DATA COMMUNICATION NETWORKS

UNIT - I

Data and Information

Data refers to the raw facts that are collected while *information* refers to processed data that enables us to take decisions. The word *data* refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data Communication

During communication, information is shared. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, remote communication takes place over distance. The term *telecommunication*, which includes telephony, telegraphy, and television, means communication at a distance.

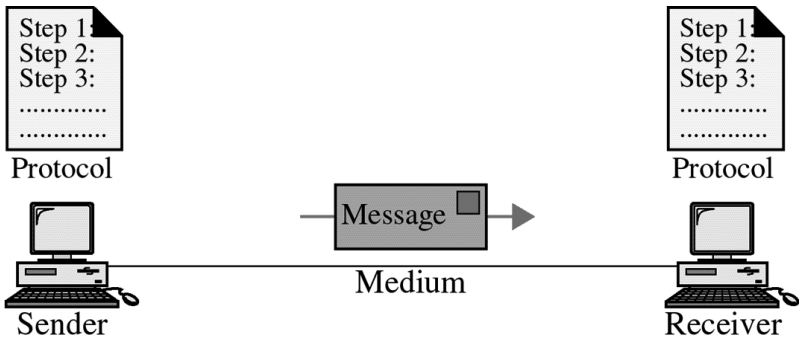
Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Fundamental Characteristics of Data Communication

The effectiveness of a data communications system depends on three fundamental characteristics: delivery, accuracy, timeliness.

- **Delivery**: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
- **Accuracy**: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
- **Timeliness**:The system must deliver data in a timely manner. Data delivered late are useless.

Components of Data Communication



- **Message**: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- **Sender**: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

- **Receiver**: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- **Transmission medium**: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
- **Protocol**: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

Networks

A network is a set of devices referred to as *nodes* connected by communication links.

A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

The links connecting the devices are called as communication channels.

Distributed Processing

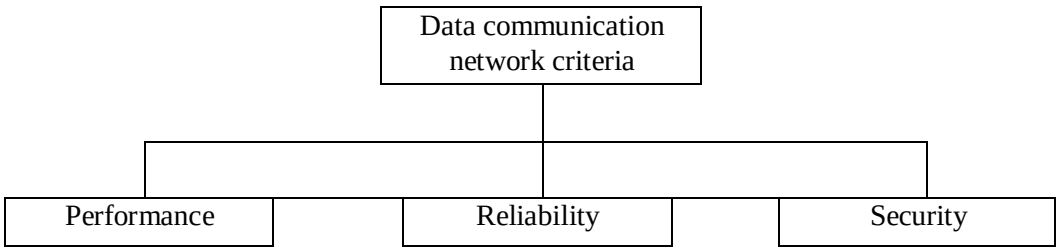
In distributed processing a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers handle its as a subset.

Advantages of distributed processing:

- **Security/encapsulation :** A system designer can limit the kinds of interactions that a given user can have with the entire system.
- **Distributed databases :** No one system needs to provide storage capacity for the entire database.
- **Faster problem solving :** Multiple computers working on parts of a problem concurrently often can solve the problem faster that a single machine working done.
- **Security through redundancy :** Multiple computers running the same program at the same time can provide security through redundancy.
- **Collaborative processing :** Both multiple computers and multiple users may interact on a task.

Network Criteria

To be an efficient and effective network must meet a certain number of criteria. The most important of these are performance, reliability, and security.



Performance

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.

The performance of a network depends on the factors, number of users, type of transmission medium, hardware, and software.

- **Number of users** : A large number of concurrent users can slow response time in a network. The design of a given network is based on an assessment of the average number of users that will be communicating at any one time. In peak load periods, the actual number of users can exceed the average and thereby decrease performance.
- **Type of transmission medium** : The medium defines the speed at which data can travel through a connection. Today's network is moving faster and faster transmission media, such as fiber-optic cabling. The speed of light imposes an upper bound on the data rate.
- **Hardware :** The types of hardware included in a network affect both the speed and capacity of transmission. A higher-speed computer with greater storage capacity provides better performance.
- **Software :** The software used to process data at the sender, receiver, and intermediate notes also affects network performance. Moving a message from node to node through a network requires processing to transform the raw data into transmittable signals, to route these signals to the proper destination, to ensure error-free delivery, and to recast the signals into a form the receiver can use. The software that provides these services affects both the speed and the reliability of a network link. Well-designed software can speed the process and make transmission more effective and efficient.

Reliability

Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

- **Frequency of failure:** All networks fail occasionally, A network that fails often, however, is of little value to a user.
- **Recovery time of a network after a failure:** A network should be restored quickly to its service. A network that recovers quickly is more useful that one that does not.
- **Catastrophe:** Networks must be protected from catastrophic events such as fire, earthquake, or theft. One protection against unforeseen damage is a reliable system to backup network software.

Security

Network security issues include protecting data from unauthorized access and viruses.

- **Unauthorised Access:** A useful network will protect sensitive data from unauthorized access. Protection can be accomplished at a number of levels. At the lowest level are user identification codes and passwords. At a higher level are encryption techniques.
- **Viruses:** A network is accessible from many points, hence it can be susceptible to computer viruses. A virus is an illicitly introduced code that damages the system. A good network is protected from viruses by hardware and software designed specifically for that purpose.

Applications of Networks

Some of the network applications in different fields are the following:

- **Marketing and sales**: Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange, and analyze data relating to customer needs and product development cycles. Sales applications include teleshopping, which uses order-entry computers or telephones connected to an order-processing network, and on-line reservation services for hotels, airlines, and so on.
- **Financial Services:** Today's financial services are totally dependent on computer networks. Applications include credit history searches, foreign exchange and investment services, and electronic funds transfer (EFT), which allows a user to transfer money without going into a bank.
- **Manufacturing:** Computer networks are used today in many aspects of manufacturing, including the manufacturing process itself. Two applications that use networks to provide essential services are computer-assisted design (CAD) and computer-assisted manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.
- **Electronic messaging:** The most widely used network application is electronic mail (e-mail).
- **Directory services:** Directory services allow lists of files to be stored in a central location to speed worldwide search operations.
- **Information services:** Network information services include bulletin boards and data banks. A World Wide Web site offering the technical specifications for a new product is an information service.
- **Electronic data interchange (EDI):** EDI allows business information (including documents such as purchase orders and invoices) to be transferred without using paper.
- **Teleconferencing:** Teleconferencing allows conferences to occur without the participants being in the same place. Applications include simple text conferencing, voice conferencing, and video conferencing.
- **Cellular telephone:** Cellular networks maintain wireless phone connections even while traveling over large distances.
- **Cable television:** The services provided by cable television networks may include video on request, as well as the same information, financial, and communications services currently provided by the telephone companies and computer networks.

PROTOCOLS AND STANDARDS

Protocols

- A Protocol is one of the components of a data communications system. Without protocol communication cannot occur.
- When the sender sends a message it may consist of text, number, images, etc. which are converted into bits and grouped into blocks to be transmitted and often certain additional information called control information is also added to help the receiver interpret the data.
- For successful communication to occur, the sender and receiver must agree upon certain rules called protocol.
- **A Protocol is defined as a set of rules that governs data communications.**
- A protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated.

Elements of a Protocol

There are three key elements of a protocol:

Syntax

- It means the structure or format of the data, meaning the order in which they are presented
- It is the arrangement of data in a particular order.

Semantics

- It tells the meaning of each section of bits and indicates the interpretation of each section.
- It also tells what action/decision is to be taken based on the interpretation.

Timing

- It refers to two characteristics: when data should be sent and how fast they can be sent.
- It tells the sender about the readiness of the receiver to receive the data
- It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

Standards

A standard provides a model for development that makes it possible for a product to work regardless of the individual manufacturer.

Standards provide guidelines to product manufacturers, vendors, government agencies and other service providers to ensure the national and international interconnectivity.

Standards are necessary in networking to ensure interconnectivity and interoperability between various networking hardware and software components.

Data communications standards are classified into two categories:

- De facto Standard
- De jure standard

De jure standard

- It means **by law** or **by regulation**.
- These standards are legislated and approved by a body that is officially recognized.

De facto Standard

- These are the standards that have been traditionally used and mean **by fact** or **by convention**
- These standards are not approved by any organized body but are adopted by widespread use.
- Subdivided into two class : *proprietary* and *nonproprietary*
- *Proprietary* standards are those originally invented by a commercial organization as a basis for the operation of its products. They are called proprietary because they are wholly owned by the company that invented them. These standards are also called as *closed* standards.
- *Nonproprietary* standards are those originally developed by groups or committees that have passed them into the public domain; they are also called *open* standards.

Examples of Standard Creation Committees :

1. International Organization for Standardization(ISO)
2. International Telecommunications Union - Telecommunications Standard (ITU-T)
3. American National Standards Institute (ANSI)
4. Institute of Electrical & Electronics Engineers (IEEE)
5. Electronic Industries Associates (EIA)

LINE CONFIGURATION

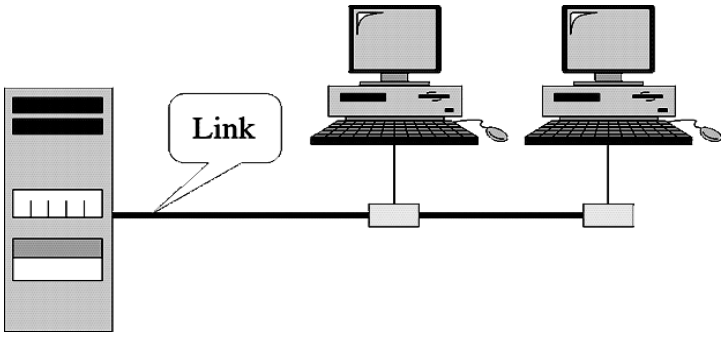
Line configuration refers to the way two or more communication devices attach to a link. A link is a communication pathway that transfers data from one device to another. There are two possible types of connections: point-to-point and multipoint.

Point-to-Point Line Configuration

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point

connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint Line Configuration



A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

TOPOLOGY

The term *physical topology* refers to the way in which a network is laid out either physically or logically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices to one another. There are five basic topologies possible: mesh, star, tree, bus, and ring.

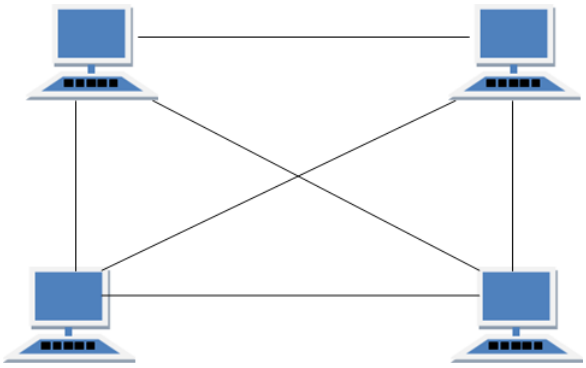
These five topologies describe how the devices in a network are interconnected rather than their physical arrangement.

Two relationships are possible: **peer-to-peer**, where the devices share the link equally, and **primary-secondary**, where one device controls traffic and the others must transmit through it.

Ring and mesh topologies are more convenient for peer-to-peer transmission, star and tree are convenient for primary-secondary. A bus topology is convenient for both.

Mesh topology

- In a mesh topology, every device has a dedicated point-to-point link to every other device, i.e., the link carries traffic only between the two devices it connects.
- A fully connected mesh network has *n(n -1) /2* physical channels to link n devices.
- every device on the network must have *n* – 1 input/output *(I/O)* ports.



Mesh Topology

Advantages

- the use of dedicated links guarantees that each connection can carry its own data load, thus eliminates the traffic problems.
- a mesh topology is robust. If one link becomes unusable, it will not affect the entire system.
- the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.
- point-to-point links make fault identification and fault isolation easy.

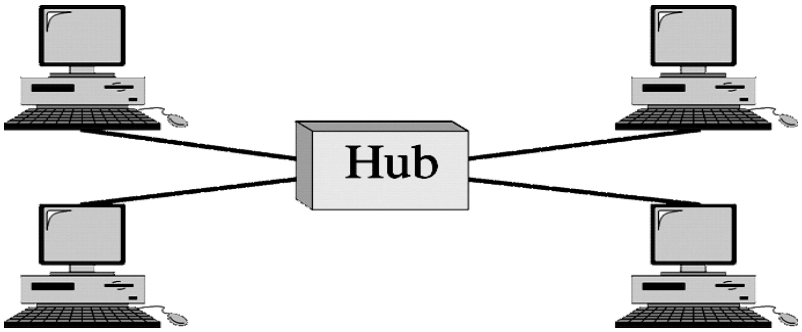
Disadvantages

- requires more amount of cabling I/O ports.
- installation and reconnection are difficult.
- the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- the hardware required to connect each link (I/O ports and cable) will be expensive.

Example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

- each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- a star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.



Star Topology

Advantages

- a star topology is less expensive than a mesh topology.
- in a star, each device needs only one link and one I/O port to connect it to any number of others.
- easy to install and reconfigure.
- less cabling needs to be housed, and additions, moves, and deletions involve only one connection.
- star topology is robust, if one link fails, only that link is affected. All other links remain active.
- easy fault identification and fault isolation.

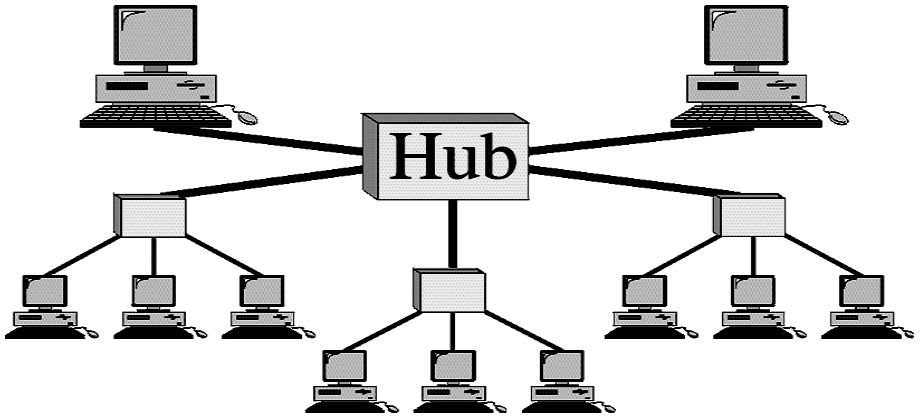
Disadvantages

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

The star topology is used in local-area networks (LANs).

Tree Topology

- a tree topology is a variation of a star. As in a star, notes in a tree are linked to a central hub that controls the traffic to the network.
- not every device plugs directly into the central hub. The majority of devices connect to a secondary hub that in turn is connected to the central hub.
- The central hub in the tree is an active hub. An active hub contains a repeater, which is a hardware device that regenerates the received bit patterns before sending them out. Repeating strengthens transmissions and increases the distance a signal can travel.
- The secondary hubs may be active or passive hubs. A passive hub provides a simple physical connection between the attached devices.



Tree Topology

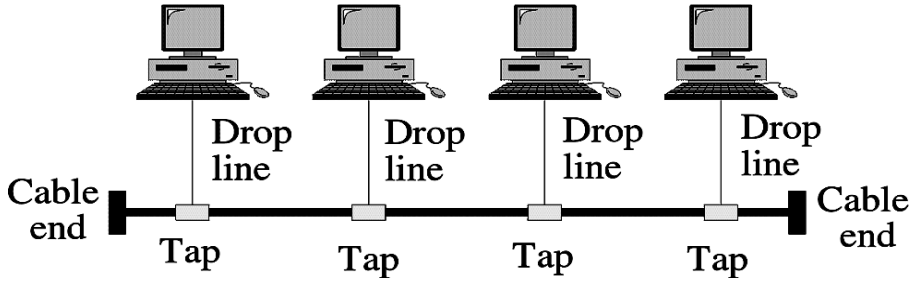
Advantages and Disadvantages

- The advantages and disadvantages are of a tree topology are the same as those of a star.
- The addition of secondary hubs, brings two further advantages. First, it allows more devices to be attached to a single central hub and can increase the distance a signal can travel. Second, it allows the network to isolate and prioritize communications from different computers.

  Example of tree topology can be cable TV technology.

Bus Topology

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



Bus Topology

Advantages

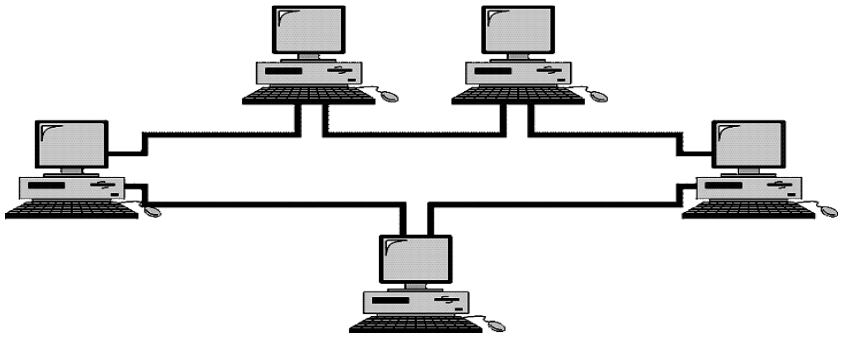
- easy to install.
- a bus uses less cabling than mesh, star or tree topologies.

Disadvantages

- difficult to reconfigure and fault isolation.
- difficult to add new devices.
- Signal reflection at the taps can cause degradation in quality.
- Adding new devices may therefore require modification or replacement of the backbone.
- a fault or break in the bus cable stops all transmission.

Ring Topology

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



Ring Topology

Advantages

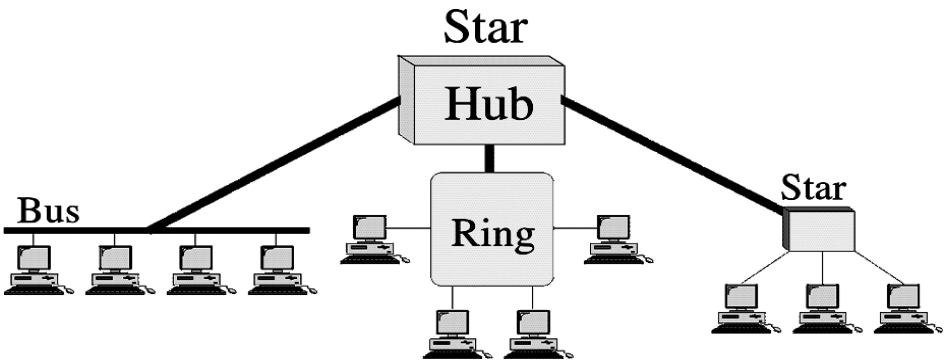
- a ring is easy to install and reconfigure.
- each device is linked to only its immediate neighbors. To add or delete a device requires changing only two connections.
- fault isolation is simplified.

Disadvantages

- unidirectional traffic can be a disadvantage.
- In a simple ring, a break in the ring can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Hybrid Topology

Hybrid topology combines several topologies as sub-networks linked together in a larger topology.

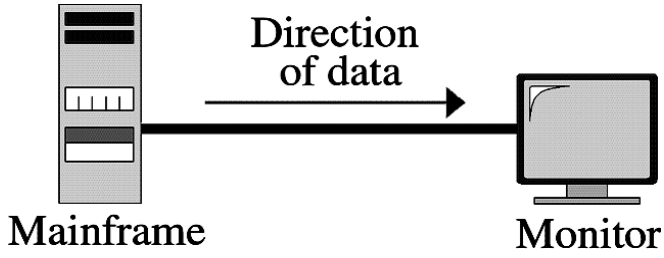


Hybrid Topology

Transmission Mode

Defines the direction of signal flow between two linked devices. There are three types of transmission modes: *Simplex, Half Duplex, Full Duplex*.

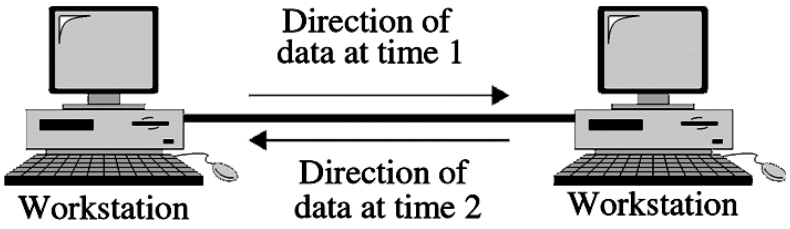
Simplex



In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.

Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.

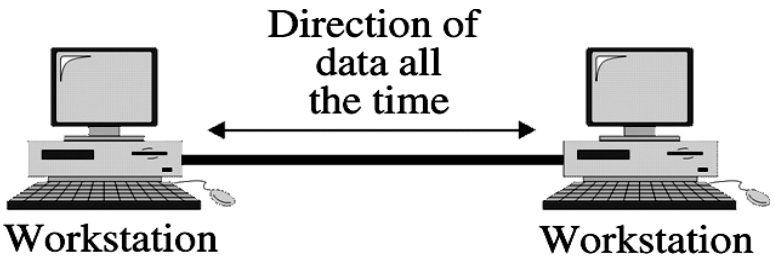
Half Duplex



In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.

Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Full Duplex



In full-duplex mode (also called duplex) both stations can transmit and receive simultaneously.

This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

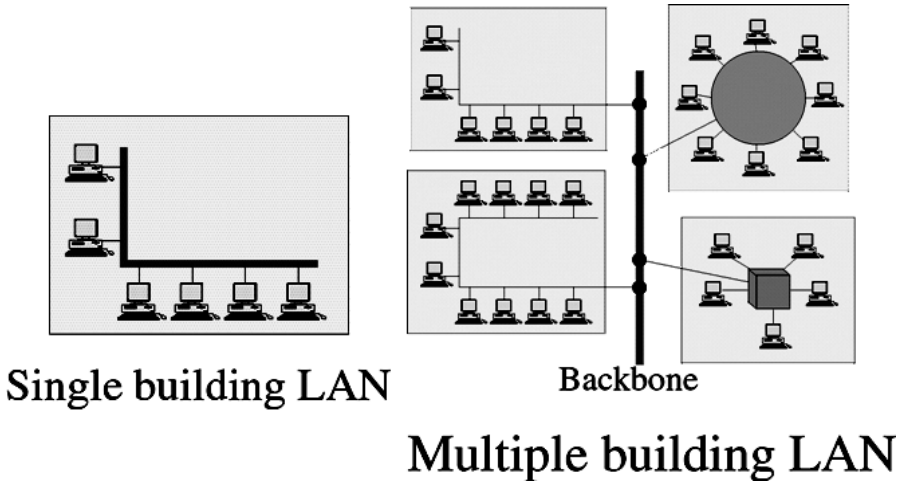
CATEGORIES OF NETWORKS

There are three primary categories of networks: local area networks, metropolitan area networks and wide area networks. The category a network falls is determined by its size, its ownership, the distance it covers, and its physical architecture.

Local Area Network (LAN)

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Size of the LAN is limited to a few kilometers.

LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.

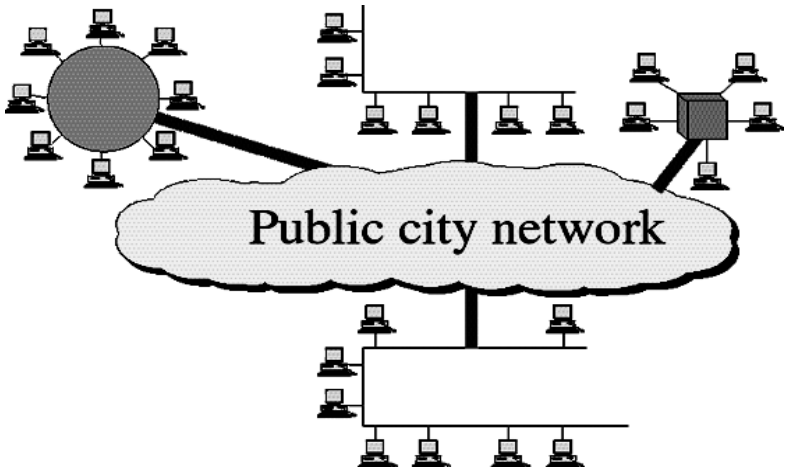


LAN

A common example of a LAN, linking a workgroup of task-related computers. A given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star.

Metropolitan Area Network (MAN)

A metropolitan area network is designed to extend over an entire city. It may be a single network like a cable television network, or it may be connecting a number of LANs into a larger network. For example, a company can use a MAN to connect the LANs in all of its offices throughout a city.

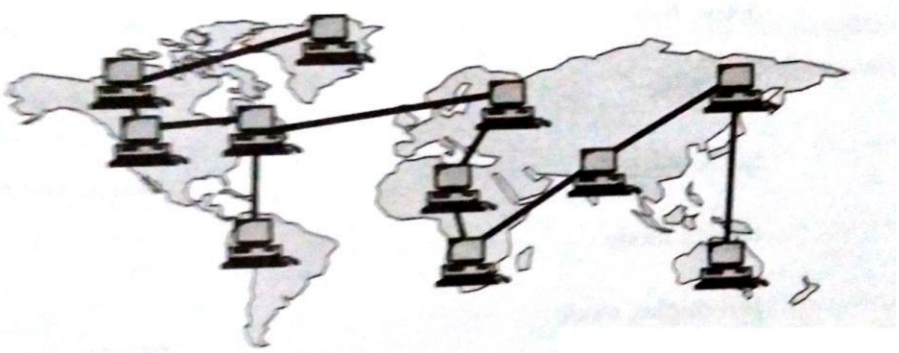


MAN

A MAN may be wholly owned by a private company, or it may be a service provided by a public company, such as local telephone company.

Wide Area Network (WAN)

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.



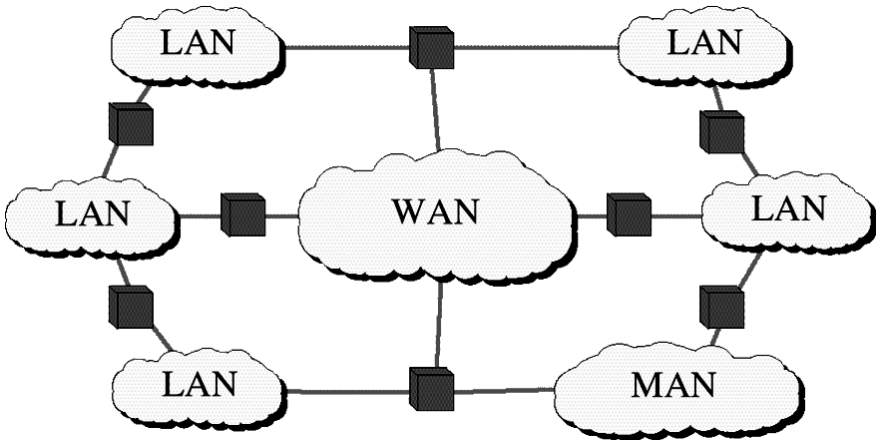
WAN

WAN may utilize public, leased, or private communication devices, usually in combinations, and can span an unlimited number of miles.

A WAN that is wholly owned by a single company is referred to as an enterprise network.

INTERNETWORKS

When two or more networks are connected, they become an internetwork, or internet. Individual networks are joined into internetworks by the use of internetworking devices. The devices can be routers and gateways.



Internetwork

DATA COMMUNICATION NETWORKS

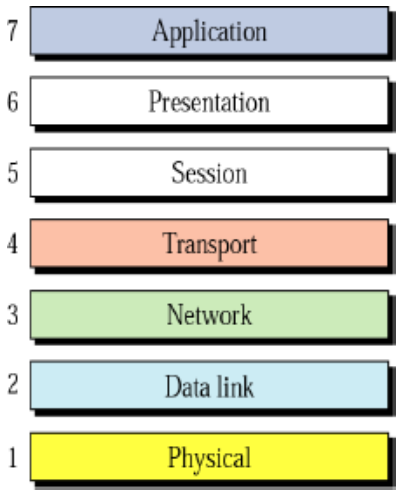
UNIT - II

The OSI Model

An ISO (Open Systems Interconnection) standard that covers all aspects of network communications is the Open Systems Interconnection model. An open system is a model that allows any two different systems to communicate regardless of their underlying architecture. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The Model

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

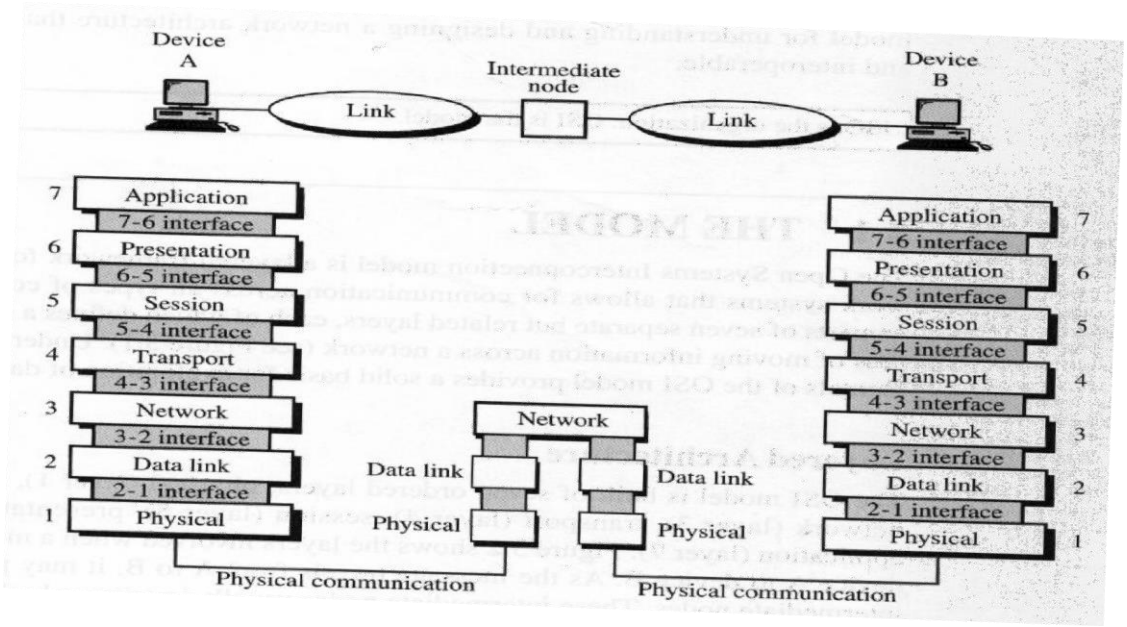


The OSI Model

Layered Architecture

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7).

In the given figure, as the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.



OSI Layers

Each layer defines a family of functions distinct from those of the other layers. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.

Peer-to-Peer Processes

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer *x* on one machine communicates with layer *x* on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

At the physical layer, communication is direct: In the above figure, device A sends a stream of bits to device B. At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers. Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers (control data added to the beginning or end a data parcel). Headers are added to the message at layers 6,5,4,3, and 2. A trailer is added at layer 2.

At layer 1 the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.

Interfaces Between Layers

The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Each interface defines the information and services a layer must provide for the layer above it.

Organization of the Layers

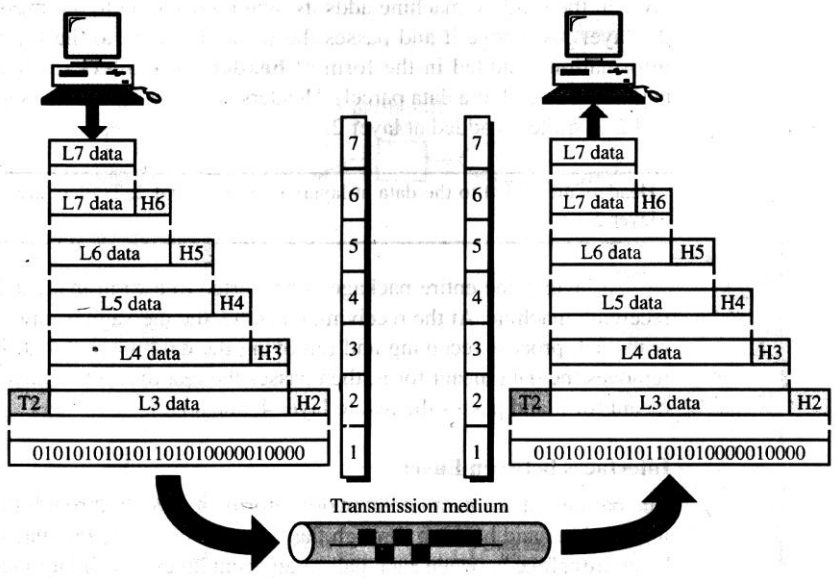
The seven layers can be belonging to three subgroups.

Layers 1, 2, and 3-physical, data link, and network-are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).

Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems.

Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.

The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

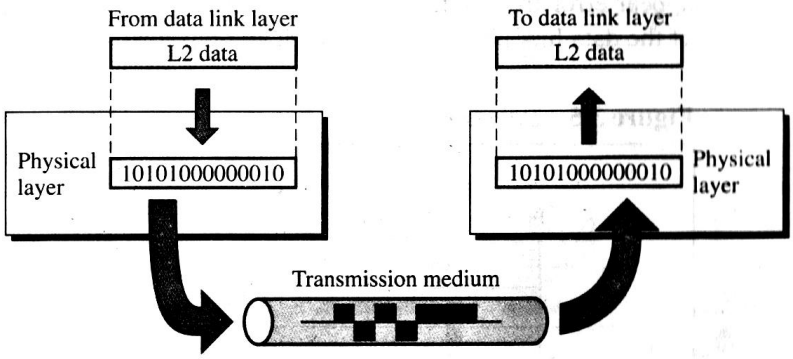


An exchange using the OSI model

Functions of the layers

Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.



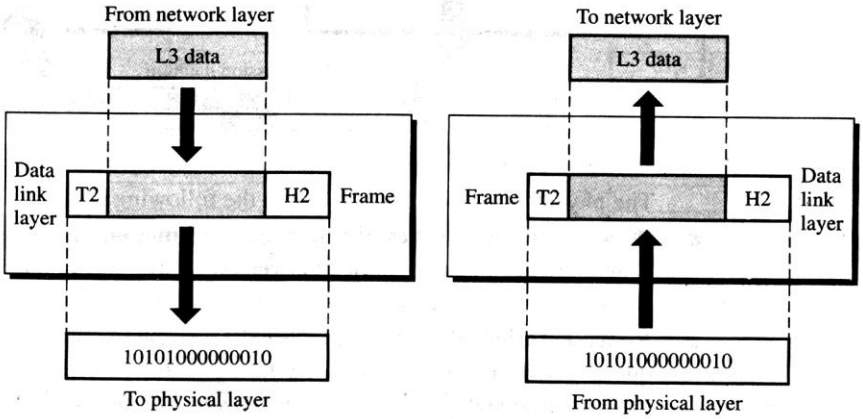
Physical Layer

The physical layer is also concerned with the following:

- Physical characteristics of interfaces and medium.
- Representation of bits
- Data rate
- Synchronization of bits
- Line configuration
- Physical topology
- Transmission mode

Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).



Data link Layer

Responsibilities of the data link layer include the following:

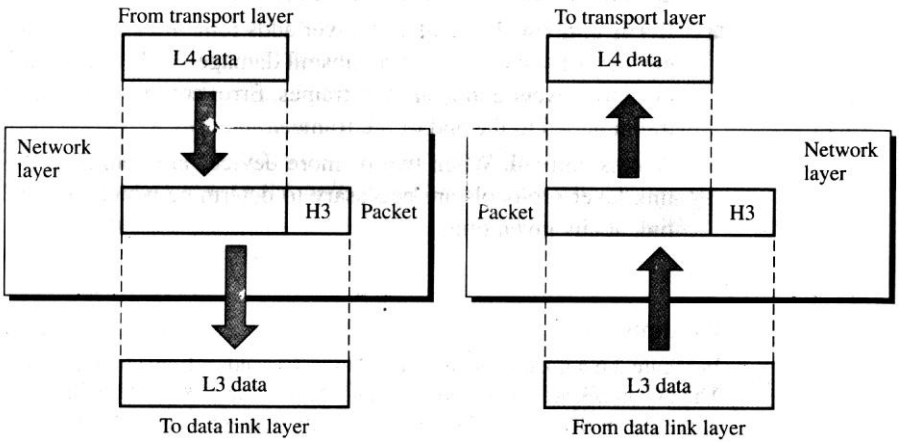
- Framing
- Physical addressing
- Flow control

- Error control
- Access control

Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.



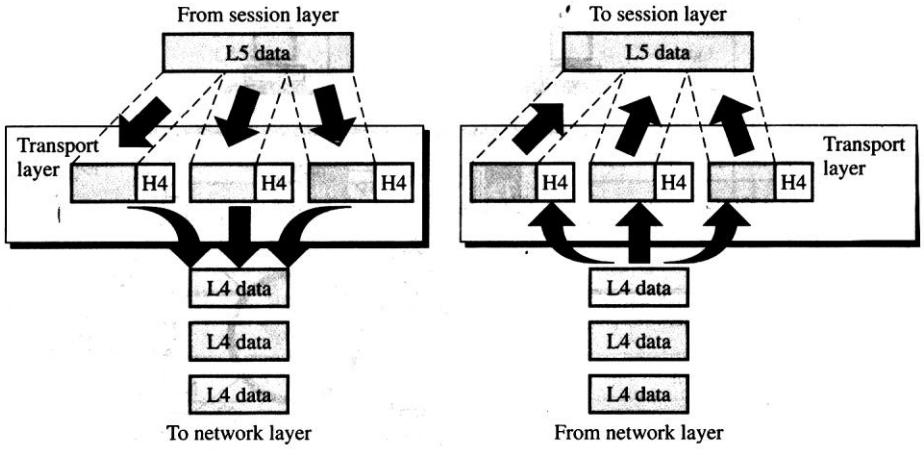
Network Layer

Responsibilities of the network layer include the following:

- Logical addressing
- Routing

Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets. The transport layer, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.



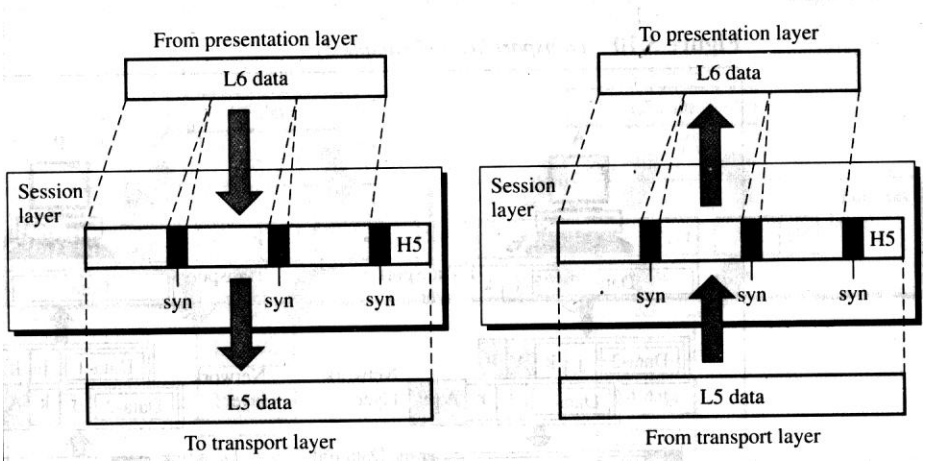
Transport Layer

The transport layer is responsible for the delivery of a message from one process to another. Other responsibilities of the transport layer include the following:

- Service-point addressing
- Segmentation and reassembly
- Connection control
- Flow control
- Error control

Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network *dialog controller*. It establishes, maintains, and synchronizes the interaction among communicating systems.



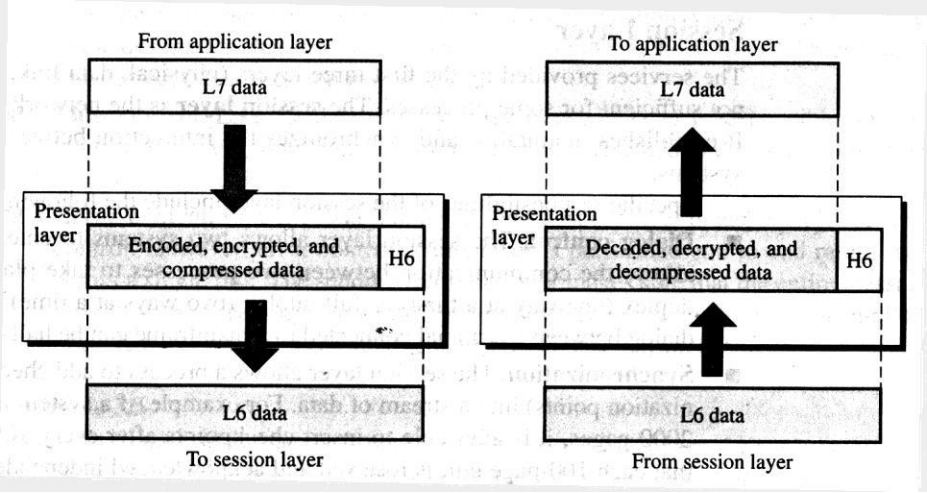
Session Layer

The session layer is responsible for dialog control and synchronization. Specific responsibilities of the session layer include the following:

- Dialog control
- Synchronization

Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.



Presentation Layer

Specific responsibilities of the presentation layer include the following:

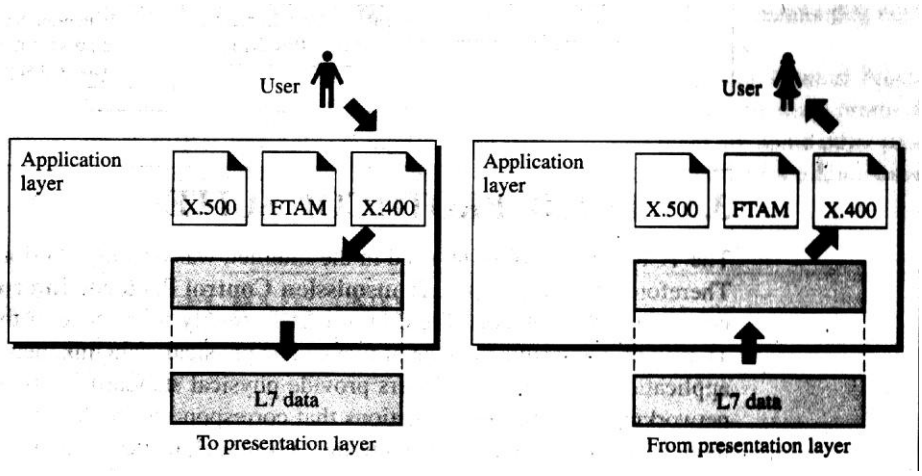
- **Translation**
- **Encryption**
- **Compression**

Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Of the many application services available, the figure shows only three: *X.400* (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs *X.400* to send an e-mail message.

The application layer is responsible for providing services to the user.



Application Layer

Specific services provided by the application layer include the following:

- **Network virtual terminal**
- **File transfer, access, and management**
- **Mail services**
- **Directory services**

Data and Signals

To be transmitted, data must be transformed to electromagnetic signals.

ANALOG AND DIGITAL

Both data and the signals that represent them can be either **analog or digital** in form.

Analog and Digital Data

Data can be analog or digital. The term **analog data** refers to information that is continuous; **digital data** refers to information that has discrete states. Analog data, such as the sounds made by a human voice, take on continuous values.

When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.

Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s.

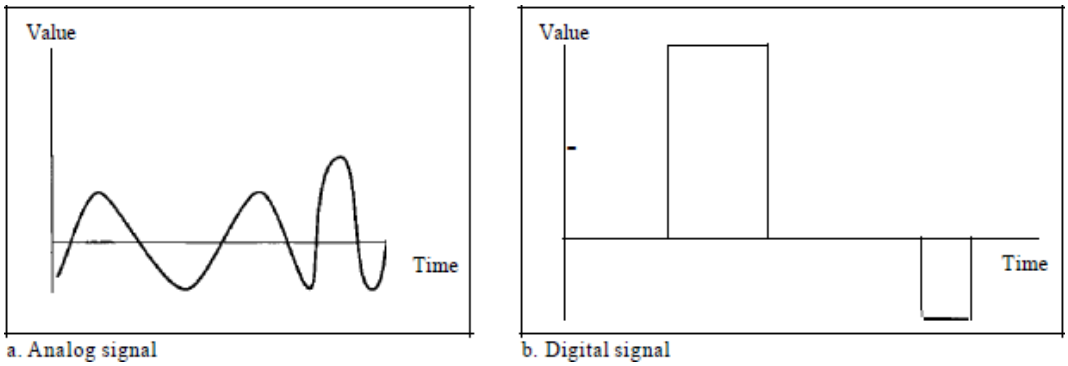
Analog and Digital Signals

Signals can be either analog or digital.

An analog signal is a continuous wave form which has infinite number of values along its path.

A digital signal, can have only a limited number of defined values (1 and 0).

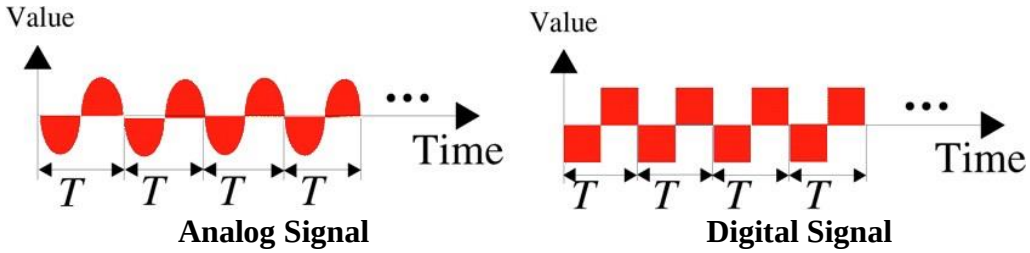
The vertical axis represents the value or strength of a signal. The horizontal axis represents time.



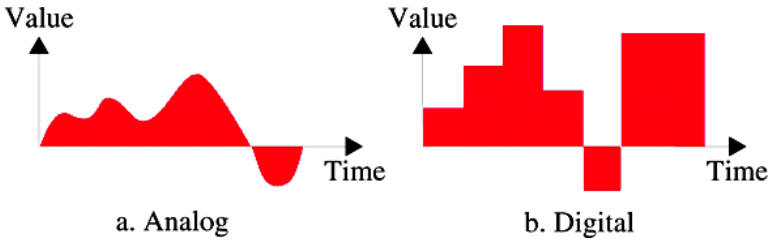
Periodic and Aperiodic Signals

Both analog and digital signals can take one of two forms: *periodic* or *aperiodic*.

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A period is defined as the amount of time required to complete one full cycle.



An aperiodic signal changes without exhibiting a pattern or cycle that repeats over time.



ANALOG SIGNALS

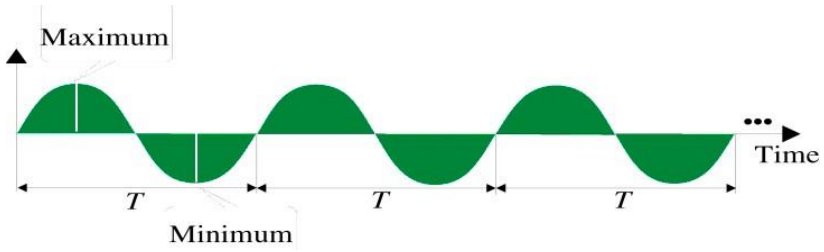
Analog signals can be classified as simple or composite. A simple analog signal, a sine wave, cannot be decomposed into simpler signals. A composite analog signal is composed of multiple sine waves.

Simple Analog Signal

The sine wave is the most fundamental form of periodic analog signal.

A Simple analog signal is a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow.

Each cycle consists of a single arc above the time axis followed by a single arc below it.



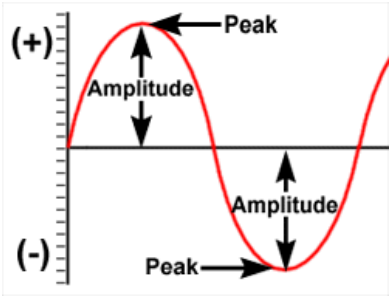
Sine Wave

Sine wave is described by three characteristics:

- ***Amplitude***
- ***Period and Frequency***
- ***Phase***

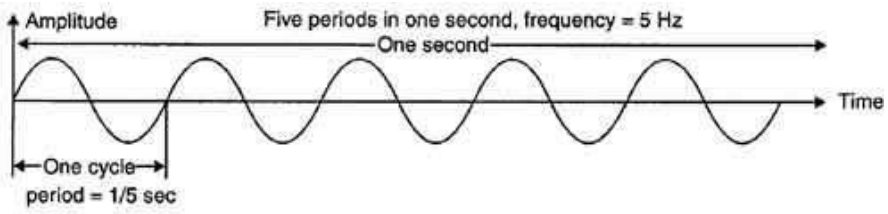
Amplitude

- Value of the signal at any point on the wave.
- It is equal to the vertical distance from a given point on the wave form to the horizontal axis.
- Maximum amplitude of a sine wave is equal to the highest value it reaches on the vertical axis.
- Amplitude is measured in either volts, amperes or watts.
- Volts refer to voltage, ampere refer to current, and watts refers to power.



Period and Frequency

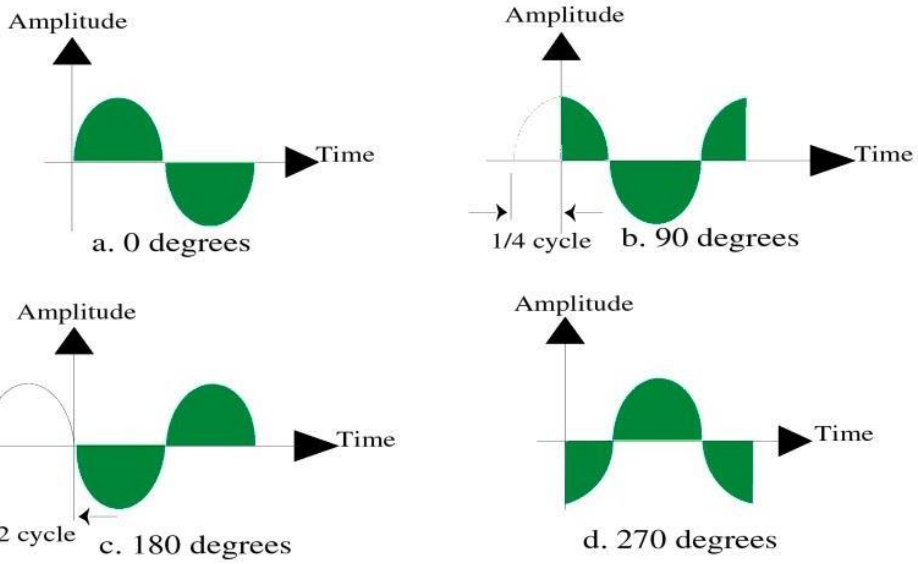
- Period refers to the amount of time, in seconds, a signal needs to complete one cycle.
- Frequency refers to the number of periods in one second. i.e., number of cycles per second.
- Unit of period is expressed in seconds.



Period and Frequency

Phase

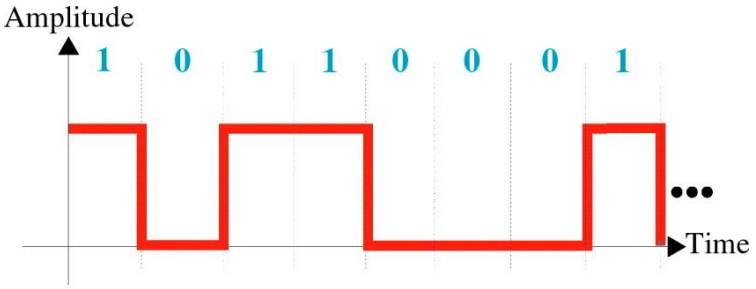
- Position of the waveform relative to time zero.
- Phase is measured in degrees or radians.



Digital Signal

- 1 can be encoded as a positive voltage and a 0 as negative voltage
- Bit Interval and Bit rate is used to describe digital signals.

Bit Rate and Bit Interval

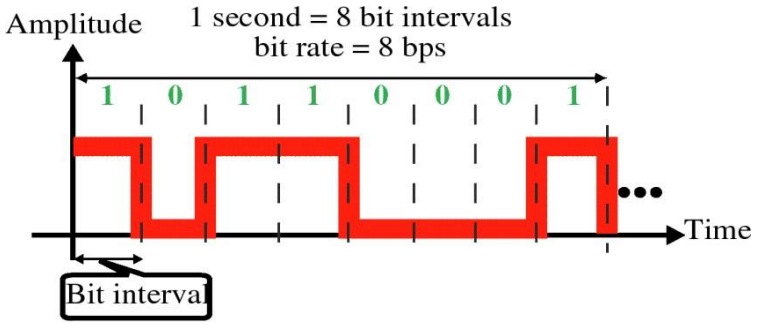


Bit Interval

- Time required to send one single bit.

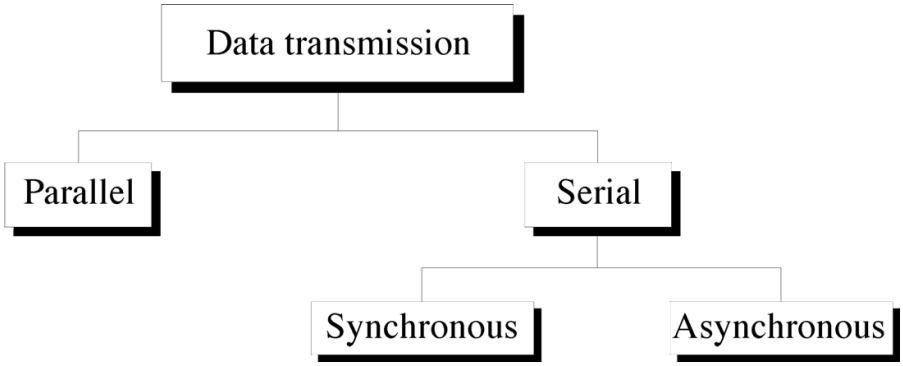
Bit rate

- Number of bit intervals per second.
- Expressed in bits per second (bps)



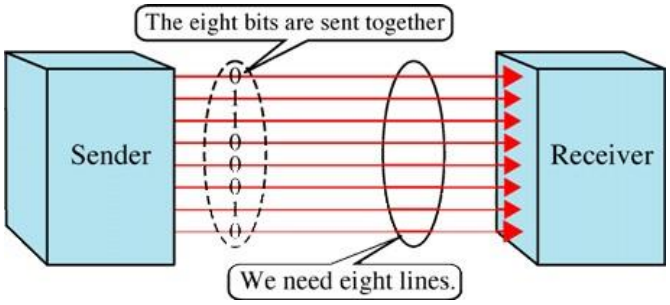
DIGITAL DATA TRANSMISSION

- The transmission of binary data across a link can be accomplished either in parallel mode or serial mode.
- In *parallel mode*, multiple bits are sent with each clock pulse.
- In *serial mode*, one bit is sent with each clock pulse.



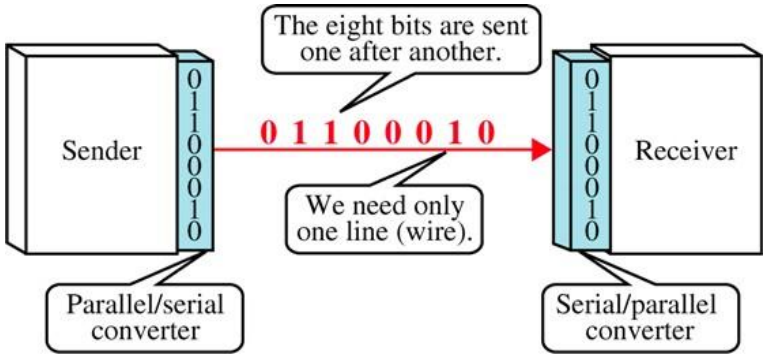
Parallel Transmission

- Binary data, consisting of 1s and 0s, may be organized into groups of *n* bits each.
- Sending *n* bits at a time instead of one is called parallel transmission.
- Uses *n* wires to send *n* bits at one time.
- **Advantage** of parallel transmission is **Speed**
- **Disadvantage** : **expensive** because, it requires *n* communication lines so it is limited to short distances.



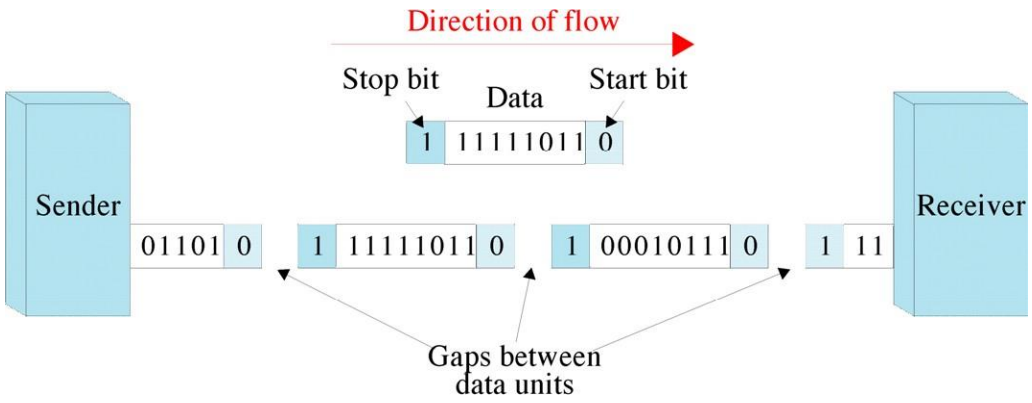
Serial Transmission

- One bit follows another.
- Require only one communication channel it reduces the cost of transmission over parallel.
- Since communication within devices is parallel, **conversion devices are required at the interface between the sender and the line** (parallel-to-serial) **and between the line and the receiver** (serial-to-parallel).
- ***Advantage* :** only one communication channel, so reduces the cost of transmission.
- Serial transmission occurs in two ways: **asynchronous, synchronous**



Asynchronous Transmission

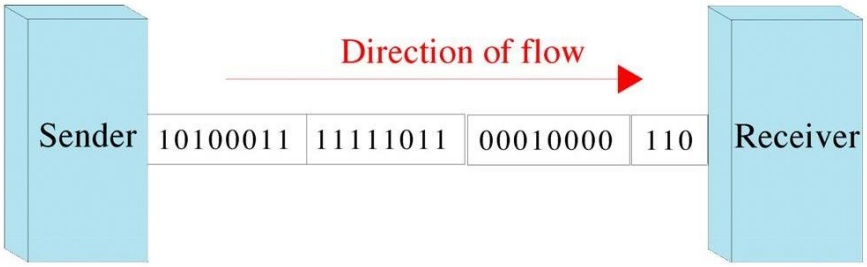
- In asynchronous transmission timing of the signal is unimportant.
- Information is **received and translated by agreed upon patterns**.
- **Patterns are based on grouping the bit stream into bytes**. Each group, **usually 8 bits**, is sent along the link as a unit.



- To alert the receiver to the arrival of a new group, an extra bit is added to the beginning of each byte. Usually a 0, is called the ***start bit***.
- To let the receiver know that the byte is finished, one or more additional bits are appended to the end of the byte. Usually 1s, are called ***stop bits***.
- Transmission of each byte may then be followed by a gap of varying duration. The gap can be represented either by an idle channel or by a stream of additional stop bits.
- *Advantage* : Cheap and effective in case of low-speed communication.

Synchronous Transmission

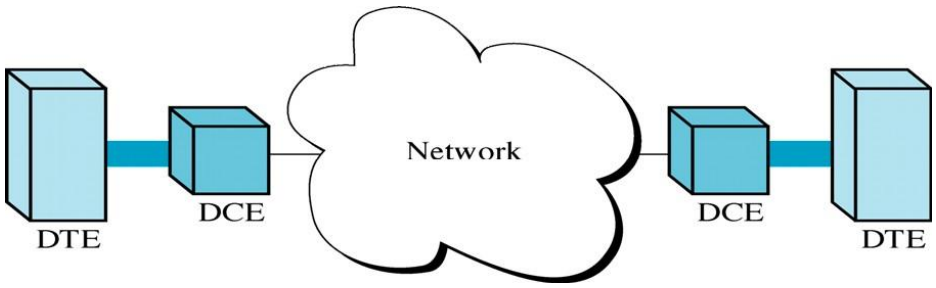
- The bit stream is combined into longer frames which may contain multiple bytes.
- Each byte is introduced on the transmission link without a gap between it and the next one.
- Data are transmitted as an unbroken string of 1s and 0s and the receiver separates that string into the bytes, or characters, it needs to reconstruct the information.
- Timing is very important.



- The accuracy of the received information is completely dependent on the ability of the receiving device to keep accurate count of the bits as they come in.
- Advantage : Speed.
- Most useful in high-speed applications like the transmission of data from one computer to another.
- Byte synchronization is accomplished in the data link layer.

DTEs and DCEs
Data Terminal Equipment / Data Circuit Terminating Equipment

- There are four basic functional units involved in the communication of data : a DTE and DCE on one end and a DCE and DTE on the other end.
- The DTE generates the data and passes them along with necessary control characters to a DCE.
- The DCE converts the signal to a format appropriate to the transmission medium and introduces it onto the network link.
- At the receiving end, this process is reversed.



Data Terminal Equipment (DTE)

- DTE includes any unit that functions either as a source of or as a destination for binary digital data.
- It can be a terminal, micro-computer, computer, printer, fax machine, or any device that generates or consumes digital data.
- DTEs do not communicate directly with one another, need an intermediary to be able to communicate.

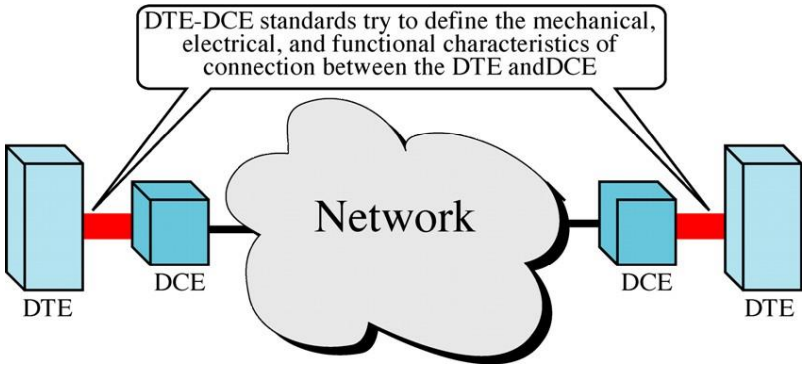
Data Circuit Terminating Equipment (DCE)

- DCE includes any functional unit that transmits or receives data in the form of an analog or digital signal through a network.
- At the physical layer, a DCE takes data generated by a DTE, converts them to an appropriate signal, and then introduces the signal onto the telecommunication link.
- Commonly used DCE is Modem.

DTE-DCE interface

Standards

- Many standards have been developed to define the connection between a DTE and a DCE.
- Each standard provides a model for the mechanical, electrical and functional characteristics of the connection.
- Organizations involved in DTE-DCE interface standards are : Electronic Industries Association (EIA), International Telecommunication Union - Telecommunication Standards Committee (ITU-T)
- The EIA standards are EIA-232, EIA-442, EIA-449 and so on.
- The ITU-T standards are V Series, X Series.



EIA-232 INTERFACE

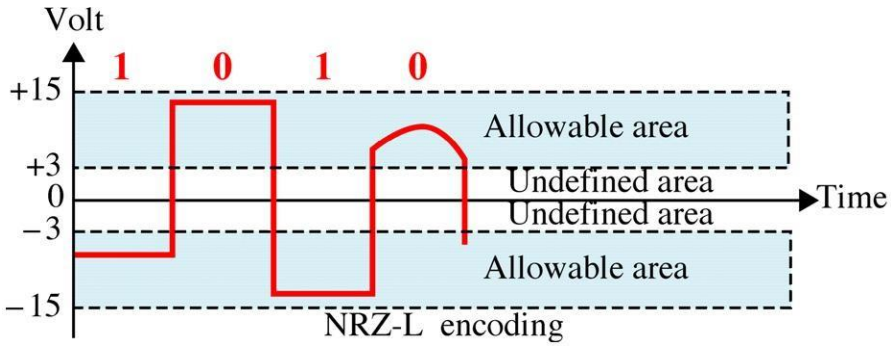
One important interface standard developed by EIA is the EIA-232, which defines the mechanical, electrical and functional characteristics of the interface between a DTE and DCE.

Mechanical Specification

- The mechanical specification of the EIA-232 standard defines the interface as a 25-wire cable with a male and a female DB-25 pin connector attached to either end.
- The length of the cable may not exceed 15 meters (about 50 feet).
- A **DB-25** connector is a plug with 25 pins or receptacles, each of which is attached to a single wire with a specific function.
- The term *male connector* refers to a plug with each wire in the cable connecting to *a* pin.
- The term *female connector* refers to a receptacle with each wire in the cable connecting to a metal tube, or sheath.
- In the DB-25 connector, these pins and tubes are arranged in two rows, with 13 on the top and 12 on the bottom.

Electrical Specification

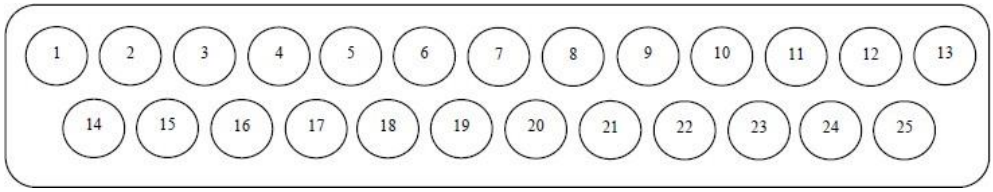
- The electrical specification of the standard defines the voltage levels and the type of signal to be transmitted in either direction between the DTE and the DCE.
- EIA-232 states that all data must be transmitted as 1s and 0s using NRZ-L encoding.
- with 0 defined as a positive voltage and 1 defined as a negative voltage.
- the amplitude of a signal must fall between 3 and 15 volts or between -3 and -15 volts to transmit data.
- Signals fall between -3 and 3 will not be recognised as data.



Control and Timing

- Only 4 wires out of the 25 available in an EIA-232 interface are used for data functions.
- The remaining 21 are reserved for functions like control, timing, grounding, and testing.
- Function is considered ON if it transmits a voltage of at least +3 and OFF if it transmits a voltage with a value less than -3 volts.
- The electrical specification of EIA-232 defines that signals other than data must be sent using OFF less than -3 volts and ON greater than +3 volts

Functions of pins in EIA-232, DB-25



1 Shield
2 Transmitted data
3 Received data
4. Request to send
5. Clear to send
6. DCE ready
7. Signal ground common return
8 Received line signal detector
9 Reserved (testing)
10 Reserved (testing)
11 Unassigned
12 Secondary received line signal detector
13 Secondary clear to send
14 Secondary transmitted data
15 Transmitter signal element timing (DCE-DTE)
16 Secondary received data
17 Receiver signal element timing (DCE-DTE)
18 Local loopback
19 Secondary request to send
20 DTE ready
21 Remote loopback & signal quality detector
22 Ring detector
23 Data signal rate select
24 Transmitter signal element timing (DTE- DCE)
25 Test mode

Functional Specification

Step 1 ***shows the preparation of the interfaces for transmission.***

- The two grounding circuits, 1 (shield) and 7 (signal ground), are active between both the sending computer/modem combination (left) and the receiving computer/modem combination (right).

Step 2 ***ensures that all four devices are ready for transmission.***

- First the sending DTE activates pin 20 and sends a DTE ready message to its DCE.
- The DCE answers by activating pin 6 and returning a DCE ready message.
- This same sequence is performed by the remote computer and modem.

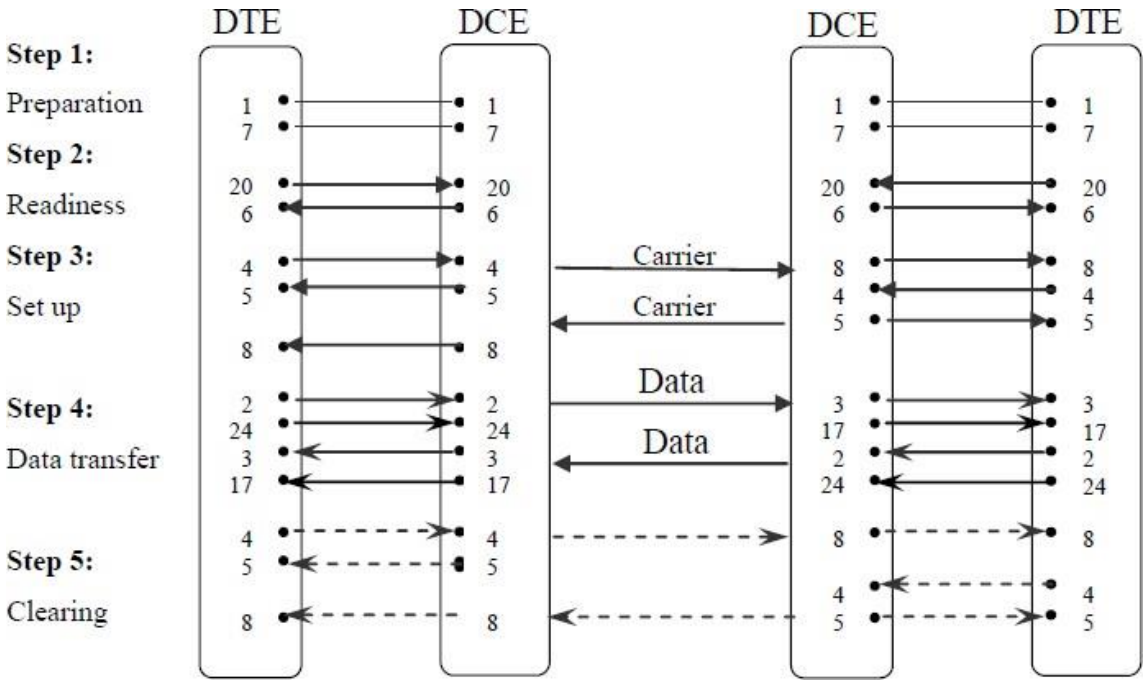
Step 3 *sets up the physical connection between the sending and receiving modems.*

- It is the first step that involves the network.
- First, the sending DTE activates pin 4 and sends its DCE a request-to-send message.
- The DCE transmits a carrier signal to the idle receiving modem.
- When the receiving modem detects the carrier signal, it activates pin 8, the received line signal detector, telling its computer that a transmission is about to begin.
- After transmitting the carrier signal, the sending DCE activates pin 5, sending its DTE a clear-to-send message.
- The remote computer and modem perform the same step.

Step 4 *is the data transfer procedure.*

- The initiating computer transfers its data stream to its modem over circuit 2, accompanied by the timing pulse of circuit 24.
- The modem converts the digital data to an analog signal and sends it out over the network.
- The responding modem retrieves the signal, converts it back into digital data and passes the data along to its computer via circuit 3, accompanied by the timing pulse of circuit 17.
- Likewise, the responding computer follows the same procedure in sending data to the initializing computer.

Step 5 Once both sides have completed their transmissions, both computers deactivate their request-to-send circuits; the modems turn off their carrier signals, their received line signal detectors (there is no longer any signal to detect), and their clear-to-send circuits.



2 Transmitted data 3 Received data

17 Receiver signal element timing

24 Transmitter signal element timing

1 Shield 4 Request to send

5 Clear to send 6 DCE ready

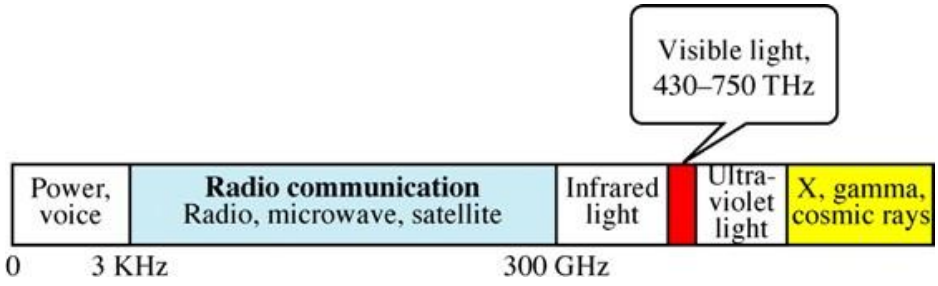
7 Signal ground 20 DTE ready

8 Received line signal detector

UNIT - III

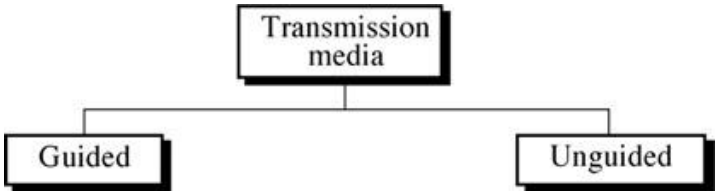
Transmission Media

- Data must be converted into electromagnetic signals to be transmitted from device to device
- Signals can travel through a vacuum, air, or other media
- May be in the form of power, voice, radio waves, infrared light, and X-rays, gamma rays, and cosmic rays
- Electromagnetic energy – combination of electrical and magnetic fields vibrating in relation to each other.
- Each of these forms constitutes a portion of the electromagnetic spectrum
- metal cables (Twisted Pair, Coaxial Cables) are suitable for Voice band frequencies
- Radio frequencies are transmitted through air or space
- Fiber optic cable transmits visible light. Light is an another form of electromagnetic signal



Electromagnetic Spectrum

Categories of Transmission Media



Broad categories:

- **Guided Media –** media with a physical boundary
  - Twisted pair, coaxial, and fiber-optic
- **Unguided Media –** no physical boundaries
  - Radio waves, infrared light, visible light, and X, gamma, and cosmic rays
  - Sent by microwave, satellite, and cellular transmission

Guided Media

- Guided Transmission media uses a cabling system that guides the data signals along a specific path.
- Guided media also known as Bounded media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- Out of these twisted-pair cable, coaxial cable transport signals in the form of electric signals and fiber-optic cable transport signals in the form of light.

Types:

1. Twisted-Pair Cable
2. Coaxial Cable
3. Fiber-Optic Cable

Twisted-Pair Cable

Twisted-pair cable comes in two forms:

- Unshielded Twisted-pair
- Shielded Twisted Pair

Unshielded Twisted Pair (UTP)

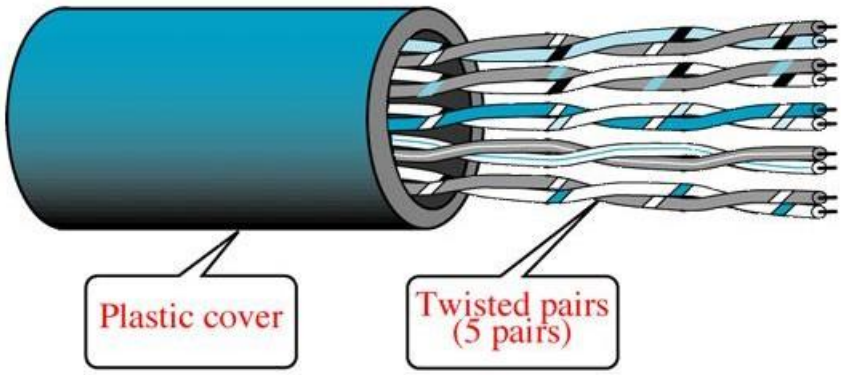
- UTP cable is the most common type of telecommunication medium used today.
- Its frequency range is suitable for transmitting both voice and data.
- A twisted pair consists of two conductors (usually copper), each with its own colored plastic insulation. The plastic insulation is color-banded for identification. Colors are used both to identify the specific conductors in a cable and to indicate which wires belong in pairs and how they relate to other pairs in a large bundle.
- The wires is twisted together in pairs.
- Frequency range is from 100 Hz to 5 MHz

Twisted-pair cable

The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into five categories. Categories are determined by cable quality, with 1 as the lowest and 5 as the highest.

- **Category 1:** The basic twisted-pair cabling used in telephone systems. This level of quality is suitable for voice and for low-speed data communication
- **Category 2:** The next higher grade, suitable for voice and for data transmission of up to 4 Mbps.

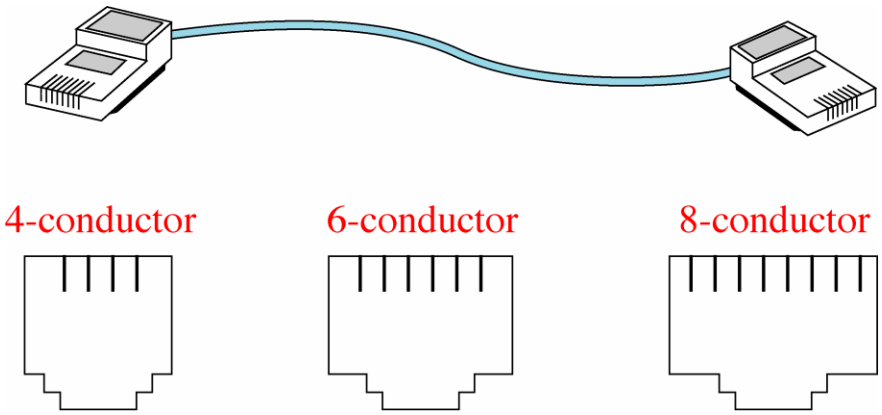
- **Category 3:** Required to have at least three twists per foot and can be used for data transmission up to 10 Mbps.
- **Category 4:** Have at least three twists per foot and possible to transmit up to 16 Mbps.
- **Category 5:** Used for data transmission up to 100 Mbps.



Cable with five unshielded twisted pairs of wires

UTP Connectors

UTP is most commonly connected to network devices via a type of snap-in plug like that used with telephone jacks. The connectors are either male (the pin) or female (the receptacle). Male connectors snap into female connectors and have a repressible tab (called key). Each wire is attached to one conductor (or pin). The most common UTP connector is RJ45 (RJ stands for registered jack).

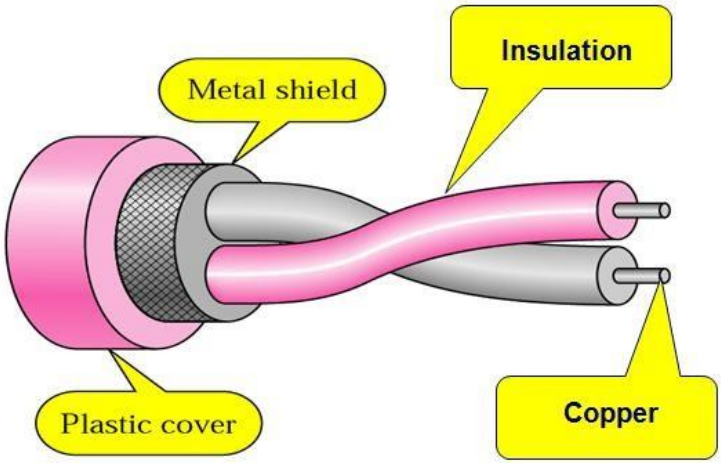


UTP Connectors

Shielded Twisted Pair (STP)

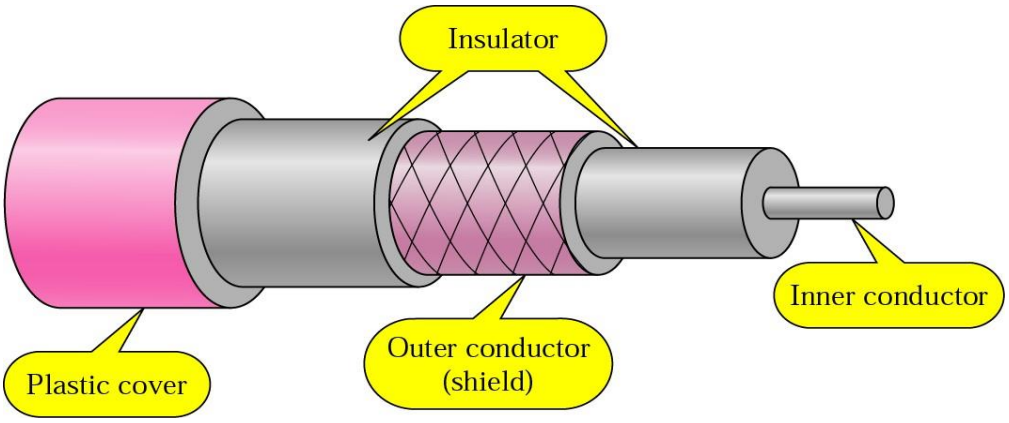
STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. The metal casing prevents the penetration of electromagnetic noise. It also can eliminate crosstalk, which is the undesired effect of one circuit on another circuit. It occurs

when one line picks up some of the signals travelling down another line. Shielding each pair of twisted pair cable can eliminate most crosstalk.



Coaxial Cable

Coaxial cable (or *coax)* carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



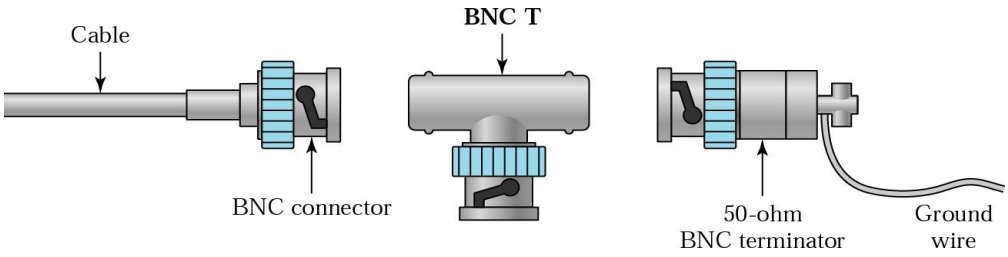
Coaxial cable standards

Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function. The following are a few of the common ones

- RG-8, RG-9, and RG-11 used in thick Ethernet
- RG-58 used in thin Ethernet
- RG-59 used for TV

Coaxial cable connectors

The most commonly used connector is a barrel connector. Of the barrel connector, the most popular is the bayonet network connector(BNC), which pushes on and locks into place with a half turn. All coaxial connectors have a single pin protruding from the center of the male connector that slides into a ferrule in the female connector. Coaxial connectors are familiar from cable TV and VCR hookups. Two other commonly used types of connectors are T-connectors and terminators. A T-connector allows a secondary cable or cables to branch off from a main line. A terminator absorbs the wave at the end and eliminates echo-back.

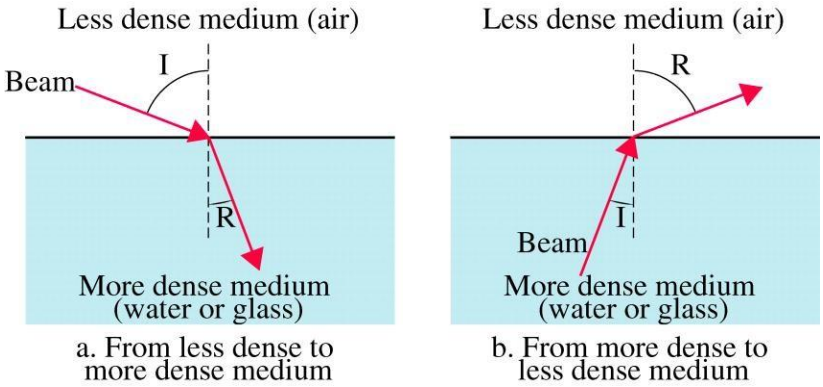


Coaxial cable connectors

Optical Fiber

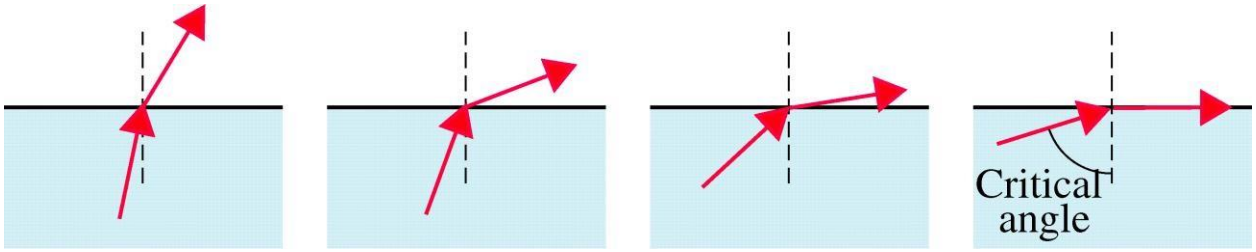
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. The change is called refraction. The two angles made by the beam of light in relation to the vertical axis are called I, for incident, and R for refracted.

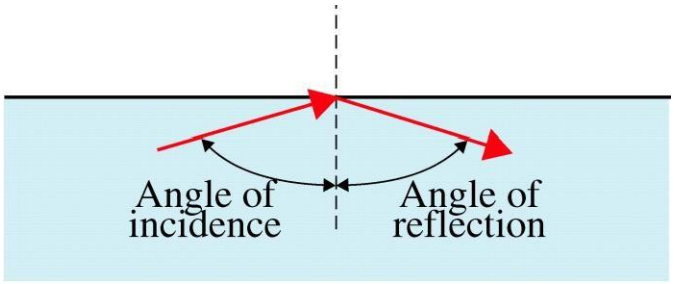


Refraction

As the following figure shows, if the angle of incidence I (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface. If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance.



Critical Angle

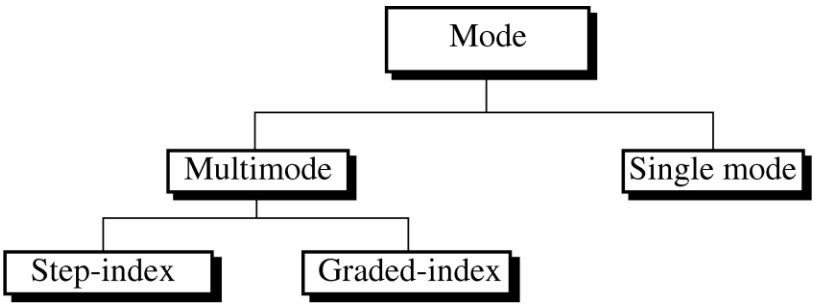


Reflection

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 the core is reflected off the cladding instead of being refracted into it.

Propagation Modes

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index.



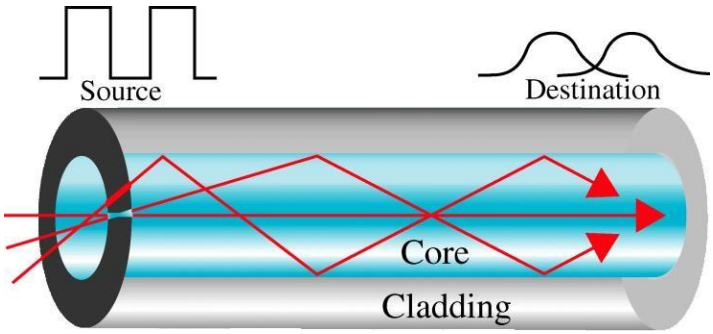
Propagation Modes

Multimode

Multimode is so named because multiple beams from a light source move through the core in different paths.

Multimode Step-Index

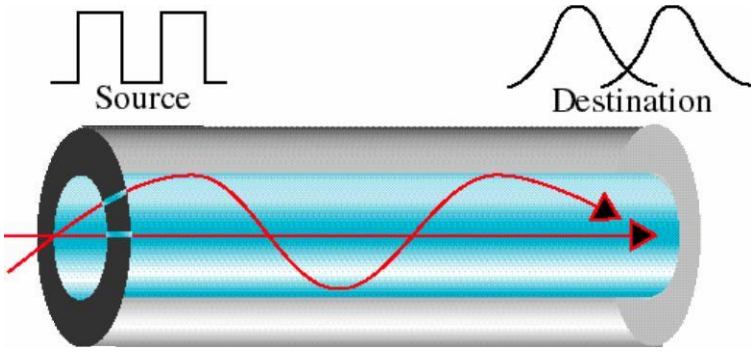
In multimode step-index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term *step index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.



Multimode Step-Index fiber

Multimode Graded-Index

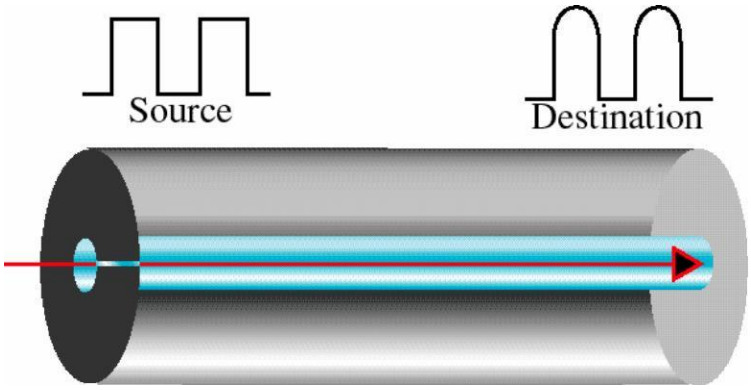
Multimode graded-index fiber, decreases this distortion of the signal through the cable. The word *index* here refers to the index of refraction. The index of refraction is related to density. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge.



Multimode Graded-Index fiber

Single-Mode

Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction). The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible. All the beams arrive at the destination "together" and can be recombined with little distortion to the signal

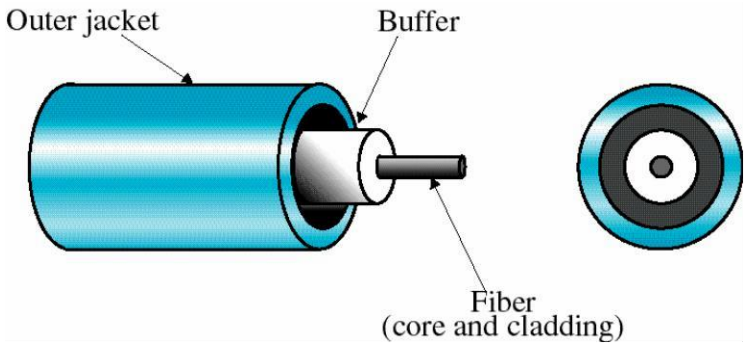


Single-mode fiber

Cable Composition

A core is surrounded by cladding, forming the fiber. The fiber is surrounded by a buffer layer that protects it from moisture. The entire cable is encased in an outer jacket.

Both core and cladding can be made of either glass or plastic with different densities. The outer jacket is made of either Teflon coating, plastic coating, fibrous plastic, metal tubing and metal mesh.



Fiber construction

Light sources for Optical Cable

For transmission to occur, the sending device must be equipped with a light source and the receiving device with a photo sensitive cell (called a photodiode) capable of translating the received light into current usable by a computer. The light source can be either a Light-Emitting-Diode(LED) or an Injection Laser Diode (ILD). LEDs are limited to short distance use. Laser signals can be transmitted to a longer distances.

Fiber-optic connectors

To connect fiber-optic cable barrel shaped connectors are popularly used and they come in male and female versions. A gap between two cores results in a dissipated signal; an overly tight connection can compress the two cores and alter the angle of reflection.

Advantages and Disadvantages of Optical Fiber

Advantages

Advantages Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial).

- **Noise resistance.** Since fiber-optic transmission uses light external electrical or electromagnetic interference will not affect the transmission except external light. The interference of external light could be blocked from the channel by the outer jacket.
- **Less signal attenuation.** Fiber-optic transmission distance is significantly greater than that of other guided media.
- **Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths than either twisted-pair or coaxial cable.

Disadvantages

There are some disadvantages in the use of optical fiber.

- **Cost.** The cable and the interfaces are relatively more expensive than those of other guided media.
- **Installation and maintenance.** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise.
- **Fragility.** Glass fiber is more easily broken than metal cables.

UNGUIDED MEDIA

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

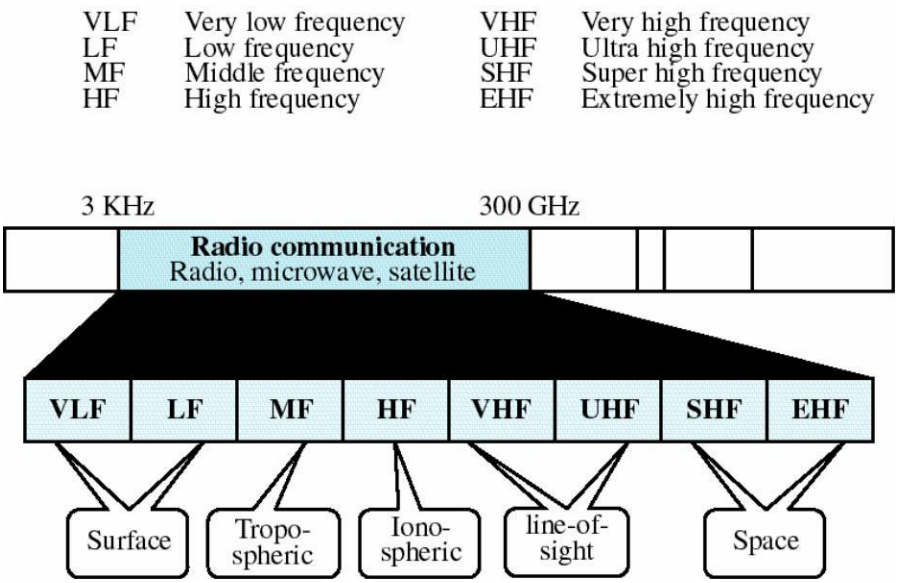
Radio Frequency Allocation

The section of the electromagnetic spectrum defined as radio communication is divided into eight ranges called bands, each regulated by government authorities.

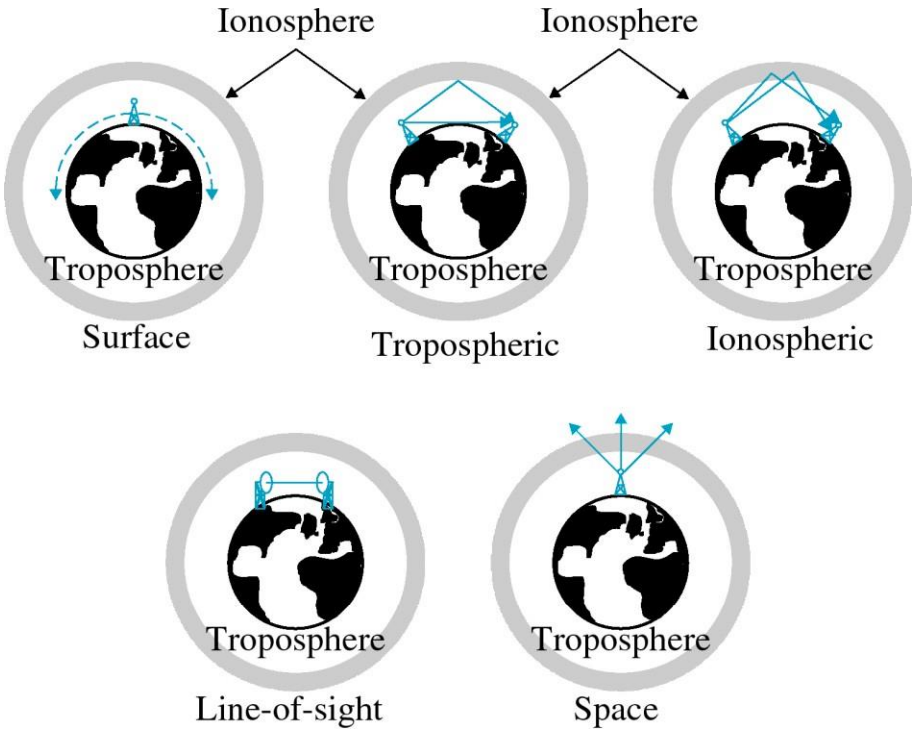
Propagation of Radio Waves

Types of propagation

Radio wave transmission utilizes five different types of propagation: surface, tropospheric, ionospheric, line-of-sight and space.



Radio Communication Band



Types of propagation

Surface propagation

In surface propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth.

Tropospheric propagation

Tropospheric propagation can work two ways. Either a signal can be directed in a straight line from antenna to antenna (line-of-sight), or it can be broadcast at an angle into the upper layers of the troposphere where it is reflected back down to the earth's surface.

Ionospheric propagation

In ionospheric propagation, higher frequency radio waves radiate upward into the ionosphere where they are reflected back to earth.

Line-of-sight propagation

In line-of-sight propagation, very high frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth.

Space propagation

Space propagation utilizes satellite relays in place of atmospheric refraction. A broadcast signal is received by an orbiting satellite, which rebroadcasts the signal to the intended receiver back on the earth.

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3-30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30-300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz-3 MHz	Sky	AM radio
HF (high frequency)	3-30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30-300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz-3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3-30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30-300 GHz	Line-of-sight	Radar, satellite

Terrestrial Microwave

Microwaves do not follow the curvature of the earth and therefore require line-of-sight transmission and reception equipment. The distance coverable by a line-of-sight signal depends to a large extent on the height of the antenna. Typically the antennas are mounted on towers that are in turn often mounted on hills ore mountains.

Microwave signals propagate in one direction at a time, which means that two frequencies are necessary for two-way communication such as telephone conversation. Each frequency requires its own transmitter and receiver, both the pieces of equipment usually are combined in a single piece of equipment called a transceiver, which allows a single antenna to serve both frequencies and functions.

Repeater

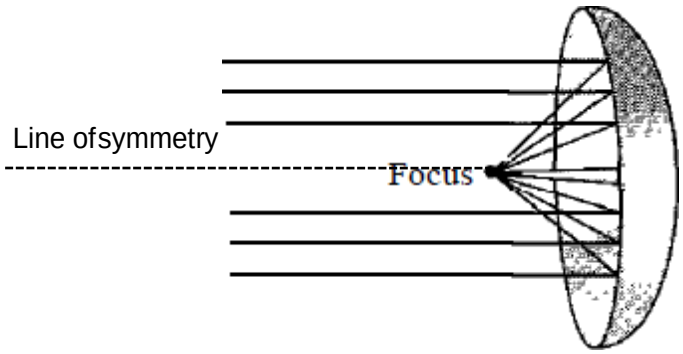
To increase the distance served by terrestrial microwave, a system of repeaters can be installed with each antenna. The distance required between repeaters varies with the frequency of the signal and the environment in which the antennas are found. A repeater may broadcast the regenerated signal either at the original frequency or at a new frequency, depending on the system.

Antennas

Two types of antennas are used for terrestrial microwave communications:

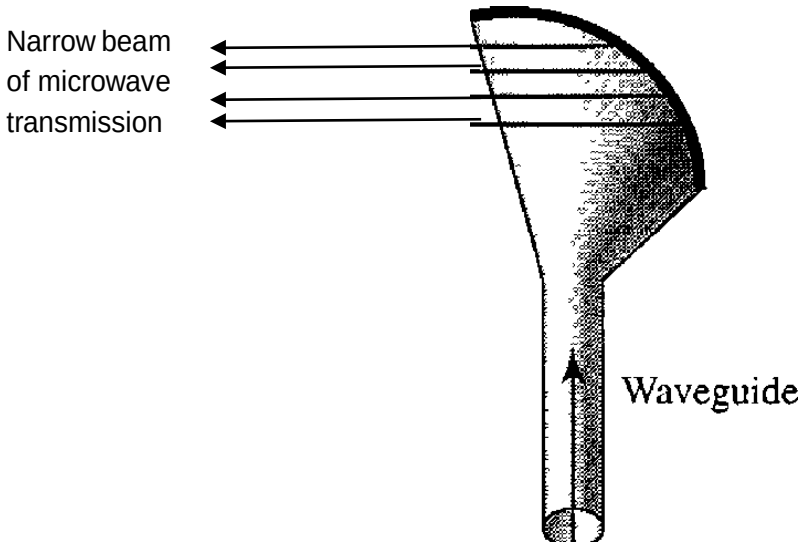
- Parabolic dish
- Horn

A **parabolic dish antenna** is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus. The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.



Parabolic dish antenna

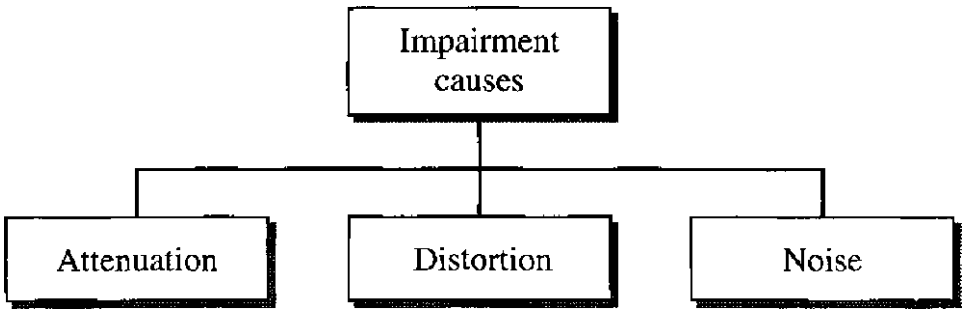
A **Horn antenna** looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem (resembling a handle) and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.



Horn Antenna

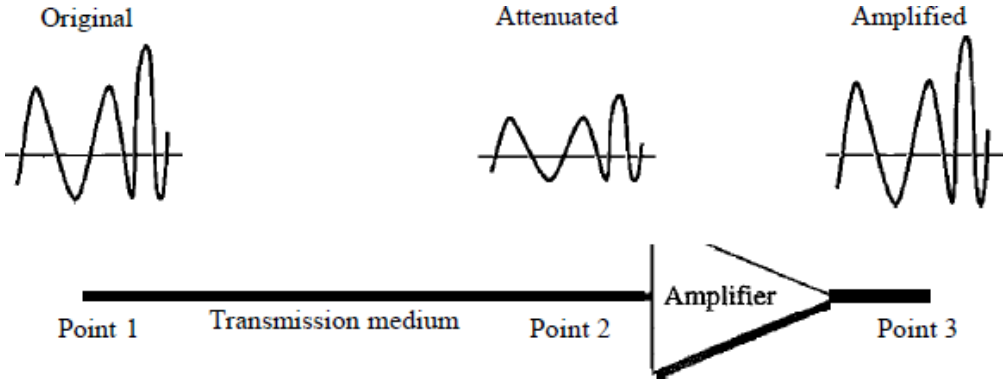
TRANSMISSION IMPAIRMENT

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise



Attenuation

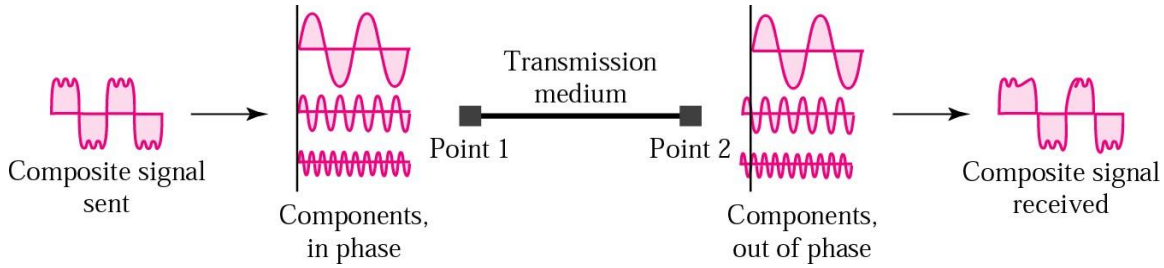
Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.



Attenuation

Distortion

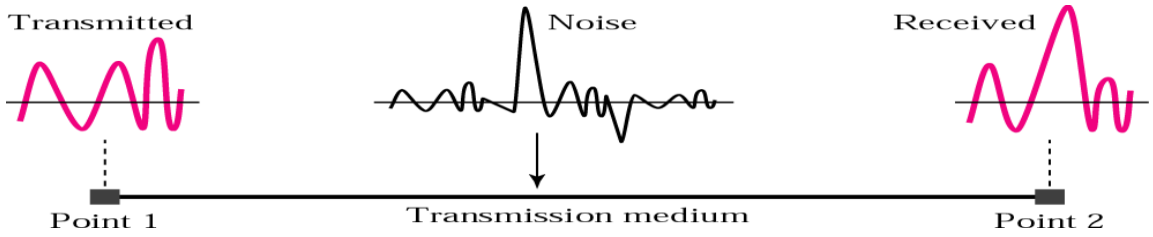
Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same.



Distortion

Noise

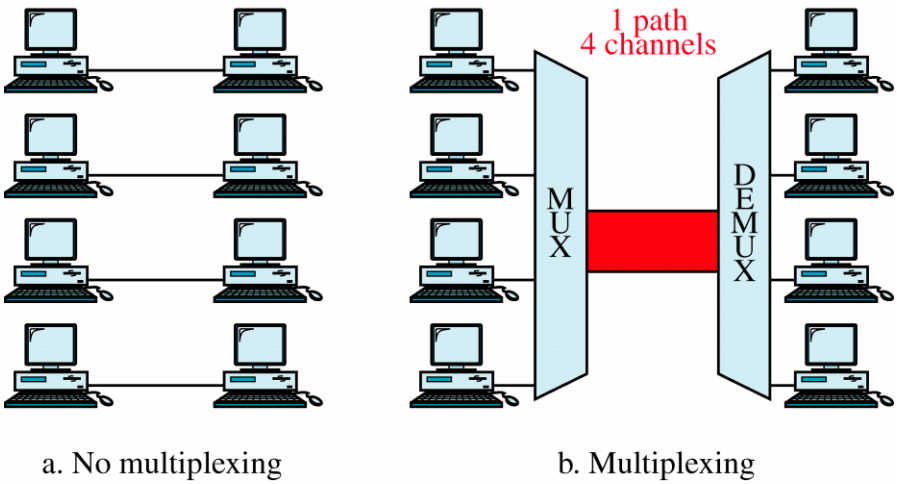
Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna. Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.



Noise

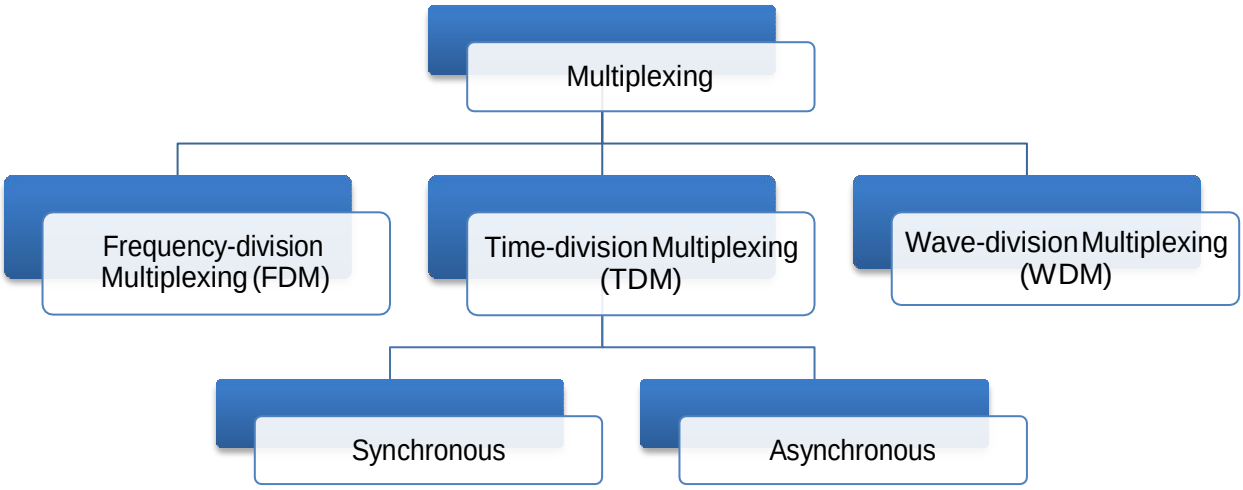
MULTIPLEXING

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. In a multiplexed system, *n* lines share the bandwidth of one link. The lines on the left direct their transmission streams to a multiplexer (MUX), which combines them into a single stream (many-to-one). At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines. In the figure, the word path refers to the physical link. The word channel refers to the portion of a path that carries a transmission between a given pair of lines. One path can have many *(n)* channels.



a. No multiplexing b. Multiplexing

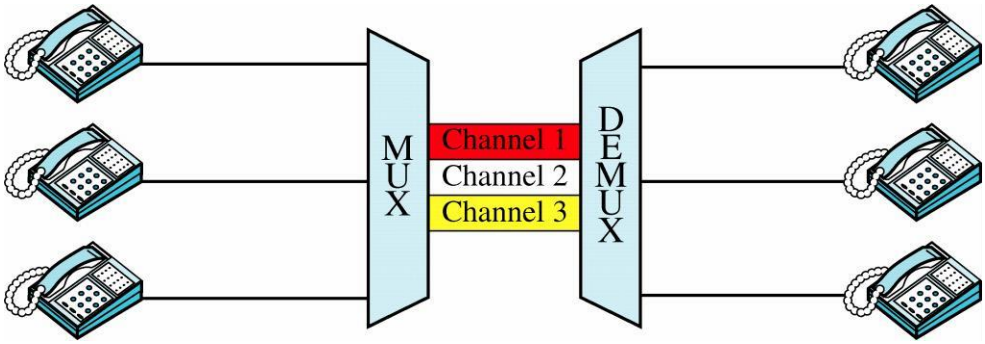
There are three basic multiplexing techniques: frequency-division multiplexing (FDM), time-division multiplexing (TDM) and wavelength-division multiplexing (WDM). TDM is further subdivided into synchronous TDM and asynchronous TDM, also called as statistical TDM or concentrator.



Categories of multiplexing

Frequency-Division Multiplexing

Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth (guard bands) to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original data frequencies.

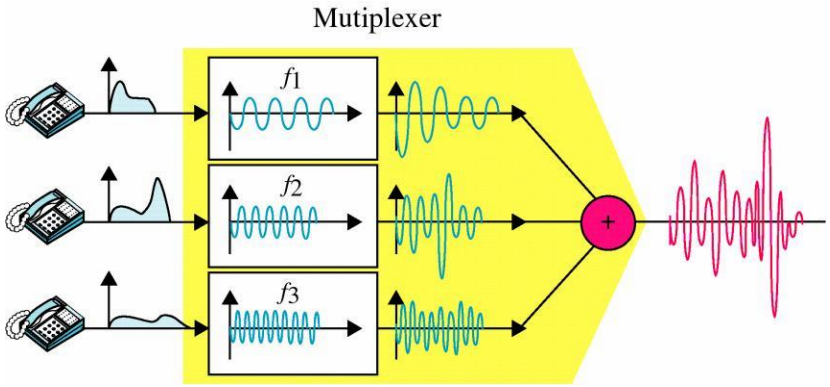


Frequency Division Multiplexing

FDM Process

Multiplexing Process

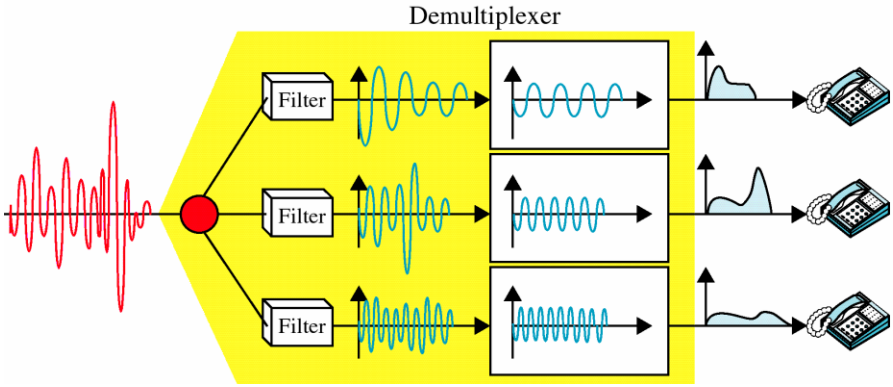
The following figure is a conceptual illustration of the multiplexing process. FDM is an analog process and it has been shown here using telephones as the input and output devices. Each telephone generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulates different carrier frequencies *(/1,12,* and *h).* The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.



FDM Multiplexing Process

Demultiplexing Process

The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines. The following figure is a conceptual illustration of demultiplexing process.

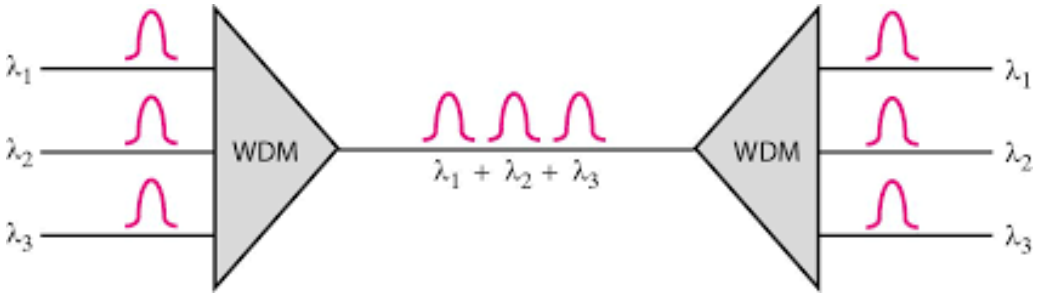


FDM Demultiplexing Process

Wavelength-Division Multiplexing

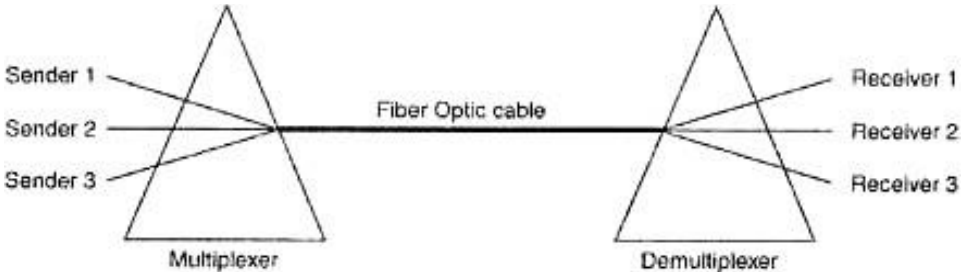
WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. Different signals of different frequencies are combined as one in WDM. The difference is that the frequencies are very high.

The following figure gives a conceptual view of a WDM multiplexer and demultiplexer. Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer.



Wave Division Multiplexing

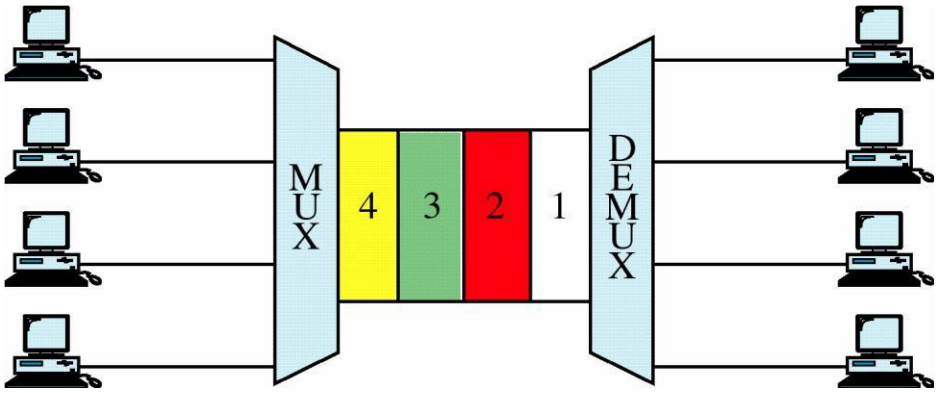
In WDM technology, multiple light sources are combined into one single light at the multiplexer and do the reverse at the demultiplexer. The combining and splitting of light sources are easily handled by a prism. Recall from basic physics that a prism bends a beam of light based on the angle of incidence and the frequency. Using this technique, a multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies. A demultiplexer can also be made to reverse the process.



Prisms in WDM multiplexing and demultiplexing

Time-Division Multiplexing

Time-Division Multiplexing is a digital process that can be applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending and receiving devices. TDM can be implemented in two ways: synchronous TDM and asynchronous TDM.



Time Division Multiplexing

Synchronous Time Division Multiplexing

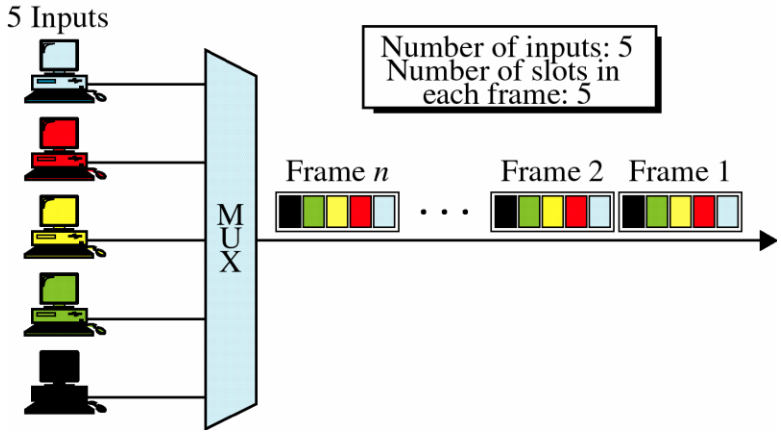
In synchronous TDM, each device is given same **time slot** to transmit the data over the link, irrespective of the fact that the device has any data to transmit or not. Hence the name Synchronous TDM. Synchronous TDM requires that the total speed of various input lines should not exceed the capacity of path.

Each device places its data onto the link when its **time slot** arrives *i.e.* each device is given the possession of line turn by turn.

If any device does not have data to send then its time slot remains empty.

The various time slots are organized into **frames** and each frame consists of one or more time slots dedicated to each sending device.

If there are *n* sending devices, there will be *n* slots in frame *i.e.* one slot for each device. As show in fig, there are 5 input devices, so there are 5 slots in each frame.



Synchronous TDM

Multiplexing Process in Synchronous TDM (STDM)

In STDM every device is given the opportunity to transmit a specific amount of data onto the link.

Each device gets its turn in fixed order and for fixed amount of time. This process is known as interleaving.

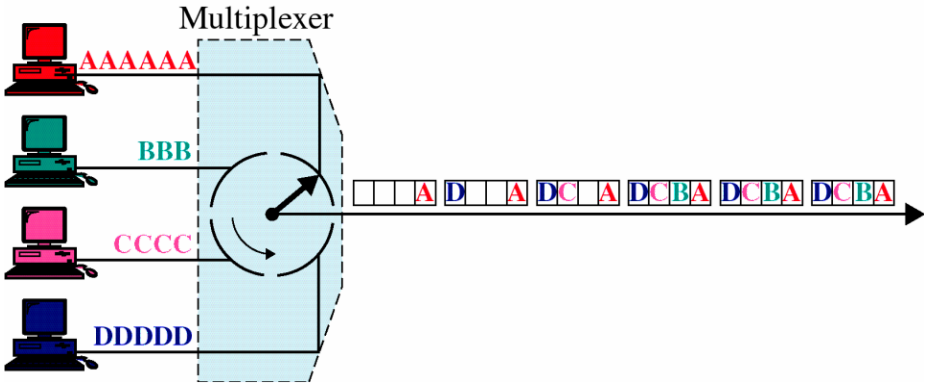
We can say that the operation of STDM is similar to that of a fast interleaved switch. The switch opens in front of a device; the device gets a chance to place the data onto the link.

Such an interleaving may be done on the basis of a hit, a byte or by any other data unit.

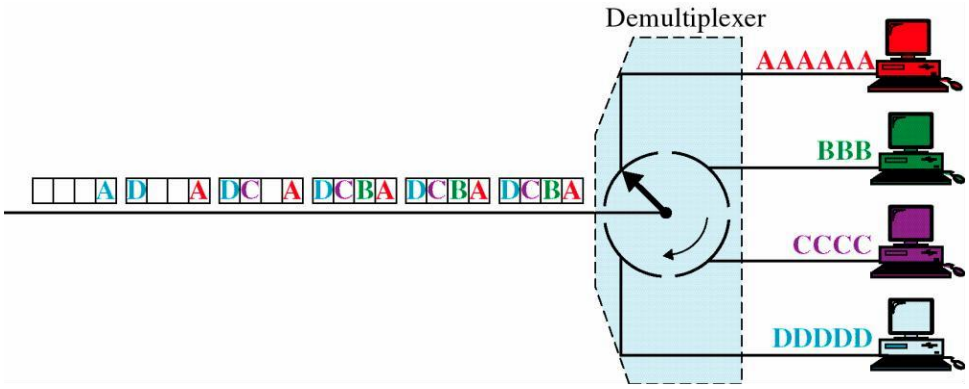
In STDM, the interleaved units are of same size *i.e.* if one device sends a byte, other will also send a byte and so on.

As shown in the fig. interleaving is done by a character (one byte). Each frame consists of four slots as there are four input devices. The slots of some devices go empty if they do not have any data to send.

At the receiver, demultiplexer decomposes each frame by extracting each character in turn. As a character is removed from frame, it is passed to the appropriate receiving device.



Multiplexing in STDM



Demultiplexing in STDM

Disadvantages of Synchronous TDM

The channel capacity cannot be fully utilized. Some of the slots go empty in certain frames. As shown in fig only first two frames are completely filled. The last three frames have 6 empty slot. It means out of 24 slots in all, 6 slots are empty. This wastes the l/4th capacity of links.

The capacity of single communication line that is used to carry the various transmission should be greater than the total speed of input lines.

Asynchronous TDM

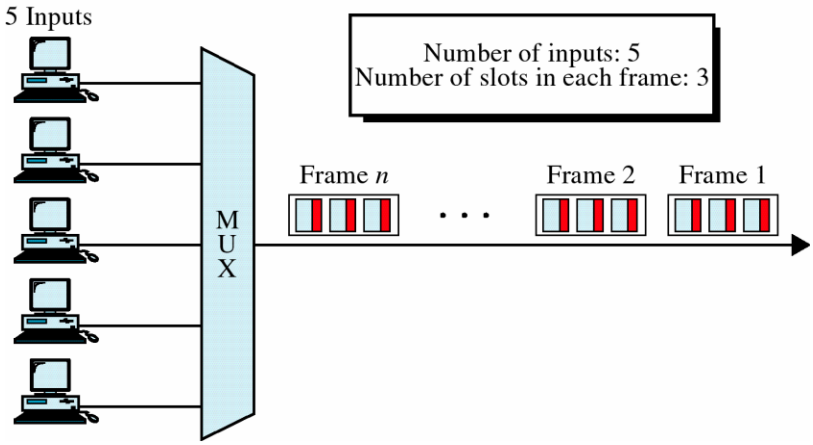
It is also known as statistical time division multiplexing.

Asynchronous TDM is called so because is this type of multiplexing, time slots are not fixed *i.e.* the slots are flexible.

Here, the total speed of input lines can be greater than the capacity of the path.

In synchronous TDM, if we have *n* input lines then there are *n* slots in one frame. But in asynchronous it is not so. In asynchronous TDM, if we have *n* input lines then the frame contains not more than *m* slots, with *m* less than *n (m < n)*.

In asynchronous TDM, the number of time slots in a frame is based on a statistical analysis of number of input lines.



Asynchronous TDM

In this system slots are not predefined, the slots are allocated to any of the device that has data to send.

The multiplexer scans the various input lines, accepts the data from the lines that have data to send, fills the frame and then sends the frame across the link.

If there are not enough data to fill all the slots in a frame, then the frames are transmitted partially filled.

Asynchronous Time Division Multiplexing is depicted in the following figure. Here we have five input lines and three slots per frame.

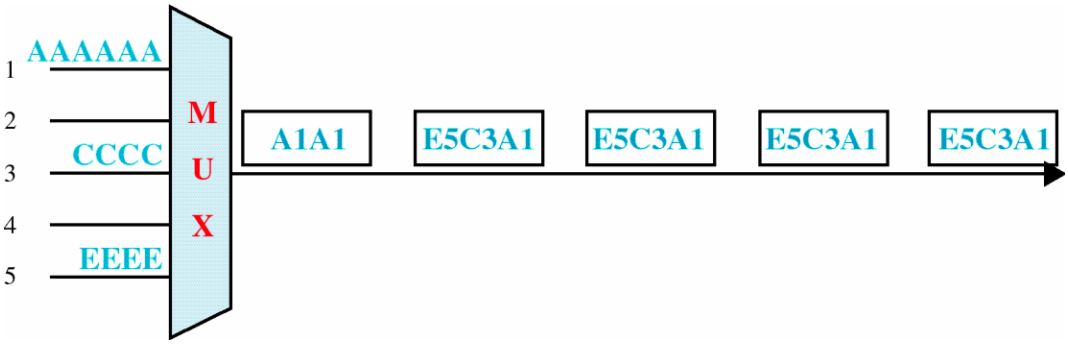
In Case 1, only three out of five input lines place data onto the link *i.e.* number of input lines and number of slots per frame are same.

In Case 2, four out of five input lines are active. Here number of input line is one more than the number of slots per frame.

In Case 3, all five input lines are active.

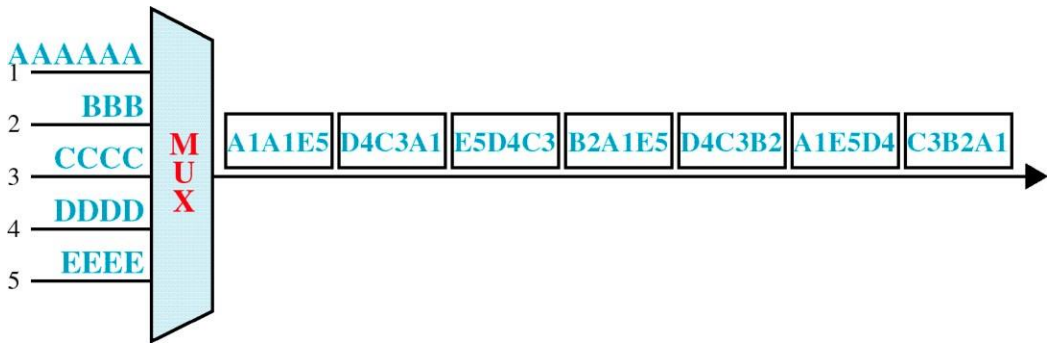
In all these cases, multiplexer scans the various lines in order and fills the frames and transmits them across the channel.

The distribution of various slots in the frames is not symmetrical. In case 2, device 1 occupies first slot in first frame, second slot in second frame and third slot in third frame.



Case 1: Only three lines sending data

Case 2: Only four lines sending data



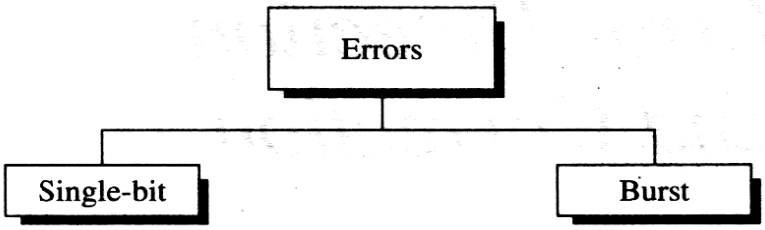
Case 3: All five lines sending data

ERROR DETECTION AND CORRECTION

Any time data are transmitted from one node to the next, they can become corrupted in passage. Many factors can alter one or more bits of a message. Some applications require a mechanism for detecting and correcting errors.

TYPES OF ERRORS

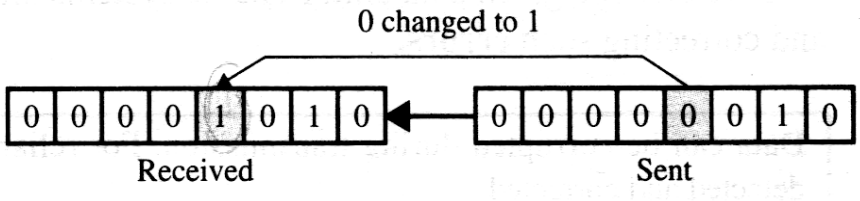
Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. In a single-bit error, a 0 is changed to a 1 or a 1 to a 0. In a burst error, multiple bits are changed.



Types of errors

Single-bit Error

The term *single-bit error* means that only one bit of given data unit (such as a byte, character, or data unit) is changed from 1 to 0 or from 0 to 1.



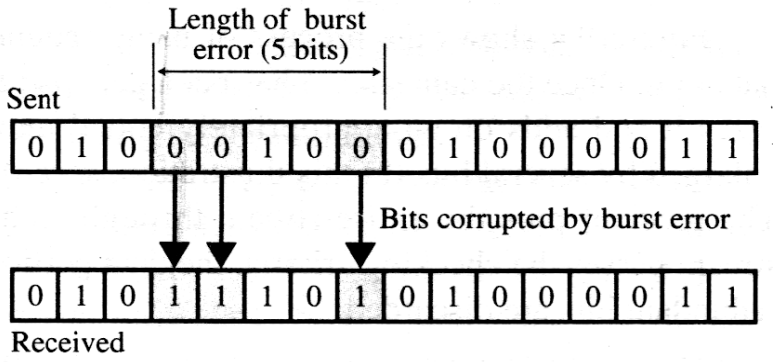
Single-bit error

Single bit errors are least likely type of errors in serial data transmission. However, a single-bit error can happen if we are having a parallel data transmission. For example, if 16 wires are used to send all 16 bits of a word at the same time and one of the wires is noisy, one bit is corrupted in each word.

Burst Error

The term *burst error* means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

The following figure shows the effect of a burst error on a data unit. In this case, 0100010001000011 was sent, but 0101110101100011 was received. Note that a burst error does not necessarily mean that the errors occur in consecutive bits. The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.



Burst error of length five

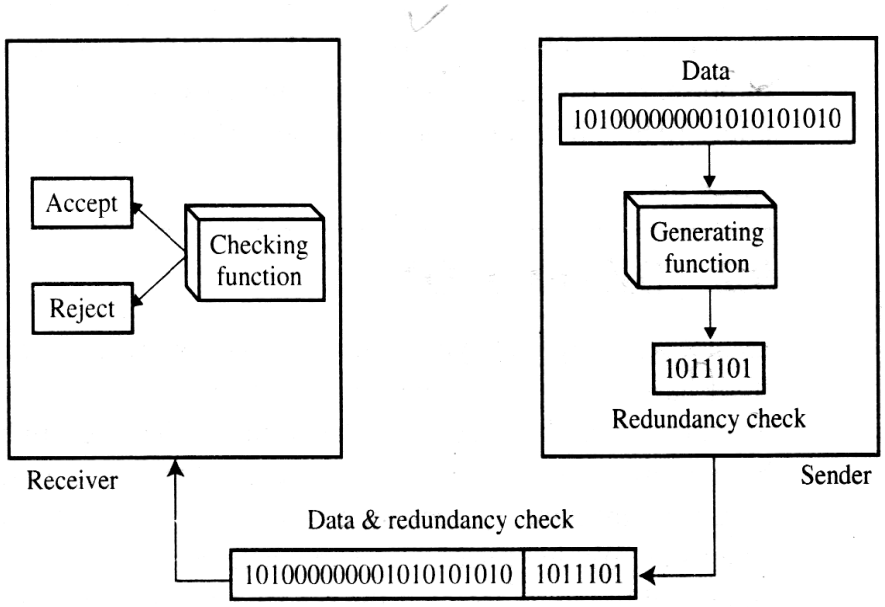
A burst error is more likely to occur than a single-bit error. The duration of noise is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits. The number of bits affected depends on the data rate and duration of noise.

DETECTION

Redundancy

One error detection mechanism that would satisfy these requirements would be to send every data unit twice. The receiving device would then be able to do a bit-for-bit comparison between the two versions of the data.

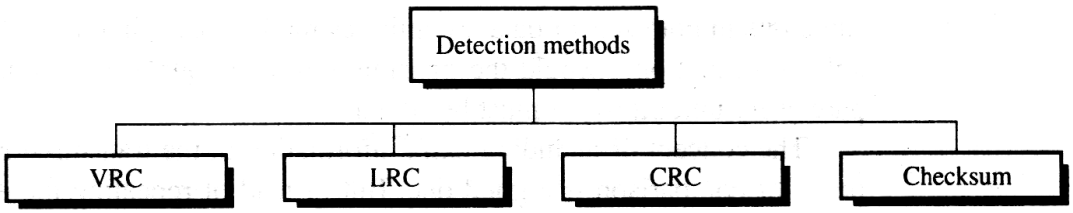
But instead of repeating the entire data stream, a shorter group of bits may be appended to the end of each unit. This technique is called **redundancy** because the extra bits are redundant to the information; they are discarded as soon as the accuracy of the transmission has been determined.



Redundancy

The above figure shows the process of using redundant bits to check the accuracy of a data unit. Once the data stream has been generated, it passes through a device that analyzes it and adds on an appropriately coded redundancy check. The data unit, now enlarged by several bits (in this illustration, seven), travels over the link to the receiver. The receiver puts the entire stream through a checking function. If the received bit stream passes the checking criteria, the data portion of the data unit is accepted and the redundant bits are discarded.

Four types of redundancy checks are used in data communications: vertical redundancy check (VRC) (also called parity check), longitudinal redundancy check (LRC), cyclical redundancy check (CRC), and checksum. The first three, VRC, LRC, ad CRC, are normally implemented in the physical layer for use in the data link layer. The fourth, checksum, is used primarily by upper layers.

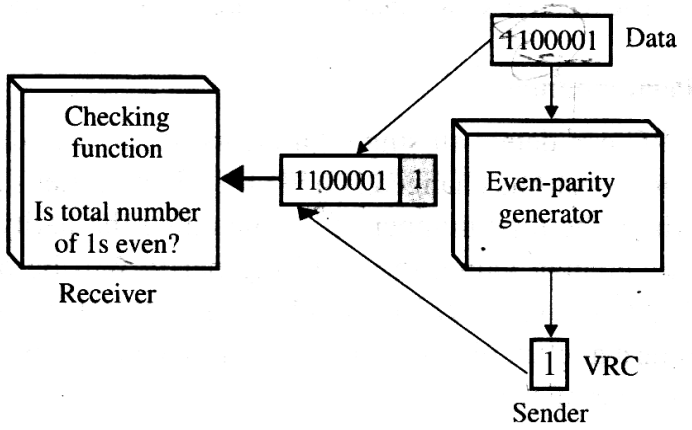


Detection Methods

Vertical Redundancy Check (VRC)

The most common and least expensive mechanism for error detection is the **vertical redundancy check (VRC),** often called a parity-check. In this technique, a redundant bit, called a **parity bit,** is appended to every data unit so that the total number of 1's in the unit (including the parity bit) becomes even.

Suppose we want to transmit the binary data unit 1100001 [ASCII *a* (97)]. Adding together the number of 1's gives us 3, an odd number. Before transmitting, we pass the data unit through a parity generator. The parity generator counts the 1's and appends the parity bit (a 1 in this case) to the end. The total number of 1' is now four, an even number. The system now transmits the entire expanded unit across the network link. When it reaches its destination, the receiver puts all eight bits through an even-parity checking function. If the receiver sees 11100001, it counts four 1's, an even number, and the data unit passes. If the data unit has been damaged in transit, instead of 11100001, the receiver sees 11100101, then, when the parity checker counts the 1's, it gets *5*, an odd number. The receiver knows that an error has been introduced into the data somewhere and therefore rejects the whole unit.

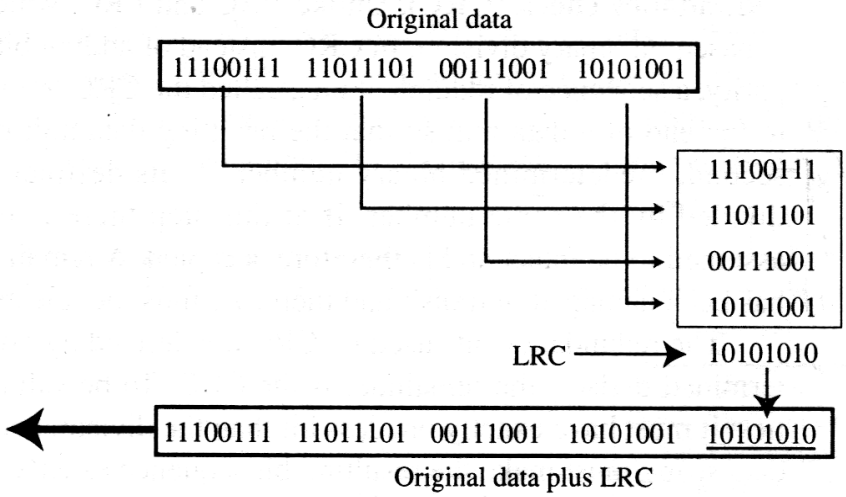


Even parity VRC concept

Longitudinal Redundancy Check (LRC)

In **longitudinal redundancy check (LRC)**, a block of bits is organized in a table (rows and columns). For example, instead of sending a block of 32 bits, it is organized as a table made of four rows and eight columns, as shown in the following figure. Then the parity bit for each column is calculated and a new row is created of eight bits, which are the parity bits for the whole block. The first parity bit in the fifth row is calculated based on all first bits. The second

parity bit is calculated based on all second bits, and so on. Then the eight parity bits are attached to the original data and send them to the receiver.



LRC

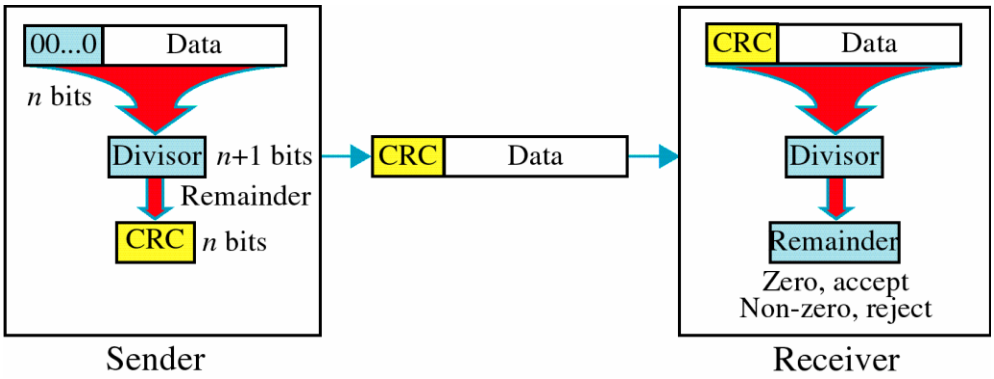
Performance

LRC increases the likelihood of detecting burst errors. A burst error of more than *n* bits is also detected by LRC with a very high probability. There is, however, pattern of errors that remains elusive. If two bits in one data unit are damaged and two bits *in exactly the same positions* in another data unit are also damaged, the **LRC** checker will not detect an error. Consider, for example, two data units: 11110000 and 11000011. If the first and last bits in each of them are changed, making the data units read *0*1110000*1* and *0*1000011*0*, the errors cannot be detected by LRC.

Cyclic Redundancy Check (CRC)

The third and most powerful of the redundancy checking techniques is the cyclic **redundancy check (CRC)**. CRC is based on binary division. In CRC, instead of adding bits together to achieve a desired parity, a sequence of redundant bits, called the CRC or the CRC remainder, is appended to the end of a data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be intact and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

The redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor; the remainder is the CRC. To be valid, a CRC must have two qualities: it must have exactly one less bit than the divisor, and appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor. The following figure provides an outline of the three basic steps.



CRC generator and checker

First, a string of n 0s is appended to the data unit. The number n is one less than the number of bits in the predetermined divisor, which is $n + 1$ bits.

Second, the newly elongated data unit is divided by the divisor using a process called binary division. The remainder resulting from this division is the CRC.

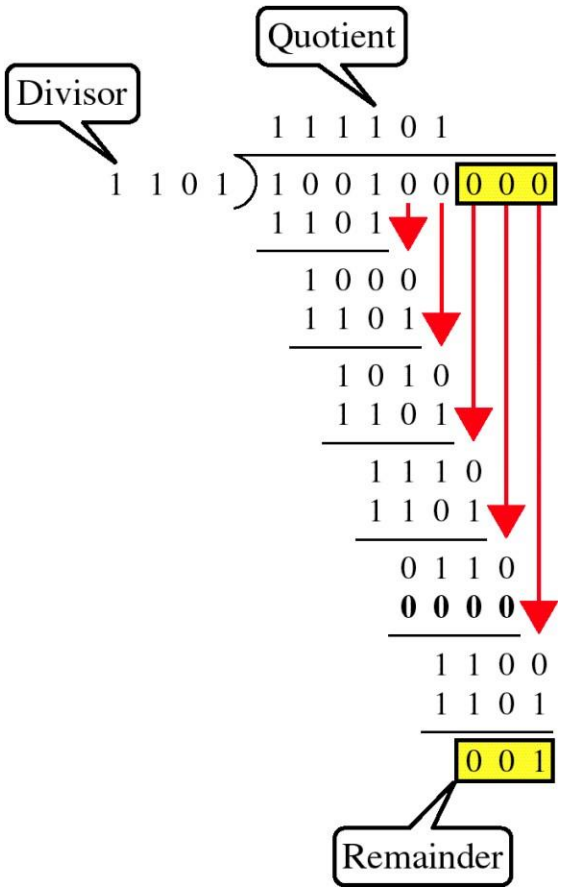
Third, the CRC of n bits derived in step 2 replaces the appended Os at the end of the data unit. Note that the CRC may consist of all 0s.

The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole string as a unit and divides it by the same divisor that was used to find the CRC remainder.

If the string arrives without error, the CRC checker yields a remainder of zero and the data unit passes. If the string has been changed in transit, the division yields a nonzero remainder and the data unit does not pass.

The CRC Generator

A CRC generator uses modulo-2 division. The following figure shows this process. In the first step, the four-bit divisor is subtracted from the first four bits of the dividend. Each bit of the divisor is subtracted from the corresponding bit of the dividend without disturbing the next higher bit. In our example, the divisor, 1101, is subtracted from the first four bits of the dividend, 1001, yielding 100 (the leading 0 of the remainder is dropped off).



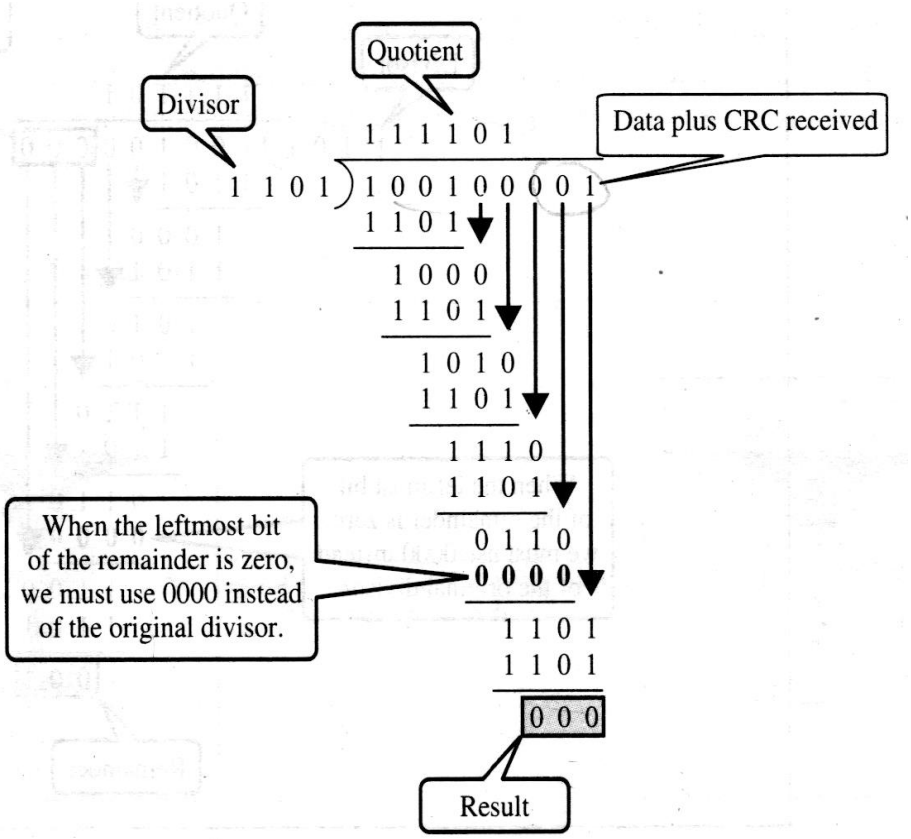
Binary division in a CRC generator

The next unused bit from the dividend is then pulled down to make the number of bits in the remainder equal to the number of bits in the divisor. The next step, therefore, is 1000 - 1101, which yields 101, and so on.

In this process, the divisor always begins with a 1; the divisor is subtracted from a portion of the previous dividend/remainder that is equal to it in length; the divisor can only be subtracted from a dividend/remainder whose leftmost bit is 1. Anytime the leftmost bit of the dividend/remainder is 0, a string of Os, of the same length as the divisor. replaces the divisor in that step of the process.

The CRC Checker

A CRC checker functions exactly like the generator. After receiving the data appended with the CRC, it does the same modulo-2 division. If the remainder is all 0s, the CRC is dropped and the data accepted; otherwise, the received stream of bits is discarded and data are resent. The following figure shows the same process of division in the receiver. We assume that there is no error. The remainder is therefore all 0s and the data are accepted.



Binary division in CRC checker

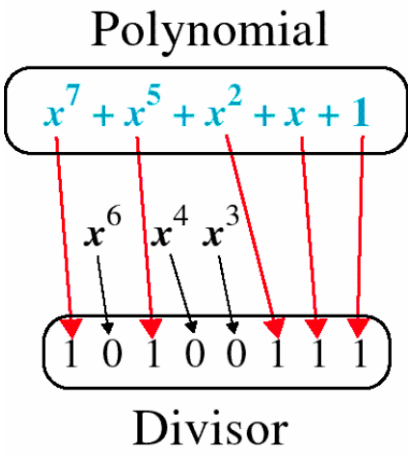
Polynomials

The CRC generator (the divisor) is most often represented not as a string of 1's and O's, but as an algebraic polynomial. The polynomial format is useful for two reasons: It is short, and it can be used to prove the concept mathematically.

$$x^7 + x^6 + x^4 + x^3 + x + 1$$

A polynomial

The relationship of a polynomial to its corresponding binary representation is shown in the following figure.

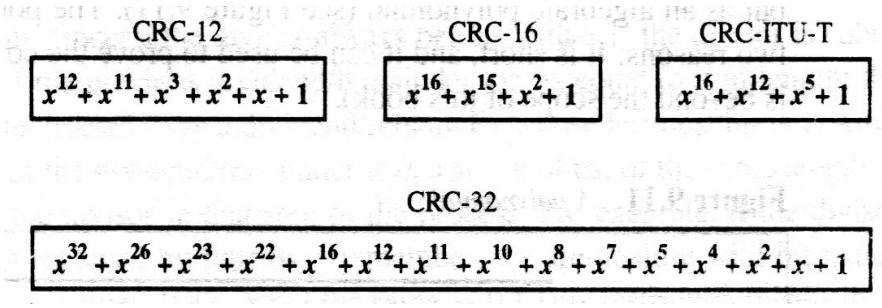


A polynomial representing a divisor

A polynomial should be selected to have at least the following properties:

- It should not be divisible by x.
- It should be divisible by (x + 1).

The first condition guarantees that all burst errors of a length equal to the degree of the polynomial are detected. The second condition guarantees that all burst errors affecting an odd number of bits are detected.



Standard polynomials

Performance

CRC is a very effective error detection method. If the divisor is chosen according to the previously mentioned rules,

- CRC can detect all burst errors that affect an odd number of bits.
- CRC can detect all burst errors of length less than or equal to the degree of the polynomial.
- CRC can detect with a very high probability burst errors of length greater than the degree of the polynomial.

CHECKSUM

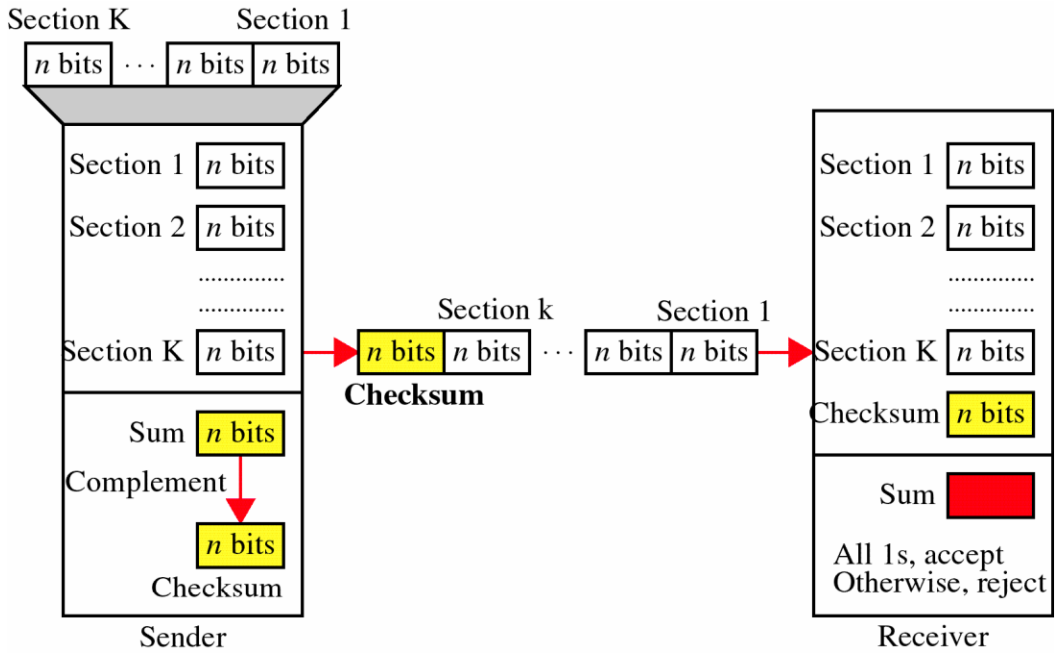
The error detection method used by the higher-layer protocols is called checksum. Like VRC, LRC, and CRC, checksum is based on the concept of redundancy.

Checksum Generator

In the sender, the checksum generator subdivides the data unit into equal segments of *n* bits (usually 16). These segments are added together using one's complement arithmetic (see Appendix C) in such a way that the total is also *n* bits long. That total (sum) is then complemented and appended to the end of the original data unit as redundancy bits, called the checksum field. The extended data unit is transmitted across the network. So if the sum of the data segment is *T*, the checksum will be *–T*.

Checksum Checker

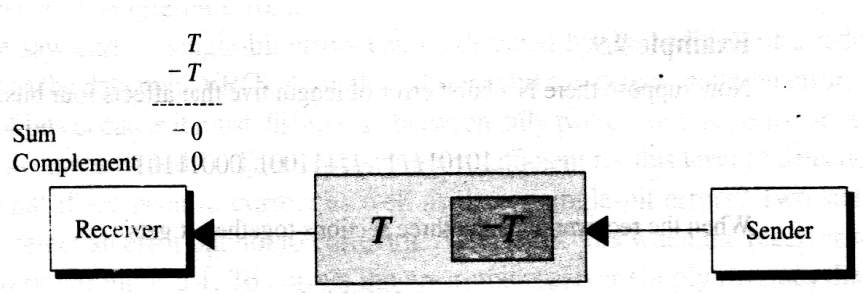
The receiver subdivides the data unit as above and adds all segments together and complements the result. If the extended data unit is intact, the total value found by adding the data segments and the checksum field should be zero. If the result is not zero, the packet contains an error and the receiver rejects it.



Checksum

The sender follows these steps:

- The unit is divided into *k* sections, each of *n* bits.
- All sections are added together using one's complement to get the sum.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data.



Data unit and Checksum

The receiver follows these steps:

- The Unit is divided into *k* sections, each of *n* bits.
- All sections are added together using one's complement to get the sum.
- The sum is complemented.
- If the result is zero, the data are accepted: otherwise, they are rejected.

Performance

The checksum detects all errors involving an odd number of bits, as well as most errors involving an even number of bits. However, if one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of those columns will not change and the receiver will not detect a problem. If the last digit of one segment is a 0 and it gets changed to a 1 in transit, then the last 1 in another segment must be changed to a 0 if the error is to go undetected. In LRC, two 0s could both change to is without altering the parity because carries were discarded. Checksum retains all carries; so, although two 0s becoming ls would not alter the value of their own column, they would change the value of the next higher column. But anytime a bit inversion is balanced by an opposite bit inversion in the corresponding digit of another data segment, the error is invisible.

ERROR CORRECTION

Error correction can be handled in two ways. In one, when an error is discovered, the receiver can have the sender retransmit the entire data unit. In the other, a receiver can use an error-correcting code, which automatically corrects certain errors.

Single-Bit Error Correction

The concept underlying error correction can be most easily understood by examining the simplest case: single-bit errors.

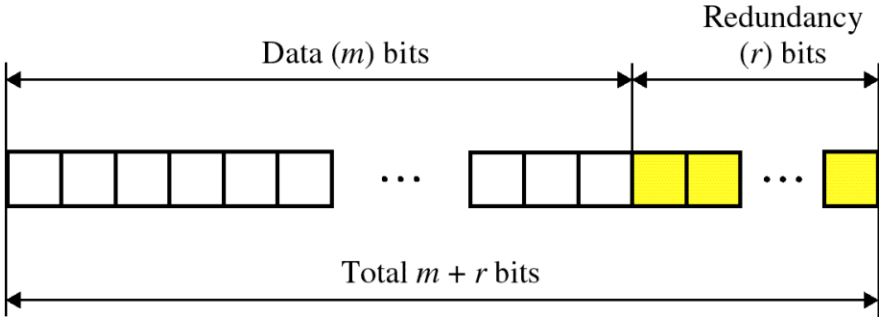
Single-bit errors can be detected by the addition of a redundant (parity) bit to the data unit (VRC). A single additional bit can detect single-bit errors in any sequence of bits because it must distinguish between only two conditions: error or no error. A bit has two states (0 and 1). These two states are sufficient for this level of detection.
But what if we want to correct as well as detect single-bit errors? Two states are enough to detect an error but not to correct it. An error occurs when the receiver reads a 1 bit as a 0 or a 0 bit as a 1. To correct the error, the receiver simply reverses the value of the altered bit. To do so,

however, it must know which bit is in error. The secret of error correction, therefore, is to locate the invalid bit or bits.

For example, to correct a single-bit error in an ASCII character, the error correction code must determine which of the seven bits has changed. In this case, we have to distinguish between eight different states: no error, error in position 1, error in position 2, and so on, up to error in position 7. To do so requires enough redundancy bits to show all eight states. A three-bit redundancy code can show eight different states (000 to 111) and can therefore indicate the locations of eight different possibilities. But what if an error occurs in the redundancy bits themselves? Seven bits of data (the ASCII character) plus three bits of redundancy equals 10 bits. Three bits, however, can identify only eight possibilities. Additional bits are necessary to cover all possible error locations.

Redundancy Bits

To calculate the number of redundancy bits (r) required to correct a given number of data bits (m), we must find a relationship between m and r. If the total number of bits in a transmittable unit is m + r, then r must be able to indicate at least m + r + 1 different states. Of these, one state means no error and m + r states indicate the location of an error in each of the m + r positions.



Data and redundancy bits

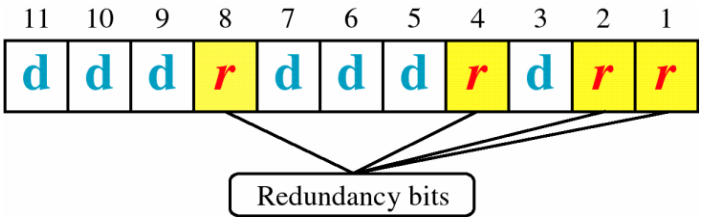
So, m + r + 1 states must be discoverable by r bits; and r bits can indicate 2^r different states. Therefore, 2' must be equal to or greater than m + r + 1:

$$2^r \geq m + r + 1$$

Hamming Code

Positioning the Redundancy Bits

The Hamming code can be applied to data units of any length and uses the relationship between data and redundancy bits. For example, a seven-bit ASCII code requires four redundancy bits that can be added to the end of the data unit or interspersed with the original data bits. In the following figure, these bits are placed in positions 1, 2. 4, and 8 (the positions in an 11-bit sequence that are powers of 2). For clarity in the examples below, we refer to these bits as r_1, r_2, r_4, and r_8.



Positions of redundancy bits in Hamming code

In the Hamming code, each r bit is the VRC bit for one combination of data bits: r_1 is the VRC bit for one combination of data bits, r_2 is the VRC bit for another combination of data bits, and so on. The combinations used to calculate each of the four r values for a seven-bit data sequence are as follows:

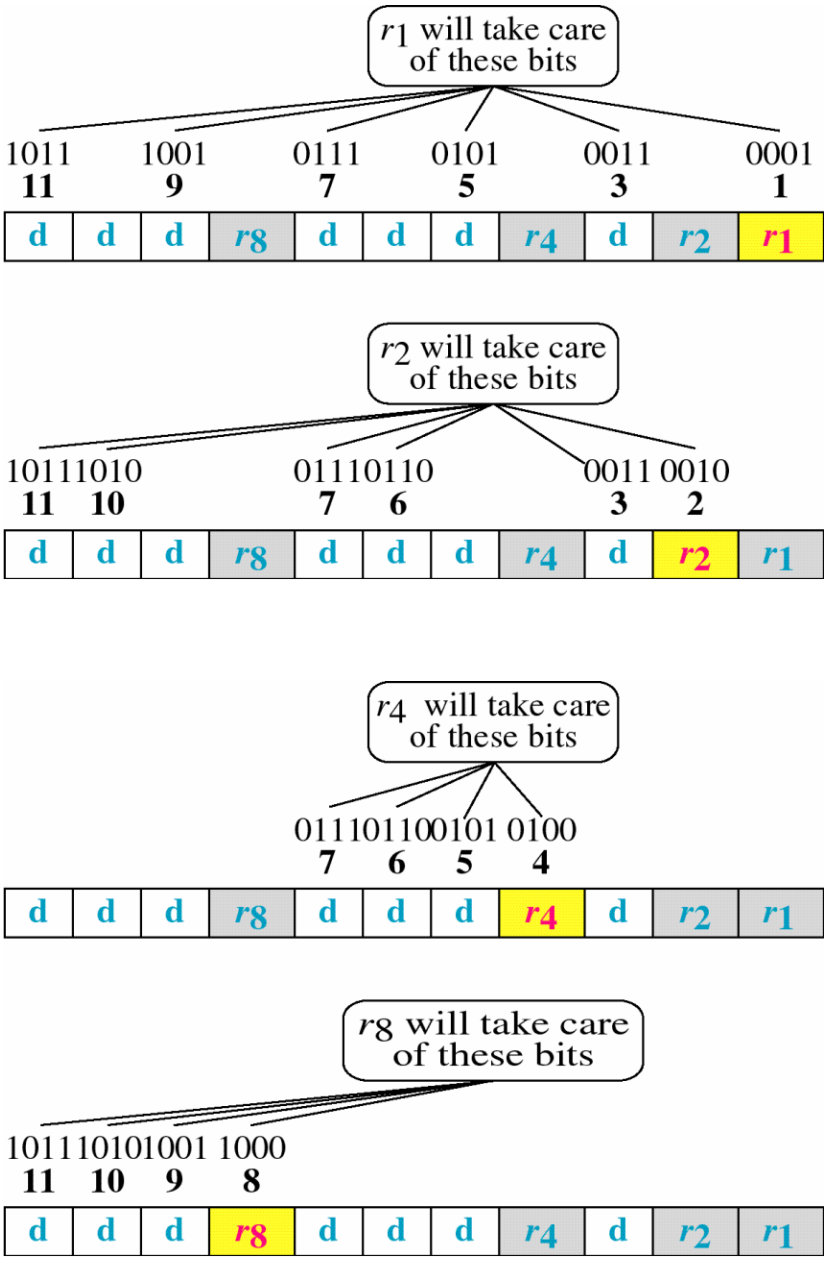
r_1: bits 1, 3, 5, 7, 9, 11

r_2: bits 2, 3, 6, 7, 10, 11

r_4: bits 4, 5, 6, 7

r_8: bits 8, 9, 10, 11

Each data bit may be included in more than one VRC calculation. In the sequences above, for example, each of the original data bits is included in at least two sets, while the r bits are included in only one. To see the pattern behind this strategy, look at the binary representation of each bit position. The r_1 bit is calculated using all bit positions whose binary representation includes a 1 in the rightmost position. The r_2 bit is calculated using all bit positions with a 1 in the second position, and so on.



Redundancy bits calculation

Calculating the r Values

The following figure shows a Hamming code implementation for an ASCII character. In the first step, we place each bit of the original character in its appropriate position in the 11-bit unit. In the subsequent steps, we calculate the even parities for the various bit combinations. The parity value for each combination is the value of the corresponding r bit. For example, the value of r_1 is calculated to provide even parity for a combination of bits 3, 5, 7, 9, and 11. The value of

r_2 is calculated to provide even parity with bits 3, 6, 7, 10, and 11, and so on. The final 11-bit code is sent through the transmission line.

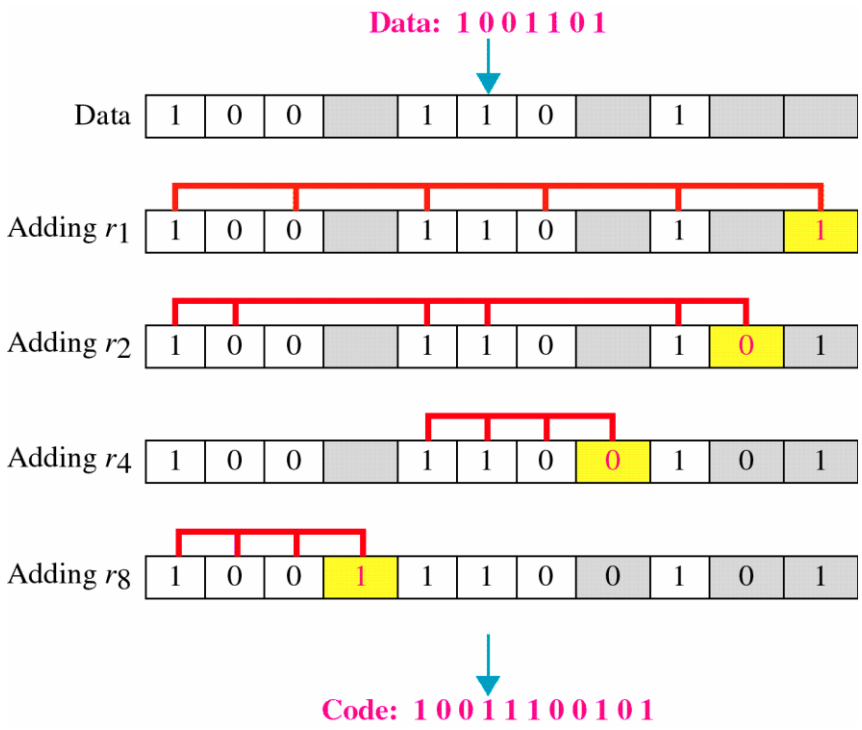
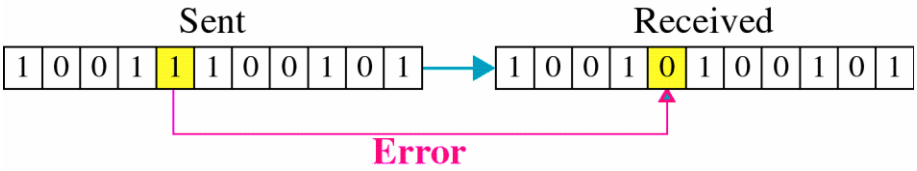


Figure 9.19 Example of redundancy bit calculation

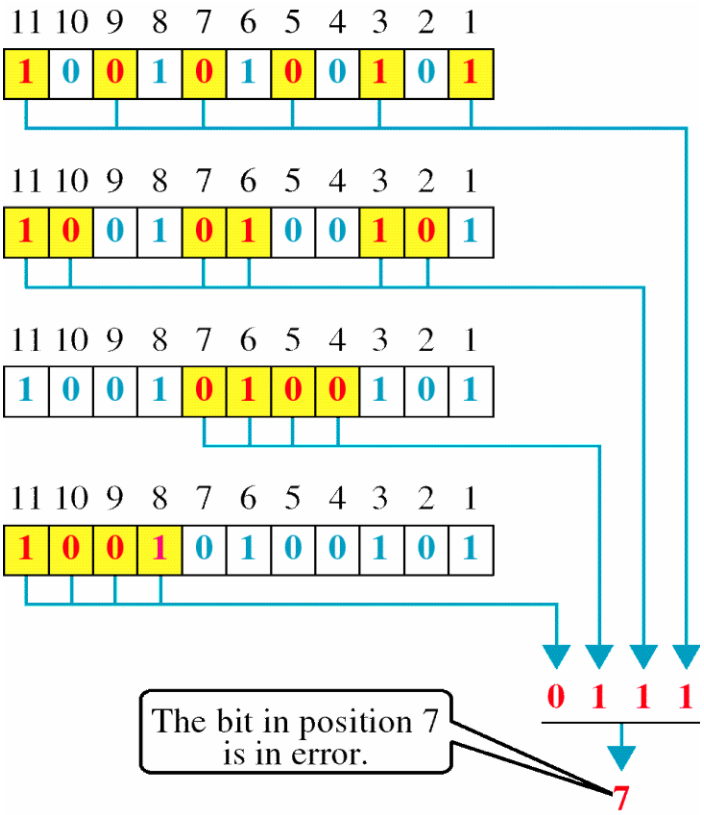
Error Detection and Correction

Consider that by the time the above transmission is received, the number 7 bit has been changed from 1 to 0.



Single-bit error

The receiver takes the transmission and recalculates four new VRCs using the same sets of bits used by the sender plus the relevant parity (r) bit for each set. Then it assembles the new parity values into a binary number in order of r position (r_8, r_4, r_2, r_1). In our example, this step gives us the binary number 0111 (7 in decimal), which is the precise location of the bit in error. Once the bit is identified, the receiver can reverse its value and correct the error.



Error detection using Hamming code

Burst Error Correction

A Hamming code can be designed to correct burst errors of certain lengths. The number of redundancy bits required to make these corrections, however, is dramatically higher than that required for single-bit errors. To correct double-bit errors, for example, we must take into consideration that the two bits can be a combination of any two bits in the entire sequence. Three-bit correction means any three Nis in the entire sequence, and so on. So the simple strategy used by the Hamming code to correct single-bit errors must be redesigned to be applicable for multiple-bit correction.

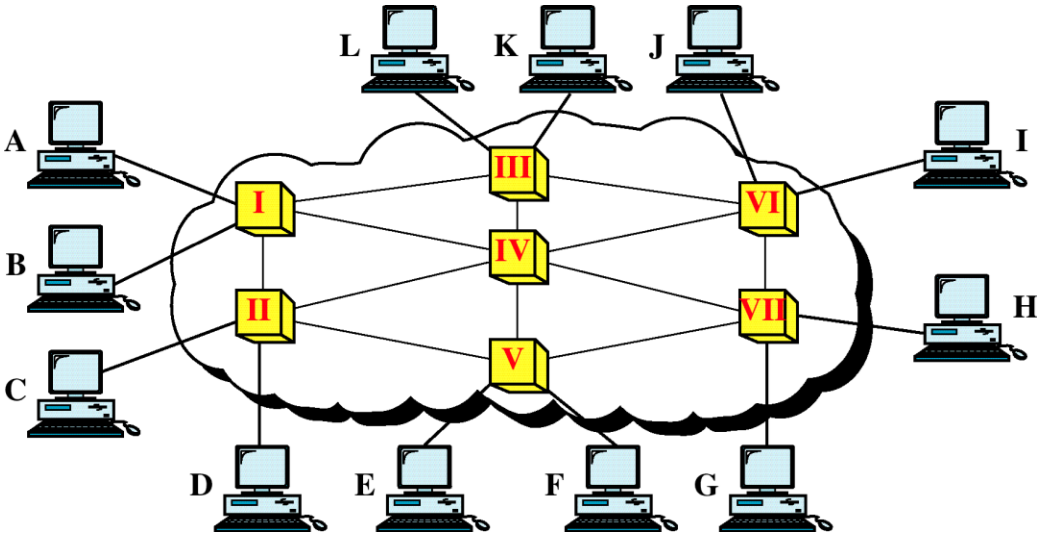
UNIT - IV

SWITCHING

Switching

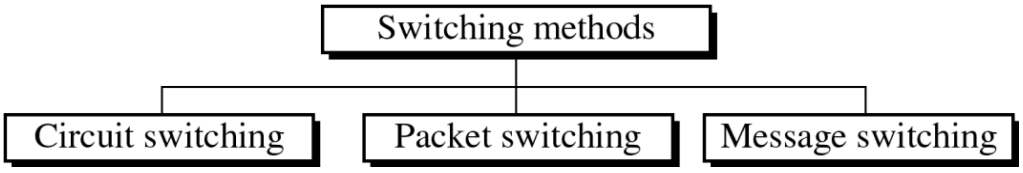
Switching is the method which enables multiple devices to be connected as one-to-one communication like point-to-point connection between each pair of devices. A switched network consists of a series of inter-linked nodes, called switches. Switches are hardware and/or software devices capable of creating temporary connections between two or more devices linked to the switch but not to each other. In a switched network, some of these nodes are connected to the communicating devices. Others are used only for routing.

The following figure shows a switched network. The communicating devices are labeled A, B, C, D, and so on, and the switches I, II, III, IV, and so on. Each switch is connected to multiple links and is used to complete the connections between them, two at a time.



Switched network

Traditionally, three methods of switching have been important: circuit switching, packet switching, and message switching.



Switching methods

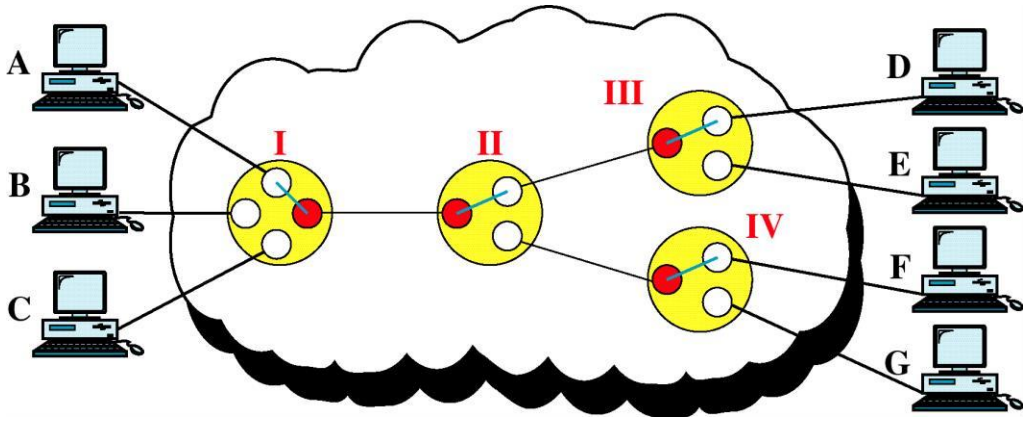
CIRCUIT SWITCHING

Circuit switching creates a direct physical connection between two devices such as phones or computers.

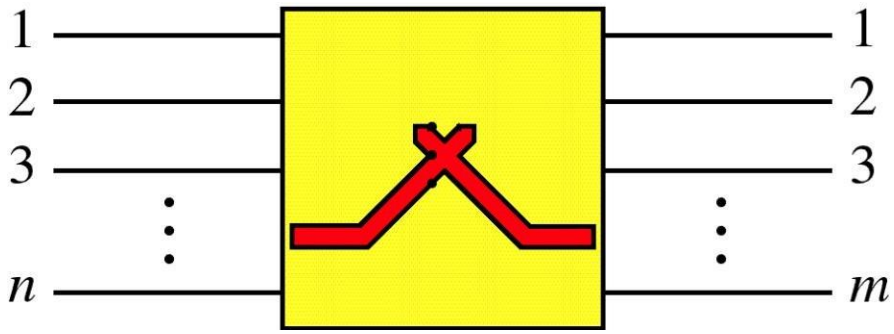
A circuit switch is a device with n inputs and m outputs that create a temporary connection between an input link and an output link.

The number of inputs does not have to match the number of outputs. An n-by-n folded switch can connect n lines in full-duplex mode.

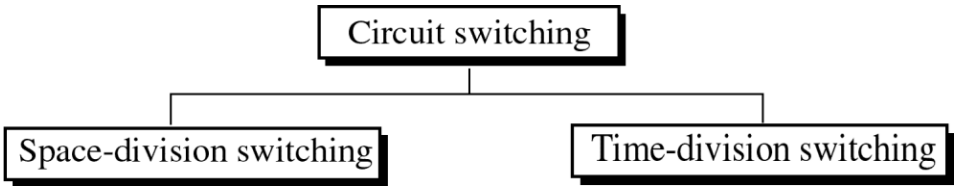
For example, in the following figure, instead of point-to-point connections between the three computers on the left (A, B, and C) to the four computers on the right (D, E, F, and G), requiring 12 links, four switches are used to reduce the number and the total length of the links.



Circuit-switched network



A Circuit switch



Circuit switching

Space-Division Switches

In space-division switching, the paths in the circuit are separated from each other spatially.

This technology was originally designed for use in analog networks but is used currently in both analog and digital networks.

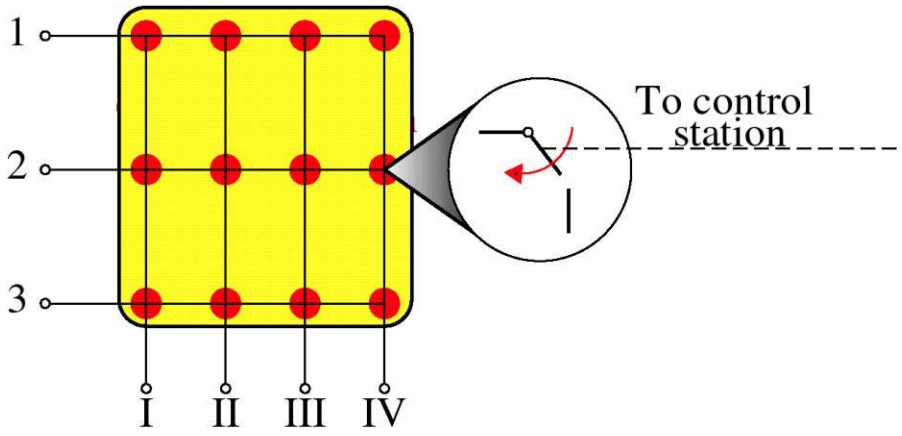
Crossbar Switches

A crossbar switch connects n inputs to m outputs in a grid, using electronic micro-switches (transistors) at each crosspoint.

The major limitation of this design is the number of crosspoints required.

Connecting n inputs to m outputs using a crossbar switch requires n x m crosspoints.

For example, to connect 1000 inputs to 1000 outputs requires a crossbar with 1,000,000 crosspoints. This factor makes the crossbar impractical because it makes the size of the crossbar huge.



Crossbar switch

Multistage Switches

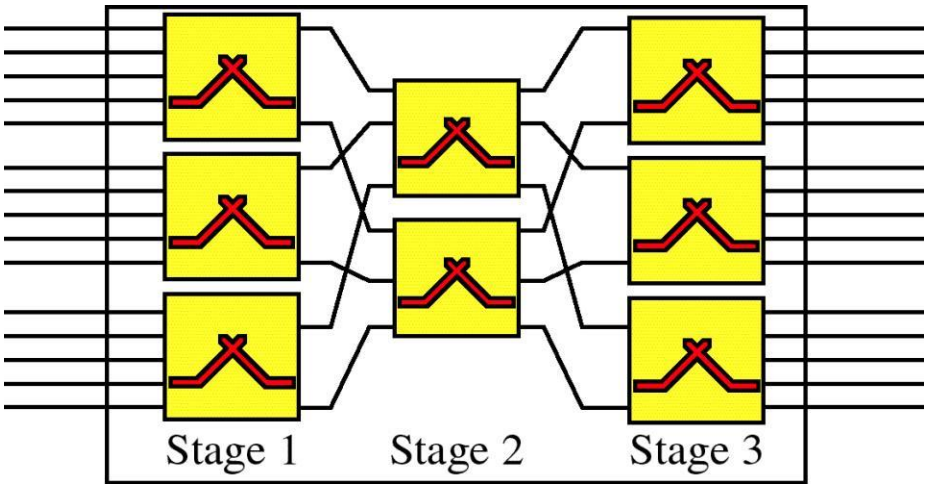
The solution to the limitations of the crossbar switch is to use multistage switches, which combine crossbar switches in several stages.

In multistage switching, devices are linked to switches that, in turn, are linked to a hierarchy of other switches.

The design of a multistage switch depends on the number of stages and the number of switches required (or desired) in each stage.

Normally, the middle stages have fewer switches than do the first and last stages.

For example, imagine that we want a multi-stage switch as in the following figure to do the job of a single 15-by-15 crossbar switch. Assume that we have decided on a three-stage design that uses three switches in the first and final stages and two switches in the middle stage. Because there are three of them, each of the first-stage switches has inputs from one-third of the input devices, giving them five inputs each (5 x 3 = 15). Next, each of the first-stage switches must have an output to each of the intermediate switches. There are two intermediate switches; therefore, each first-stage switch has two outputs. Each third-stage switch must have inputs from each of the intermediate switches; two intermediate switches mean two inputs. The intermediate switches must connect to all three first-stage switches and all three last-stage switches, and so must have three inputs and three outputs each. Multistage switches provide multiple paths for connecting each pair of linked devices.



Multistage switch

Time-Division Switches

Time-division switching uses time-division multiplexing to achieve switching.

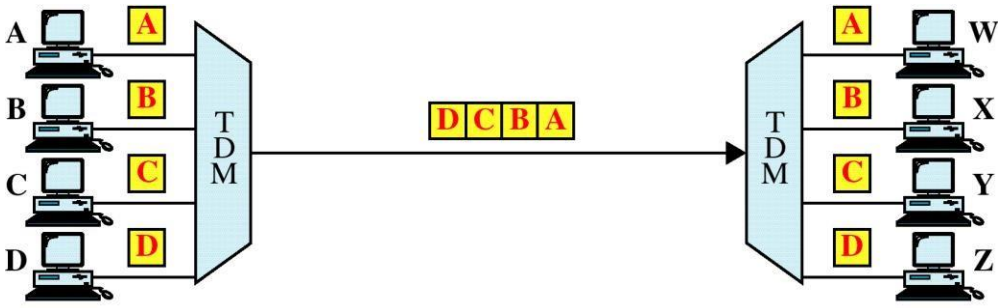
There are two popular methods used in time-division multiplexing: the time-slot interchange and the TDM bus.

Time-Slot Interchange (TSI)

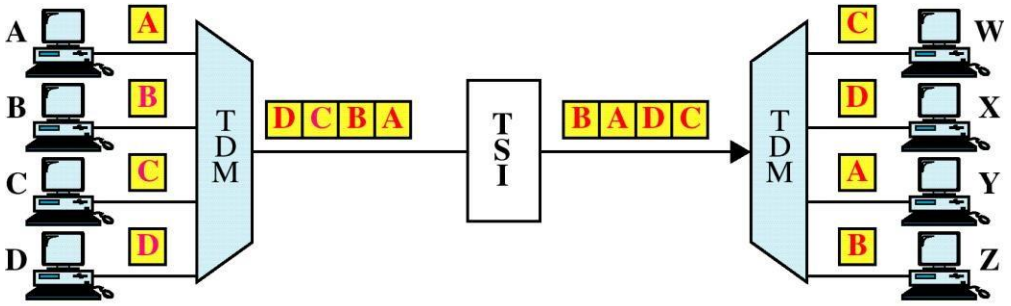
The following figure shows a system connecting four input lines to four output lines. Imagine that each input line wants to send data to an output line according to the following pattern:

$1 \rightarrow 3, \qquad 2 \rightarrow 4, \qquad 3 \rightarrow 1, \qquad 4 \rightarrow 2$

The following figure *a* shows the results of ordinary time-division multiplexing. As you can see, the desired task is not accomplished. Data are output in the same order as they are input. Data from 1 go to 1, from 2 go to 2, from 3 go to 3, and from 4 go to 4. In the figure *b*, a device called a time-slot interchange (TSI) is inserted into the link. A TSI changes the ordering of the slots based on the desired connections. In this case, it changes the order of data from A, B, C, D to C, D, A, B. Now, when the demultiplexer separates the slots, it passes them to the proper outputs.

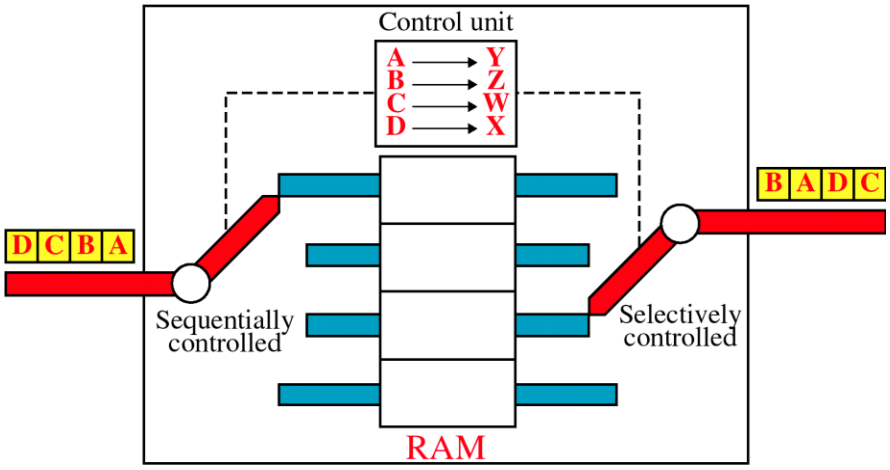


a. No switching



b. Switching

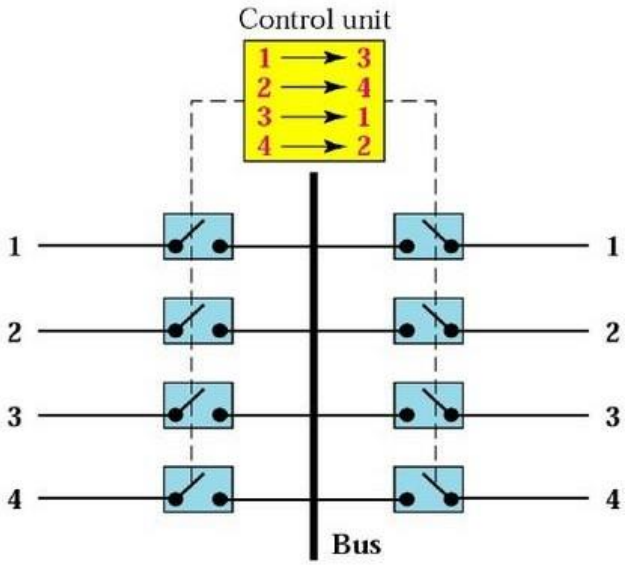
A TSI consists of random access memory (RAM) with several memory locations. The size of each location is the same as the size of a single time slot. The number of locations is the same as the number of inputs (in most cases, the number of inputs and outputs are equal). The RAM fills up with incoming data from time slots in the order received. Slots are then sent out in an order based on the decisions of a control unit.



Time-slot interchange

TDM Bus

The input and output lines are connected to a high-speed bus through input and output gates (micro switches). Each input gate is closed during one of the four time slots. During the same time slot, only one output gate is also closed. This pair of gates allows a burst of data to be transferred from one specific input line to one specific output line using the bus. The control unit opens and closes the gates according to switching need. For example, in the figure, at the first time slot the input gate 1 and output gate 3 will be closed; during the second time slot, input gate 2 and output gate 4 will be closed; and so on.

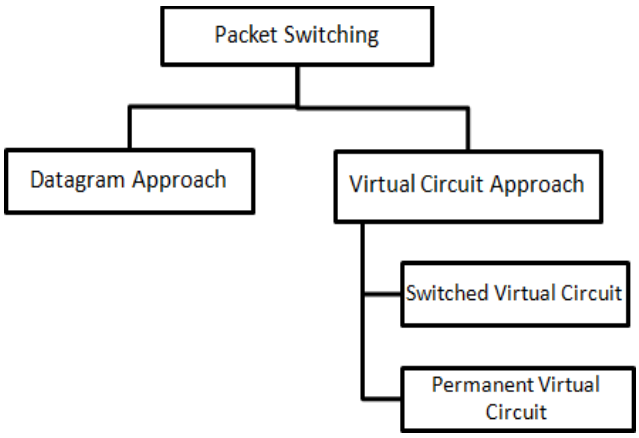


TDM bus

PACKET SWITCHING

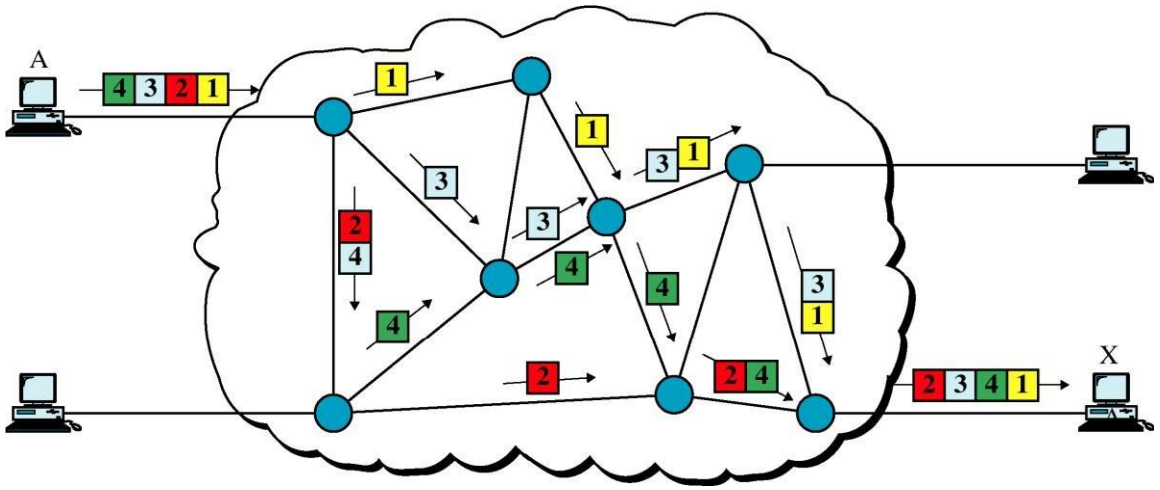
Circuit switching is less well suited to data and other non-voice transmissions. Non-voice transmissions tend to be bursty, meaning that data come in spurts with idle gaps between them. When circuit-switched links are used for data transmission, the line is often idle and its facilities wasted. A circuit-switched link creates the equivalent of a single cable between two devices and thereby assumes a single data rate for both devices. Third, circuit switching is inflexible. Once, a circuit has been established, that circuit is the path taken by all parts of the transmission whether or not it remains the most efficient or available.

A better solution for data transmission is packet switching. In a packet-switched network, data are transmitted in discrete units of variable length blocks called packets. Longer transmissions are broken up into multiple packets. Each packet contains data also a header with control information (such as priority codes and source and destination addresses). The packets are sent over the network node to node. At each node, the packet is stored briefly then routed according to the information in its header. There are two popular approaches to packet switching: datagram and virtual circuit.

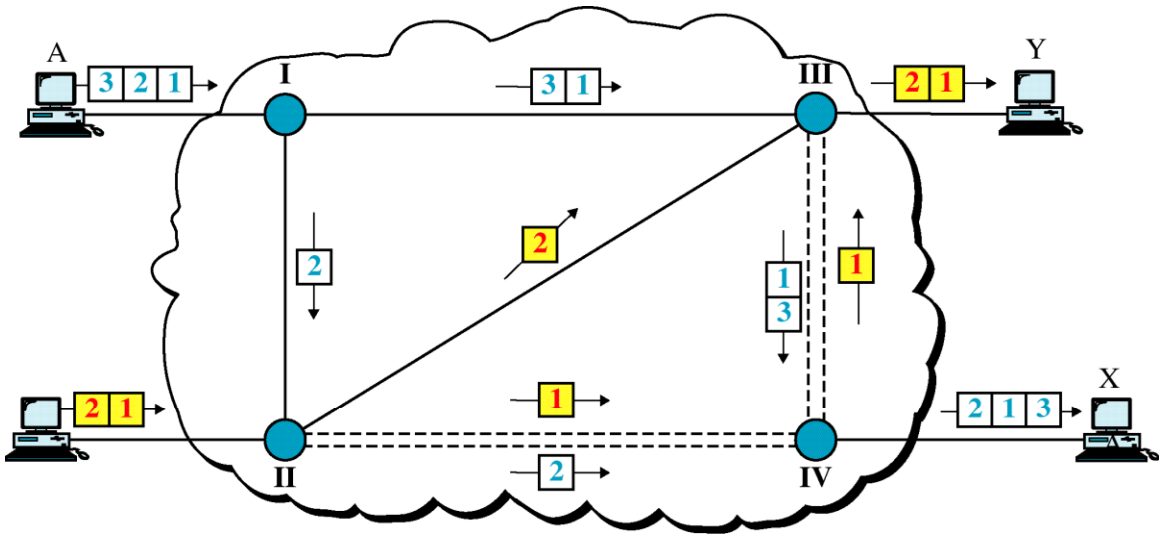


Packet switching approaches

Datagram Approach In the datagram approach to packet switching, each packet is treated independently from all others. One packet represents just a piece of a multipacket transmission, packets are referred to as datagrams. The packets in the datagram approach belong to the same message will go by different paths to reach the destination. This approach can cause the datagrams to arrive at their destination out of order. It is the responsibility of the transport layer to reorder the datagrams before passing them on to the destination port.



a. Datagram approach

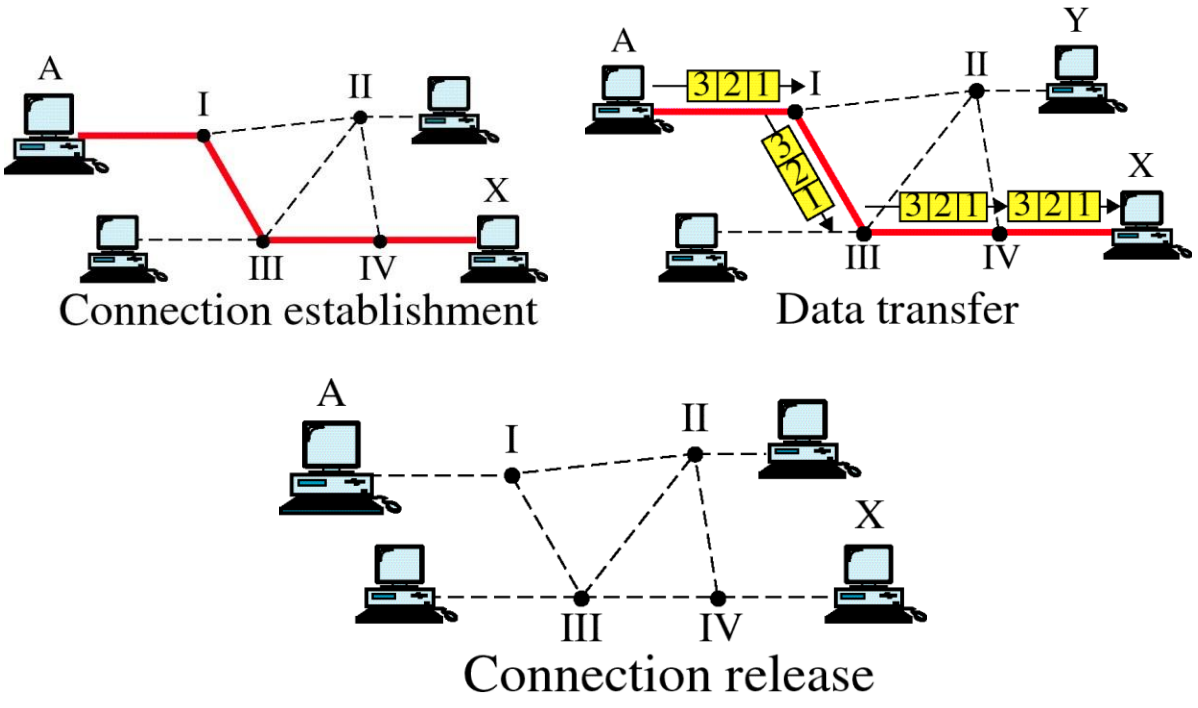


b. Multiple channels in datagram approach

Virtual Circuit Approach In the virtual circuit a single route is chosen between sender and receiver at the beginning of the session. When the data are sent, all packets of the transmission travel one after another along that route. Virtual circuit transmission is implemented in two formats: switched virtual circuit (SVC) and permanent virtual circuit (PVC).

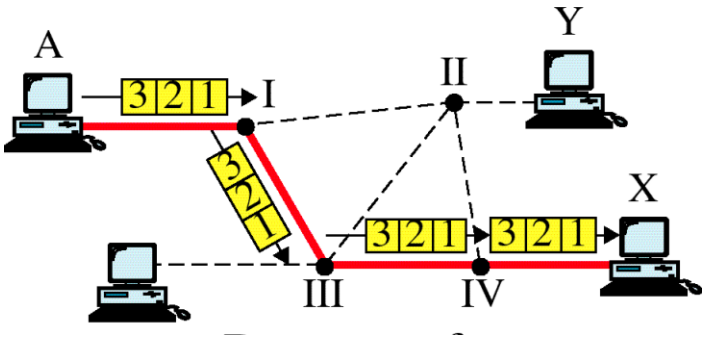
Switched Virtual Circuit The switched virtual circuit (SVC) format is like a dial-up lines in circuit switching. In this method, a virtual circuit is created whenever it is needed and exists only for the duration of the specific exchange. Once the connection is in place, the packets are sent one after another and in sequential order. When the last packet has been received and, if necessary, acknowledged, the connection is released and that virtual circuit is disconnected.

Only one single route exists for the duration of transmission. Each time a new route is established. The route may be the same each time, or it may differ in response to varying network conditions.



Switched virtual circuit

Permanent Virtual Circuit Permanent virtual circuits (PVC) are comparable to leased lines in circuit switching. In this method, the same virtual circuit is provided between two users on a continuous basis. The circuit is dedicated to the specific users. No one else can use it and, because it is always in place, it can be used without connection establishment and connection termination. Whereas two SVC users may get a different route every time they request a connection, two PVC users always get the same route.

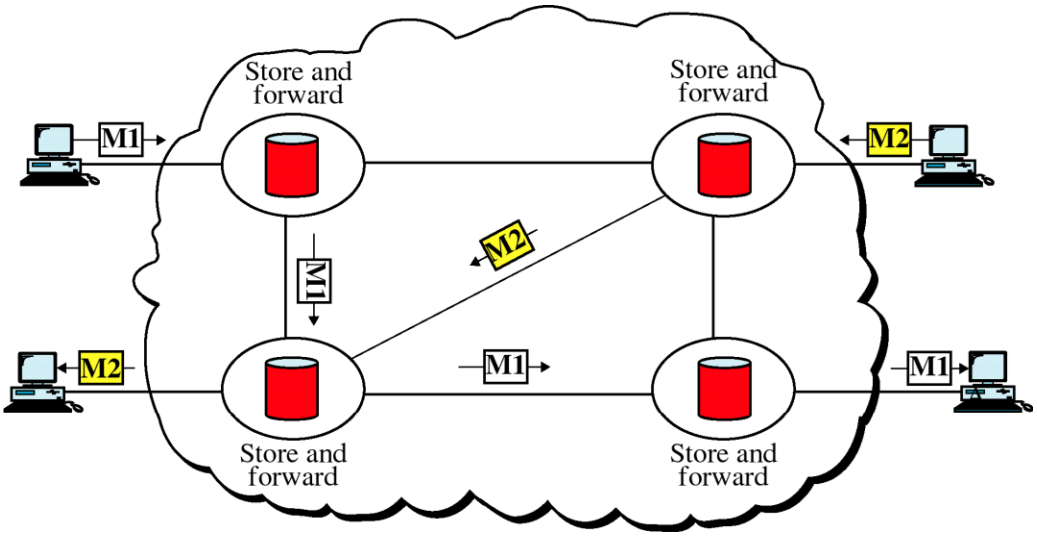


Permanent connection for the duration of the lease

MESSAGE SWITCHING

Message switching is best known as store and forward. In this mechanism, a node (usually a special computer with a number of disks) receives a message, stores it until the appropriate route is free, then sends it along. Store and forward is considered a switching technique because there is no direct link between the sender and receiver of a transmission. A message is delivered

to the node along one path then rerouted along another to its destination. Note that in message switching, the messages are stored and relayed from secondary storage (disk), while in packet switching the packets are stored and forwarded from primary storage (RAM).



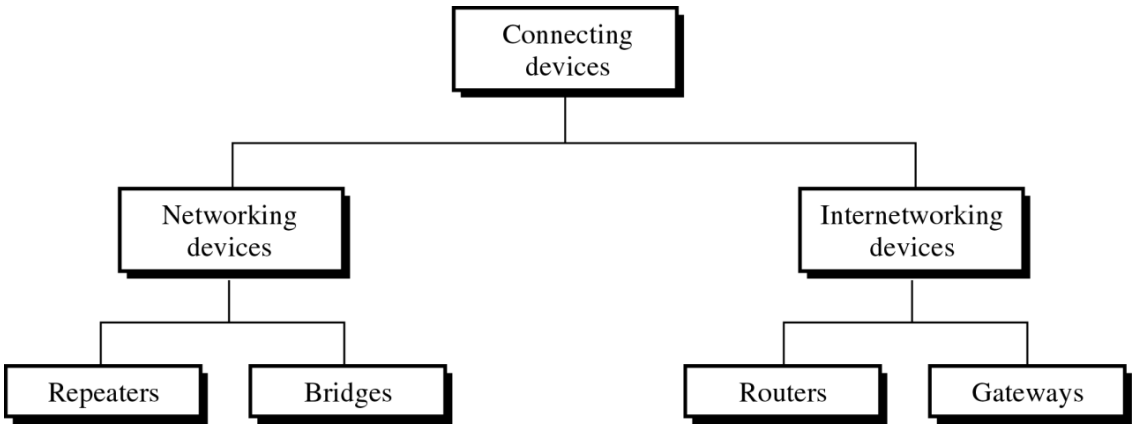
Message switching

Networking and Internetworking Devices

Two or more devices connected for the purpose of sharing data or resources can form a network. In a local area network (LAN) to cover more distance a repeater or regenerator is inserted into the network. To subdivide the network a bridge is inserted for traffic management.

Two or more separate networks are connected for exchanging data or resources, they become an internetwork. Linking a number of LANs into an internet requires additional internetworking devices called routers and gateways.

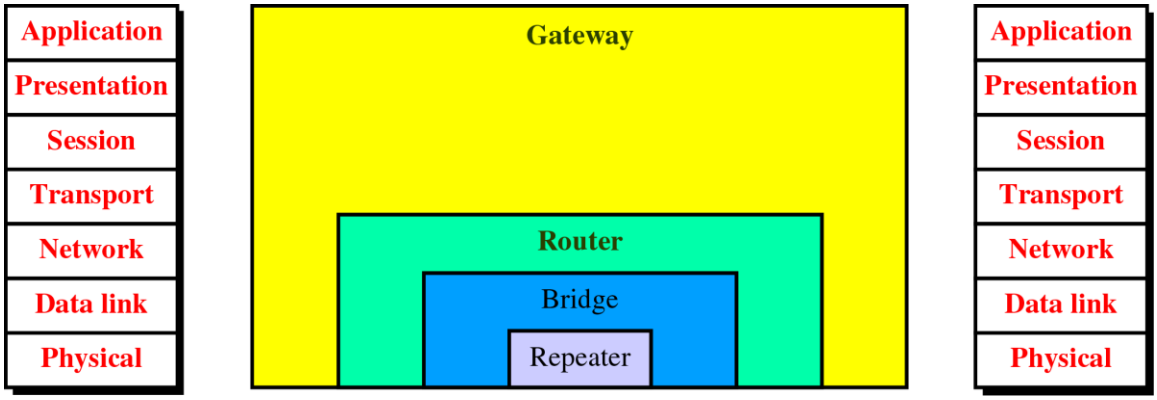
Networking and internetworking devices are divided into four categories: repeaters, bridges, routers and gateways.



Connecting devices

Repeaters act only upon the electrical components of a signal and are therefore active only at the physical layer. Bridges utilize addressing protocols and can affect the flow control

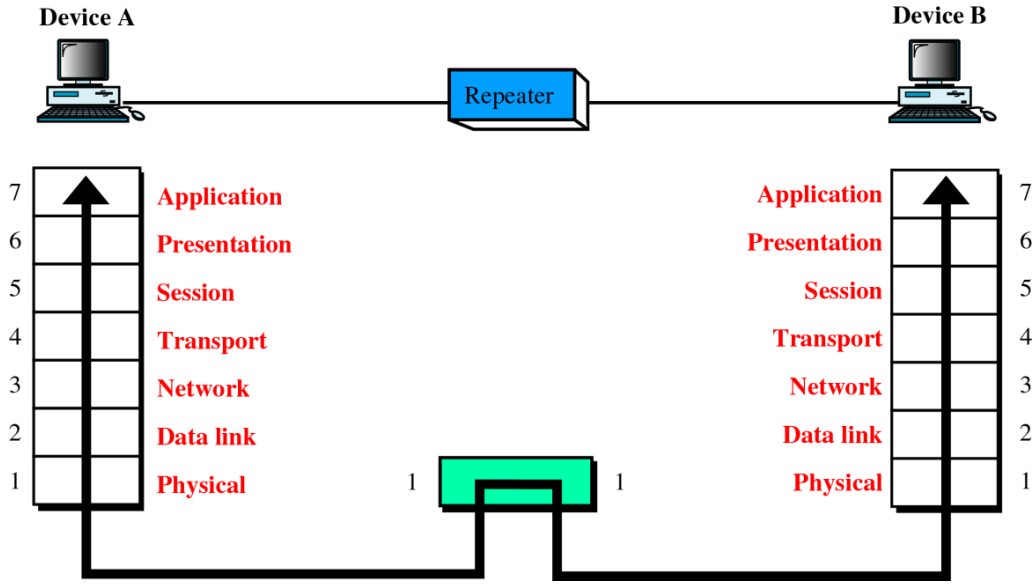
of a single LAN; they are most active at the data link layer. Routers provide links between two separate but same-type LANs and are most active at the network layer. Gateways provide translation services between incompatible LANs or applications and are active in all of the layers.



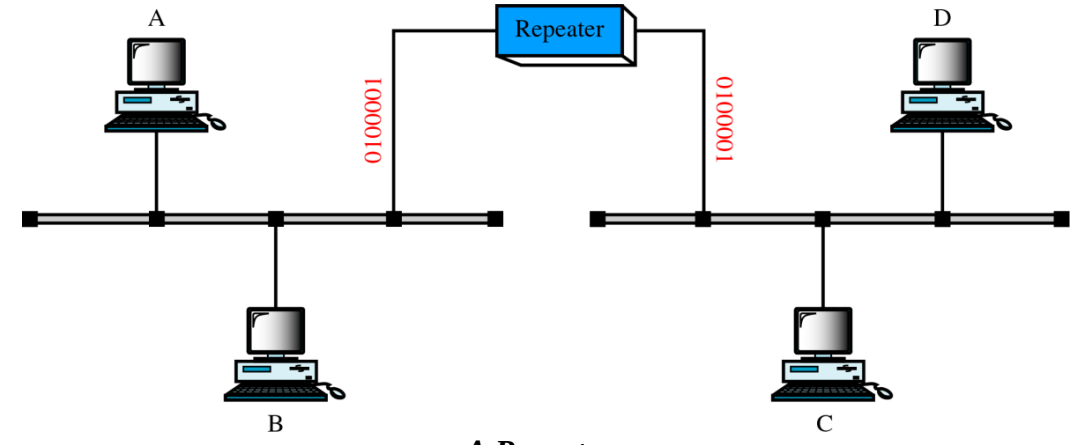
Connecting Devices and the OSI Model

REPEATERS

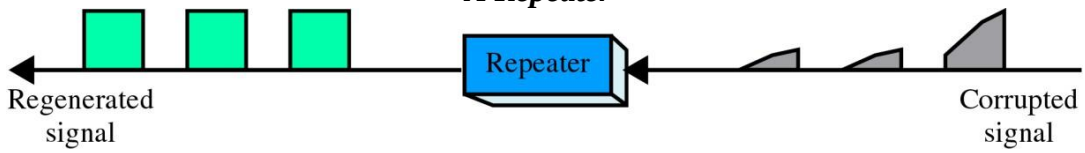
- A Repeater is an electronic device that operate on only the Physical Layer of the OSI model.
- A repeater allows to extend the physical length of a network.
- A repeater is not an amplifier. It does not amplify the signal, it regenerates it. When it receives a weakened or corrupted signal, it creates a copy bit for bit, at the original strength.
- A repeater must be placed so that a signal reaches it before any noise changes the meaning of any of its bits.



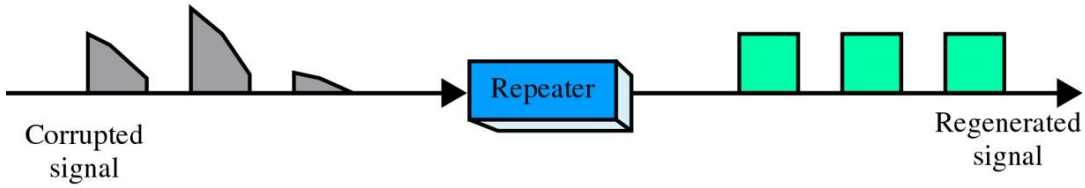
A Repeater in the OSI Model



A Repeater



(a) Right-to-left transmission.

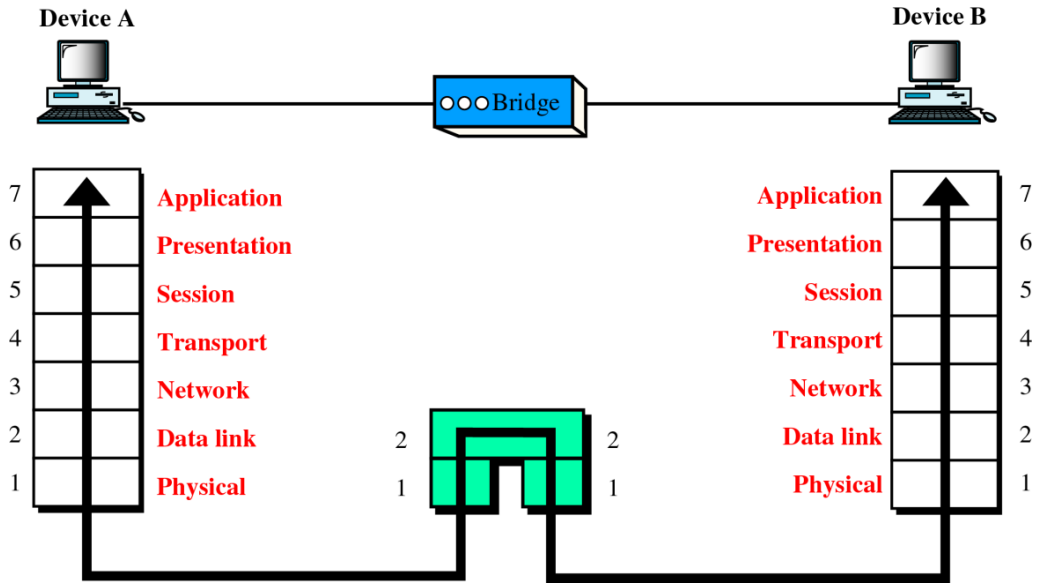


(b) Left-to-right transmission.

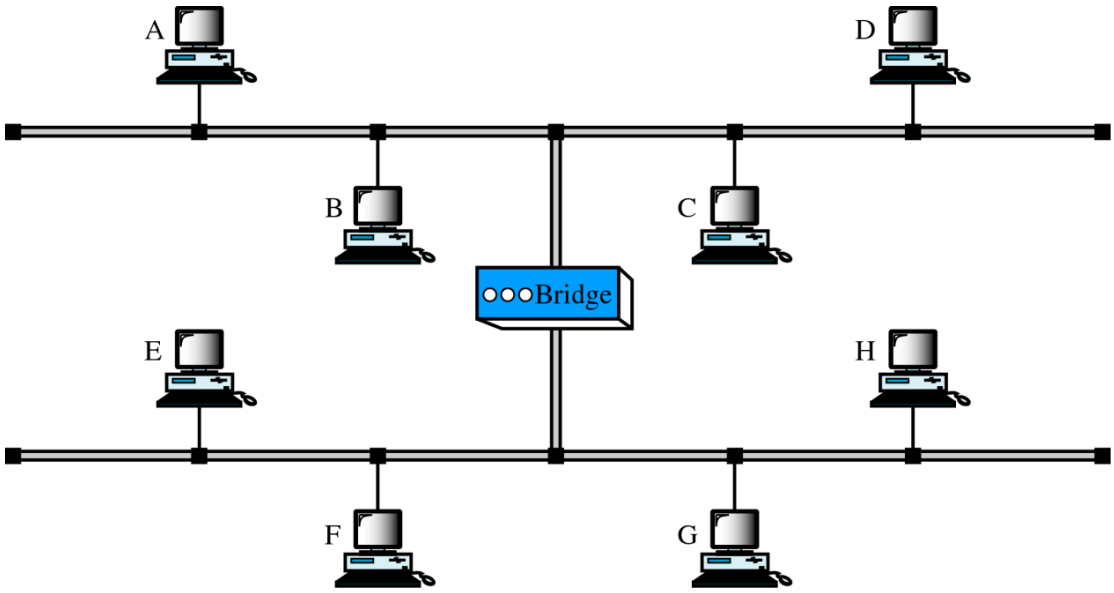
Function of a Repeater

BRIDGES

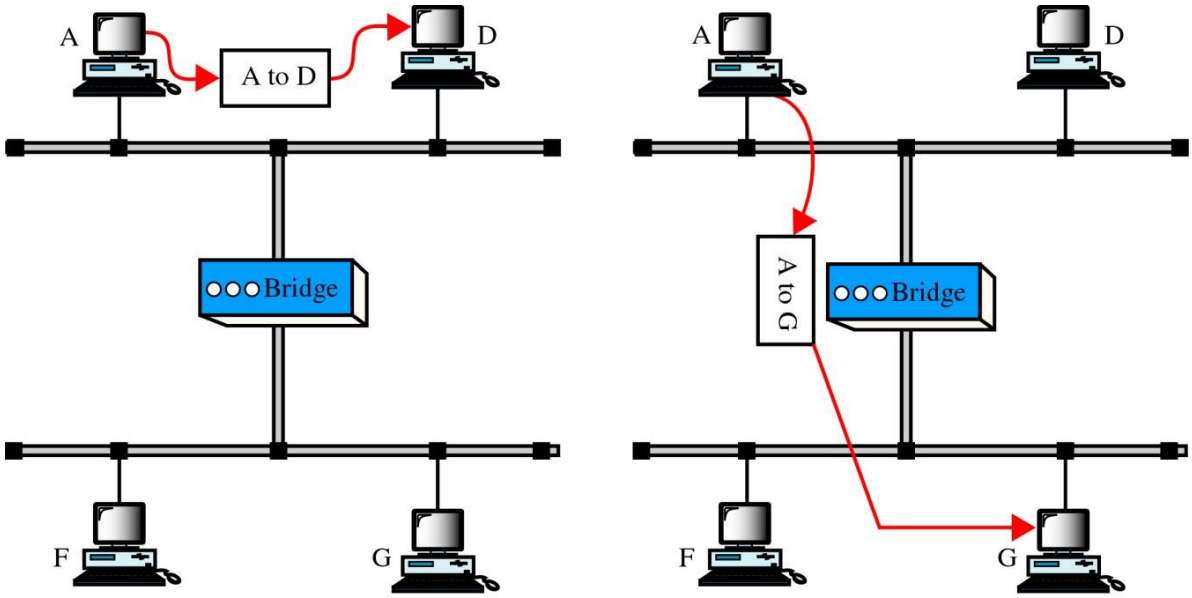
- Bridges operate in both the physical and data link layers of the OSI model.
- Bridges can divide a larger network into smaller segments. They can also relay frames between two originally separate LANs.
- Bridges contain logic that allows them to keep the traffic for each segment separate. It also provide security through partitioning of traffic.



A Bridge in the OSI Model



A Bridge



a. A packet from A to D

b. A packet from A to G

Function of a Bridge

Types of Bridges

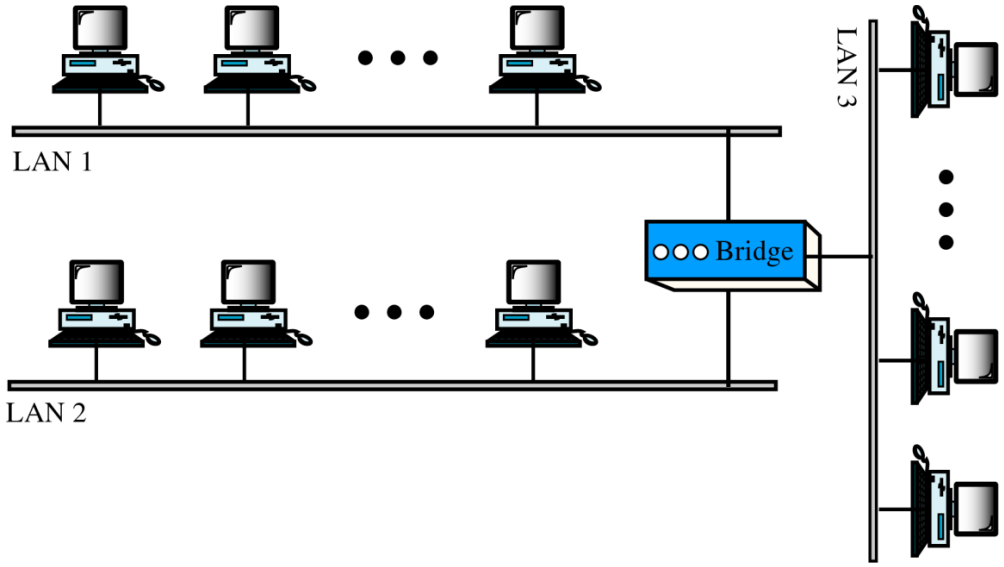
- Simple Bridge
- Multiport Bridge
- Transparent Bridge

Simple Bridge

- Simple bridges are the most primitive and least expensive type of bridge.
- A simple bridge link two segments and contains a table that lists the addresses of all the stations included in each of them.
- In a simple bridge the physical addresses must be entered manually.
- Installation and maintenance of simple bridges are time-consuming and potentially more trouble than the cost savings are worth.

Multiport Bridge

A multiport bridge can be used to connect more than two LANs.



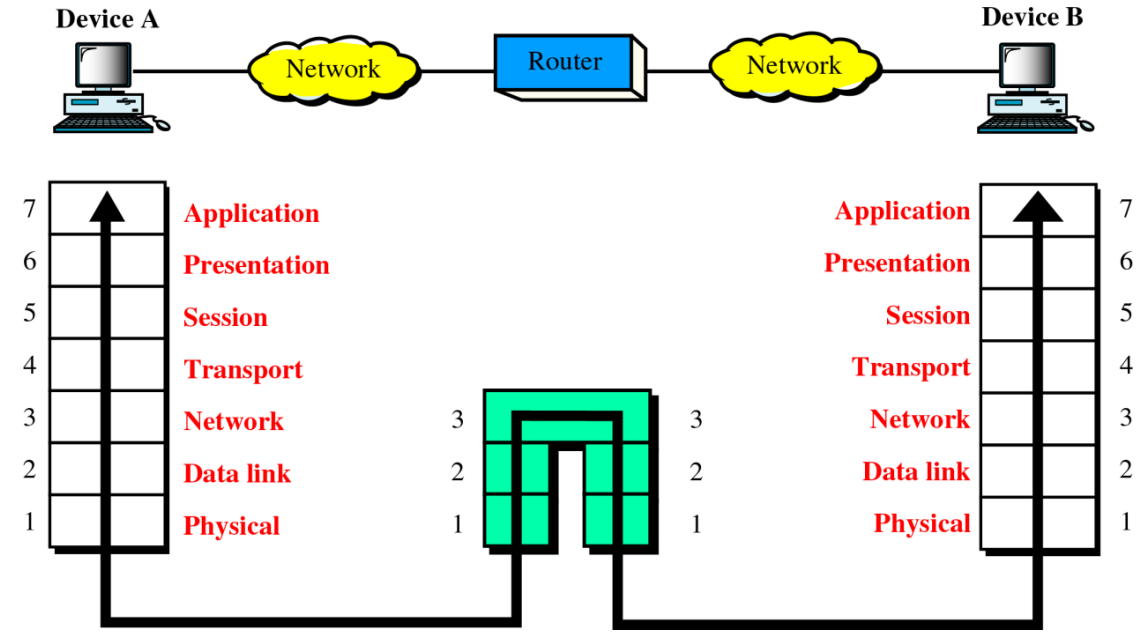
Multiport Bridge

Transparent Bridge

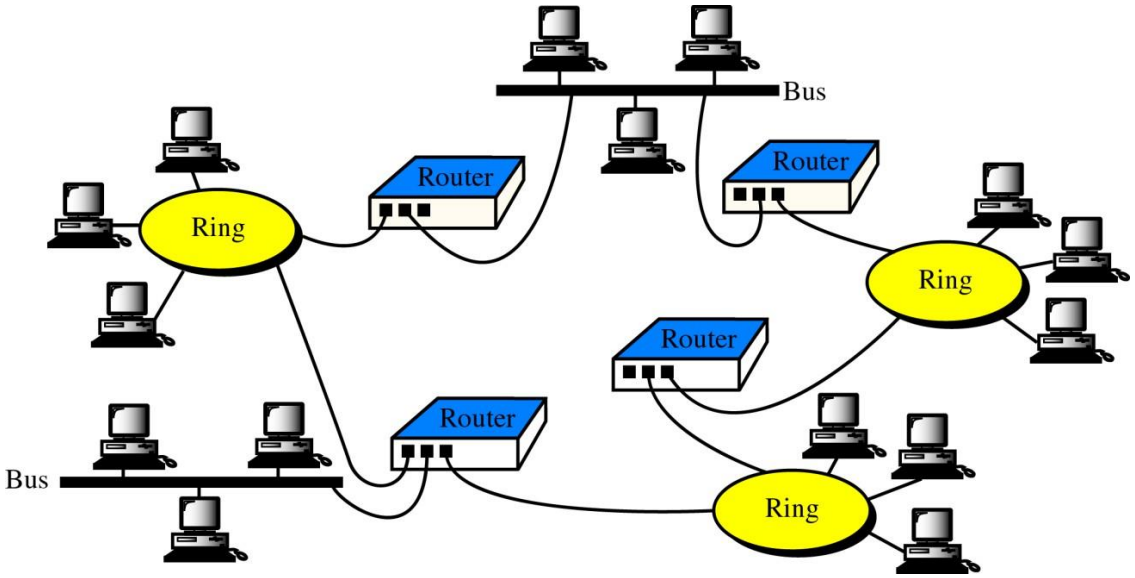
- A transparent bridge is otherwise called as learning bridge.
- It builds its table of station on its own.
- Transparent bridges use Spanning Tree Algorithm or Source Routing to avoid loop.
- A bridge will be able to connect LANs using different protocols at the data link layer, such as Ethernet LAN to a Token Ring LAN. It addresses many issues which includes, Frame Format, Payload Size, Data Rate, Address Bit Order, Other issues such as acknowledgement, collision, and priority.

ROUTERS

- Routers relay packets among multiple interconnected networks.
- The router forwards the packet to the next router on the path, and so on, until the destination is reached.
- Routers act like stations on a network.
- The router checks the destination address, finds what it considers the best route for the packet, and passes it to the destination network or across a neighbouring network to the next router on the chosen path.



A router in the OSI model



Routers in an internet

Least Cost Routing

- Least cost routing is based on efficiency; which of the available paths is the cheapest or shortest?
- Shortest means the smallest number of relays it is called hop-count routing, in which every link is considered to be of equal length and given the value one. One-hop routes are equal to one, two-hop routes are always equal to two, and so on.

Types of routing

Routing is classified as non-adaptive or adaptive.

Non-adaptive routing

In non-adaptive routing, once a pathway to a destination has been selected, the router sends all packets for that destination along that one route.

Adaptive routing

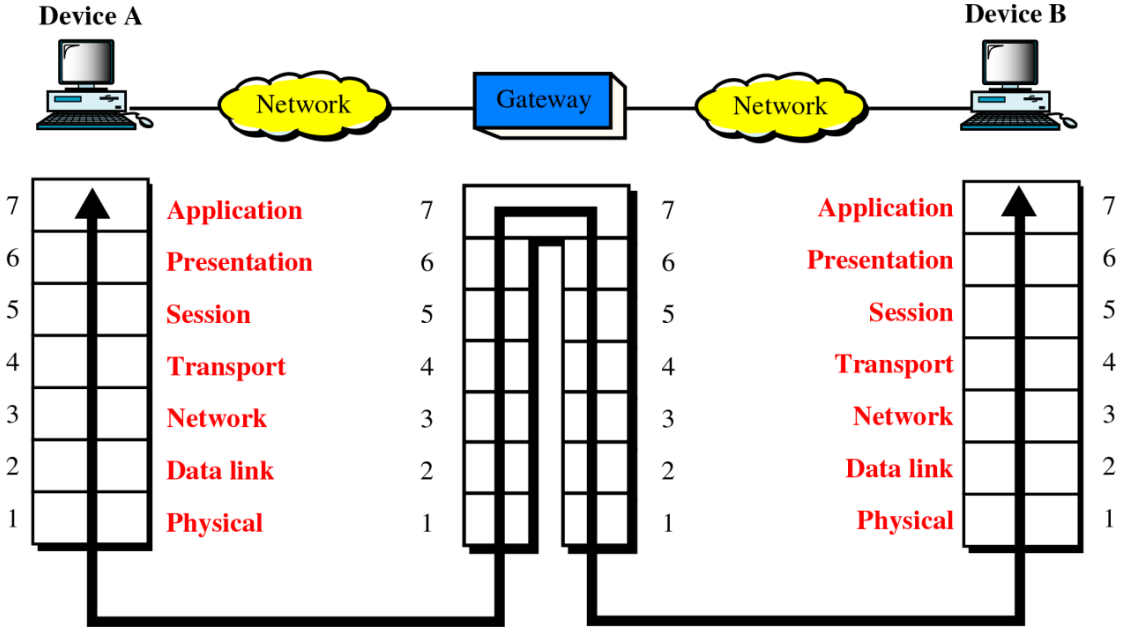
In adaptive routing, a router may select a new route for each packet in response to changes in condition and topology of the networks.

Packet Life time

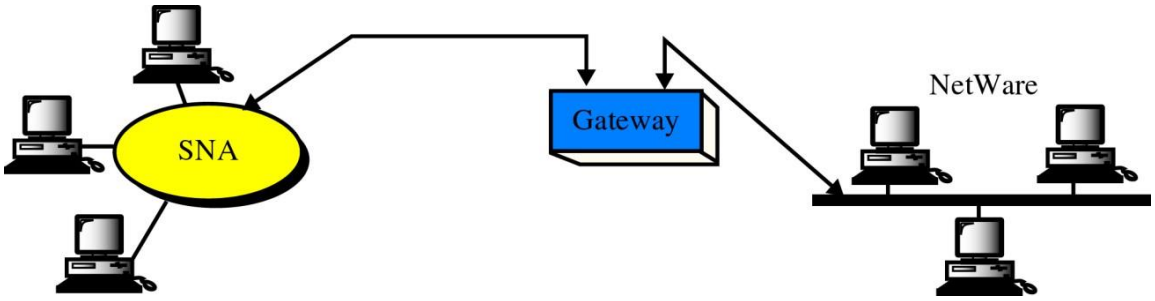
Packet Life time or Time to Live (TTL) is added with every packet. As a packet is generated, each packet is marked with a lifetime, usually the number of hops that are allowed before a packet is considered lost and, accordingly, destroyed. Each router to encounter the packet subtracts 1 from the total before passing it on. When the lifetime reaches 0, the packet is destroyed.

GATEWAYS

- Gateways operate on all seven layers of the OSI model.
- A gateway is a protocol convertor
- A router by itself transfers, accepts, and relays packets only across networks using similar protocols.
- A gateway, can accept a packet formatted for one protocol and convert it to a packet formatted for another protocol before forwarding.
- A gateway is generally software installed within a router.
- In some cases, it modifies Headers and Trailer of the packet, in other cases, it adjusts *data rate*, *size* and *format*.



A Gateway in the OSI Model



A Gateway

UNIT - V

ROUTING ALGORITHMS

In routing the pathway with the lowest cost is considered the best. As long as the cost of each link is known, a router can find the optimal combination for any transmission. Two common methods are used to calculate the shortest path between two routers: distance vector routing and link state routing

DISTANCE VECTOR ROUTING

In distance vector routing, each router periodically shares its knowledge about the entire network with its neighbors. The three keys to understanding how this algorithm works are as follows:

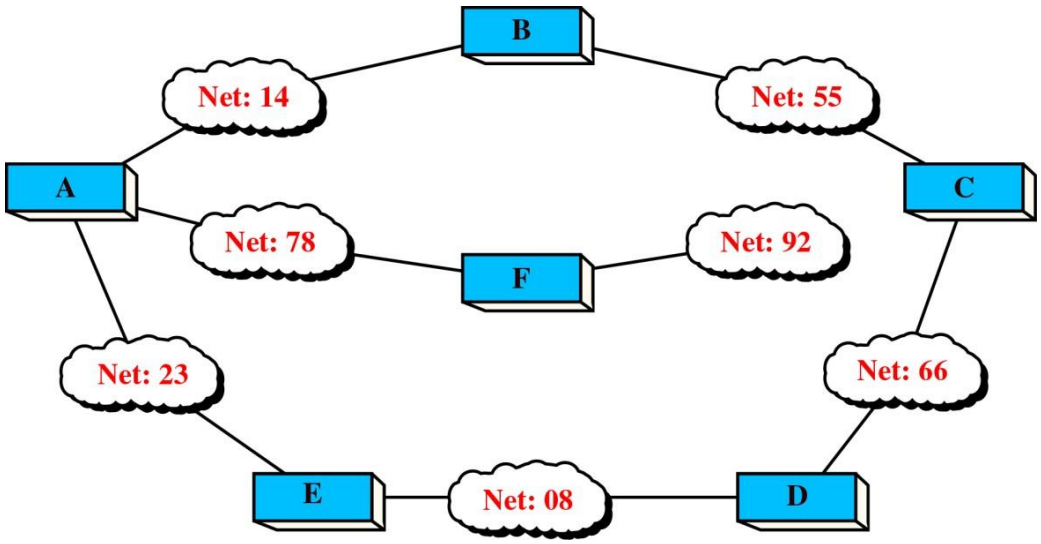
1. Knowledge about the whole network. Each router shares its knowledge about the entire network. It sends all of its collected knowledge about the network to its neighbors. At the outset, a router's knowledge of the network may be sparse. How much it knows, however, is unimportant: it sends whatever, it has.

2. Routing only to neighbors. Each router periodically sends its knowledge about the network only to those routers **to which it** has direct links. It sends whatever knowledge it has about the whole network through all of its ports. This information is received and kept by each neighboring router and used to update that router's own information about the network.

3. Information sharing at regular intervals. For example, every 30 seconds, each router sends its information about the whole network to its neighbors. This sharing occurs whether or not the network has changed since the last time information was exchanged
In distance vector routing, each router periodically shares its knowledge about the entire network with its neighbors.

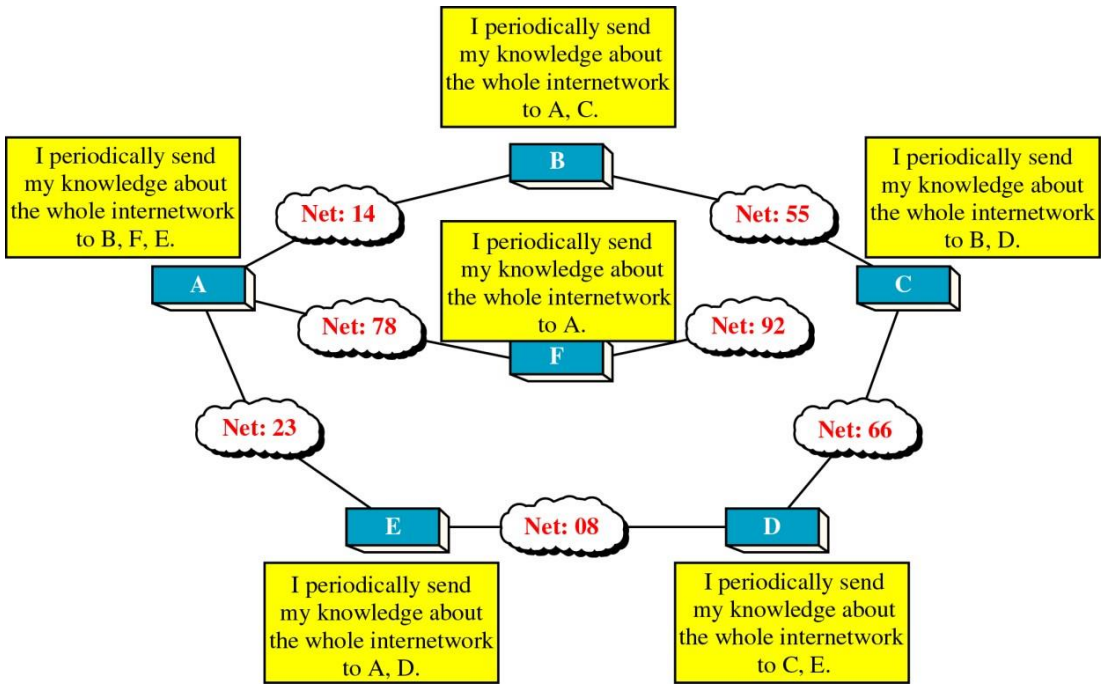
Sharing Information

To understand how distance vector routing works, examine the internet shown in the following figure. In this example, the clouds represent local area networks (LANs). The number inside each cloud is that LAN's network ID. These LANs can be of any type (Ethernet, Token Ring, FDDI, etc.). The LANs are connected by routers (or gateways), represented by the boxes labeled A, B, C, D, E, and F.



Example of an internet

The following figure shows the first step in the algorithm. The text boxes indicate the relationships of the routers in the above figure to their neighbors. Each router sends its information about the internetwork only to its immediate neighbors.



The concept of distance vector routing

A router sends its knowledge to its neighbors. The neighbors add this knowledge to their own knowledge and send the whole table to their own neighbors. In this way, the first router gets its own information back plus new information about its neighbor's other neighbors. Each of

these neighbors adds its knowledge and sends the updated table on to its own neighbors and so on. Eventually, every router knows about every other router in the internetwork.

Routing Table

Creating the Table

At start-up, a routers knowledge of the internetwork is sparse. All it knows is that it is connected to some number of LANs (two or more). Because a router is a station on each of those LANs, it also knows the ID of each station. In most systems, a station port ID and a network ID share the same prefix. So a router can discover to which networks it is connected by examining its own logical addresses (remember, a router has as many logical addresses as it has connected ports). This information is enough for it to construct its original routing table.

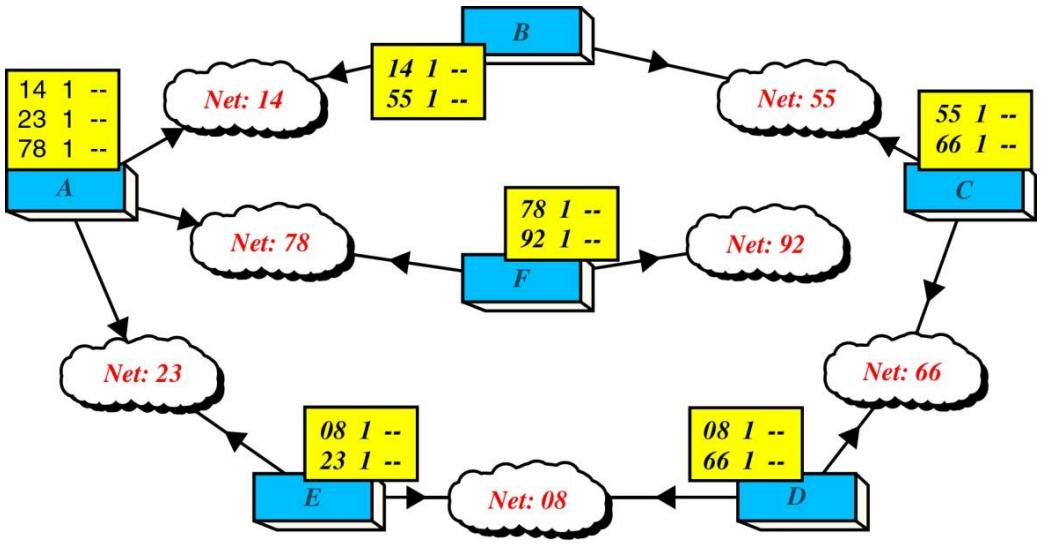
Network ID	Cost	Next Hop
. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .

Distance vector routing table

Network ID Cost Next Hop

A routing table has columns for at least three types of information: the network ID, the cost, and the ID of the next router (next hop). The network ID is the final destination of the packet. The cost is the number of hops a packet must make to get there. And the next router is the router to which a packet must be delivered on its way to a particular destination. The table tells a router that it costs x to reach network Y via router Z.

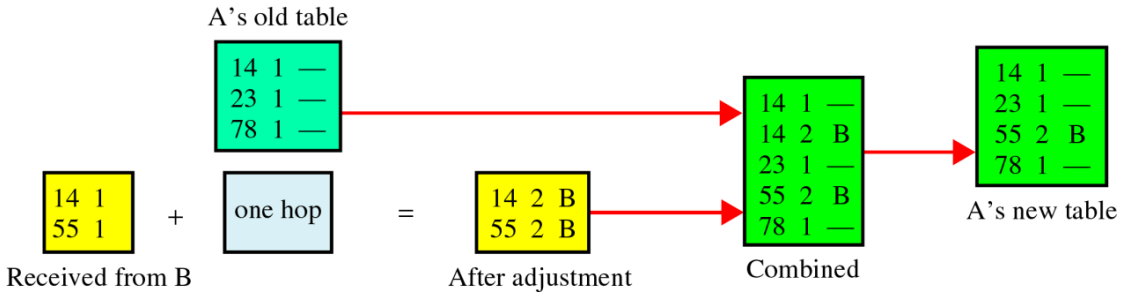
The original routing tables for our sample internetwork are shown in the following figure. At this point, the third column is empty because the only destination networks identified are those attached to the current router. No multiple-hop destinations and therefore no next routers have been identified. These basic tables are sent out to neighbors. For example, A sends its routing table to routers B, F, and E; B sends its routing table to routers C and A; and so on.



Routing Table Distribution in distance vector routing

Updating the Table

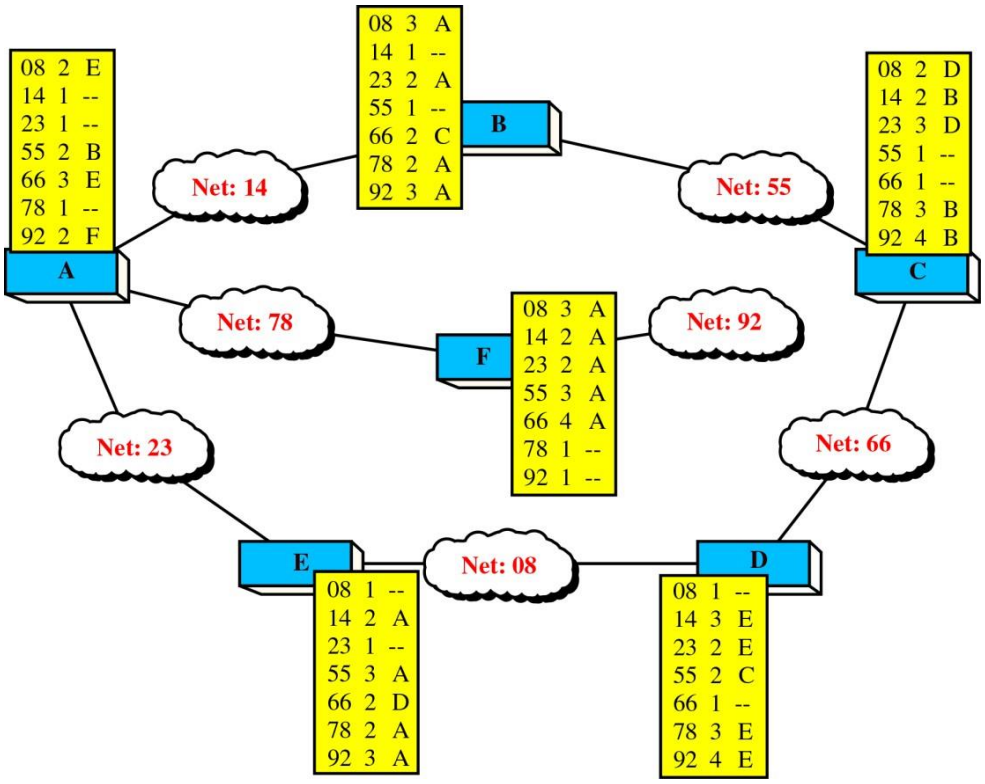
When A receives a routing table from B, it uses the information to update its own table (see the following figure). It says to itself: "B has sent me a table that shows how its packets can get to networks 55 and 14. I know that B is my neighbor, so my packets can reach B in one hop. So, if I add one hop to all of the costs shown in B's table, the sum will be my cost for reaching those other networks." Therefore, A adjusts the information shown in B's table by adding one to each listed cost. It then combines this table with its own to create a new, more comprehensive table.



Updating routing table for router A

This combined table may contain duplicate data for some network destinations. Router A therefore finds and purges any duplications and keeps whichever version shows the lowest cost. For example, as Figure 21.21 shows, router A can send a packet to network 14 in two ways. The first, which uses no next router, costs one hop. The second, via router B, requires two hops (A to B, then B to 14). The first option has the lower cost; it is kept and the second entry is dropped. This selection process is the reason for the cost column: the cost allows the router to differentiate between various routes to the same destination.

This process continues for all routers. Every router receives information from neighbours and updates its routing table.



Final Routing Tables

Updating algorithm

- Add one hop to the hop count for each advertised destination.
- Repeat the following steps for each advertised destination:
- If (destination is not in the routing table)

```
        Add the advertised information to the table.
    Else
      If (next-hop field is the same)
          Replace entry in the table with the new one.
      Else
          If (new hop count < the one in the table)
                Replace entry in the routing table.
```

LINK STATE ROUTING

In link state routing. each router shares its knowledge of its neighborhood with every other router in the internetwork. The following are true of link state routing:

1. Knowledge about the neighborhood. Instead of sending its entire routing table, a router sends information about its neighborhood only.

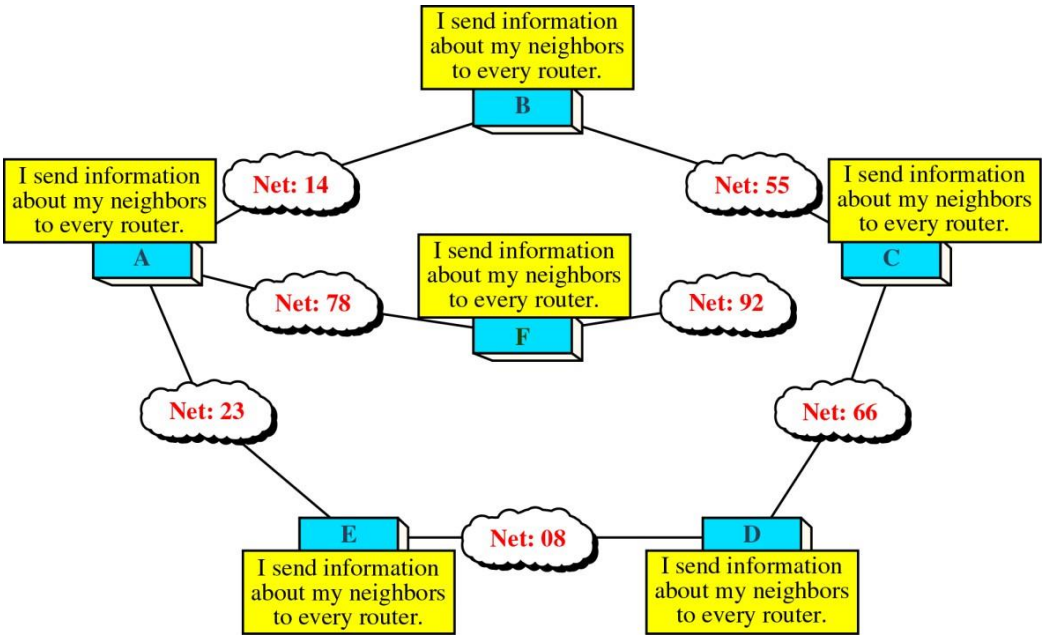
2. To all routers. Each router sends this information to every other router on the internetwork, not just to its neighbors. It does so by a process called **flooding.** Flooding means that a router sends its information to all of its neighbors (through all of its output ports). Each neighbor sends the packet to all of its neighbors, and so on. Every router that receives the packet sends copies to all of its neighbors. Finally, every router (without exception) receives a copy of the same information.

3. Information sharing when there is a change. Each router sends out information about the neighbors when there is a change.

In link state routing, each router shares its knowledge of its neighborhood with all routers in the internetwork.

Information Sharing

The first step in link state routing is information sharing. Each router sends its knowledge about its neighborhood to every other router in the internetwork.

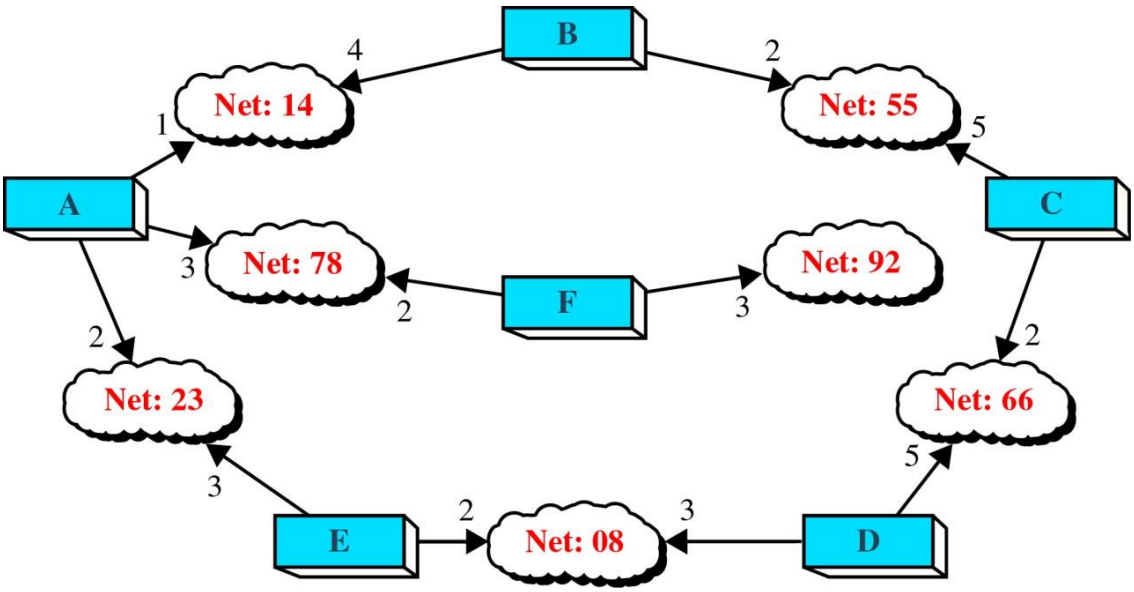


Concept of Link State Routing

Both distance vector and link state routing are lowest-cost algorithms. In distance vector routing, cost refers to hop count. In link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic, or the state of the link. The cost from router A to network 14, therefore, might be different from the cost from A to 23.

In determining a route, the cost of a hop is applied to each packet as it leaves a router and enters a network. This cost is an outbound cost, meaning that it is applied when a packet leaves the router. Two factors govern how cost is applied to packets in determining a route:

- Cost is applied only by routers and not by any other stations on a network. Remember, the link from one router to the next is a network, not a point-to-point cable.
- Cost is applied as a packet leaves the router rather than as it enters.



Cost in Link State Routing

Link State Packet

When a router floods the network with information about its neighborhood, it is said to be advertising. The basis of this advertising is a short packet called a **link state packet (LSP)**. An LSP usually contains four fields: the ID of the advertiser, the ID of the destination network, the cost, and the ID of the neighbor router.

Advertiser	Network	Cost	Neighbor
. . . . .	. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .	. . . . .

Link state packet

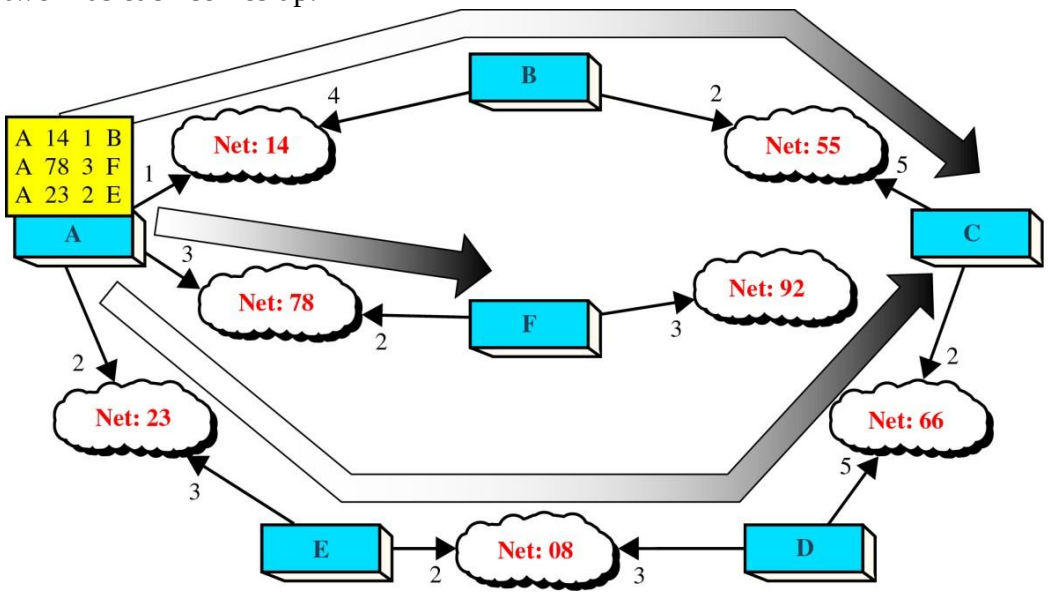
Getting Information about Neighbors

A router gets its information about its neighbors by periodically sending them a short greeting packet. If the neighbor responds to the greeting as expected, it is assumed to be alive and functioning. If it does not, a change is assumed to have occurred and the sending router then alerts the rest of the network in its next LSP.

Initialization

Each router sends a greeting packet to its neighbors to find out the state of each link. It

then prepares an LSP based on the results of these greetings and floods the network with it. The following figure shows this process for router A. The same steps are performed by every router in the network as each comes up.



Flooding of A's LSP

Link State Database

Every router receives every LSP and puts the information into a **link state database.** The following table shows the database for our sample internetwork.

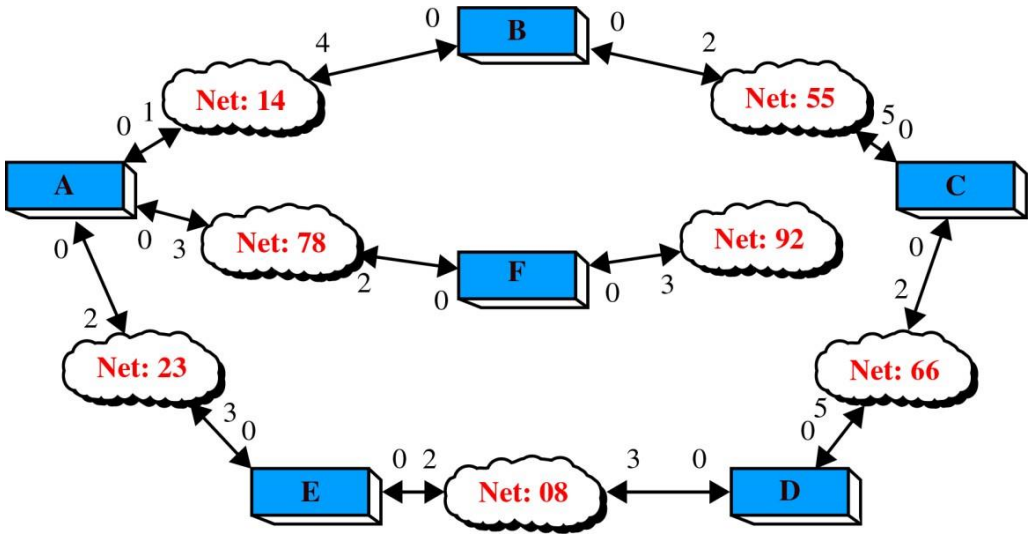
Advertiser	Network	Cost	Neighbor
A	14	1	B
A	78	3	F
A	23	2	E
B	**14**	**4**	**A**
B	**55**	**2**	**C**
C	55	5	B
C	66	2	D
D	**66**	**5**	**C**
D	**08**	**3**	**E**
E	23	3	A
E	08	2	D
F	**78**	**2**	**A**
F	**92**	**3**	**—**

Link state database

Because every router receives the same LSPs, every router builds the same database. It stores this database on its disk and uses it to calculate its routing table. If a router is added to or deleted from the system, the whole database must be shared for fast updating.

The Dijkstra Algorithm

To calculate its routing table, each router applies an algorithm called the **Dijkstra algorithm** to its link state database. The Dijkstra algorithm calculates the shortest path between two points on a network using a graph made up of nodes and arcs. Nodes are of two types: networks and routers. Arcs are the connections between a router and a network (router to network and network to router). Cost is applied only to the arc from router to network. The cost of the arc from network to router is always zero.



Costs in the Dijkstra algorithm

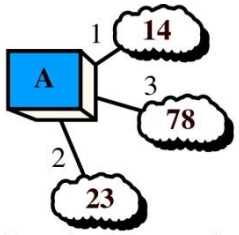
Shortest Path Tree

The Dijkstra algorithm follows four steps to discover what is called the **shortest path tree** (routing table) for each router:

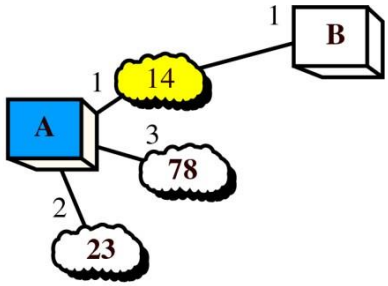
1. Start with the local node (router) as the root of the tree and make it the first permanent node.
2. Examine each neighbour of the node that was the last permanent node.
3. Assign a cumulative cost to each node and make it tentative.
4. Among the list of tentative nodes
   i. Find the node with the smallest cost and make it permanent.
   ii. If a node can be reached from more than one route then select the route with the shortest cumulative cost.
5. Repeat steps 2 to 4 until every node becomes permanent.

The following figure shows the steps of the Dijkstra algorithm applied by node A of our sample internet. The cost number next to each node represents the cumulative cost from the root

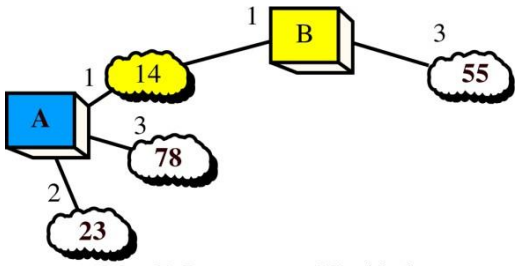
node, not the cost of the individual arc. The second and third steps are until four more nodes have become permanent.



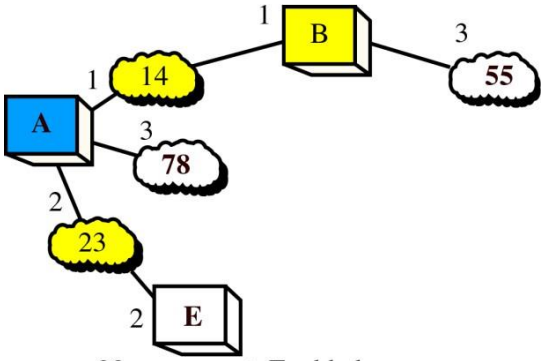
Root is A, networks 14, 78, 23 added



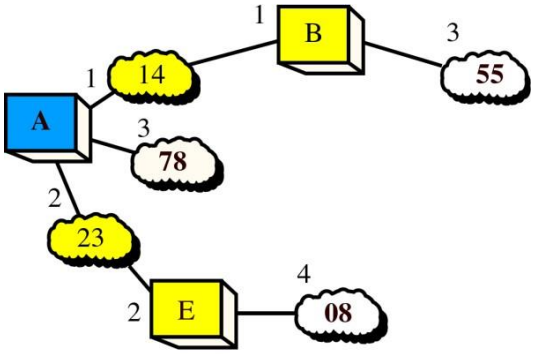
14 permanent, B added



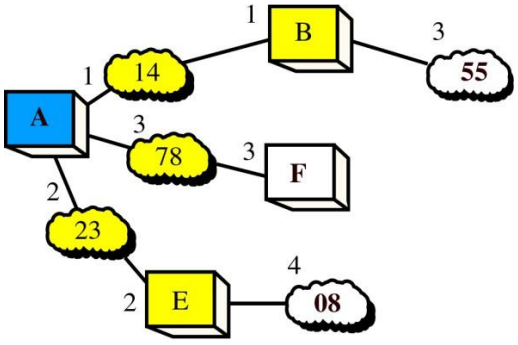
B Permanent, 55 added



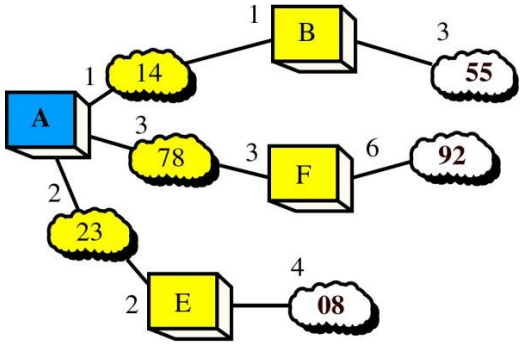
23 permanent, E added



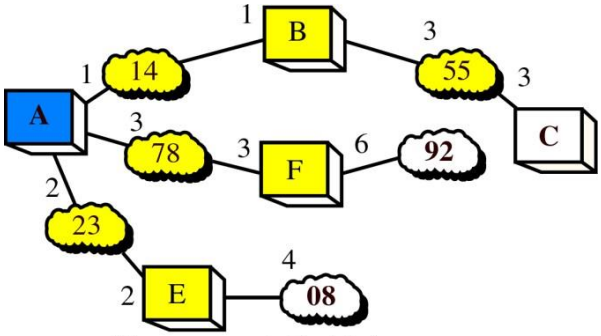
E permanent, 08 added



78 permanent, F added



F permanent, 92 added



55 permanent, C added

C permanent, 66 added

08 permanent, D added

D permanent, 66 added.
But 9 > 5, so that link deleted

66 permanent

92 permanent

Routing Table

Each router now uses the shortest path tree to construct its routing table, Each router uses the same algorithm and the same link state database to calculate its own shortest path tree and routing table: these are different for each router. The following table shows the table developed by router A.

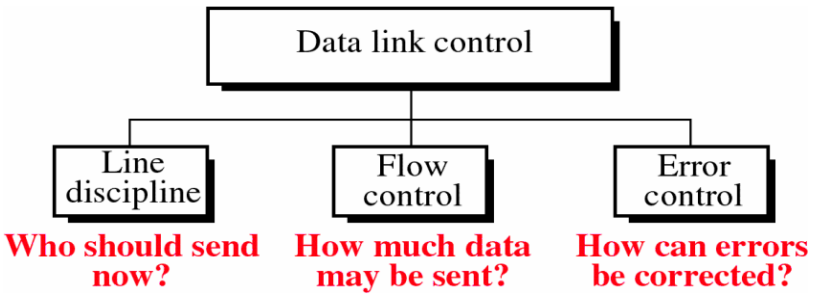
Net	Cost	Next router
08	4	E
14	1	--
23	2	--
55	3	B
66	5	B
78	3	--
92	6	F

Routing Table for Router A

DATA LINK CONTROL

The functions of data link control:

- Line discipline coordinates the link systems. It determines which device can send and when it can send.
- Flow control coordinates the amount of data that can be sent before receiving acknowledgment. It also provides the receiver's acknowledgment of frames received intact, and so is linked to error control.
- Error control means error detection and correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender.



Data link layer functions

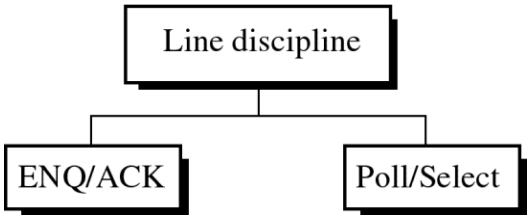
LINE DISCIPLINE

The line discipline functions of the data link layer oversee the establishment of links and the right of a particular device to transmit at a given time.

Line discipline can be done in two ways: enquiry/acknowledgment (ENQ/ACK) and poll/select. The first method is used in peer-to-peer communication; the second method is used in primary-secondary communication.

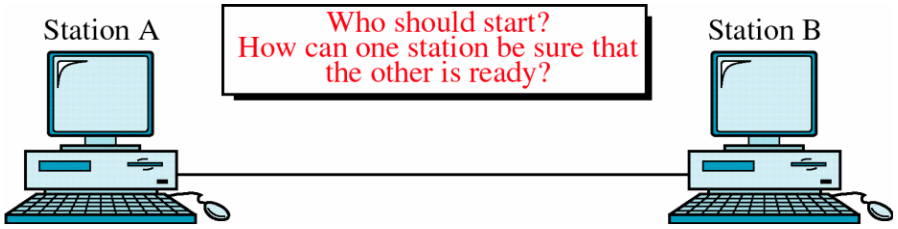
ENQ/ACK

Enquiry/acknowledgment (ENQ/ACK) is used primarily in systems where there is no question of the wrong receiver getting the transmission, that is, when there is a dedicated link between two devices so that the only device capable of receiving the trans-mission is the intended one.



Line discipline categories

ENQ/ACK coordinates which device may start a transmission and whether or not the intended recipient is ready and enabled. Using ENQ/ACK, a session can be initiated by either station on a link as long as both are of equal rank - a printer, for example, cannot initiate communication with a CPU.

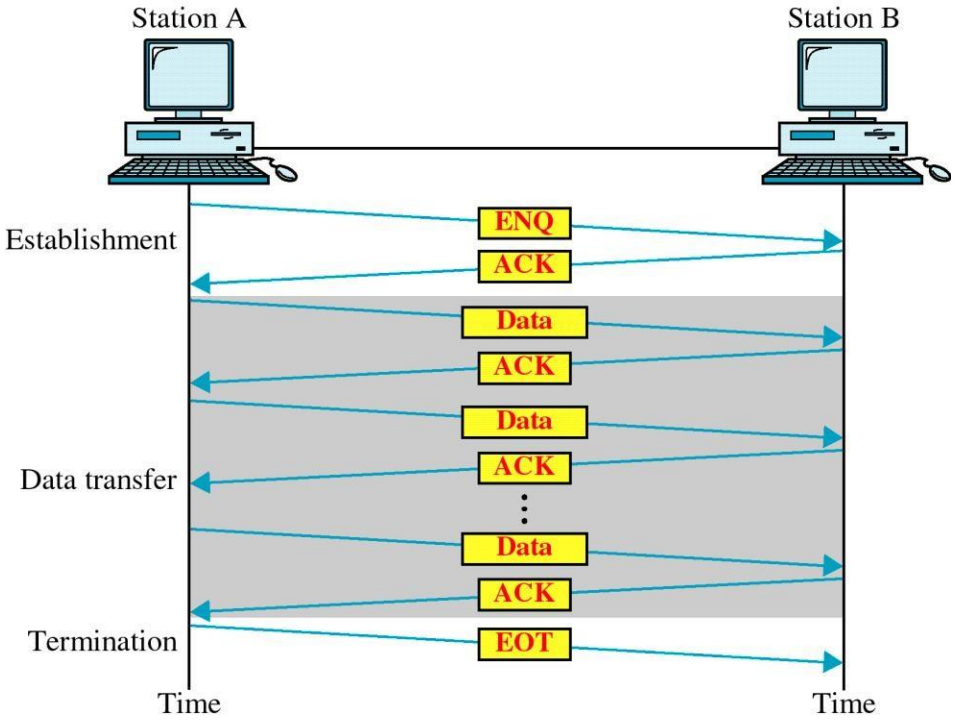


Line discipline concept: ENQ/ACK

In both half-duplex and full-duplex transmission, the initiating device establishes the session. In half-duplex, the initiator then sends its data while the responder waits. The responder may take over the link when the initiator is finished or has requested a response. In full-duplex, both devices can transmit simultaneously once the session has been established.

How It Works The initiator first transmits a frame called an enquiry (ENQ) asking if the receiver is available to receive data. The receiver must answer either with an acknowledgement (ACK) frame if it is ready to receive or with a negative acknowledgement (NAK) frame if it is not. By requiring a response even if the answer is negative, the initiator knows that its enquiry was in fact received even if the receiver is currently unable to accept a transmission. If neither an ACK nor a NAK is received within a specified time limit, the initiator assumes that the ENQ frame was lost in transit, disconnects, and sends a replacement. An initiating system ordinarily makes three such attempts to establish a link before giving up.

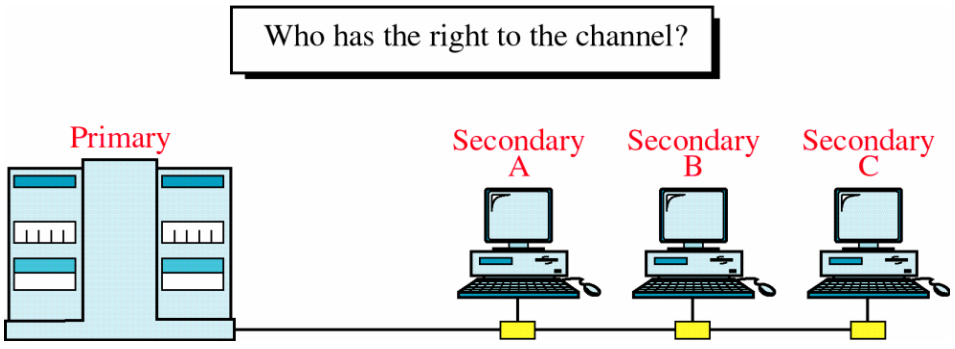
If the response to the ENQ is negative for three attempts, the initiator disconnects and begins the process again at another time. If the response is positive, the initiator is free to send its data. Once all of its data have been transmitted, the sending system finishes with an end of transmission (EOT) frame. This process is illustrated in the following figure.



ENQ/ACK line discipline

Poll/Select

The poll/select method of line discipline works with topologies where one device is designated as a primary station and the other devices are secondary stations. Multi-point systems must coordinate several nodes, not just two. The primary device controls the link; the secondary devices follow its instructions. It is up to the primary to determine which device is allowed to use the channel at a given time. The primary, therefore, is always the initiator of a session. If the primary wants to receive data, it asks the secondaries if they have anything to send; this function is called polling. If the primary wants to send data, it tells the target secondary to get ready to receive; this function is called selecting.

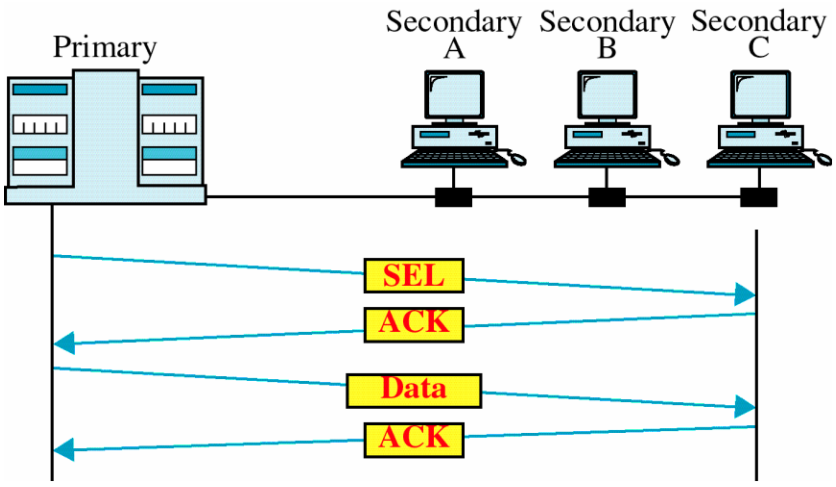


Poll/select discipline

Addresses For the primary device in a multipoint topology to be able to identify and communicate with a specific secondary device, however, there must be an addressing convention. For this reason, every device on a link has an address that can be used for identification. Poll/select protocols identify each frame as being either to or from a specific device on the link. Each secondary device has an address that differentiates it from the others. In any transmission, that address will appear in a specified portion of each frame, called an address field or header depending on the protocol. If the transmission comes from the primary device, the address indicates the recipient of the data. If the transmission comes from a secondary device, the address indicates the originator of the data.

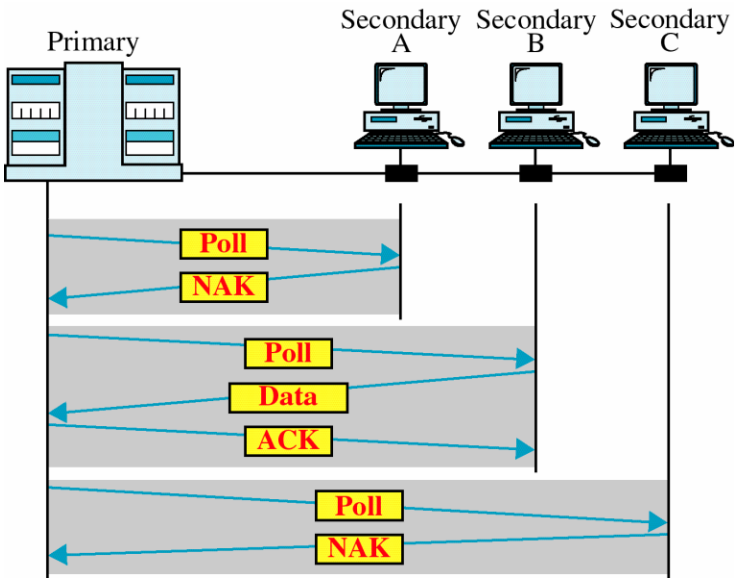
Select The select mode is used whenever the primary device has something to send. If the primary is not either sending or receiving data, it knows the link is available. If it has something to send, it sends it. What it does not know, however, is whether the target device is prepared to receive (usually, prepared to receive means on). So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgment of the secondary's ready status. Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary. Multipoint topologies use a single link for several devices, which means that any frame on the link is available to every device. As a frame makes its way down the link, each of the secondary devices checks the address field. Only when a device recognizes its own address does it open the frame and read the data. In the case of a SEL frame, the enclosed data consist of an alert that data are forthcoming. If the secondary is awake and running, it returns an ACK frame to the primary. The primary then sends one or more data frames, each addressed to the intended secondary. The following figure illustrates this procedure.

Poll The polling function is used by the primary device to solicit transmissions from the secondary devices. The secondaries are not allowed to transmit data unless asked. By keeping all control with the primary, the multipoint system guarantees that only one transmission can



Select

occur at a time, thereby ensuring against signal collisions without requiring elaborate precedence protocols. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send. When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data if it does. If the response is negative (a NAK frame), the primary then polls the next secondary in the same way until it finds one with data to send. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame) verifying its receipt. The secondary may send several data frames one after the other or it may be required to wait for an ACK before sending each one, depending on the protocol being used. There are two possibilities for terminating the exchange: either the secondary sends all its data, finishing with an end of transmission (EOT) frame, or the primary says, "Time's up."

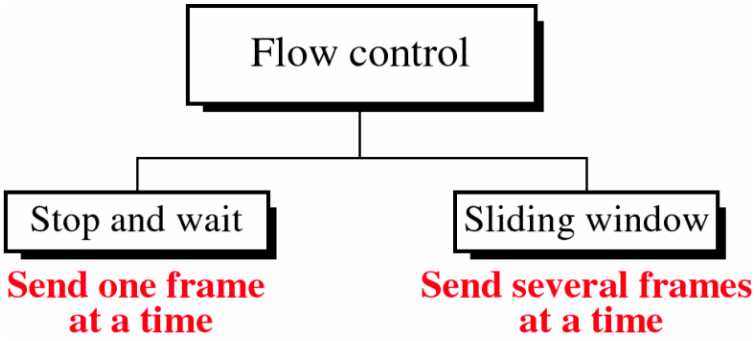


Poll

FLOW CONTROL

Flow control is a set of procedures that tells the sender bow much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data must not be allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a *buffer*, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

Two methods have been developed to control the flow of data across communications links: stop-and-wait (send one frame at a time) and sliding window (send several frames at a time).

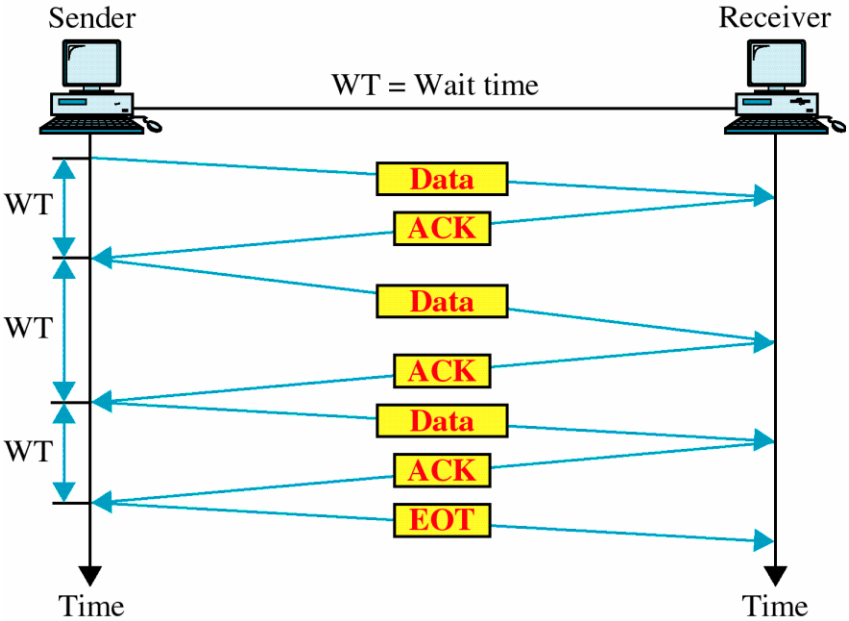


Categories of flow control

Stop-and-wait Flow Control

In a stop-and-wait method of flow control, the sender waits for an acknowledgment after every frame it sends. Only when an acknowledgement has been received the next frame is sent. This process of alternately sending and waiting repeats until the sender transmits an end of transmission (EOT) frame.

The advantage of stop-and-wait is simplicity: each frame is checked and acknowledged before the next frame is sent. The disadvantage is inefficiency: stop-and-wait is slow. Each frame must travel all the way to the receiver and an acknowledgement must travel all the way back before the next frame can be sent. In other words, each frame is alone on the line. Each frame sent and received uses the entire time needed to traverse the link. If the distance between devices is long, the time spent waiting for ACKs between each frame can add significantly to the total transmission time.

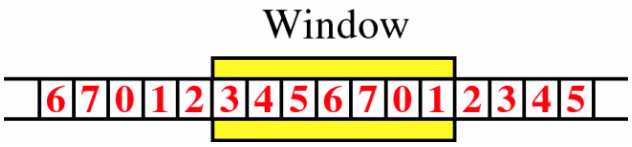


Stop-and-wait

Sliding Window

In the sliding window method of flow control, the sender can transmit several frames before needing an acknowledgment. Frames can be sent one after another. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames. The sliding window refers to imaginary boxes at both the sender and the receiver. This window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement. Frames may be acknowledged at any point without waiting for the window to fill up and may be transmitted as long as the window is not yet full. The frames are numbered modulo-n, which means they are numbered from 0 to n-1. For e.g., if n = 8, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1 …

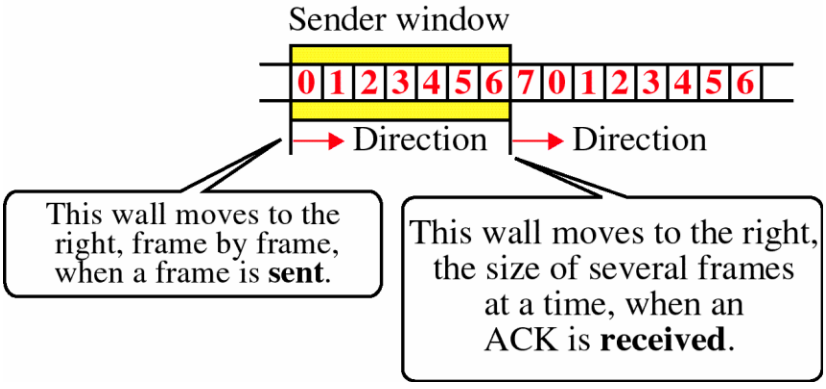
When the receiver sends an ACK, it includes the number of the next frame it expects to receive. To acknowledge the receipt of a string of frames ending in frame 4, the receiver sends an ACK containing the number 5. When the sender sees an ACK with number 5, it knows that all frames up through number 4 have been received. As the window can hold n-1 frames at either end; a maximum of n-1 frames may be sent before an acknowledgement is required.



Sliding window

Sender Window

At the beginning of a transmission, the sender's window contains n-1 frames. As frames are sent out, the left boundary of the window moves inward, shrinking the size of the window. Given a window size 7, as shown in the following figure, if frames 0 through 5 have been sent and no acknowledgment has been received, the sender's window contains two



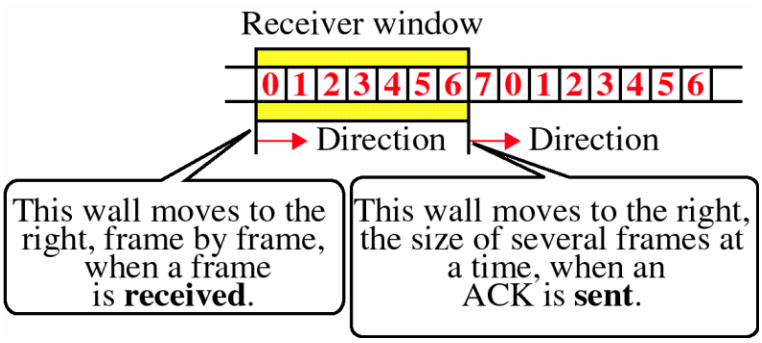
Sender sliding window

frames 5 and 6. Now, if an ACK numbered 4 is received, the frames 0 through 3 are known to have arrived undamaged and the sender's window expands to include the next four frames in its

buffer. At this point, the sender's window contains frames 5, 6, 7, 0, 1, 2. If an ACK numbered 2 is received, the sender's window would have expanded by only two frames, to contain a total of four.

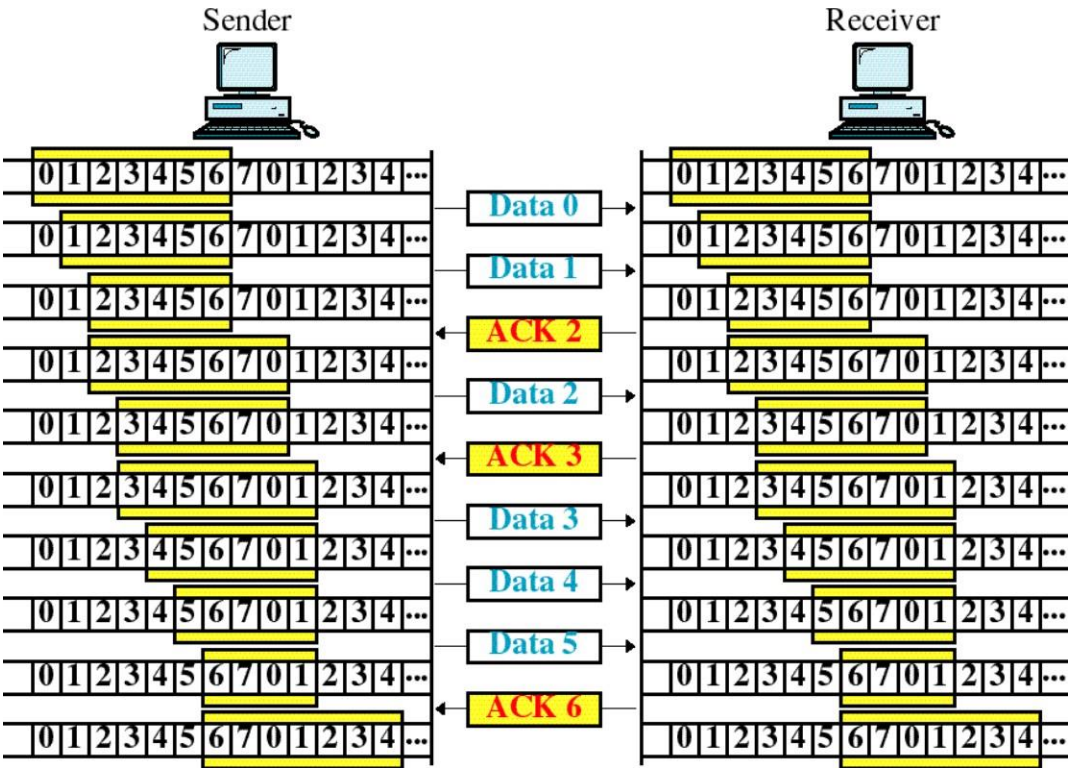
Receiver Window

At the beginning of the transmission, the receiver window contains n-1 spaces for frames. As new frames come in, the size of the receiver window shrinks. The receiver window therefore represents not the number of frames received but the number of frames that may still be received before an ACK must be sent. Figure 10.13 shows a window size 7. With the arrival of the first frame, the receiving window shrinks, moving the boundary space 0 to 1. The window has shrunk by one, so the receiver may now accept six frames before it is required to



Receiver sliding window

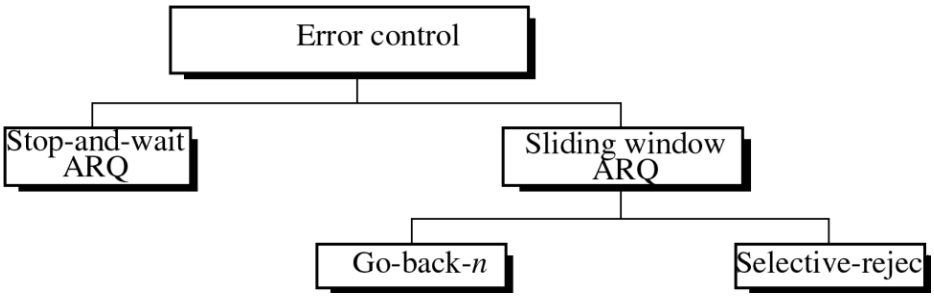
send an ACK. If frames 0 through 3 have arrived but have not been acknowledged, the window will contain three frame spaces. As each ACK is send out, the window expands to include a number of new frame spaces equal to the number of the most recently acknowledged frame minus the number of the previously acknowledged frame. In a seven frame window, if the prior ACK was for frame 2 and the current ACK is for frame 5, the window expands by three (5 – 2). If the prior ACK was for frame 3 and the current ACK is for frame 1, the window expands by six (1+8-3).



Example of sliding window

ERROR CONTROL

In the data link layer, error control refers to methods of error detection and retransmission.



Categories of error control

Automatic Repeat Request (ARQ)

Error correction in the data link layer is implemented anytime when an error is detected in an exchange, a negative acknowledgement (NAK) is returned and the specified frames are retransmitted. This process is called automatic repeat request (ARQ).

Sometimes a frame may be damaged by noise during transmission that the receiver does not recognize it as a frame at all. In those cases, ARQ allows us to say that the frame is lost. The second function of ARQ is the automatic retransmission of lost frames, including lost ACK and NAK frames.

Stop-and-wait flow control is usually implemented as stop-and-wait ARQ and sliding window is usually implemented as one of two variants of sliding window ARQ, called go-back-n or selective-reject.

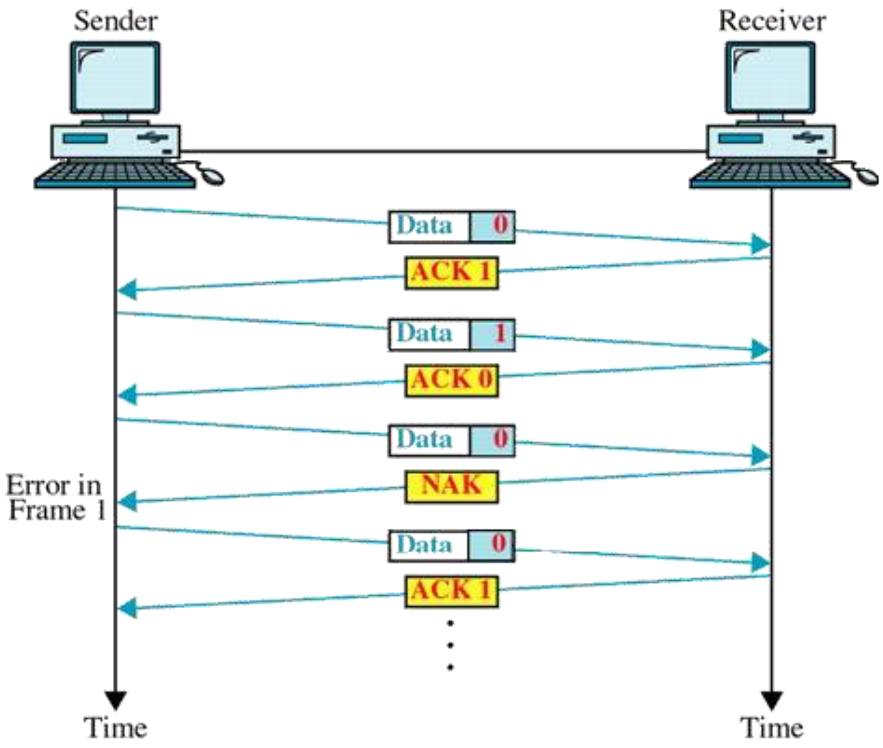
Stop-and-Wait ARQ

Stop-and-wait ARQ is a form of stop-and-wait flow control extended to include re-transmission of data in case of lost or damaged frames. For retransmission to work, four features are added to the basic flow control mechanism:

- The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame. Keeping a copy allows the sender to retransmit lost or damaged frames until they are received correctly.
- For identification purposes, both data frames and ACK frames are numbered alternately 0 and 1. A data 0 frame is acknowledged by an ACK 1 frame, indicating that the receiver has gotten data 0 and is now expecting data 1. This numbering allows for identification of data frames in case of duplicate transmission.
- If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are not numbered, tell the sender to retransmit the last frame sent. Stop-and-wait ARQ requires that the sender wait until it receives an acknowledgment for the last frame transmitted before it transmits the next one. When the sending device receives a NAK, it re-sends the frame transmitted after the last acknowledgment, regardless of number.
- The sending device is equipped with a timer. If an expected acknowledgment is not received within an allotted time period, the sender assumes that the last data frame was lost in transit and sends it again.

Damaged Frames

When a frame is discovered by the receiver to contain an error, it returns a NAK frame and the sender retransmits the last frame. For example, in the following figure, the sender transmits a data frame: data 0. The receiver returns an ACK 1, indicating that data 0 arrived undamaged and it is now expecting data 1. The sender transmits its next frame: data 1. It arrives undamaged, and the receiver returns ACK 0. The sender transmits its next frame: data 0. The receiver discovers an error in data 0 and returns a NAK. The sender retransmits data 0. This time data 0 arrives intact, and the receiver returns ACK 1.

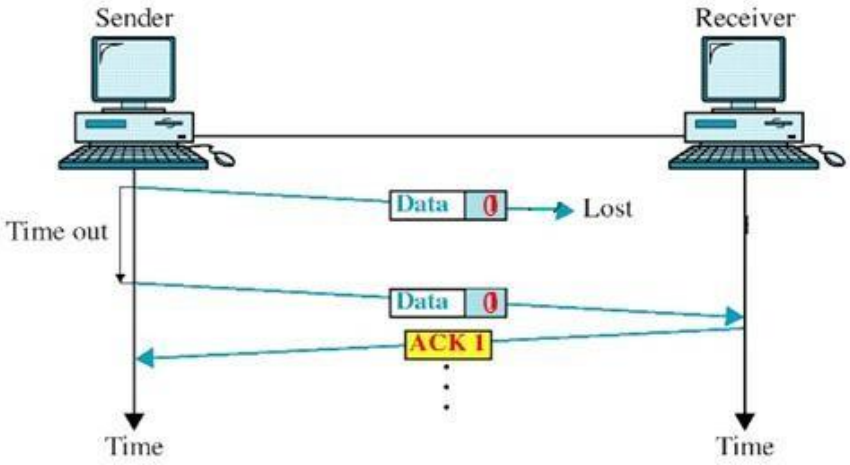


Stop-and-wait ARQ, damaged frame

Lost Frame

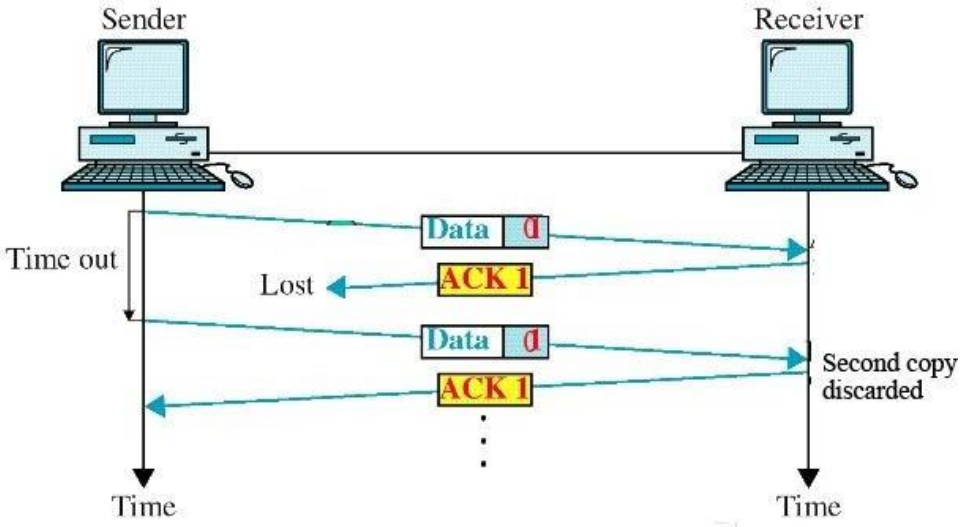
Any of the three frame types can be lost in transit.

Lost Data Frame the following figure shows how stop-and-wait ARQ handles the loss of a data frame. The sender is equipped with a timer that starts every time a data frame is transmitted. If the frame never makes it to the receiver, the receiver can never acknowledge it, positively or negatively. The sending device waits for an ACK or NAK frame until its timer goes off, at which point it tries again. It retransmits the last data frame, restarts its timer, and waits for an acknowledgment.



Stop-and-wait ARQ, lost data frame

Lost Acknowledgment In this case, the data frame has made it to the receiver and has been found to be either acceptable or not acceptable. But the ACK or NAK frame returned by the receiver is lost in transit. The sending device waits until its timer goes off, then retransmits the data frame. The receiver checks the number of the new data frame. If the lost frame was a NAK, the receiver accepts the new copy and returns the appropriate ACK (assuming the copy arrives undamaged). If the lost frame was an ACK, the receiver recognizes the new copy as a duplicate, acknowledges its receipt, then discards it and waits for the next frame.



Stop-and-wait ARQ, lost ACK frame

Sliding Window ARQ

Among the several popular mechanisms, for continuous transmission error control, two protocols are the most popular: go-back-n ARQ and selective-reject ARQ, both based on sliding window flow control. Three features are added to the basic flow control mechanism:

- The sending device keeps copies of all transmitted frames until they have been acknowledged. If frames 0 through 6 have been transmitted, and the last acknowledgment was for frame 2 (expecting 3), the sender keeps copies of frames 3 through 6 until it knows that they have been received undamaged.
- In addition to ACK frames, the receiver has the option of returning a NAK frame if the data have been received damaged. The NAK frame tells the sender to retransmit a damaged frame. Because sliding window is a continuous transmission mechanism both ACK and NAK frames must be numbered for identification. ACK frames will carry the number of the next frame expected. NAK frames, on the other hand, carry the number of the damaged frame itself. In both cases, the message to the sender is the number of the frame that the receiver expects next.
- Like stop-and-wait ARQ, the sending device in sliding window ARQ is equipped with a timer to enable it to handle lost acknowledgments. In sliding window ARQ, n - 1 frames (the size of the window) may be sent before an acknowledgment must be received. If n - 1 frames are awaiting acknowledgment, the sender starts a timer and waits before sending any more. If

the allotted time has run out with no acknowledgment, the sender assumes that the frames were not received and re-transmits one or all of the frames depending on the protocol. By retransmitting the data frames, two possibilities are covered: lost data and lost NAK. If the lost frame was an ACK frame, the receiver can recognize the redundancy by the number on the frame and discard the redundant data.

Go-Back-n ARQ

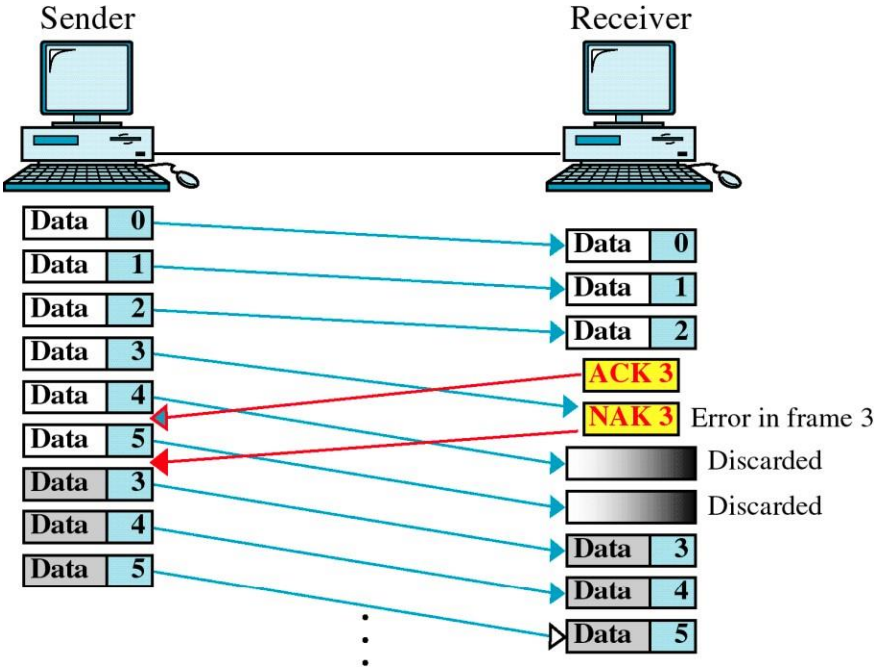
In this sliding window go-back-n ARQ method, if one frame is lost or damaged, all frames sent since the last frame acknowledged are retransmitted.

Damaged Frame What if frames 0, 1, 2, and 3 have been transmitted, but the first acknowledgment received is a NAK 3? Remember that a NAK means two things:

(1) a positive acknowledgment of all frames received prior to the damaged frame and

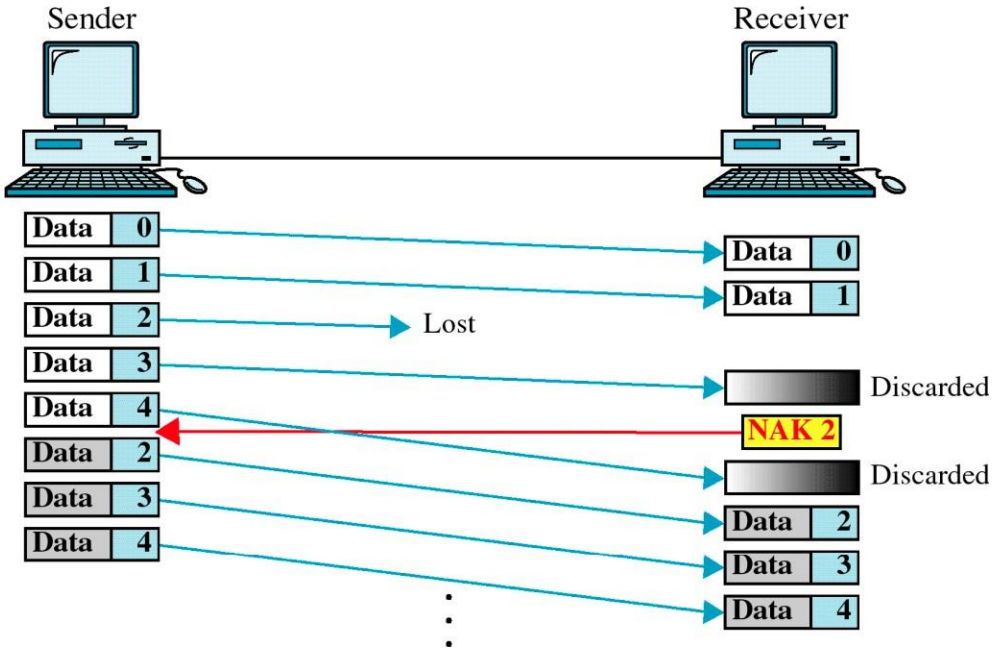
(2) a negative acknowledgment of the frame indicated.

If the first acknowledgment is a NAK 3, it means that data frames 0, 1, and 2 were all received in good shape. Only frame 3 must be resent. The following figure gives an example where six frames have been transmitted before an error is discovered in frame 3. In this case, an ACK 3 has been returned, telling the sender that frames 0, 1, and 2 have all been accepted. In the figure, the ACK 3 is sent before data 3 has arrived. Data 3 is discovered to be damaged, so a NAK 3 is sent immediately and frames 4 and 5 are discarded as they come in. The sending device retransmits all three frames (3, 4, and 5) sent since the last acknowledgment, and the process continues. The receiver discards frames 4 and 5 (as well as any subsequent frames) until it receives a good data 3.



Go-back-n, damaged data frame

Lost Data Frame Sliding window protocols require that data frames be transmitted sequentially. If one or more frames are so noise corrupted that they become lost in transit, the next frame to arrive at the receiver will be out of sequence. The receiver checks the identifying number on each frame, discovers that one or more have been skipped, and returns a NAK for the first missing frame. A NAK frame does not indicate whether the frame has been lost or damaged, just that it needs to be resent. The sending device then retransmits the frame indicated by the NAK, as well as any frames that it had transmitted after the lost one.

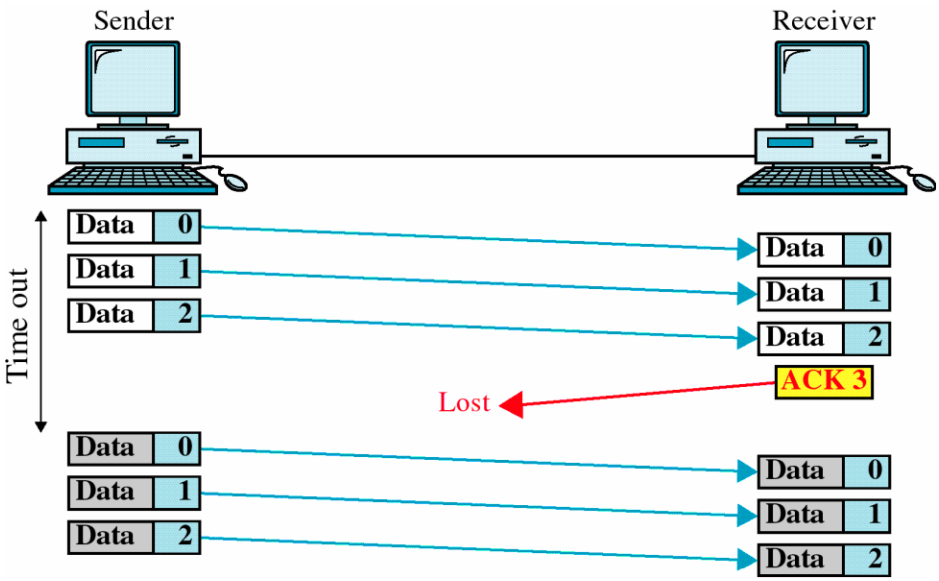


Go-back-n, lost data frame

In the above figure, data 0 and data 1 arrive intact but data 2 is lost. The next frame to arrive at the receiver is data 3. The receiver is expecting data 2 and so considers data 3 to be an error, discards it, and returns a NAK 2, indicating that 0 and 1 have been accepted but 2 is in error (in this case lost). In this example, because the sender has transmitted data 4 before receiving the NAK 2, data 4 arrives at the destination out of sequence and is therefore discarded. Once the sender receives the NAK 2, it retransmits all three pending frames (2, 3, and 4).

Lost Acknowledgment The sender is not expecting to receive an ACK frame for every data frame it sends. It cannot use the absence of sequential ACK numbers to identify lost ACK, or NAK frames. Instead, it uses a timer. The sending device can send as many frames as the window allows before waiting for an acknowledgment. Once that limit has been reached or the sender has no more frames to send, it must wait. If the ACK (or, especially, if the NAK) sent by the receiver has been lost, the sender could wait forever. To avoid tying up both devices, the sender is equipped with a timer that begins counting whenever the window capacity is reached. If an acknowledgment has not been received within the time limit, the sender retransmits every frame transmitted since the last ACK. The following figure shows a situation in which the

sender has transmitted all of its frames and is waiting for an acknowledgment that has been lost along the way. The sender waits a predetermined amount of time, then retransmits the unacknowledged frames. The receiver recognizes that the new transmission is a repeat of an earlier one, sends another ACK, and discards the redundant data.



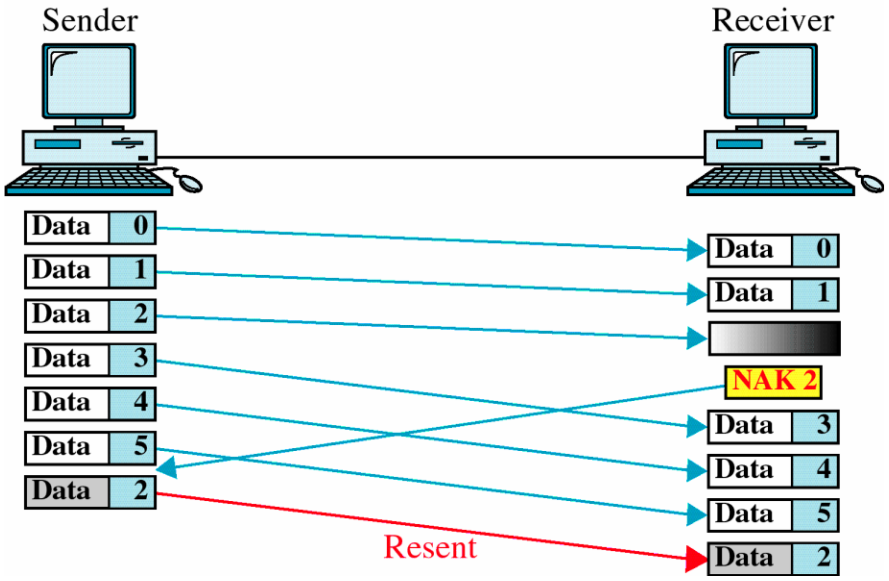
Go-back-n, lost ACK

Selective-Reject ARQ

In selective-reject ARQ, only the specific damaged or lost frame is retransmitted. If a frame is corrupted in transit, a NAK is returned and the frame is resent out of sequence. The receiving device must be able to sort the frames it has and insert the retransmitted frame into its proper place in the sequence. To make such selectivity possible, a selective-reject ARQ system differs from a go-back-n ARQ system in the following ways:

- The receiving device must contain sorting logic to enable it to reorder frames received out of sequence. It must also be able to store frames received after a NAK has been sent until the damaged frame has been replaced.
- The sending device must contain a searching mechanism that allows it to find and select only the requested frame for retransmission.
- A buffer in the receiver must keep all previously received frames on hold until all retransmissions have been sorted and any duplicate frames have been identified and discarded.
- To aid selectivity, ACK numbers, like NAK numbers, must refer to the frame received (or lost) instead of the next frame expected.
- This complexity requires a smaller window size than is needed by the go-back-n method if it is to work efficiently. It is recommended that the window size be less than or equal to (n + 1)/2, where n — 1 is the go-back-n window size.

Damaged Frames the following figure shows a situation in which a damaged frame is received. As you can see, frames 0 and 1 are received but not acknowledged. Data 2 arrives and is found to contain an error, so a NAK 2 is returned. Like NAK frames in go-back-n error correction, a NAK here both acknowledges the intact receipt of any previously unacknowledged data frames and indicates an error in the current frame. In the figure, NAK 2 tells the sender that data 0 and data 1 have been accepted, but that data 2 must be resent. Unlike the receiver in a go-back-n system, however, the receiver in a selective-reject system continues to accept new frames while waiting for an error to be corrected. However, because an ACK implies the successful receipt not only of the specific frame indicated but of all previous frames, frames received after the error frame cannot be acknowledged until the damaged frames have been retransmitted. In the figure, the receiver accepts data 3, 4, and 5 while waiting for a new copy of data 2. When the new data 2 arrives, an ACK 5 can be returned, acknowledging the new data 2 and the original frames 3, 4, and 5.



Selective-reject, damaged data frame

Lost Frames Although frames can be accepted out of sequence, they cannot be acknowledged out of sequence. If a frame is lost, the next frame will arrive out of sequence. When the receiver tries to reorder the existing frames to include it, it will discover the discrepancy and return a NAK. Of course, the receiver will recognize the omission only if other frames follow. If the lost frame was the last of the transmission, the receiver does nothing and the sender treats the silence like a lost acknowledgment.

Lost Acknowledgment Lost ACK and NAK frames are treated by selective-reject ARQ just as they are by go-back-n ARQ. When the sending device reaches either the capacity of its window or the end of its transmission, it sets a timer. If no acknowledgment arrives in the time allotted, the sender retransmits all of the frames that remain unacknowledged. In most cases, the receiver will recognize any duplication and discard them.