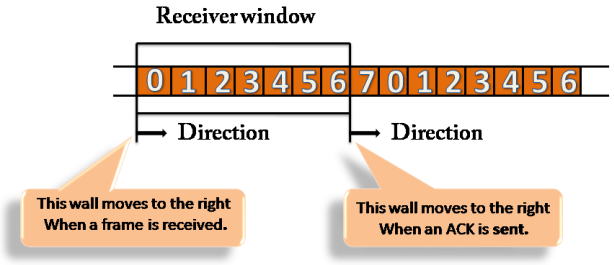
Sender Window

- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.
- For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).



Receiver Window

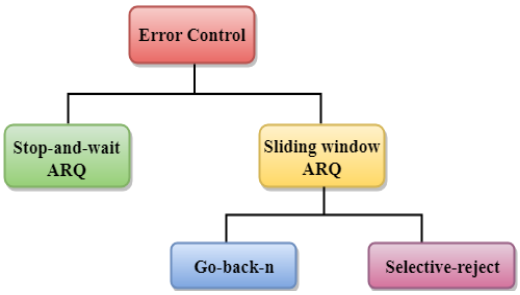
- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.



Error Control

Error Control is a technique of error detection and retransmission.

Categories of Error Control:



Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.
- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.
- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

Sliding Window ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

- In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
- The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that

represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.

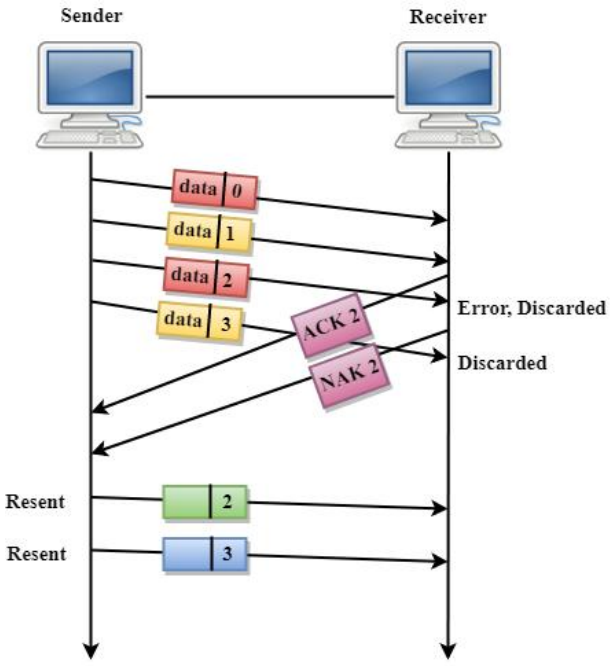
- The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

- **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

- **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame.



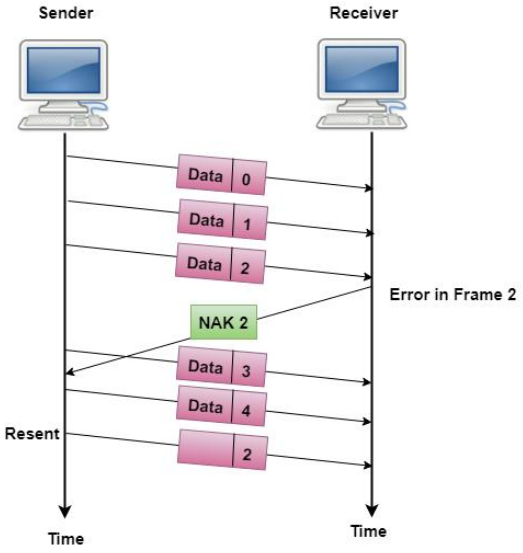
In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.
- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the

acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.



Network Layer

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

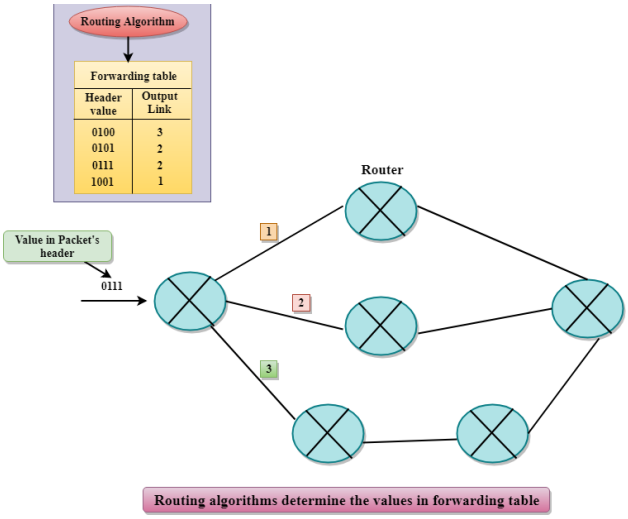
The main functions performed by the network layer are:

- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Forwarding & Routing

In Network layer, a router is used to forward the packets. Every router has a forwarding table. A router forwards a packet by examining a packet's header field and then using the header field value to index into the forwarding table. The value stored in the forwarding table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded.

For example, the router with a header field value of 0111 arrives at a router, and then router indexes this header value into the forwarding table that determines the output link interface is 2. The router forwards the packet to the interface 2. The routing algorithm determines the values that are inserted in the forwarding table. The routing algorithm can be centralized or decentralized.



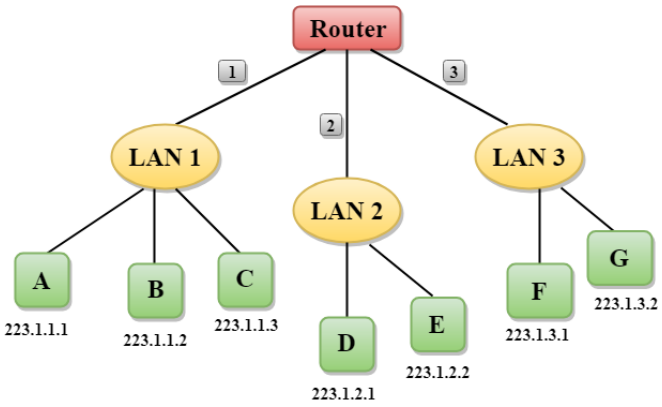
Services Provided by the Network Layer

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Network Addressing

- Network Addressing is one of the major responsibilities of the network layer.
- Network addresses are always logical, i.e., software-based addresses.
- A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
- A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
- Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

Let's understand through a simple example.



- In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
- Each host contains its own interface and IP address.
- All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.
- Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

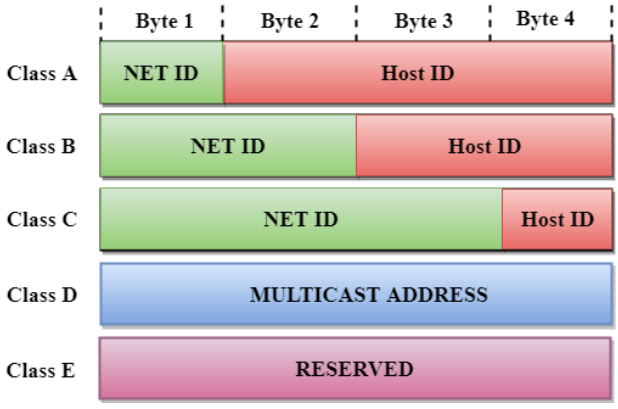
Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = 2^8 - 2 = 254 host address

Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.

Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.

Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

- The Host ID must be unique within any network.
- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

- The network ID cannot start with 127 as 127 is used by Class A.
- The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

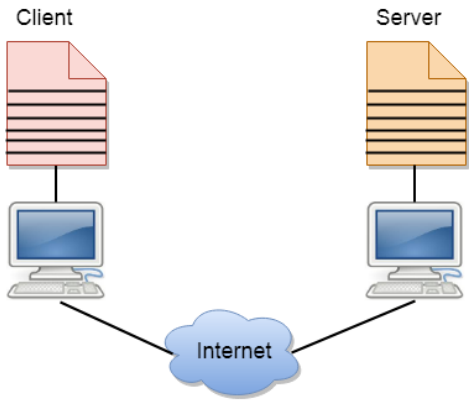
Classful Network Architecture

Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

Application Layer

Client and Server model

- A client and server networking model is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. This model is known as client-server networking model.
- The application programs using the client-server model should follow the given below strategies:



- An application program is known as a client program, running on the local machine that requests for a service from an application program known as a server program, running on the remote machine.
- A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.

- A server provides a service for many clients not just for a single client. Therefore, we can say that client-server follows the many-to-one relationship. Many clients can use the service of one server.
- Services are required frequently, and many users have a specific client-server application program. For example, the client-server application program allows the user to access the files, send e-mail, and so on. If the services are more customized, then we should have one generic application program that allows the user to access the services available on the remote computer.

Client

A client is a program that runs on the local machine requesting service from the server. A client program is a finite program means that the service started by the user and terminates when the service is completed.

Server

A server is a program that runs on the remote machine providing services to the clients. When the client requests for a service, then the server opens the door for the incoming requests, but it never initiates the service.

A server program is an infinite program means that when it starts, it runs infinitely unless the problem arises. The server waits for the incoming requests from the clients. When the request arrives at the server, then it responds to the request.

Advantages of Client-server networks:

- **Centralized:** Centralized back-up is possible in client-server networks, i.e., all the data is stored in a server.
- **Security:** These networks are more secure as all the shared resources are centrally administered.
- **Performance:** The use of the dedicated server increases the speed of sharing resources. This increases the performance of the overall system.
- **Scalability:** We can increase the number of clients and servers separately, i.e., the new element can be added, or we can add a new node in a network at any time.

Disadvantages of Client-Server network:

- **Traffic Congestion** is a big problem in Client/Server networks. When a large number of clients send requests to the same server may cause the problem of Traffic congestion.
- It does not have a robustness of a network, i.e., when the server is down, then the client requests cannot be met.
- A client/server network is very decisive. Sometimes, regular computer hardware does not serve a certain number of clients. In such situations, specific hardware is required at the server side to complete the work.
- Sometimes the resources exist in the server but may not exist in the client. For example, If the application is web, then we cannot take the print out directly on printers without taking out the print view window on the web.

UNIT-3: TCP/IP Addressing

TCP/IP Reference Model (Internet Protocol Stack layers)

- Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide.
- TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all.
- TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.
- The TCP/IP model has five layers.
    1. Application Layer
    2. Transport Layer
    3. Internet Layer
    4. Data Link Layer
    5. Physical Network

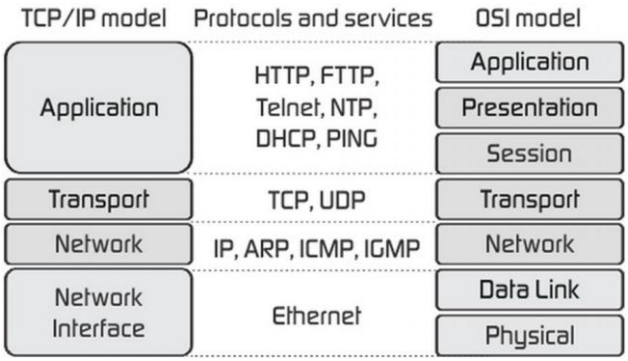


Figure 16: TCP/IP Reference Model

As we can see from the above figure, presentation and session layers are not there in TCP/IP model. Also note that the Network Access Layer in TCP/IP model combines the functions of Data link Layer and Physical Layer.

Application Layer

- Application layer is the top most layer of four layer TCP/IP model.
- Application layer is present on the top of the Transport layer.
- Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.
- Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Transport Layer

- The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation.
- Transport layer defines the level of service and status of the connection used when transporting data.
- The transport layer provides the end-to-end data transfer by delivering data from

an application to its remote peer.

- The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides:
  - Reliable delivery data
  - Duplicate data suppression
  - Flow control Congestion control

- Another transport layer protocol is the User Datagram Protocol (UDP), which provides:
  - Connectionless
  - Unreliable
- UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.
  - Best-effort service

Network Layer (Internet Layer)

- The internet layer also called the network layer.
- Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks.
- The Internet layer is also responsible for routing of IP datagrams.
- Internet Protocol (IP) is the most important protocol in this layer.
- It is a connectionless protocol that does not assume reliability from lower layers. IP does not provide reliability, flow control or error recovery.
- IP provides a routing function that attempts to deliver transmitted messages to their destination.
- These message units in an IP network are called an IP datagram.
- Example: IP, ICMP, IGMP, ARP, and RARP.

Network Interface Layer (Network Access Layer)

- Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signalled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.
- The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

OSI(Open System Interconnection)	TCP/IP (Transmission Control Protocol/ Internet Protocol)
OSI provides layer functioning and also defines functions of all the layers.	TCP/IP model is more based on protocols and protocols are not flexible with other layers.
In OSI model the transport layer guarantees the delivery of packets	In TCP/IP model the transport layer does not guarantees delivery of packets.
Follows horizontal approach	Follows vertical approach.
OSI model has a separate presentation layer	TCP/IP doesn't have a separate presentation layer
OSI is a general model.	TCP/IP model cannot be used in any other application
Network layer of OSI model provide both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
OSI model has a problem of fitting the protocols in the model	TCP/IP model does not fit any protocol
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	In TCP/IP it is not clearly separated its services, interfaces and protocols.
It has 7 layers	It has 4 layers

Understanding of Delay, Loss and Throughput in the Packet Switching Network

Basics

- Recall that a packet starts in a host (the source), passes through a series of routers, and ends its journey in another host (the destination).
- As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several types of delays at each node along the path.
- The most important of these delays are the
    - Nodal processing delay
    - Queuing delay
    - Transmission delay
    - Propagation delay
- Together, these delays accumulate to give a total nodal delay.
- The performance of many Internet applications—such as search, Web browsing, email, maps, instant messaging, and voice-over-IP—are greatly affected by network delays.

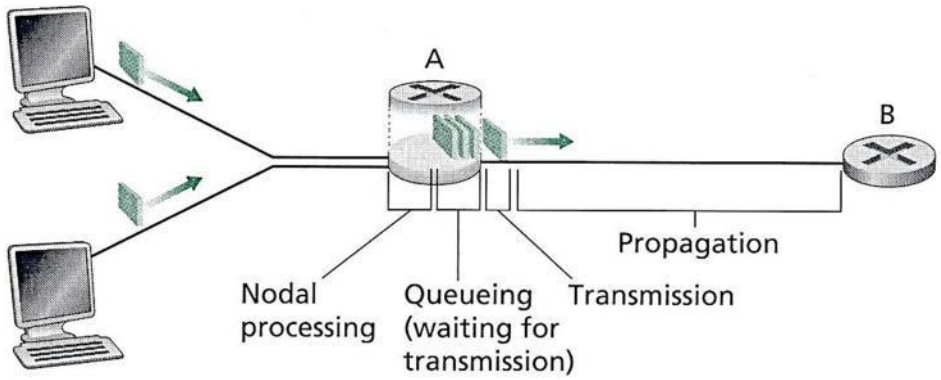


Figure 17: Delay in Packet Switched Network

Processing Delay

- The time required to examine the packet's header and determine where to direct the packet is part of the processing delay.
- The processing delay can also include other factors, such as the time needed to check for bit- level errors in the packet that occurred in transmitting the packet's bits from the upstream node to router.

 It is typically on the order of microseconds or less.

Queuing Delay

- At the queue, the packet experiences a queuing delay as it waits to be transmitted onto the link.
- The length of the queuing delay of a specific packet will depend on the number of earlier- arriving packets that are queued and waiting for transmission onto the link.
- If the queue is empty and no other packet is currently being transmitted, then our packet's queuing delay will be zero.
- On the other hand, if the traffic is heavy and many other packets are also waiting to be transmitted, the queuing delay will be long.

 Queuing delays can be on the order of microseconds to milliseconds in practice.

Transmission Delay

- Assuming that packets are transmitted in a first-come-first-served manner like packet-switched networks.
- Now packet can be transmitted only after all the packets that have arrived before it have been transmitted.
- Denote the length of the packet by L bits, and denote the transmission rate of the link from router to router by R bits/sec.
- The transmission delay is L/R.
- Transmission delays are typically on the order of microseconds to milliseconds in practice.

Propagation Delay

- Once a bit is pushed into the link, it needs to propagate to router B. The time required to propagate from the beginning of the link to router B is the propagation delay.
- The bit propagates at the propagation speed of the link.
- The propagation speed depends on the physical medium of the link.
- Propagation delays are on the order of milliseconds.
- Propagations delay=d (Length of Physical Link) /s (Propagation speed in medium).

Packet Loss

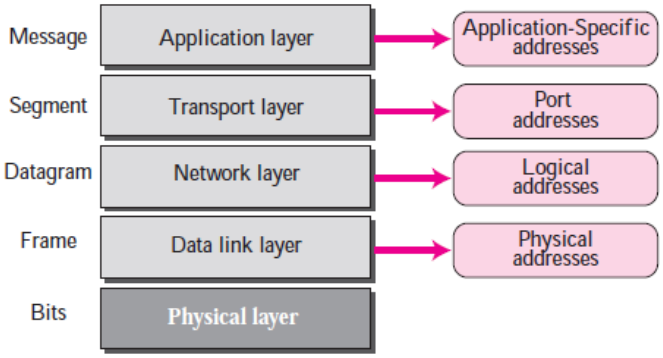
- Packet loss is the failure of one or more transmitted packets to arrive at their destination.
- This event can cause noticeable effects in all types of digital communications.
- The loss of data packets depends on the switch queue. The loss of data packets increases with the increases in the traffic intensity.
- It affects the performance of the network.

Throughput

- Throughput or Network Throughput is the rate of successful message delivery over a communication channel.
- The data these messages belong to may be delivered over a physical or logical link or it can pass through a certain network node.
- Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.

Addresses used in the TCP/IP protocol.

Four levels of addresses are used in the TCP/IP protocol: **physical address, logical address, port address, and application-specific address** as shown in Figure.



Physical Addresses

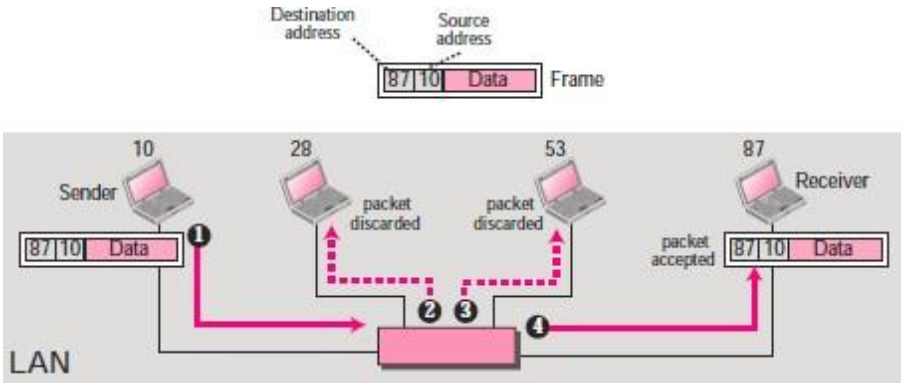
- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address.
- Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network.
- Example: Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below: A 6-byte (12 hexadecimal digits) physical address **07:01:02:01:2C:4B**

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

Example (1)

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

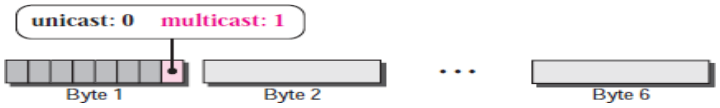
Note that in most data link protocols, the destination address 87 in this case, comes before the source address (10 in this case). The frame is propagated through the LAN. Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its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



Unicast, Multicast, and Broadcast Physical Addresses

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

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



Q: Define the type of the following destination addresses:

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

Logical Addresses

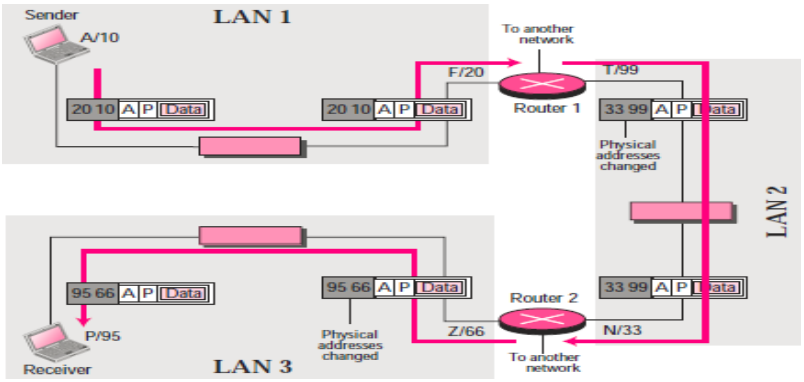
- Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. An internet address in IPv4 in decimal numbers **132.24.75.9**
- No two publicly addressed and visible hosts on the Internet can have the same IP address.
- The physical addresses will change from hop to hop, but the logical addresses remain the same.
- The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network). There are limitations on broadcast addresses.

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

Example (2)

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

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



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

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

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

Unicast, Multicast, and Broadcast Addresses

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

Port Addresses

- There are many application running on the computer. Each application run with a port no.(logically) on the computer.
- A port number is part of the addressing information used to identify the senders and receivers of messages.
- Port numbers are most commonly used with TCP/IP connections.
- These port numbers allow different applications on the same computer to share network resources simultaneously.
- The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.
- Example: a port address is a 16-bit address represented by one decimal number **753**

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

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

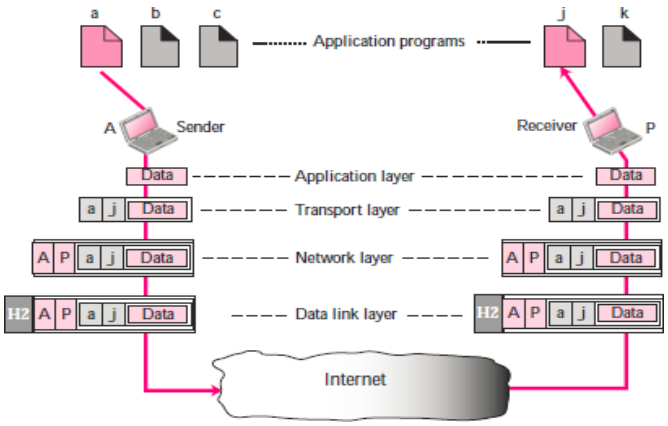
A port address is a 16-bit address represented by one decimal number as shown.

753

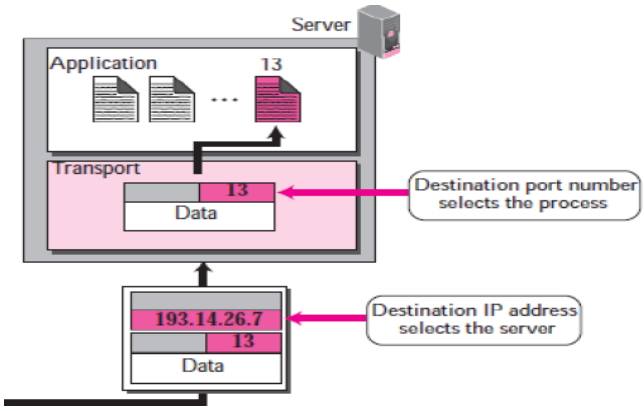
A 16-bit port address represented as one single number

Example (3)

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



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



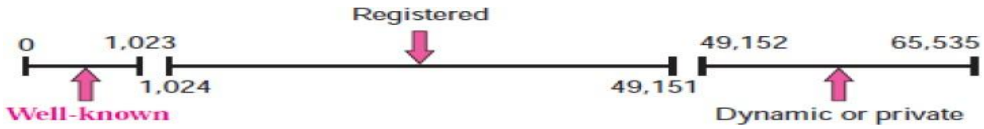
- In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535.
- The client program defines itself with a port number, called the **ephemeral port number**

(chosen randomly). The word ephemeral means *short lived*.

- The server process must also define itself with a port number (called well-known port numbers). This port number, however, cannot be chosen randomly.

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

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



- **Well-known ports:** The ports ranging from 0 to 1,023 are assigned and controlled by ICANN..
- **Registered ports:** The ports ranging from 1,024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.

Dynamic ports: The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers. The original recommendation was that the ephemeral port numbers for clients be chosen from this

range. However, most systems do not follow this recommendation.

Application-Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific application.
- Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.

Network Addressing

- Network Addressing is one of the major responsibilities of the network layer.
- Network addresses are always logical, i.e., software-based addresses.
- A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
- A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
- Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

TCP/IP Addressing Scheme:

TCP/IP uses a 32 bit addressing scheme to identify the devices on a network. These 32 bits are divided into four octets, of eight bits each. Each of these four octets is represented in a decimal form, and separated by a dot. For example, 198.172.168.10 is an IP address. This format of representing IP address is called the dotted decimal format.

The octets in an IP address can take a decimal value from 9 to 255 because the largest decimal value that can be represented by eight binary bits is 255(11111111 in binary). For example, the 32 bit binary address 11000110.10101100.1010100.0001010 represents the IP address 198.172.168.10.

The addressing provided by a network layer protocol to a device is called its network address. For example, 198.172.168.10 is the network address of a device. This is different from the MAC address which is the hardware address of the NIC or the device (routers or switch). The network addresses in a TCP/IP network are also known as IP addresses. Therefore, 198.172.168.10 is also known as the IP address.

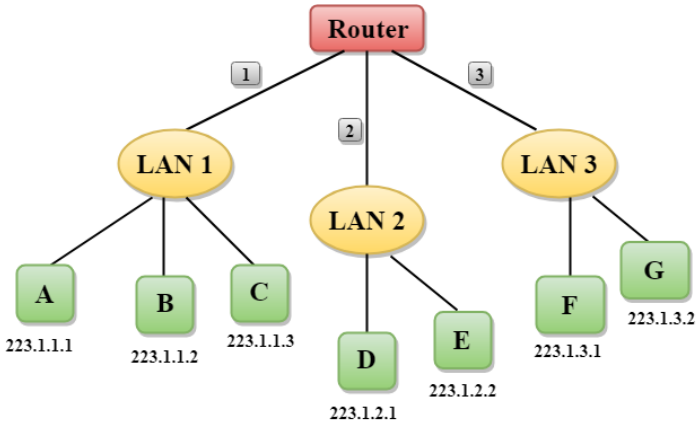
Components of IP address:

For continence sake we use IP address dotted-decimal notation, while the computer converts this into binary. However, even though these sets of 32 bits are considered a single "entity", they have an internal structure containing two components:

§ **Network Identifier (Network ID):** A certain number of bits, starting from the left-most bit, is used to identify the network where the host or other network interface is located. This is also sometimes called the network prefix or even just the prefix. **This is the address of the network itself, and is used by other networks to identify this network.**

§ **Host Identifier (Host ID):** The remainder of the bits is used to identify the host on the network. This is the address of the device with in the network.

The fundamental division of the bits of an IP address is into a network ID and host ID. Here, the network ID is 8 bits long and the host ID is 24 bits in length.



- In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
- Each host contains its own interface and IP address.
- All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.
- Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

Classful Addressing

IP Address Classes:

Internet addresses are allocated by the InterNIC the organization that administers the internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of class A, B and C Internet addresses, each with an example address:

· Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.

· Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as

their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

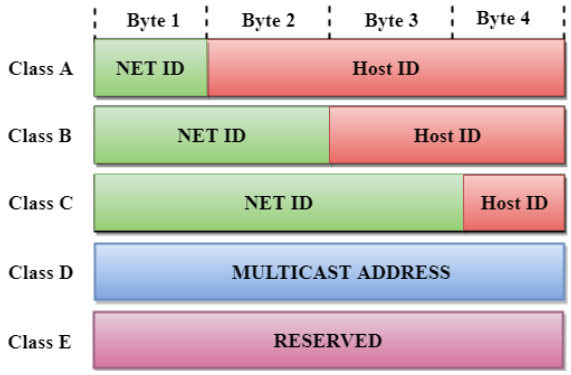
· Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

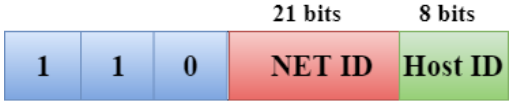
In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.
The total number of networks in Class B = 2^{14} = 16384 network address
The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.
The total number of networks = 2^{21} = 2097152 network address
The total number of hosts = 2^{8} - 2 = 254 host address



Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.

Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.

Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

- The Host ID must be unique within any network.
- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

- The network ID cannot start with 127 as 127 is used by Class A.
- The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Classful Network Architecture

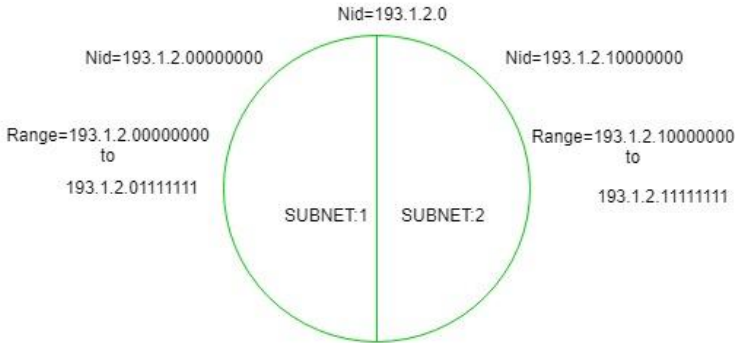
Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

Introduction To Subnetting

When a bigger network is divided into smaller networks, in order to maintain security, then

that is known as Subnetting. so, maintenance is easier for smaller networks.

Now, let's talk about dividing a network into two parts:
so to divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



IP Subnetting:

Subnets are an efficient method for logically dividing a network into segments, such that the network performance is optimized. Subnets are defined as the segments of a network that use schemes different from one another but corresponding to the addressing schemes different from one another but corresponding to the addressing scheme used by the main network. Therefore, devices in one subnet cannot directly communicate with devices represented by 192.168.30.0, in which 192.168.30 represents the network address, and the value in the fourth octet would represent the host on the network. For example, the address of a particular host in this network would be 192.168.30.4. The fourth octet in a Class C address can take a value between 0 and 225, and therefore, this network can have up to 256 hosts. However, configuring 255 components in a single network would significantly degrade the performance of the network as well as the network router. Therefore, the network, 192.168.30.x can be divided into subnets, with each subnet consisting of, say, 16 computers.

On a network without subnets, a device outside the network can identify a host eith the help of the network and host addresses. On a network with subnets, however, an additional piece of information, called the subnet mask, is needed to identify a host. The network address helps determine the network in which is located, whereas the subnet mask responsible for locating the subnet on the network to which the host belongs. The host address identifies the individual host.

However, the addressing scheme used by IP has only four octets that can be used to represent the network address or the host depending on the IP address class. It is not possible to include information on the subnet in the IP address itself, and therefore, the subnet mask is a separate 32bit address, accompanying the IP address of a device.

The default subnet mask values for a class A, class B, class C IP addresses are listed in Table.

IP Address Class	Default Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

The default subnet masks are used when a network does not have any subnets. For creating subnets, the default values are modified to obtain customized, only the octets that denote the host address are modified, and not the octet(s) that represent the network address. For example 255.244.0.0 is a valid subnet mask for a class A network but not 252.124.0.0 in fact, 252.124.0.0 is not a valid subnet mask for a network of any IP address class.

The subnet masks and IP addresses on the network are dependent on one another because of network that belongs to a particular IP addresses class can accommodate only a particular number of devices irrespective of the number of subnets. For example, a class B network can have a maximum of only 65,536 devices irrespective of the number subnets that are created. Therefore, the subnet mask values are derived from the IP address of the network. Fig. 6.19, represents divided to depict the subnet address.

As represented in Fig.6.19, the bits of the octet (s) representing the host address are subdivided to represent the subnet address and the host address. For example, In class C IP address, the bits of the last octet represent the subnet address as well as the host address. The number of bits used by the subnet address, and the number of bits used by the host address are determined by the subnet mask. The following sub-topic explains the steps involved in creating subnets.

Supernetting in Network Layer

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.
Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically,

- When multiple networks are combined to form a bigger network, it is termed as super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

There are some points which should be kept in mind while supernetting:

1. All the Networks should be contiguous.
2. The block size of every networks should be equal and must be in form of 2^n.
3. First Network id should be exactly divisible by whole size of supernet.

Example – Suppose 4 small networks of class C:

200.1.0.0,

200.1.1.0,

200.1.2.0,

200.1.3.0

Build a bigger network which have a single Network Id.

Explanation – Before Supernetting routing table will be look like as:

NETWORK ID	SUBNET MASK	INTERFACE
200.1.0.0	255.255.255.0	A

NETWORK ID	SUBNET MASK	INTERFACE
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C
200.1.3.0	255.255.255.0	D

First, lets check whether three condition are satisfied or not:

1. **Contiguous:** You can easily see that all network are contiguous all having size 256 hosts.
   Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all network are contiguous.
2. **Equal size of all network:** As all networks are of class C, so all of the have a size of 256 which in turn equal to 2^8.
3. **First IP address exactly divisible by total size:** When a binary number is divided by 2^n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Supernet Network. You can check that if last n v=bits are 0 or not.
   In given example first IP is 200.1.0.0 and whole size of supernet is $4*2^8 = 2^{10}$. If last 10 bits of first IP address are zero then IP will be divisible.

11001000	00000001	00000000	00000000
200	1	0	0

   Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Therefore, you can join all these 4 networks and can make a Supernet. New Supernet Id will be 200.1.0.0.

Advantages of Supernetting –

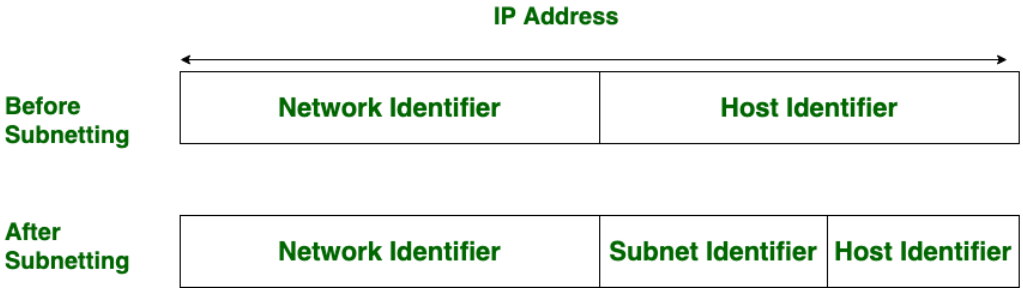
1. Control and reduce network traffic
2. Helpful to solve the problem of lacking IP addresses
3. Minimizes the routing table

Disadvantages of Supernetting –

- It cannot cover different area of network when combined
- All the networks should be in same class and all IP should be contiguous

Difference between Subnetting and Supernetting

Subnetting:
Subnetting is the procedure to divide the network into sub-networks or small networks.
Supernetting:
Supernetting is the procedure of combine the small networks into larger space. In subnetting, Network addresses's bits are increased. on the other hand, in subnetting, Host addresses's bits are increased. Subnetting is implemented via Variable-length subnet masking, While supernetting is implemented via Classless interdomain routing.



Difference between Subnetting and Supernetting:

S.NO	SUBNETTING	SUPERNETTING
1.	Subnetting is the procedure to divide the network into sub-networks.	While supernetting is the procedure of combine the small networks.
2.	In subnetting, Network addresses's bits are increased.	While in subnetting, Host addresses's bits are increased.
3.	In subnetting, The mask bits are moved towards right.	While In supernetting, The mask bits are moved towards left.
4.	Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
5.	In subnetting, Address depletion is reduced or removed.	While It is used for simplify routing process.

Loopback

A loopback test is the process of sending digital data streams from a source back to the same point without any intentional modifications. It's generally performed to determine whether a device works properly and whether there are failing nodes in a network.

Loopback testing is a diagnostic procedure in which a signal is transmitted and returned back to the same sending device after passing through all or a portion of a network to test transportation or transportation infrastructure. A comparison of the returned signal with the transmitted signal conveys the integrity of the transmission path. A loop plug, called a wrap plug, is inserted into the port of a communication device to facilitate the loopback test. Loopback tests can readily be used to test computer serial ports and radio interfaces, and are one of the easiest ways to verify RS-232 communications. Interfaces such as aggregated Ethernet, gigabit Ethernet, fast Ethernet, etc. can also be configured to execute a loopback test to verify circuit connectivity. The loopback test isolates circuit segments so that they can be tested separately.

IPv4 datagram format

The Internet Protocol version 4 (**IPv4**) is a protocol for use on packet-switched Link Layer networks (e.g. Ethernet). **IPv4** provides an addressing capability of approximately 4.3 billion addresses.

- **Version number**: These 4 bits specify the IP protocol version of the datagram. It determines how to interpret the header. Currently the only permitted values are 4 (0100) or 6 (0110).
- **Header length:** Specifies the length of the IP header, in 32-bit words.
- **Type of service:** The type of service (TOS) bits were included in the IPv4 header to allow different types of IP datagrams (for example, datagrams particularly requiring low delay, high throughput, or reliability) to be distinguished from each other.
- **Datagram length:** This is the total length of the IP datagram (header plus data), measured in bytes.
- **Identifier:** Uniquely identifies the datagram. It is incremented by 1 each time a datagram is sent. All fragments of a datagram contain the same identification value. This allows the destination host to determine which fragment belongs to which datagram.
- **Flags:** In order for the destination host to be absolutely sure it has received the last fragment of the original datagram, the last fragment has a flag bit set to 0, whereas all the other fragments have this flag bit set to 1.
- **Fragmentation offset:** When fragmentation of a message occurs, this field specifies the offset, or position, in the overall message where the data in this fragment goes. It is specified in units of 8 bytes (64 bits).

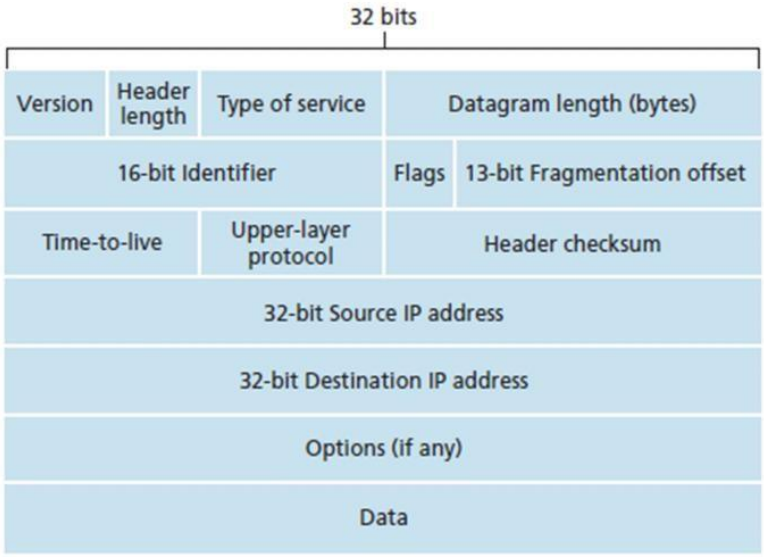


Fig. 7 IPv4 datagram format

- **Time-to-live:** Specifies how long the datagram is allowed to "live" on the network. Each router decrements the value of the TTL field (reduces it by one) prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.
- **Protocol***:* This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport-layer protocol to which the data portion of this IP datagram should be passed. For example, a value of 6 indicates that the data portion is passed to TCP, while a value of 17 indicates that the data is passed to UDP.
- **Header checksum:** The header checksum aids a router in detecting bit errors in a received IP datagram.

- **Source and destination IP addresses:** When a source creates a datagram, it inserts its IP address into the source IP address field and inserts the address of the ultimate destination into the destination IP address field.
- **Options:** The options fields allow an IP header to be extended.
- **Data (payload):** The data to be transmitted in the datagram, either an entire higher-layer message or a fragment of one.

IP addressing: introduction

- **IP address:** It is 32-bit identifier for host, router interface
- **Interface:** It is a connection between host/router and physical link.
  - A router's typically have multiple interfaces
  - A host typically has one or two interfaces
- There is an IP addresses associated with each interface.
- **Subnets:** To determine the subnets, detach each interface from its host or router, creating islands of isolated networks, with interfaces terminating the end points of the isolated networks. Each of these isolated networks is called a subnet.
- **Subnet part**: high order bits defines subnet
- **Host part:** low order bits defines host.

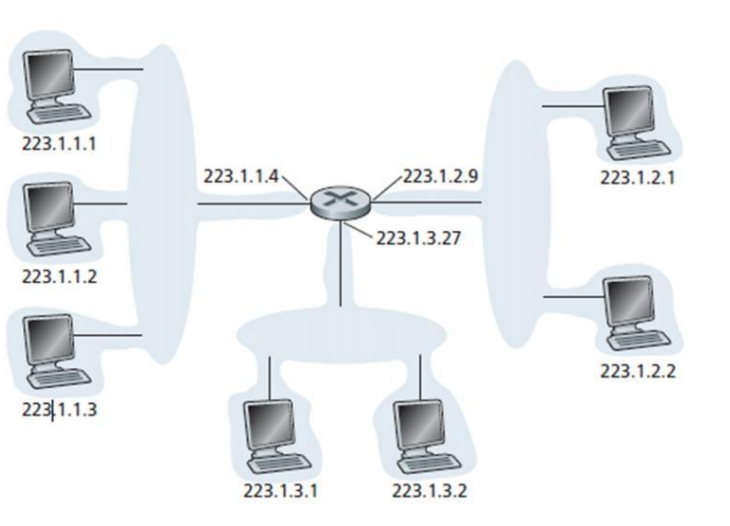


Fig. 8 Interface addresses and subnets

IPv6 Datagram Format

The Internet Protocol version 6 (**IPv6**) is more advanced and has better features compared to **IPv4**.

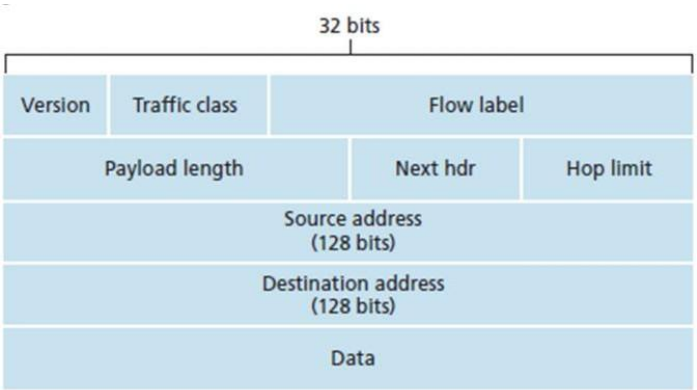


Fig. 12 IPv6 datagram format

- **Version:** The size of the Version field is 4 bits. The Version field shows the version of IP and is set to 6.
- **Traffic Class**: The size of Traffic Class field is 8 bits. Traffic Class field is similar to the IPv4 Type of Service (ToS) field. The Traffic Class field indicates the IPv6 packet's class or priority.
- **Flow Label**: The size of Flow Label field is 20 bits. The Flow Label field provide additional support for real-time datagram delivery and quality of service features. The purpose of Flow Label field is to indicate that this packet belongs to a specific sequence of packets between a source and destination and can be used to prioritized delivery of packets for services like voice.
- **Payload Length**: The size of the Payload Length field is 16 bits. The Payload Length field shows the length of the IPv6 payload, including the extension headers and the upper layer protocol data
- **Next Header**: The size of the Next Header field is 8 bits. The Next Header field shows either the type of the first extension (if any extension header is available) or the protocol in the upper layer such as TCP, UDP, or ICMPv6.
- **Hop Limit**: The size of the Hop Limit field is 8 bits The Hop Limit field shows the maximum number of routers the IPv6 packet can travel. This Hop Limit field is similar to IPv4 Time to Live (TTL) field.
- **Source Address:** The size of the Source Address field is 128 bits. The Source Address field shows the IPv6 address of the source of the packet.
- **Destination Address:** The size of the Destination Address field is 128 bits. The Destination Address field shows the IPv6 address of the destination of the packet.
- **Data:** The data to be transmitted in the datagram, either an entire higher-layer message or a fragment of one.

Difference between IPv4 and IPv6

IPv4	IPv6
• IPv4 addresses are 32 bit length.	• IPv6 addresses are 128 bit length.
• Fragmentation done by sender is forwarding and routers.	• Fragmentation is done only by sender.
• No packet flow identification.	• Packet flow identification is available within the IPv6 header using the Flow Label field.
• Checksum field is available in header	• No checksum field in header.
• Options fields are available in header.	• No option fields, but Extension headers are available.
• Address Resolution Protocol (ARP)is available to map IPv4 addresses to MAC addresses.	• Address Resolution Protocol (ARP) is replaced with Neighbour Discovery Protocol.
• Broadcast messages are available.	• Broadcast messages are not available.
• Manual configuration (Static) of IP addresses or DHCP (Dynamic configuration) is required to configure IP addresses.	• Auto-configuration of addresses is available.

UNIT-4: Network Architecture

A **Computer Architecture** is a design in which all computers in a computer network are organized. A architecture defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc. The two most popular computer architectures are **P2P (Peer to Peer)** and **Client-Server architecture**.

Ethernet

Computer networking has become an integral part of business today. Individuals, professionals and academics have also learned to rely on computer networks for capabilities such as electronic mail and access to remote databases for research and communication purposes. Networking has thus become an increasingly pervasive, worldwide reality because it is fast, efficient, reliable and effective. Just how all this information is transmitted, stored, categorized and accessed remains a mystery to the average computer user.

Over the years, the Ethernet standard has developed to meet the ongoing requirements of the industry. It has grown to reflect the changing approaches of the IT industry, enabling it to provide connectivity for local area networks and metropolitan area networks.

Today, there are many Ethernet standards, and looking at their development over the years, it is possible to see how the standard has moved with the times, increasing speeds and introducing more capabilities.

As a result, today, Ethernet is used for everything from use within large scale networks where Ethernet switches, routers and other items are used to the smaller home and business local area networks where items like Ethernet switches, Ethernet routers, computers, printers and many other items use Ethernet. As Ethernet has been standardized.

Evolution of Ethernet

Xerox Corporation usually receives credit for inventing Ethernet. However, Xerox actually acquired the original technology (then known as Aloha Net) in the 1970s from the University of Hawaii. Xerox then joined with DEC and Intel to develop the earliest Ethernet standard, called Version 1, which it released in 1980. The three companies released a follow-up standard, Ethernet Version 2, in 1982.

In the mid-1980s, the IEEE 802 committee adopted Ethernet as the 802.3 standard. All current and future development on Ethernet technologies ostensibly builds on this base standard.

Since its inception, Ethernet has become the most popular LAN standard used throughout the world.

Is Ether net a Protocol?

First on the list **is Ethernet**. **Ethernet** is one of the most common **protocols** used today for communications between systems and operates at the first two levels of the OSI model (physical and data link).

IEEE specifies in the family of standards called IEEE 802.3 that the Ethernet protocol touches both Layer 1 (**physical layer**) and Layer 2 (**data link layer**) on the Open Systems Interconnection (**OSI**) network protocol model. Ethernet defines two units of transmission: packet and frame.

Are LAN and Ethernet Same?

LAN stands for Local Area Network. **Ethernet** is a type of network used extensively for setting up **LAN**. **LAN** port means your Local Area Network port which invariably ends up being an **Ethernet** port. So for all practical purpose **LAN** port is the **same** as **Ethernet** port.

Standard Ethernet Code

In order to understand standard Ethernet code, one must understand what each digit means. Following is a guide:

Guide to Ethernet Coding

10	at the beginning means the network operates at 10Mbps.
BASE	means the type of signaling used is baseband.
2 or 5	at the end indicates the maximum cable length in meters.
T	the end stands for twisted-pair cable.
X	at the end stands for full duplex-capable cable.
FL	at the end stands for fiber optic cable.

For example: *100BASE-TX indicates a Fast Ethernet connection (100 Mbps) that uses a twisted pair cable capable of full-duplex transmissions.*

The major difference between **Ethernet** and **LAN** is that the working of **Ethernet** is not centralized while **LAN** functions in a centralized manner.

...

Comparison Chart.

Basis for comparison	Ethernet	LAN
Transmission media	Only wired	Wired as well as wireless.
Reliability	Low	High

Base Band and Broad Band Ethernet

Common **Ethernet** Standards use **Baseband** for LAN data transfer. **Broadband** is used for long distance data transfer. Entire bandwidth of the cable is used for multiple signal transmission at different frequencies. Home Internet connection and TV cables use **broadband** for data transfer.

- **Baseband** refers to the original frequency range of a transmission signal before it is converted, or modulated, to a different frequency range. ... A common example is the **Ethernet** protocol, which transfers data using the original **baseband** signal.
- A signal at **baseband** is often used to modulate a higher frequency carrier signal in order that it may be transmitted via radio. Modulation results in shifting the signal up to much higher frequencies (radio frequencies, or RF) than it originally spanned. **Broadband** is the name given to a permanent internet connection that brings an internet signal to and from a device through a telephone line.

How Base band Work

A **chip** in a smartphone or tablet that handles the cellular transmission.
The **baseband processor** converts the data to a signal that can be used to modulate the carrier frequency for transmission and vice versa. That signal is handed off to the RF **processor**, which may also be part of the **baseband chip**.

ETHERNET Standards: Introduction

An important part of designing and installing an Ethernet is selecting the appropriate Ethernet medium. There are four major types of media in use today: Thickwire for 10BASE5 networks; thin coax for 10BASE2 networks; unshielded twisted pair (UTP) for 10BASE-T networks; and fiber optic for 10BASE-FL or Fiber-Optic Inter-Repeater Link (FOIRL) networks. This wide variety of media reflects the evolution of Ethernet and also points to the technology's flexibility. Thickwire was one of the first cabling systems used in Ethernet, but it was expensive and difficult to use. This evolved to thin coax, which is easier to work with and less expensive. It is important to note that each type of Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, has its own preferred media types.

For specialized applications, fiber-optic, or 10BASE-FL, Ethernet segments are popular. Fiber-optic cable is more expensive, but it is invaluable in situations where electronic emissions and environmental hazards are a concern. Fiber-optic cable is often used in inter-building applications to insulate networking equipment from electrical damage caused by lightning. Because it does not conduct electricity, fiber-optic cable can also be useful in areas where heavy electromagnetic interference is present, such as

on a factory floor. The Ethernet standard allows for fiber-optic cable segments up to two kilometers long, making fiber-optic Ethernet perfect for connecting nodes and buildings that are otherwise not reachable with copper media. When household internet first started it used a dial-up connection and the technology didn't allow for the same speeds we commonly enjoy today.

Cable Grade Capabilities

Cable Name	Makeup	Frequency Support	Data Rate	Network Compatibility
Cat-5	4 twisted pairs of copper wire — terminated by RJ45 connectors	100 MHz	Up to 1000Mbps	ATM, Token Ring,1000Base-T, 100Base-TX, 10Base-T
Cat-5e	4 twisted pairs of copper wire — terminated by RJ45 connectors	100 MHz	Up to 1000Mbps	10Base-T, 100Base-TX, 1000Base-T
Cat-6	4 twisted pairs of copper wire — terminated by RJ45 connectors	250 MHz	1000Mbps	10Base-T, 100Base-TX, 1000Base-T

Broadband refers to various high-capacity **transmission** technologies that are used to **transmit** data, voice, and video across long distances and at high speeds. Common mediums of **transmission** include coaxial cable, fiber optic cable, and radio waves.

Important Points:

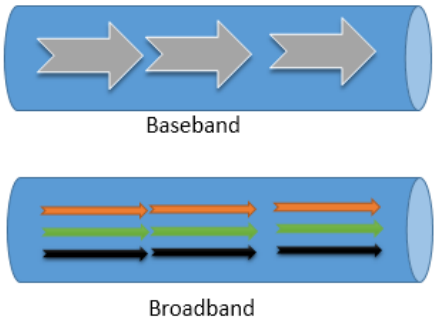
- **Ethernet** cable and **broadband** are not the **same**. **Ethernet** cable is used to connect computers, printers, routers, switches and other devices on a local-area network (LAN). ... **Broadband** refers to a number of technologies used to provide fast Internet access to residences and businesses.
- Whereas baseband uses **digital** signaling, **broadband** uses **analog** signals in the form of optical or electromagnetic waves over multiple transmission frequencies. For signals to be both sent and received, the transmission media must be split into two channels.

Differences between Baseband and Broadband Explained

This tutorial explains the differences between the baseband and broadband transmissions in detail. Learn what the baseband and broadband transmissions are and how they differ from each other.

Both baseband and broadband describe how data is transmitted between two nodes. Baseband technology transmits a single data signal/stream/channel at a time while broadband technology transmits multiple data signals/streams/channels simultaneously at the same time.

The following image shows an example of both technologies.



To understand the basic differences between both technologies, consider the baseband as a railway track and the broadband as a highway. Like, at a time, only one train can go on a railway track, in the baseband transmission only one data signal can be transmitted at a time.

Unlike a railway track on a highway, multiple vehicles can go simultaneously. For example, on a 3 lanes highway, 3 vehicles can go at the same time. Same as a highway, in the broadband transmission, multiple data signals can be transmitted at the same time.

Technical differences between the baseband and broadband transmissions

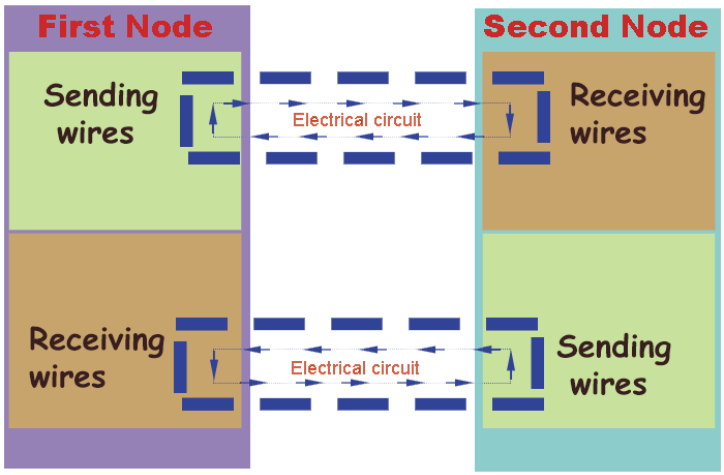
Baseband technology uses digital signals in data transmission. It sends binary values directly as pulses of different voltage levels. Digital signals can be regenerated using repeaters in order to travel longer distances before weakening and becoming unusable because of attenuation.

Baseband supports bidirectional communication. It means, this technology can send and receive data simultaneously. To support bidirectional communication, this technology uses two separate electric circuits together; one for sending and another for receiving.

Although baseband transmits only a single data stream at a time, it is possible to transmit signals of multiple nodes simultaneously. This is done by combining all the signals into a single data stream. To combine the signals of multiple nodes, a technology known as multiplexing is used. Baseband supports the Time Division Multiplexing (TDM).

Baseband technology is mainly used in Ethernet networks to exchange data between nodes. This technology can be used on all three popular cable media types of Ethernet; coaxial, twisted-pair, fiber-optic.

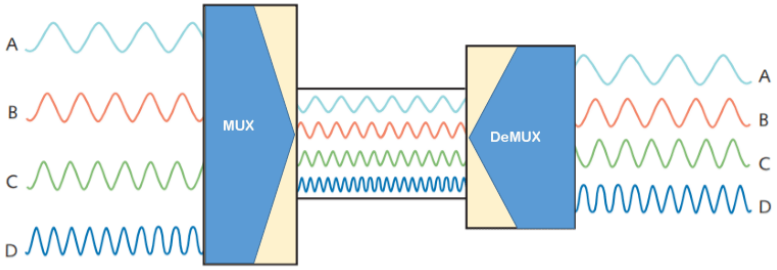
The following image shows an example of this.



Broadband technology uses analog signals in data transmission. This technology uses a special analog wave known as the **carrier wave**. A carrier wave does not contain any data but contains all properties of the analog signal. This technology mixes data/digital signal/binary values into the carrier wave and sends the carrier wave across the channel/medium.

To transmit data of multiple nodes simultaneously, this technology supports the Frequency Division Multiplexing. FDM (Frequency Division Multiplexing) divides the channel (medium or path) into several sub-channels and assigns a sub-channel to each node. Each sub-channel can carry a separate carrier wave.

The following image shows an example of this process.



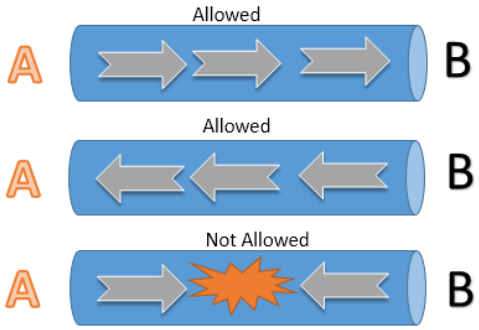
Analog signals can be regenerated using amplifiers in order to travel longer distances.

Broadband supports only unidirectional communication. It means, nodes connected at both ends of a medium can send or receive data but can't perform both actions simultaneously. Only one action is allowed at a time.

For example, two nodes A and B are connected through a cable that uses broadband technology to transmit signals. When node A transmits signals, node B receives the

transmitted signals and when node B transmits signals, node A receives the transmitted signals.

The following image shows this example.



Broadband is typically used in an environment that transmits audio, video, and data simultaneously. For example, Cable TV Networks, Radio stations, and Telephone companies. Usually radio waves, coaxial, fiber-optic cables are used for broadband transmission.

Key differences between baseband and broadband transmissions

Baseband transmission	Broadband transmission
• Transmit digital signals	• Transmit analog signals
• To boost signal strength, use repeaters	• To boost signal strength, use amplifiers
• Can transmit only a single data stream at a time	• Can transmit multiple signal waves at a time
• Support bidirectional communication simultaneously	• Support unidirectional communication only
• Support TDM based multiplexing	• Support FDM based multiplexing
• Use coaxial, twisted-pair, and fiber-optic cables	• Use radio waves, coaxial cables, and fiber optic cables
• Mainly used in Ethernet LAN networks	• Mainly used in cable and telephone networks

Ethernet Versus IEEE 802.3

It is important to note that Ethernet is *not* the same as the IEEE 802.3 implementations, and the terms should not be used interchangeably (although they sometimes are). Whereas Xerox, DEC, and Intel developed Version 1 and Version 2 with somewhat similar parameters, the IEEE committee added several features that gave its standard expanded capabilities not shared with its predecessors.

Table provides an overview of the similarities and differences between the three implementations.

Table: Ethernet Versions 1, 2, and IEEE 802.3

Version 1	Version 2	IEEE 802.3
Data Link layer architecture	Includes Ethernet_II frame (the de facto industry frame to carry IP traffic over Ethernet LANs)	Adds jabber control (or jabber inhibit) to detect and disable faulty transceivers
Delivered data at 10Mbps as linear bus topology	Delivers data at 10Mbps as linear bus topology	Expands physical topology support to star configurations
Could use only thick coaxial media	Can use only thick coaxial media	Adds media types such as thin coaxial, fiber, and twisted pair
Used unbalanced signaling with ground as reference point (susceptible to noise and EMI)	Uses balanced signaling	1995 enhancements provide 100Mbps transfer rates (802.3u)
Did not support Signal Quality Error (SQE) (also known as heartbeat), so more difficult to detect collisions	Adds SQE	Supports SQE but is only necessary with external transceive

General Ethernet Operation

The IEEE 802.3 specification defines the general operation, components, and distance limitations of Ethernet. They are as follows:

- Defines all Data Link and Physical layer components, functions, channel access method, and operations.
- Provides vendors with rules to follow when implementing or developing Ethernet 802.3 LAN technologies.
- Is based on the IEEE standard known as 10Base5, which all other 802.3 standards follow with minor variations.

The IEEE 802.3 standard defines a 10Mbps broadcast-based linear network architecture using a contention channel access method known as CSMA/CD.

Base Band Ethernet Standards

Name	IEEE Standard	Data Rate
Ethernet	802.3	10 Mbps
Fast **Ethernet**/ 100Base-T	802.3u	100 Mbps
Gigabit **Ethernet**/ GigE	802.3z	1000 Mbps
10 Gigabit **Ethernet**	IEEE 802.3ae	10 Gbps

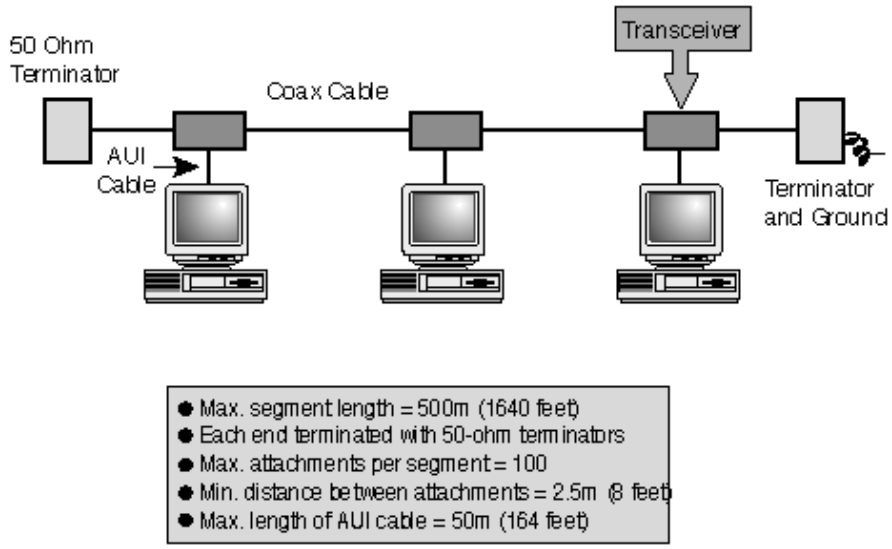
Slow Ethernet Specifications and Limitations

Slow (10Mbps) Ethernet has been the mainstay of LAN networks since it came out in the mid-1980s. In the sense that the early days of networking were somewhat chaotic, with vendors making strictly proprietary products and the rules that governed them, it is interesting to follow the development toward de facto industry standards and recent improvements in them. Despite the emergence of standards-defining bodies to provide clear rules for implementing technologies (such as 802.3), desire to exceed limitations drives the industry to ignore many of those rules.

Slow Ethernet specifications include the following:

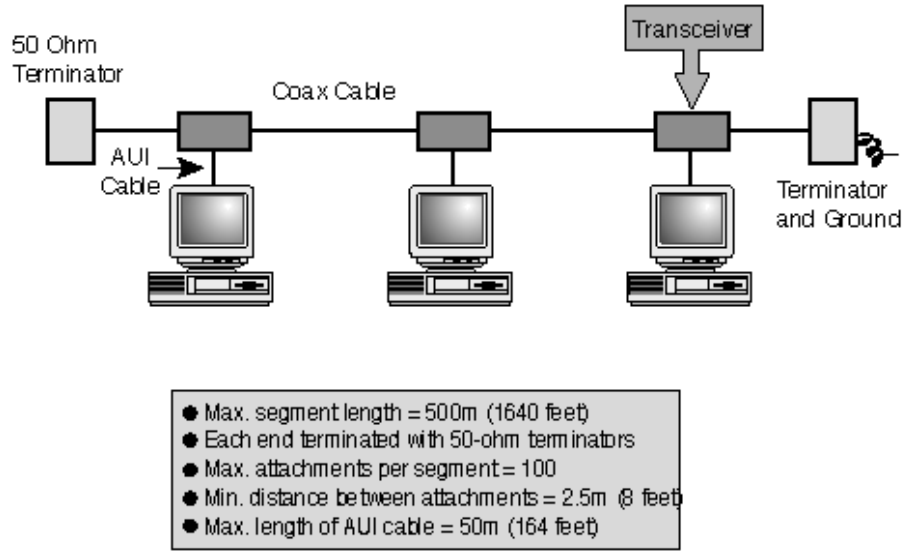
- 10Base5
- 10Base2
- 10BaseT
- 10Base5 (Thicknet)

10Base5 connections have the following parameters (as shown in fig)



- Transmission takes place at 10Mbps using thick coaxial cable on a linear bus.
- External transceivers attach directly to the medium through vampire taps.
- Tap placements should be at exactly 2.5m or multiples thereof.
- Devices attach to taps using Attachment Unit Interface (AUI) cables connecting to the network card's 15-pin DIX interface.
- Each segment should not exceed 500m; segment extension takes place through repeating devices that provide signal retiming and amplification.

Fig shoes, 10Base5 Thick Ethernet uses coaxial cable as opposed to UTP (Unshielded Twisted Pair), which is commonly used today.

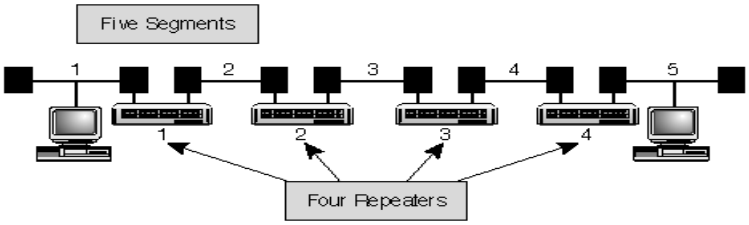


Rule of 10Base5

This rule states that two communicating devices should

- Not be separated by more than five maximum length segments and should have the following:
    - Fifty-ohm terminators at both ends of each segment, with one end connected to a common ground reference
    - A maximum of 100 node attachments per segment
    - A maximum AUI lobe cable distance of 50m
- Not pass through more than four repeaters

Of the five segments, only three should be populated (the remaining two are used strictly to add distance to the overall network as shown in fig:



The 5-4-3 Rule states that communicating devices should not be separated by more that five segments connected through four repeaters, with three segments supporting end host connections, while the remaining links are used as unpopulated LAN extensions. See fig above.

10Base2

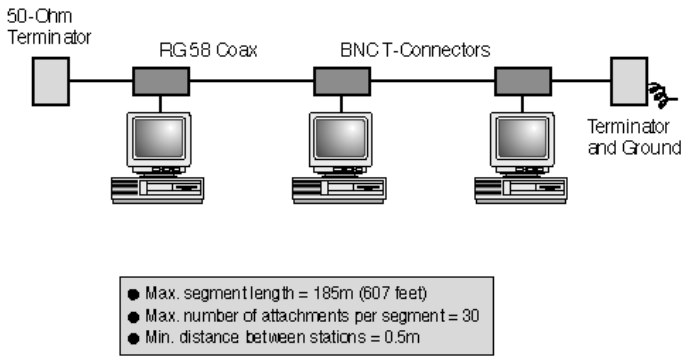
10Base2 networks are wired together in a bus topology, in which individual stations (computers) are connected directly to one long cable. The maximum length of any particular segment of a **10Base2** network is 185 meters. If distances longer than this are required, two or more segments must be connected using repeaters.

10BASE2 (also known as cheapernet, thin Ethernet, thinnet, and thinwire) is a variant of Ethernet that uses thin **coaxial** cable terminated with **BNC connectors** to build a local area network.

10Base2 connections have the following parameters

- Transceivers are generally internal to the network card.
- Transceivers attach to a physical layer thin coaxial (RG-58) bus through BNC connectors.
- Maximum segment distance for RG-58 is 185m.
- Repeaters provide segment extension.
- Segment termination and ground requirements are the same as 10Base5.
- Maximum number of node attachments per segment is 30, with a minimum separation of .5m between each.
- Is also subject to the 5-4-3 Rule.

Fig.:10Base2 Parameters

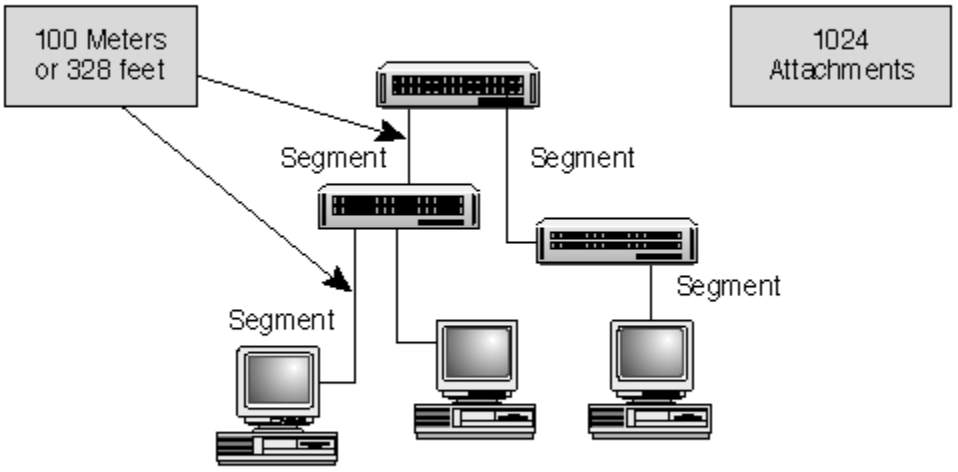


Features of 10Base2

10Base2 networks are wired together in a bus topology, in which individual stations (computers) are connected directly to one long cable. The maximum length of any particular segment of a **10Base2** network is 185 meters. If distances longer than this are required, two or more segments must be connected using repeaters.

10BaseT

10BaseT connections have the following parameters (as shown in Figure):

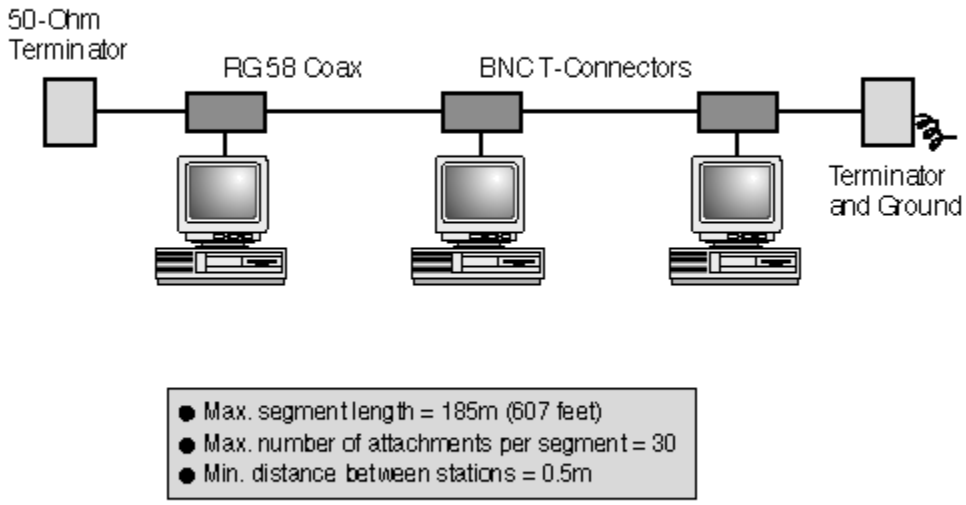


- Transmit 10Mbps over twisted pairs in a physical star configuration.
- Use two pairs—Pins 1 and 2 for transmitting; pins 3 and 6 for receiving.
- Devices connect to central hubs (known as *concentrators*) through unshielded twisted pair (UTP) cables with RJ45 connectors.
- Hub-to-hub connections extend the network; the connections require UTP crossover cables unless the conversion is internal.

10Base2 Thin Ethernet has a shorter maximum segment length than 10Base5.

- Maximum of 100m cable distance for node-to-hub or hub-to-hub connections.
- Unused hub ports do not require termination.
- Maximum number of node attachments is 1,024.
- Subject only to the 5-4 portion of the 5-4-3 Rule (maximum of five segments through four hubs; each segment can be populated).

Fig.: 10Base2 ThinNet:



10Base2 ThinNet segments cannot be longer than 185 meters, although it is often exaggerated to 200 meters, and you can't put more than 30 devices on each populated segment. The entire cabling scheme, including all five segments, can't be longer than 925 meters.

Gigabit Ethernet

Although Gigabit Ethernet technology is just beginning to emerge, it is likely that it will eventually see wide deployment. Its advantages include

- Cost efficiency and savings
- Simplicity of implementation
- Nearly seamless integration with existing Ethernet deployments due to compatibility with existing 10BaseT cabling infrastructures

Key Concept

Feel free to skip over this coverage of Gigabit Ethernet because it's not covered on the exam. I did think it was important to at least mention it, however, because Gigabit Ethernet is an emerging technology that you'll no doubt encounter later.

Gigabit Ethernet Overview

The Gigabit Ethernet standard enables transmission speeds of up to 1000Mbps using Category 5 UTP cabling.

The task force specification is the IEEE 802.3z, which uses 802.3 Ethernet frame formats, as well as the CSMA/CD access method. Note that the continuing use of the 802.3 standard supports backward compatibility with the 100BaseT and 10BaseT technologies.

Table 3.8 shows the cable types and their respective distance limitations on which Gigabit Ethernet is designed to run.

Table: Gigabit Ethernet Cable Types and Distance Limits

Cable Type	**Distance Limit**
Category 5 UTP	100 meters
Fiber Optic (FDDI) Single-mode	5 kilometers
Fiber Optic Multi-mode	550 meters
Balanced Shielded Copper 10Base	25 meters

Media Connectivity

VSAT

SATs (Very Small Aperture Terminals) is a two way, lost cost, ground micro station for transmitting data to and from communication satellites. A VSAT has a dish antenna with diameters between 75 cm to 1 m, which is very small in comparison with 10 m diameter of a standard GEO antenna. It accesses satellites in geosynchronous orbits or geostationary orbits. Data rates in VSATs ranges from 4 Kbps to 16 Mbps.

VSAT : Introduction

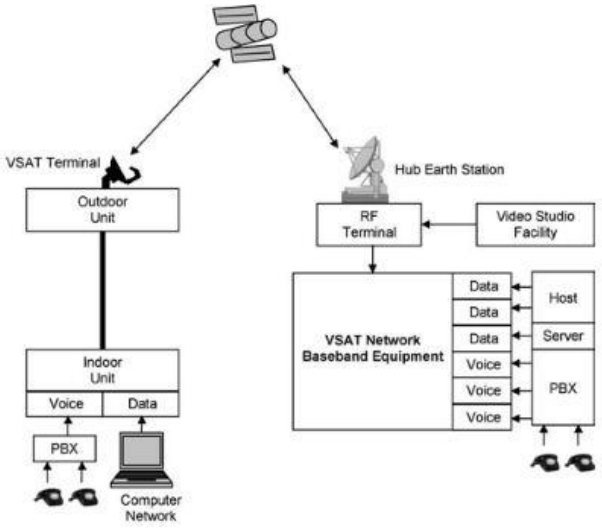
VSATs stand for very small aperture terminals and are used for providing one-way or two-way data broadcasting services, point-to-point voice services and one way video broadcasting services.

VSAT networks are ideal for centralized networks with a central host and a number of geographically dispersed terminals. Typical examples are small and medium businesses with a central office, banking institutions with branches all over the country, reservation and airline ticketing systems etc.

VSATs offer various advantages like wide geographical area coverage, high reliability, low cost, independence from terrestrial communication infrastructure, flexible network configurations etc. However it suffer from a major problem of delay between transmission and reception of data(around 250ms) due to the use of GEO satellites

VSAT Network:

- The ground segment of a typical VSAT network consists of a high performance hub Earth station and a large number of low performance terminals referred to as VSATs.
- The space segment comprises GEO satellites acting as communication links between the hub station and the VSAts.
- A typical VSAT network is shown below.



A typical VSAT network

- VSATs employ a high performance central station so that the various remote stations can be simpler and smaller in design, thus enabling the VSAT networks to be extremely economical and flexible.
- The hub station is usually a large, high performance Earth Station comprising an outdoor antenna (with a diameter of between 6 to 9 metres) for transmission, RF terminals for providing a wideband uplink of one digital carrier per network, base band equipment comprising modems, multiplexers and encoders, a control centre for managing the network and various kinds of interfacing equipment to support a wide variety of terrestrial links.
- These terrestrial links connect the hub station to the head office or to the data processing centre from where the data have to be broadcasted.
- In the case of bidirectional networks, the outdoor antenna is also configured for reception of signals and the RF equipment comprises several narrowband downlink channels for reception from various remote VSATs.
- VSATs are smaller and simpler in design as compared to the hub centre and comprise an outdoor antenna (0.5 to 2.4m diameter), an RF terminal comprsing an LNB (low noise block) for reception and baseband equipment. The also comprise an up-converter and power amplifier for uplinking in the case of bidirectional networks.
- VSAT networks employ either C band or Ku band. The sharing problem is less severe at the Ku band.
- VSATs are generally used for carrying digital signals. Binary phase shift keying(BPSK) or Quadrature phase shift keying modulation schemes with forward error correction using Viterbi or sequential decoding technique are often used.

Advantages of VSAT

Following are the **advantages of VSAT**:

- Installation: VSAT services are deployed in hours or minutes.
- Coverage: It can be available anywhere with clear line of sight between VSAT antenna disc and satellite over the earth.
- It is popular in hilly areas where other mode of communication is either not available or difficult to install.
  Price: VSAT terminals are cheaper.
- Upgradaion: It is flexible to add a VSAT site and increase the bandwidth as per future requirements.
  Service charges: It depends on the bandwidth allocated as per user requirements.
- Most modern VSAT systems use TCP/HTTP and other acceleration protocols to have superior performance inspite of latency limitation as outlined below.
- VSAT provides same quality of service and speed at all the locations across the entire VSAT network.
  VSAT services are independant of other wired and wireless mediums used as transmission network service provider. Hence it is a great backup system which is available during disaster and emergency situations.
- VSAT terminals and indoor/outdoor hardwares can be installed on truck or van and can be used even in mobility conditions.
- There are no last mile issues in VSAT operation.

Disadvantages of VSAT

Following are the **disadvantages of VSAT**:

- As mentioned it requires clear Line of Sight between VSAT dish and satellite in the space. The malfunctioning of satellite and Hub station (in case of star topology) will lead to disruption of VSAT services. To avoid this situation, redundant systems and switch over units are needed to have backup systems available for hot switching in faulty situations. But this increases overall cost of the VSAT system as a whole.
- Latency for packet transmission from source to destination is higher due to distance of satellite from earth is about 36000 Km. Latency further increases in star topology of VSAT, as it requires two hops to reach at final destination.
- VSAT services get affected in bad weather conditions.
- As information transmitted by VSAT goes over the air till it reaches destination, it is prone to intrusion by hackers. Hence encryption-decryption units are needed to have secure communication. This increases the overall VSAT terminal cost.

Configurations of VSATs

- **Star Topology** – This has a central uplink site which transmits data from and to each VSAT through the satellite.
- **Mesh Topology** – Each VSAT transmits data via the satellite to the other stations. The above diagram shows mesh topology of VSATs.
- Combination of the above

Uses of VSATs

- In narrowband data – e.g. point – of – sale transactions using debit cards or credit cards, RFID data
- In broadband data – e.g. Internet access to remote locations, VoIP
- Mobile communications
- Maritime communications

The Public Switched Telephone Network (PSTN)

Whether you're interested in voice, data or networking, it is important to have an understanding of the structure and operation of the telephone network.

We begin with a basic model for the telephone network in this slide, and build on it in subsequent discussions. At the top of the diagram, we have a telephone and a telephone switch. The telephone is located in a building called a Customer Premise (CP), and the telephone switch is located in a building called a Central Office (CO). One could refer to the telephone as Customer Premise Equipment (CPE).

The Public Switched Telephone Network (PSTN)

The telephone is connected to the telephone switch with two copper wires, often called a local loop or a subscriber loop, or simply a *loop*. This a dedicated access circuit from the customer premise into the network. We usually have the same arrangement at the other end, with the far-end telephone in a different customer premise and the far-end telephone switch usually in a different central office.

There is a maximum length for the local loop, which is usually 18,000 feet – about three miles or five kilometers. Copper is a good conductor of electricity - but not perfect: it has some resistance to the flow of electricity through it. Because of this, the signals on the loop diminish in intensity or attenuate with distance… if the loop was too long, you wouldn't be able to hear what the other person was saying. Thus, COs traditionally had a serving area of three miles radius around them, about 27 square miles or 75 km^2.

With suburban sprawl, we can't build COs every five miles, so in practice, new subdivisions are served from remote switches, which are low-capacity switches in small huts or underground controlled environment vaults. The remote provides telephone service locally on the loops in the subdivision. The *backhaul* connects the remote switch back to the nearest CO via fiber.

Other equipment in the *outside plant* includes remote DSLAMs, the device containing the network-side modems that customer modems communicate with, housed in an enclosure by the side of the road. The backhaul for these devices is fiber plus often copper wires carrying electricity to power the DSLAM.

In the future, these two remote devices will merge together.

- Telephone switches were historically connected with *trunks*. While subscriber loops are dedicated access circuits from the customer premise to the CO, trunks are shared connections between COs.
- To establish a connection between one customer premise and another, the desired network address (telephone number) is signaled by the customer to the switch over their loop, the switch selects an unused trunk circuit going in that direction and reserves it, called seizing the trunk, then connects the caller's loop to that trunk, for the duration of the call. When one end or the other hangs up, the trunk is released for someone else to connect between those two COs. This method for sharing the trunks is known as *circuit switching*.
- In systems installed up until about 2005, trunks were carried on the transmission network using channelized fiber optic transmission systems. A *channel* is a reserved fraction of the capacity of the transmission system, 64 kb/s, called a DS0. The caller's voice would be carried from one end to the other at 64 kb/s over reserved channels. This happens in both directions at the same time, and 64 kb/s is transmitted whether the caller is speaking or not.
- However, the new-generation all-IP network moves IP packets, as needed, not reserved channels, and the telephones communicate packets directly one to another once a call is set up.
- The transition between the two plans, channels and packets, is and will be a long process.
- For obvious business reasons, telephone companies do not replace equipment just because something new comes along. There are still many CO switches that perform the previous technique, circuit switching.

- To keep operating the "old" circuit switch with the "new" IP backbone, a Packet Voice Gateway is installed between the switch and the transmission network, transcoding between packets and channels, and between the different call control messages used on each side.
- To keep operating "old" channelized transmission systems with the "new" IP backbone, all of the channels are combined together to make one high-speed channel, used all at once to connect routers at each end, which communicate packets to each other.
- It is important to note that even though today there is digital switching, routing and transmission, the last 3 miles or 5 km of the network, the subscriber loop, still has its original characteristics, and is still used to carry an analog voiceband signal... technology that dates back to the late 1800s (!) that is part of Plain Ordinary Telephone Service (POTS).