# SEC1306-DATA COMMUNICATION AND NETWORKING

## UNIT-I DATA COMMUNICATION- BASICS

**Digital data - digital signals - Bit rate - Bit length - Data rate limits - noise less channels - Noisy channel - Shanon capacity - Performance - Bandwidth - throughput - latency - Bandwidth delay product - jitters. Circuit switched networks - Datagram networks - virtual circuit networks - connection oriented and connection less services - Structure of circuit switches and packet switches - OSI reference model - TCP/IP reference model - comparison of both models.**

**Data communications** refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media.

**Digital data** is information stored on a computer system as a series of 0's and 1's in a binary language. Information is stored on computer disks and drives as a magnetically charged switch which is in either a 0 or 1 state.

**A digital signal** refers to an electrical signal that is converted into a pattern of bits. Unlike an analog signal, which is a continuous signal that contains time-varying quantities, a digital signal has a discrete value at each sampling point. The precision of the signal is determined by how many samples are recorded per unit of time.

**Bit rate** describes the **rate** at which **bits** are transferred from one location to another. In other words, it measures how much data is transmitted in a given amount of time.

**Bitrate** is commonly measured in **bits** per second (bps), kilobits per second (Kbps), or megabits per second (Mbps).

**Bit length** is the distance one bit occupies on the transmission medium

Bit Length = propagation speed X bit duration

## Data rate limits

A very important consideration in data communications is how fast we can send data, in bits per second, over a channel.

Data rate depends on 3 factors:

1. The bandwidth available
2. The level of the signals we use
3. The quality of the channel

## Noise less channels

For noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

Bit rate = 2 X bandwidth X $\log_2 L$

## Noisy channel

For noisy channel, **Shannon capacity** formula defines the theoretical maximum bit rate

Capacity = bandwidth X $\log_2 (1 + SNR)$

SNR is the signal to noise ratio and the capacity of the channel is in bits per second

## Performance

## Bandwidth

Is a range of frequencies within a given band, in particular that used for transmitting a signal, measured in hertz. **Or** bits per second (bit/s)

### Throughput

Throughput refers to how much data can be transferred from one location to another in a given amount of time

### Latency

It is an expression of how much time it takes for a packet of data to get from one designated point to another. It is sometimes measured as the time required for a packet to be returned to its sender.

Latency = propagation time + transmission time + queuing time + processing delay

### Propagation Time

The amount of **time** it takes for a bit to travel from the source to the destination. It can be computed as the ratio between the distance and the **propagation** speed over the specific medium.

### Bandwidth delay product

It defines the number of bits that can fill the link

### Jitters

Jitter is simply the difference in packet delay. In other words, jitter is measuring time difference in packet inter-arrival time.

### Switching

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks. The number and length of the links require too much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time. Other topologies employing multipoint connections, such as a bus, are ruled out because the distances between devices and the total number of devices increase beyond the capacities of the media and equipment.

A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. Figure 1.1 shows a switched network.

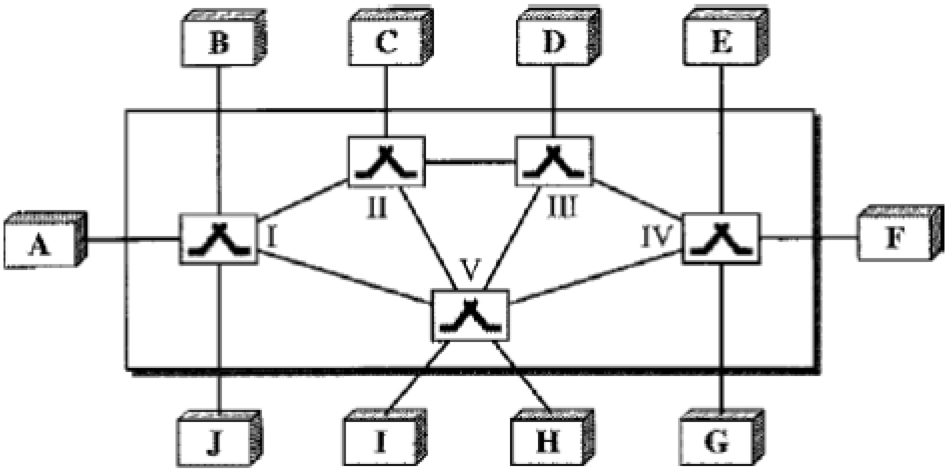
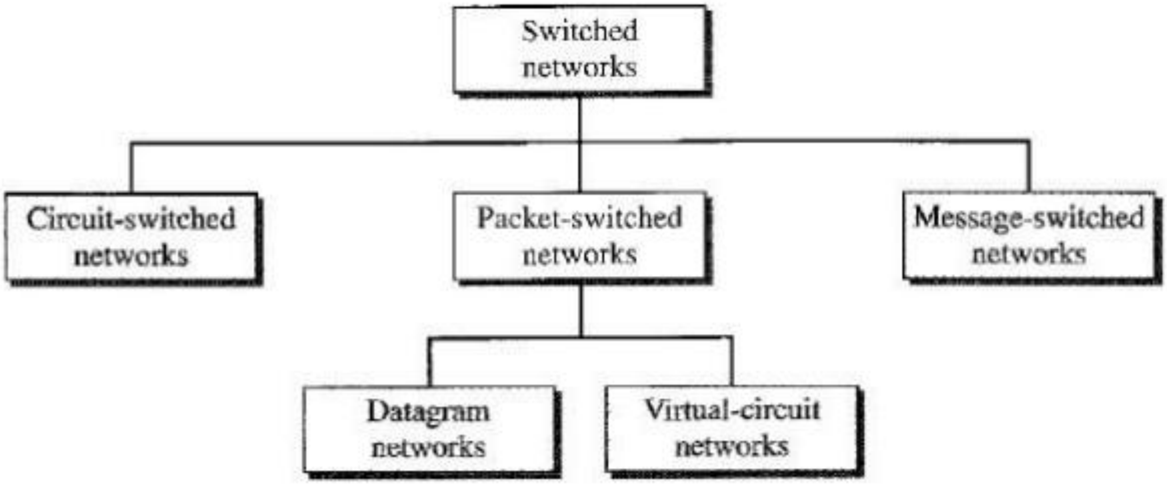


Fig.1.1 switched network

The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

**Taxonomy of switched networks**



## CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM

Figure 1.2 shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.

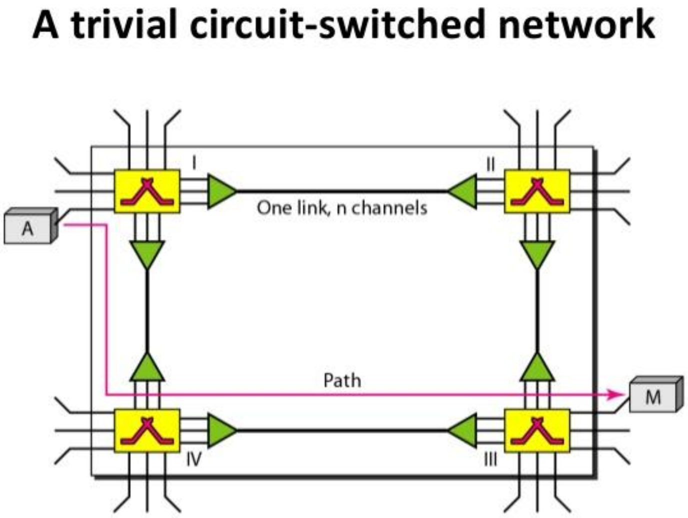


Fig 1.2 trivial circuit-switched network

**Three Phases**

The actual communication in a circuit-switched network requires three phases:

1. Connection setup

2. Data transfer,

3. Connection teardown

**1. Setup Phase**:

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. For example, in Figure 1.2, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time.

In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established. Note that end-to-end addressing is required for creating a connection between the two end systems. These can be, for example, the addresses of the computers assigned by the administrator in a TDM network, or telephone numbers in an FDM network.

**2. Data Transfer Phase**:

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

**3. Teardown Phase**: When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

**Efficiency:**

It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation. However, in computer networks, a computer can be connected to another computer even if there is no activity for a long time. In this case, allowing resources to be dedicated means that other connections are deprived.

**Delay**: Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection.

Figure 1.3 shows the idea of delay in a circuit switched network when only two switches are involved. As Figure shows, there is no waiting time at each switch. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

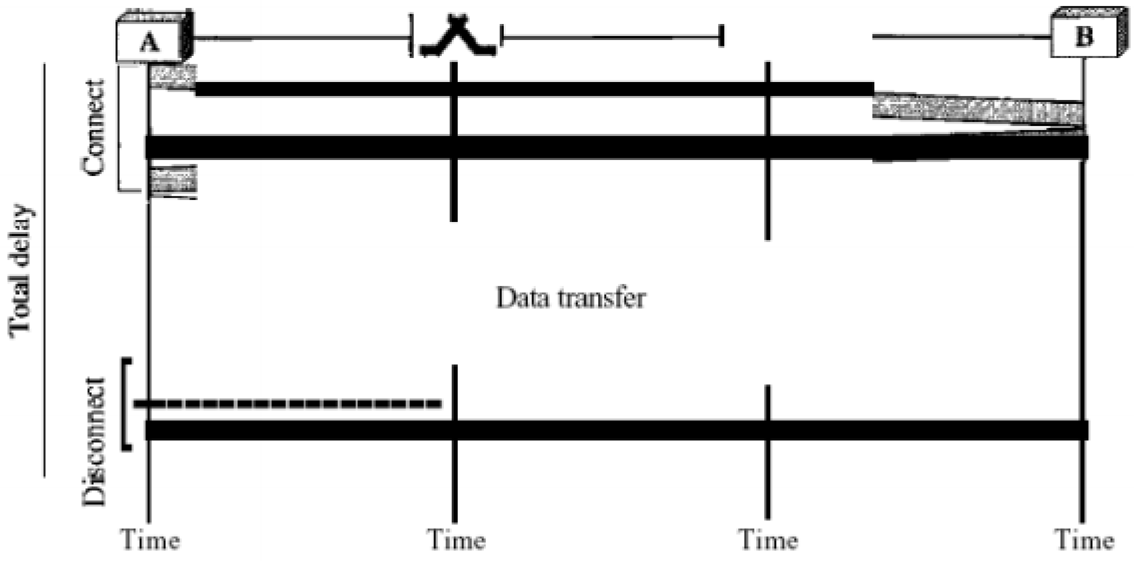


Fig 1.3 delay in a circuit switched network

The delay caused by the setup is the sum of four parts: the propagation time of the source computer request (slope of the first gray box), the request signal transfer time (height of the first gray box), the propagation time of the acknowledgment from the destination computer (slope of the second gray box), and the signal transfer time of the acknowledgment (height of the second gray box).

The delay due to data transfer is the sum of two parts: the propagation time (slope of the colored box) and data transfer time (height of the colored box), which can be very long. The third box shows the time needed to tear down the circuit. We have shown the case in which the receiver requests disconnection, which creates the maximum delay.

**DATAGRAM NETWORKS**

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer. Figure 1.4 shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers. That is why we use a different symbol for the switches in the figure.

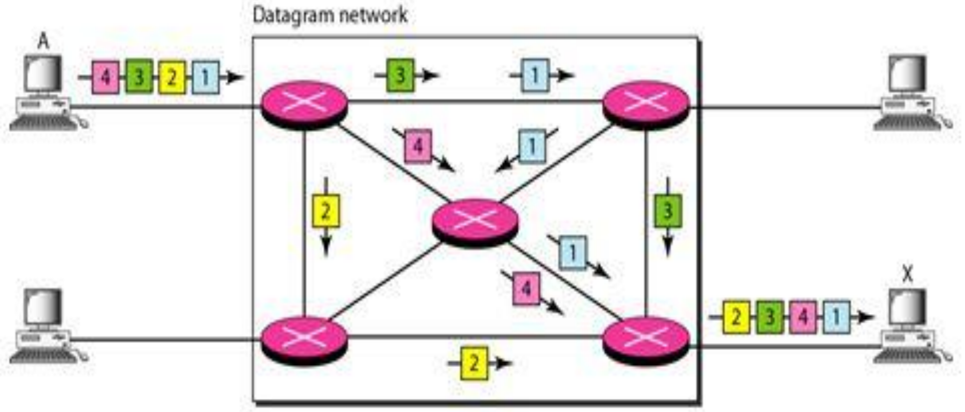


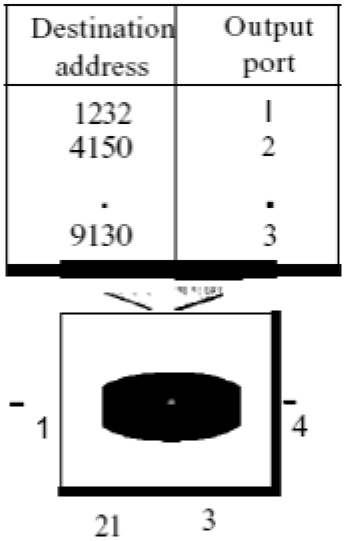
Fig 1.4 datagram network

In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources.

In most protocols, it is the responsibility of an upperlayer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application. The datagram networks are sometimes referred to as connectionless networks. The term connectionless here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

**Routing Table:**

If there are no setup or teardown phases, how are the packets routed to their destinations in a datagram network? In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over. Figure 1.5 shows the routing table for a switch.



| Destination address | Output port |
|---|---|
| 1232 | 1 |
| 4150 | 2 |
| . | . |
| 9130 | 3 |

Fig 1.5 Routing table in a datagram network

**Destination address**:

Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded. This address, unlike the address in a virtual circuit-switched network, remains the same during the entire journey of the packet.

**Efficiency**:

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

**Delay:**

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

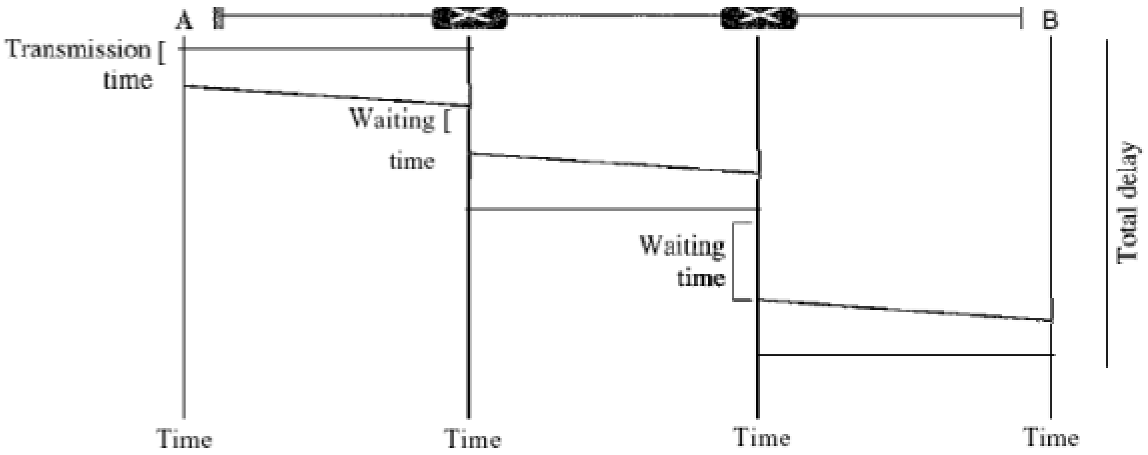


Fig 1.6 Delay in a datagram network

The packet travels through two switches. There are three transmission times (3T), three propagation delays (slopes 3't of the lines), and two waiting times (WI + w2)' we ignore the processing time in each switch.

The total delay is Total delay =3T + 3t + WI + W2

**VIRTUAL-CIRCUIT NETWORKS**:

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packet is being canied), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no

final destination address carried by a packet. The answer will be clear when we discuss virtual circuit identifiers in the next section.

4. As in a circuit-switched network, all packets follow the same path established during the connection.

5. A virtual-circuit network is normally implemented in the data link layer, while a circuit switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future. Figure 1.7 is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

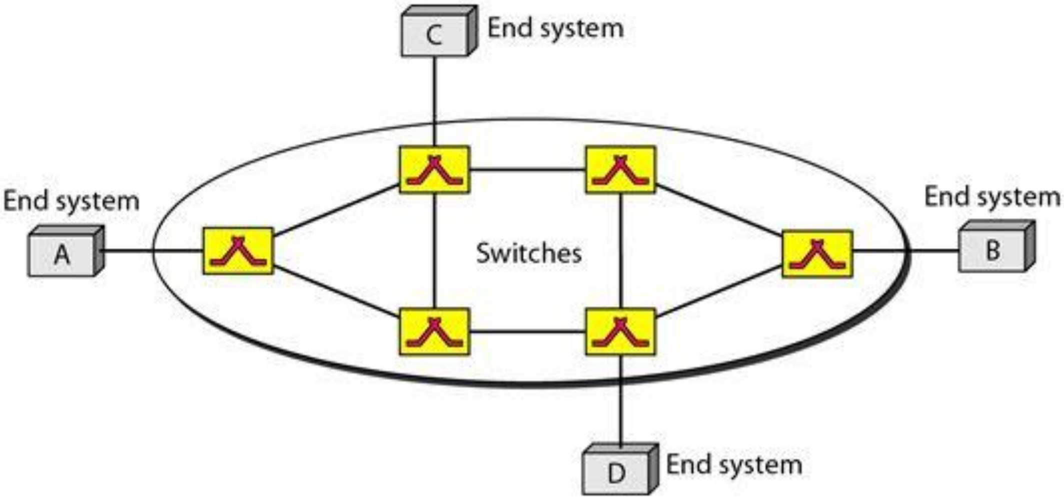


Fig 1.7 Virtual-circuit network

**Addressing**

In a virtual-circuit network, two types of addressing are involved:

Global and local (virtual-circuit identifier).

Global Addressing: A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally if the network is part of an international network. However, we will see that a global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

**Virtual-Circuit Identifier**: The identifier that is actually used for data transfer is called the virtual circuit identifier (Vel). A vel, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl. Figure 1.8 shows how the VCI in a data frame changes from one switch to another. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCls.

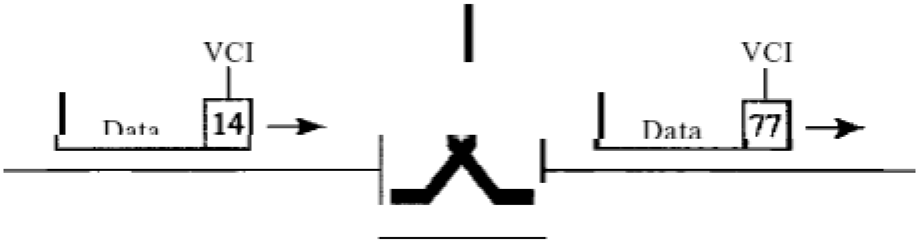


Fig 1.8 Virtual-circuit identifier

**Three Phases**

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.

**In the setup phase**,

The source and destination use their global addresses to help switches make table entries for the connection. In the teardown phase, the source and destination inform the switches to delete the corresponding entry. Data transfer occurs between these two phases. We first discuss the data transfer phase, which is more straightforward; we then talk about the setup and teardown phases.

**Data Transfer Phase**:

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up. We show later how the switches make their table entries, but for the moment we assume that each switch has a table with entries for all active virtual circuits. The process creates a virtual circuit, not a real circuit, between the source and destination.

**Setup Phase**

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment

**Efficiency**

As we said before, resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data transfer phase. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays. There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it. Consider a family that wants to dine at a restaurant. Although the restaurant may not accept reservations (allocation of the tables is on demand), the family can call and find out the waiting time. This can save the family time and effort.

**Delay in Virtual-Circuit Networks**

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Below Figure 1.9 shows the delay for a packet traveling through two switches in a virtual circuit network.

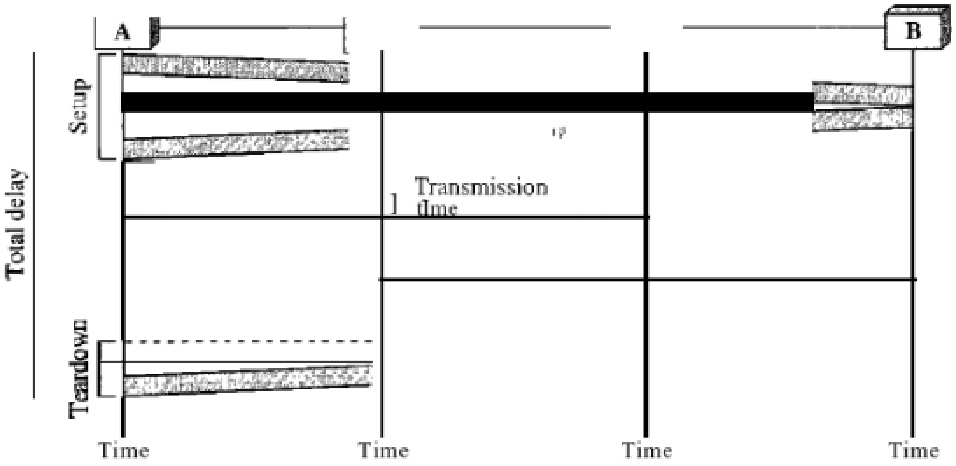


Fig 1.9 Delay in a virtual-circuit network

The packet is traveling through two switches (routers). There are three transmission times (3T), three propagation times (3't), data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction). We ignore the processing time in each switch.

The total delay time is Total delay = 3T+ 3't + setup delay + teardown delay

**Differences between Virtual Circuits & Datagram Networks**

**Virtual Circuits-**

1. It is connection-oriented simply meaning that there is a reservation of resources like buffers, CPU, bandwidth,etc. for the time in which the newly setup VC is going to be used by a data transfer session.
2. First packet goes and reserves resources for the subsequent packets which as a result follow the same path for the whole connection time.
3. Since all the packets are going to follow the same path, a global header is required only for the first packet of the connection and other packets generally don’t require global headers.
4. Since data follows a particular dedicated path, packets reach inorder to the destination.
5. From above points, it can be concluded that Virtual Circuits are highly reliable means of transfer.
6. Since each time a new connection has to be setup with reservation of resources and extra information handling at routers, its simply costly to implement Virtual Circuits.

**Datagram Networks:**

1. It is connectionless service. There is no need of reservation of resources as there is no dedicated path for a connection session.
2. All packets are free to go to any path on any intermediate router which is decided on the go by dynamically changing routing tables on routers.

3. Since every packet is free to choose any path, all packets must be associated with a header with proper information about source and the upper layer data.

4. The connectionless property makes data packets reach destination in any order, means they need not reach in the order in which they were sent.

5. Datagram networks are not reliable as Virtual Circuits.

6. But it is always easy and cost efficient to implement datagram networks as there is no extra headache of reserving resources and making a dedicated each time an application has to communicate.

**ISO / OSI MODEL**:

ISO refers International Standards Organization was established in 1947, it is a multinational body dedicated to worldwide agreement on international standards. OSI refers to Open System Interconnection that covers all aspects of network communication. It is a standard of ISO. Here open system is a model that allows any two different systems to communicate regardless of their underlying architecture. Mainly, it is not a protocol it is just a model.

**OSI MODEL**

The open system interconnection model is a layered framework. It has seven separate but interrelated layers. Each layer having unique responsibilities.

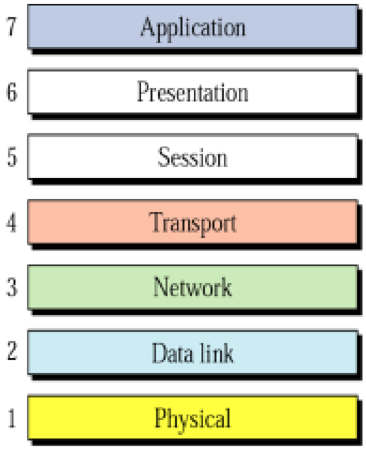


Fig 1.10 The OSI Model

The OSI model shown in figure 1.10 is based on the proposal developed by the International Standards Organization (ISO) as a first step towards international standardization of the protocols used in the various layers. The model is called the OSI (Open System Interconnection) reference model because it deals with connecting open systems, i.e., systems that are open for communication with other systems. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

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 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 principles that were applied to arrive at the seven layers are as follows:

* A layer should be created where a different level of abstraction is needed. * Each layer should perform a well-defined function.

* The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

* The layer boundaries should be chosen to minimize the information flow across the interfaces. * The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

**Layered Architecture** :

The OSI model is composed of seven layers: Physical, Data link, Network, Transport, Session, Presentation, Application layers.

Figure 1.11 shows the layers involved when a message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes involve only the first 3 layers of the OSI model. Within a single machine, each layer calls upon the services of the layer just below it, layer 3 for ex. Uses the services provided by layer 2 & 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 & 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.

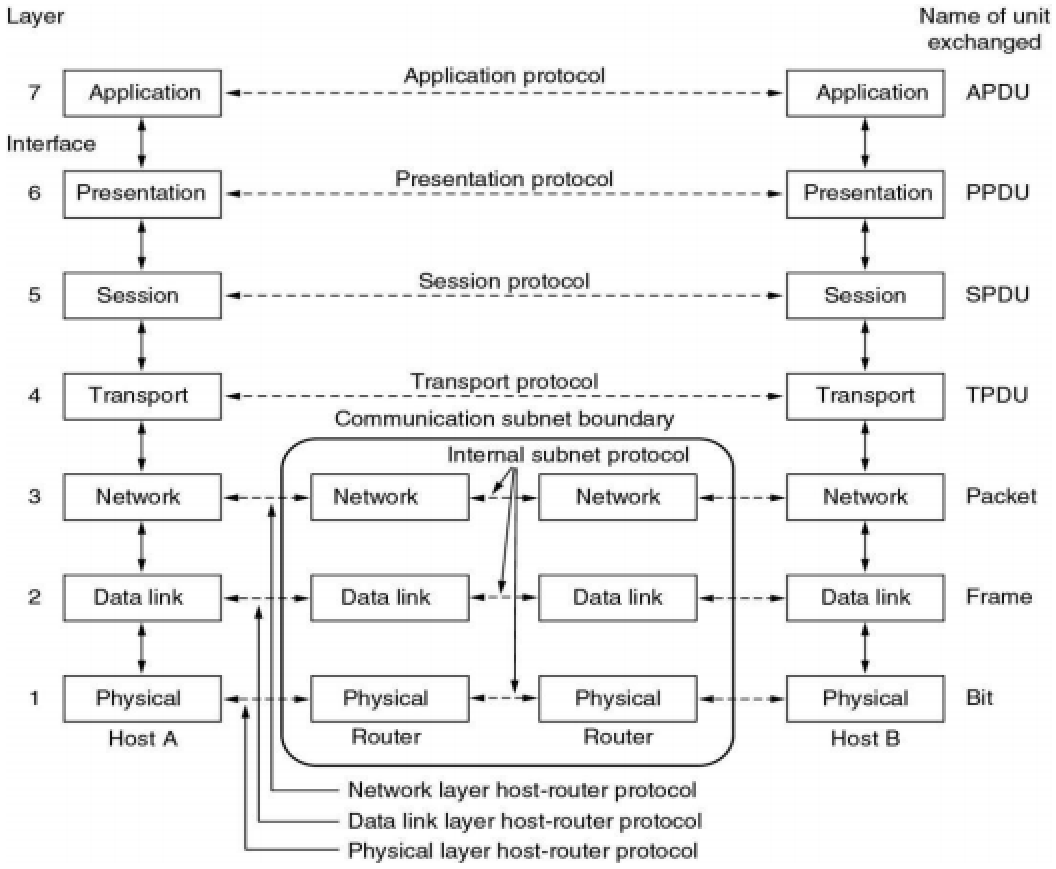


Figure 1.11 the interaction between layers in the OSI model

## ORGANIZATION OF LAYERS

The seven layers are arranged by three sub groups.

1. Network Support Layers

2. User Support Layers

3. Intermediate Layer

**Network Support Layers**:

Physical, Datalink and Network layers come under the group. They deal with the physical aspects of the data such as electrical specifications, physical connections, physical addressing, and transport timing and reliability.

**User Support Layers**:

Session, Presentation and Application layers comes under the group. They deal with the interoperability between the software systems.

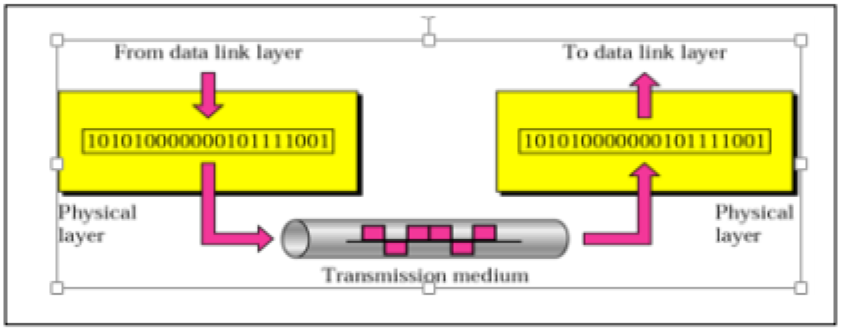
**Intermediate Layer**:

The transport layer is the intermediate layer between the network support and the user support layers.

## FUNCTIONS OF THE LAYERS

### PHYSICAL LAYER

The physical layer coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and the transmission medium.



The functions are,

1. Physical Characteristics of Interfaces and Media: It defines the electrical and mechanical characteristics of the* interface and the media. It defines the types of transmission medium

2. Representation of Bits: To transmit the stream of bits they must be encoded into signal. It defines the type of encoding weather electrical or optical.

3. Data Rate: It defines the transmission rate i.e. the number of bits sent per second.

4. Synchronization of Bits: The sender and receiver must be synchronized at bit level.

5. Line Configuration: It defines the type of connection between the devices.

Two types of connection are

1. Point to point 2. Multipoint

6. Physical Topology: It defines how devices are connected to make a network.

Five topologies are,

1. mesh 2. star 3. tree 4. bus 5. ring

7. Transmission Mode It defines the direction of transmission between devices.

Three types of transmission are, 1. simplex 2. half duplex3. full duplex

**DATALINK LAYER**

Datalink layer responsible for node-to-node delivery

The responsibilities of Datalink layer are,

1. Framing: It divides the stream of bits received from network layer into manageable data units called frames.

2. Physical Addressing: It adds a header that defines the physical address of the sender and the receiver. If the sender and the receiver are in different networks, then the receiver address is the address of the device which connects the two networks.

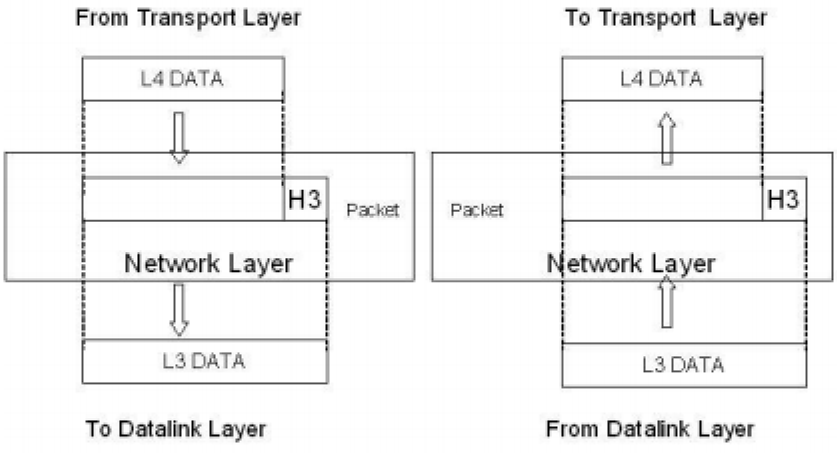
3. Flow Control: It imposes a flow control mechanism used to ensure the data rate at the sender and the receiver should be same.

4. Error Control: To improve the reliability the Datalink layer adds a trailer which contains the error control mechanism like CRC, Checksum etc

5. Access Control: When two or more devices connected at the same link, then the Datalink layer used to determine which device has control over the link at any given time.

**NETWORK LAYER**

When the sender is in one network and the receiver is in some other network then the network layer has the responsibility for the source to destination delivery.



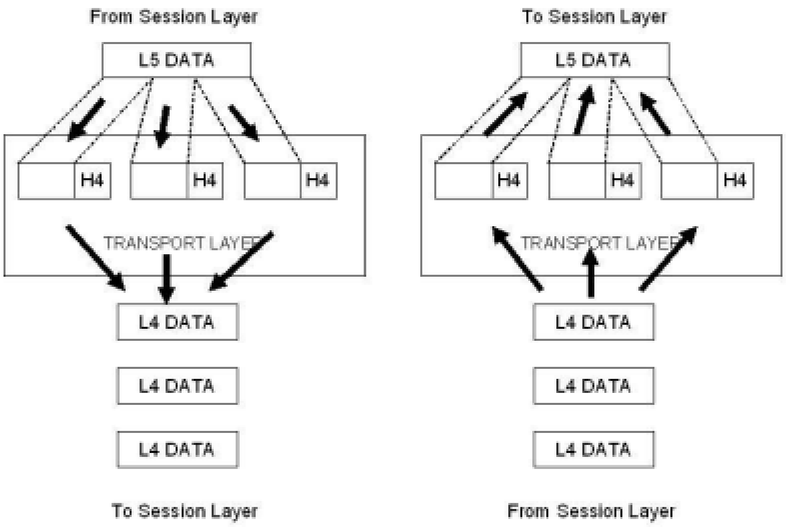
The responsibilities are,

1. Logical Addressing: If a packet passes the network boundary that is when the sender and receiver are places in different network then the network layer adds a header that defines the logical address of the devices.

2. Routing: When more than one networks connected and to form an internetwork, the connecting devices route the packet to its final destination. Network layer provides this mechanism.

**TRANSPORT LAYER**

The network layer is responsible for the end to end delivery of the entire message. It ensures that the whole message arrives in order and intact. It ensures the error control and flow control at source to destination level.



The responsibilities are,

1. Service point Addressing: A single computer can often run several programs at the same time. The transport layer gets the entire message to the correct process on that computer. It adds a header that defines the port address which used to identify the exact process on the receiver.

2. Segmentation and Reassembly: A message is divided into manageable units called as segments. Each segment is reassembled after received that information at the receiver end. To make this efficient each segment contains a sequence number.

3. Connection Control: The transport layer creates a connection between the two end ports. It involves three steps. They are,

1. Connection establishment

2. Data transmission

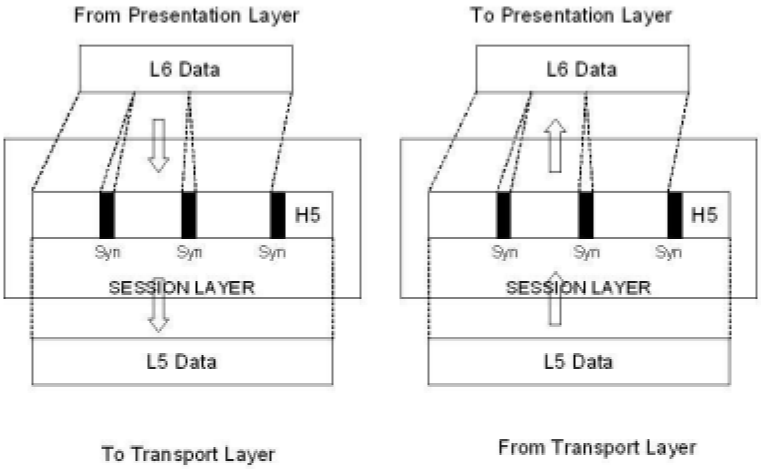
3. Connection discard

4. Flow Control Flow control is performed at end to end level

5. Error Control Error control is performed at end to end level.

## SESSION LAYER

It acts as a dialog controller. It establishes, maintains and synchronizes the interaction between the communication devices.



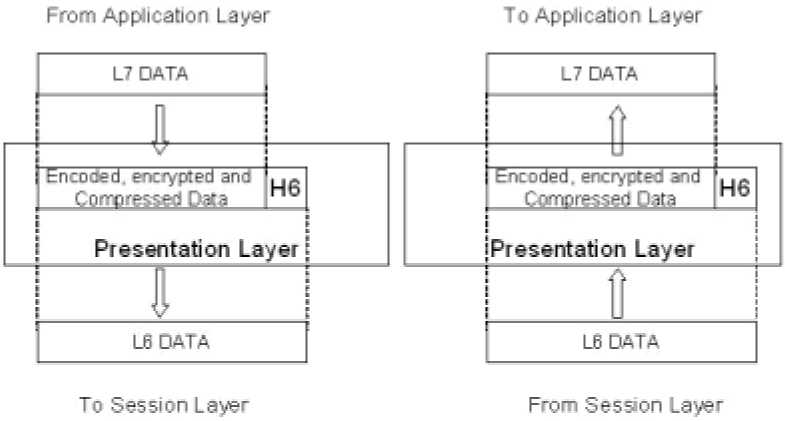
The responsibilities are,

1. Dialog Control: The session layer allows two systems to enter into a dialog. It allows the communication between the devices.

2. Synchronization: It adds a synchronization points into a stream of bits.

## PRESENTATION LAYER

The presentation layer is responsible for the semantics and the syntax of the information exchanged.



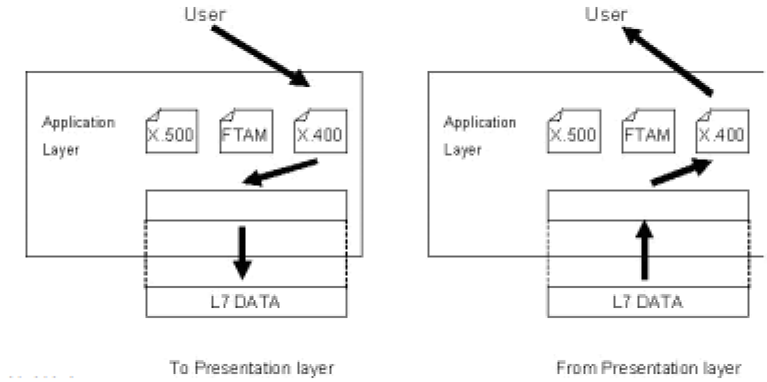
1. Translation: Different systems use different encoding systems. The presentation layer is responsible for interoperability between different systems. The presentation layer t the sender side translates the information from the sender dependent format to a common format. Likewise, at the receiver side presentation layer translate the information from common format to receiver dependent format.

2. Encryption: To ensure security encryption/decryption is used. Encryption means transforms the original information to another form. Decryption means retrieve the original information from the encrypted data

3. Compression: It used to reduce the number of bits to be transmitted.

## APPLICATION LAYER

The application layer enables the user to access the network. It provides interfaces between the users to the network.



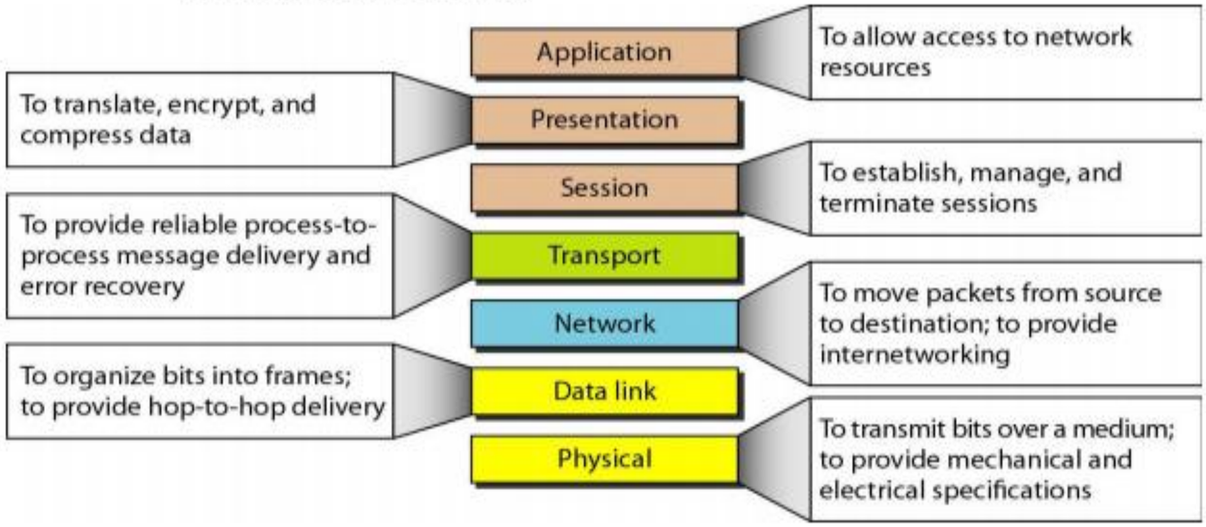
The responsibilities are,

1. Network Virtual Terminal: It is a software version of a physical terminal and allows a user to log on to a remote host.

2. File Transfer, Access, and Management: It allows a user to access files in a remote computer, retrieve files, and manage or control files in a remote computer.

3. Mail Services: It provides the basis for e-mail forwarding and storage.

4. Directory Services: It provides distributed database sources and access for global information about various objects and services.

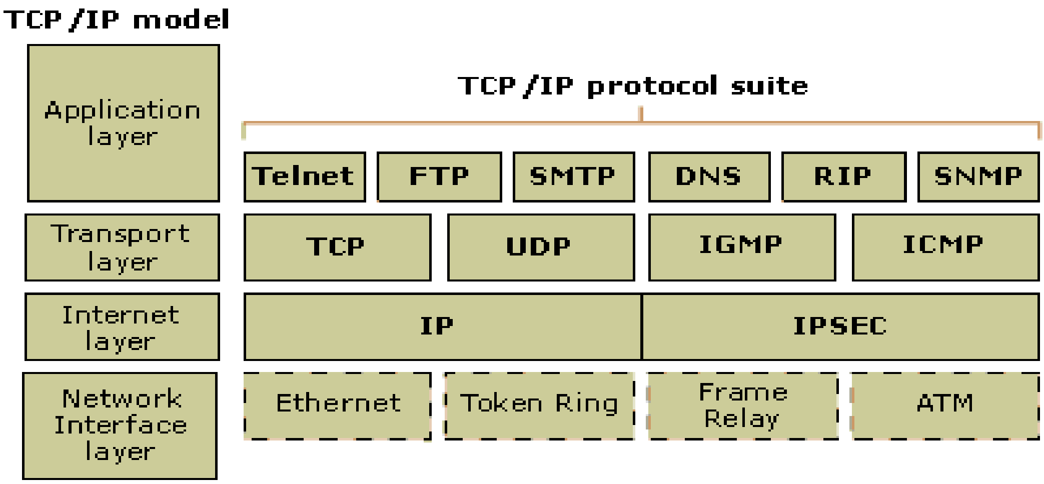


Summary of layer functions

Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

## TCP/IP reference model

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.



## Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network

## Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
   - Delivering IP packets
   - Performing routing

- Avoiding congestion

**Layer 3: Transport Layer**

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

**Layer 4: Application Layer**

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
   - **TCP (Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.

- **UDP (User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service

**Merits of TCP/IP model**

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

**Demerits of TCP/IP**

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

**Questions**

**Part A**

1. Define Bit rate
2. What are the Data rate limits
3. Differentiate Noise less channels and Noisy channel
4. Define Bandwidth , throughput and latency
5. Define jitter
6. Differentiate connection oriented and connection less services
7. What are the different types of switching networks
8. Differentiate circuit switches and packet switches
9. What is function of dialog control

10. What are layers in OSI model

11. What are the Merits and Demerits of TCP/IP model

12. Compare OSI and TCP/IP model

**Part B**

1. Draw and explain the layers in OSI model
2. Draw and explain the layers in TCP/IP model
3. Draw the structure of Circuit switched networks and explain the functions
4. Explain different types of packet switched networks

# UNIT 2
# NETWORKING

**Network Topologies - mesh, star, bus, and ring - hybrid topology - Network Standardization - De facto and De jure standards of networks - ITU - ISO - IETF - NIST - IEEE - Different IEEE802 working groups – internet Architecture of the internet - Third generation mobile networks - UMTS Architecture - Wired Ethernet - Wireless LANs IEEE 802.11 - RFID - Different types - sensor networks - Multi hop topology of sensor networks.**

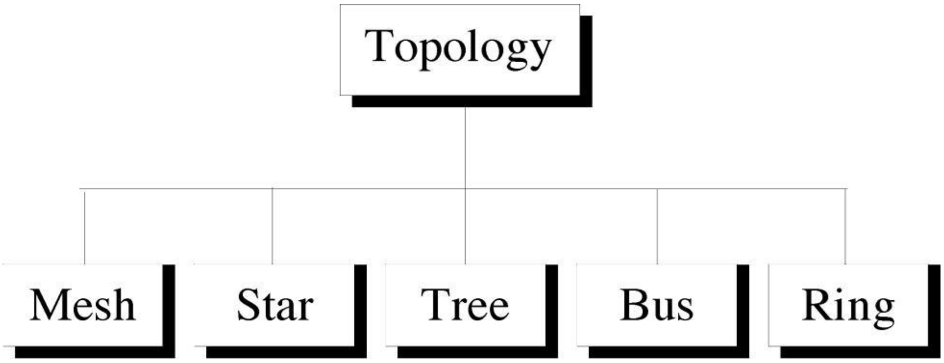
## Network Topologies

The term topology refers to the way a network is laid out, either physically or logically.

- Two or more devices connect to a link; two or more links form topology.

- The topology of a network is the geometric representation of the relationship of all the links and linking devices to each other.

- There are five basic topologies possible :



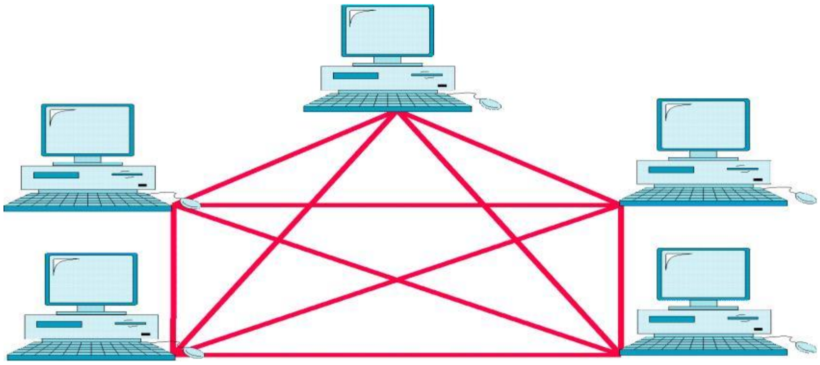
## Mesh topology

- In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only

- Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

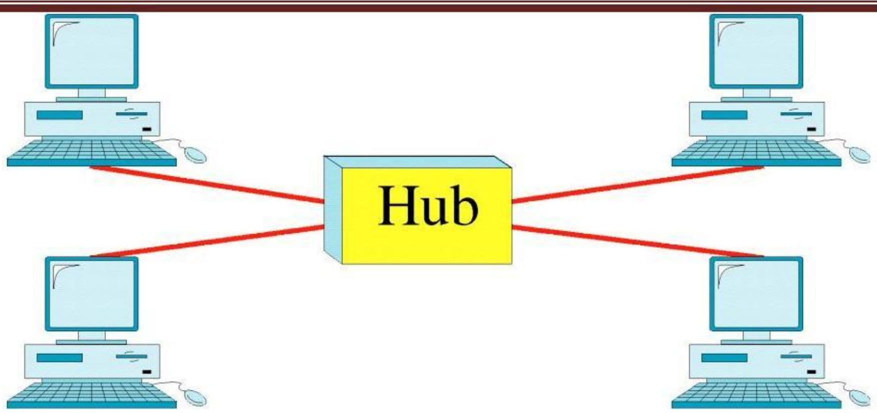
    - **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.

- **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.



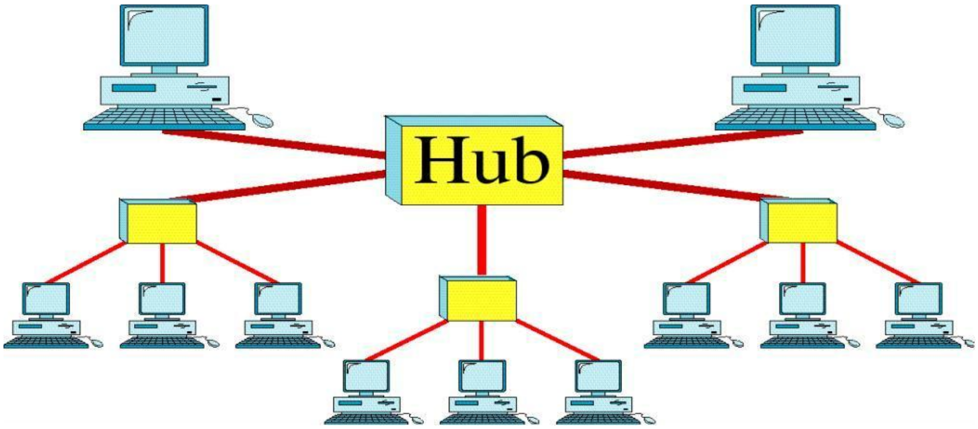
**Star topology**

- All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:
    - Layer-1 device such as hub or repeater
    - Layer-2 device such as switch or bridge
    - Layer-3 device such as router or gateway
- As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails.
- Every communication between hosts, takes place through only the hub.
- Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

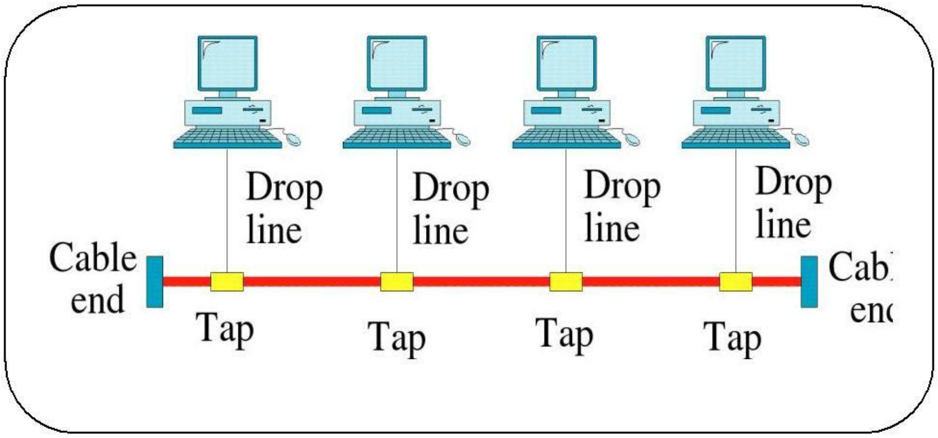


**Tree Topology**

- Nodes in a tree are linked to central hub that controls the traffic to the network.
- Not every device plugs directly to the central hub
- Majority of devices connected to secondary hub, that in turns connect to the central hub.
- The central hub in the tree is an active hub
- An active hub contains repeater
- The secondary hub may be active or passive
- A passive hub provides a simple physical connection between two attached devices.
- Repeater which is a hardware device that regenerates the received bit pattern before sending them out
- Repeating strengthens transmission and increases the distance a signal can travel.

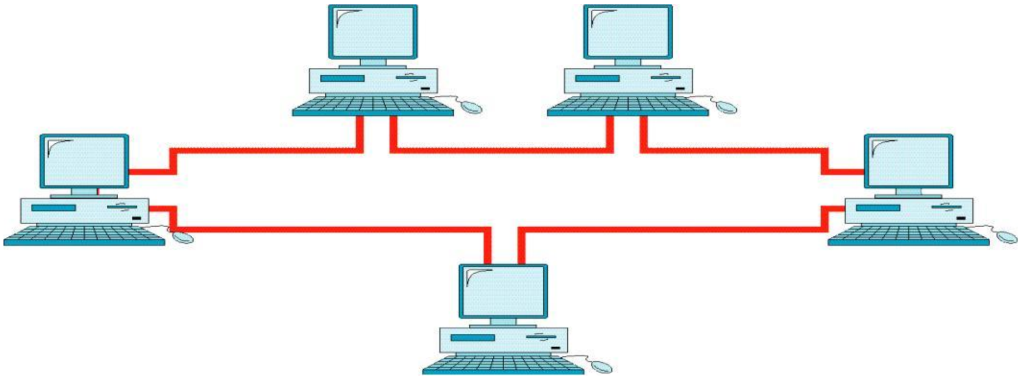


## Bus topology

- The bus topology is an example of multipoint configurations.
- One long cable acts as backbone, links all devices in the network.
- Nodes are connected to the bus cable by drop line and taps.
- A drop line is a connection running between the devices and the main cable.
- A tap is a connector that either splices in to the main cable or punctures the sheathing of a cable to create a contact with the metallic core
- 

## Ring topology

- In a ring topology ,each device has a dedicated point-to-point line configuration only with the two devices on either side of it.
- A signal is passed along the ring in one direction, from a 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



## STANDARDS IN NETWORKING

Standards are necessary in networking to ensure interconnectivity and interoperability between various networking hardware and software components.
Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.

### Concept of Standard

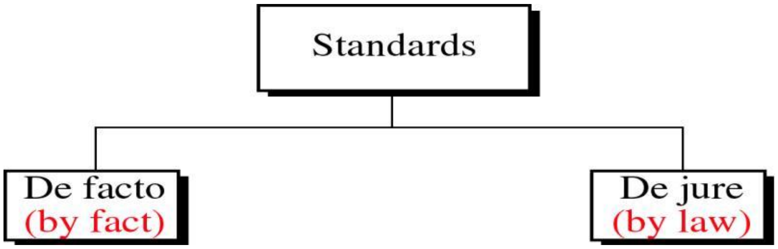
Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity.
Data communications standards are classified into two categories:

### 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.

### De jure standard

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



### Standard Organizations in field of Networking

- Standards are created by standards creation committees, forums, and government regulatory agencies.

- **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)

**Examples of Forums**

1. ATM Forum
2. MPLS Forum
3. Frame Relay Forum

**Examples of Regulatory Agencies:**

1. Federal Communications Committee (FCC)

**IEEE 802** is a family of IEEE standards dealing with local area networks and metropolitan area networks.

More specifically, the IEEE 802 standards are restricted to networks carrying variable-size packets. By contrast, in cell relay networks data is transmitted in short, uniformly sized units called cells. Isochronous networks, where data is transmitted as a steady stream of octets, or groups of octets, at regular time intervals, are also out of the scope of this standard. The number 802 was simply the next free number IEEE could assign, though "802" is sometimes associated with the date the first meeting was held — February 1980.

The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named logical link control (LLC) and media access control (MAC), so the layers can be listed like this:

- Data link layer
    - LLC sublayer
    - MAC sublayer
- Physical layer

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual working group provides the focus for each area.

**Wireless LAN and IEEE 802.11**

A wireless LAN (WLAN or WiFi) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure

In the corporate enterprise, wireless LANs are usually implemented as the final link between the existing wired network and a group of client computers, giving these users wireless access to the full resources and services of the corporate network across a building or campus setting.

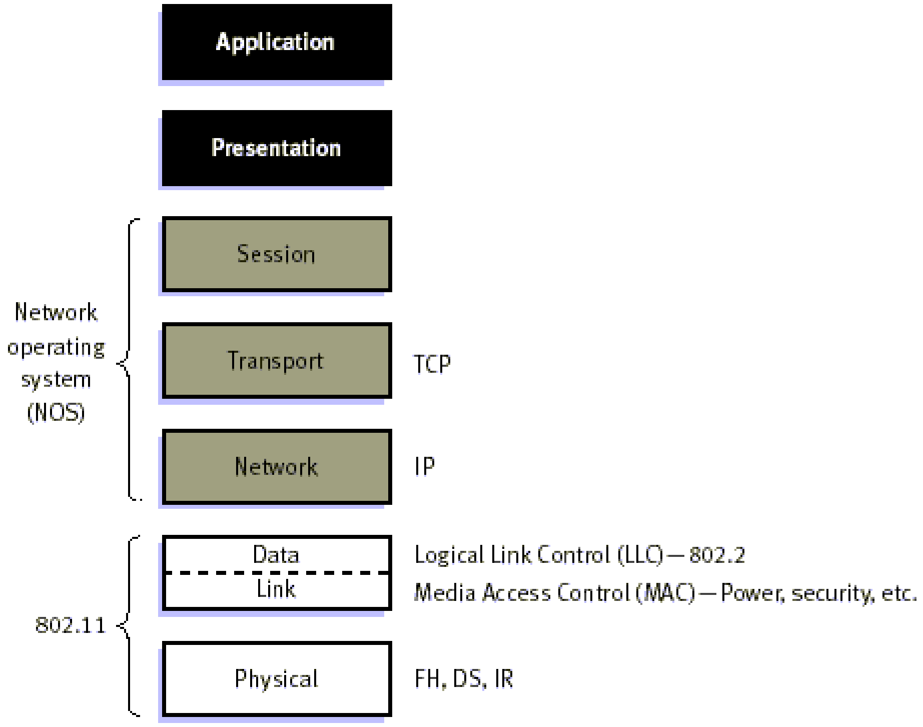
The widespread acceptance of WLANs depends on industry standardization to ensure product compatibility and reliability among the various manufacturers.

The 802.11 specification as a standard for wireless LANS was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in the year 1997. This version of 802.11 provides for 1 Mbps and 2 Mbps data rates and a set of fundamental signaling methods and other services. Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels the ISO model, the physical layer and link layer (see figure below). Any LAN application, network operating system, protocol, including TCP/IP and Novell NetWare, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

The major motivation and benefit from Wireless LANs is increased mobility. Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere.
The other advantages for WLAN include cost-effective network setup for hard-to-wire locations such as older buildings and solid-wall structures and reduced cost of ownership-particularly in dynamic environments requiring frequent modifications, thanks to minimal wiring and installation costs per device and user. WLANs liberate users from dependence on hard-wired access to the network backbone, giving them anytime, anywhere network access. This freedom to roam offers numerous user benefits for a variety of work environments, such as:

- Immediate bedside access to patient information for doctors and hospital staff
- Easy, real-time network access for on-site consultants or auditors
- Improved database access for roving supervisors such as production line managers, warehouse auditors, or construction engineers
- Simplified network configuration with minimal MIS involvement for temporary setups such as trade shows or conference rooms
- Faster access to customer information for service vendors and retailers, resulting in better service and improved customer satisfaction
- Location-independent access for network administrators, for easier on-site troubleshooting and support
- Real-time access to study group meetings and research links for students

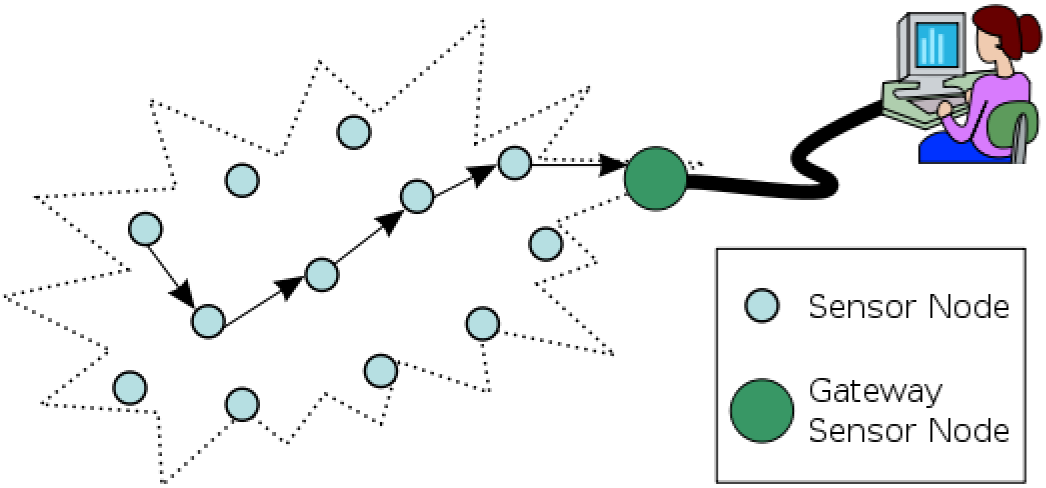
*Fig 1: "IEEE 802.11 and the ISO Model"*


Application
Presentation
Session
Network operating system (NOS)
Transport
TCP
Network
IP
Data Link
Logical Link Control (LLC)—802.2
Media Access Control (MAC)—Power, security, etc.
802.11
Physical
FH, DS, IR

**Wireless sensor network** (**WSN**) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on.

These are similar to **wireless ad hoc networks** in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. Sometimes they are called **dust networks**, referring to minute sensors as small as dust. **Smart dust** is a U C Berkeley project sponsored by DARPA. Dust Networks Inc., is one of the early companies that produced wireless sensor network products. WSNs are spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main locations. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

\



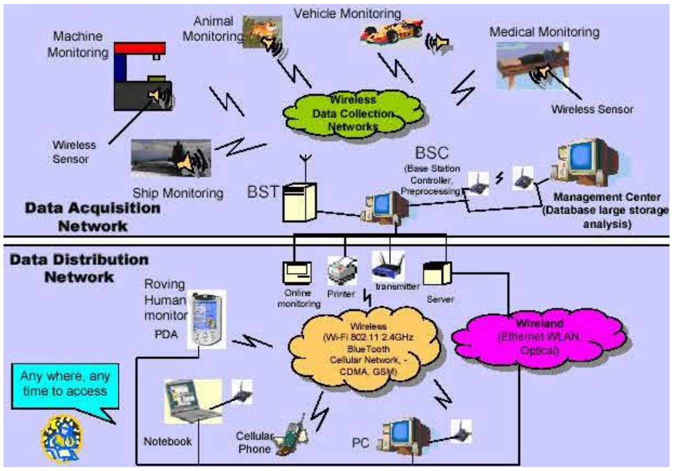
The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year, for example IPSN, SenSys, and EWSN.

**Wireless Sensor Networks (WSNs)**

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

wSN is a wireless network that consists of base stations and numbers of nodes (wireless sensors).These networks are used to monitor physical or environmental conditions like sound, pressure, temperature and co-operatively pass data through the network to a main location as shown in the figure.


Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Data Collection Networks
Wireless Sensor
Wireless Sensor
Ship Monitoring
BST
BSC
(Base Station Controller, Preprocessing)
Management Center (Database large storage analysis)
Data Acquisition Network
Data Distribution Network
Roving Human monitor
PDA
Online monitoring
Printer
transmitter
Server
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

Depending on the environment, the types of networks are decided so that those can be deployed underwater, underground, on land, and so on. Different types of WSNs include:

1. Terrestrial WSNs
2. Underground WSNs
3. Underwater WSNs
4. Multimedia WSNs
5. Mobile WSNs

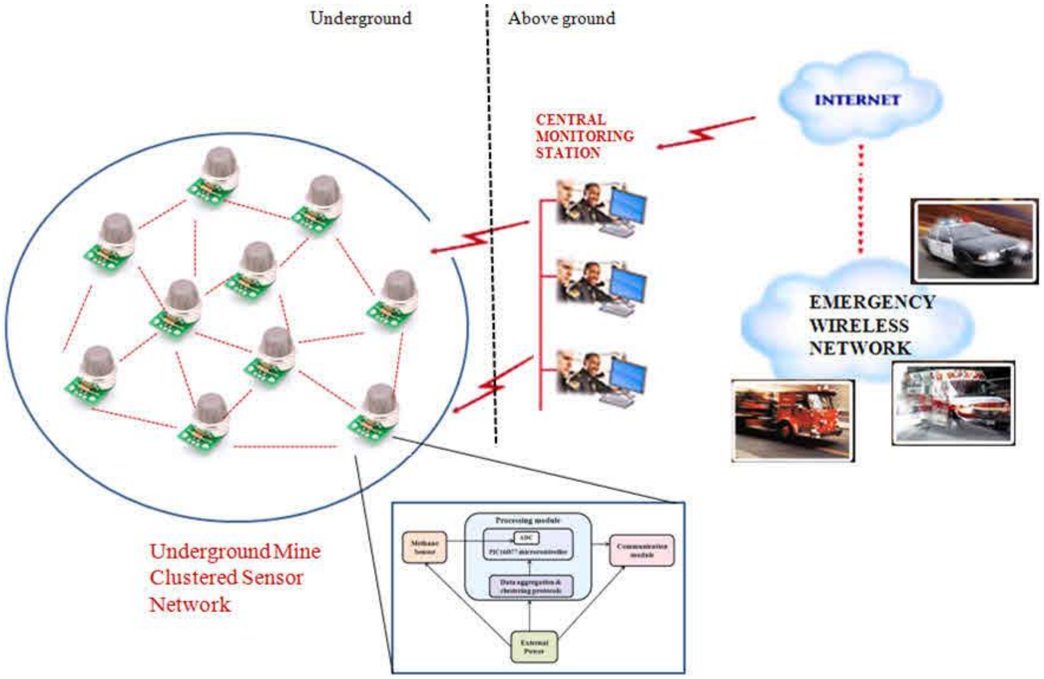
**1. Terrestrial WSNs**

Terrestrial WSNs are capable of communicating base stations efficiently, and consist of hundreds to thousands of wireless sensor nodes deployed either in unstructured (ad hoc) or structured (Preplanned) manner. In an unstructured mode, the sensor nodes are randomly distributed within the target area that is dropped from a fixed plane. The preplanned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models.

In this WSN, the battery power is limited; however, the battery is equipped with solar cells as a secondary power source. The Energy conservation of these WSNs is achieved by using low duty cycle operations, minimizing delays, and optimal routing, and so on.

**2. Underground WSNs**

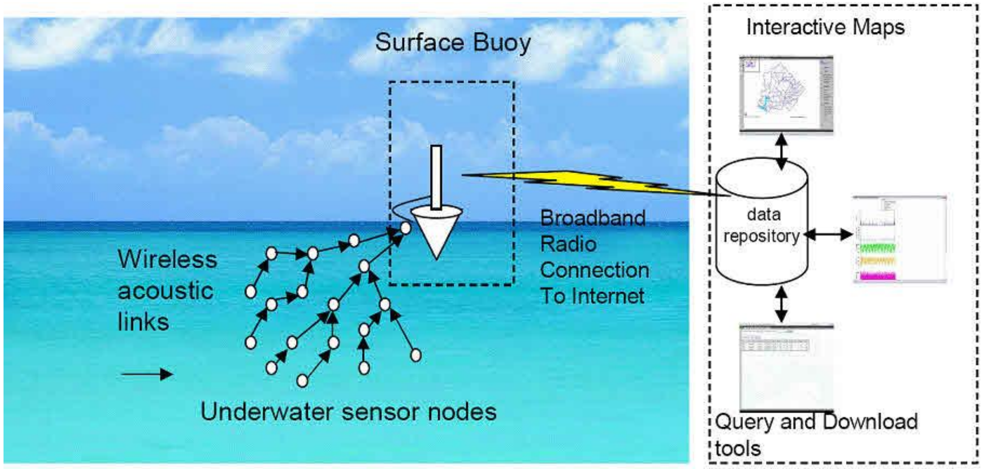
The underground wireless sensor networks are more expensive than the terrestrial WSNs in terms of deployment, maintenance, and equipment cost considerations and careful planning. The WSNs networks consist of a number of sensor nodes that are hidden in the ground to monitor underground conditions. To relay information from the sensor nodes to the base station, additional sink nodes are located above the ground.


Underground
Above ground
INTERNET
CENTRAL MONITORING STATION
EMERGENCY WIRELESS NETWORK
Underground Mine Clustered Sensor Network
Processing module
Methane Sensor
ADC
PIC16F877 microcontroller
Communication module
Data aggregation & clustering protocols
External Power

The underground wireless sensor networks deployed into the ground are difficult to recharge. The sensor battery nodes equipped with a limited battery power are difficult to recharge. In addition to this, the underground environment makes wireless communication a challenge due to high level of attenuation and signal loss.

**3. Under Water WSNs**

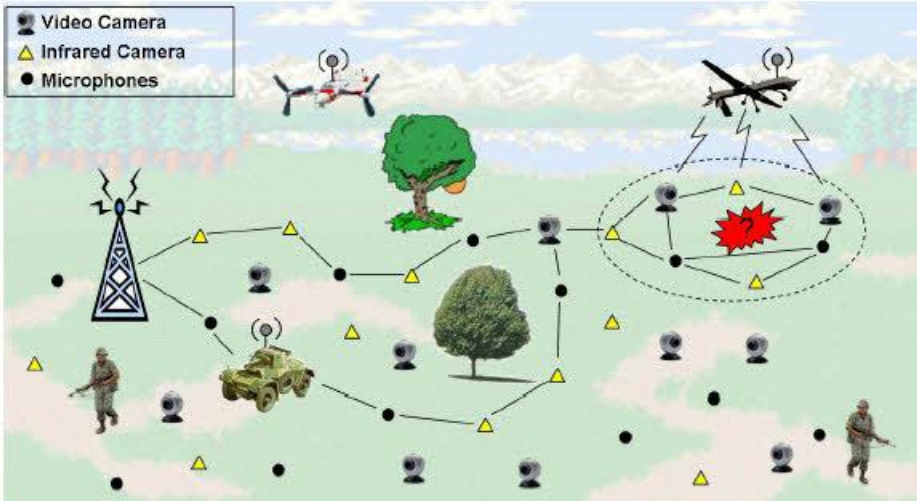
More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water. Autonomous underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a long propagation delay, and bandwidth and sensor failures.



Under water WSNs are equipped with a limited battery that cannot be recharged or replaced. The issue of energy conservation for under water WSNs involves the development of underwater communication and networking techniques.

### 4. Multimedia WSNs

Muttimedia wireless sensor networks have been proposed to enable tracking and monitoring of events in the form of multimedia, such as imaging, video, and audio. These networks consist of low-cost sensor nodes equipped with micrpphones and cameras.These nodes are interconnected with each other over a wireless connection for data compression, data retrieval and correlation.



The challenges with the multimedia WSN include high energy consumption, high bandwidth requirements, data processing and compressing techniques. In addition to this, multimedia contents require high bandwidth for the contents to be delivered properly and easily.

### 5. Mobile WSNs

These networks consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sense and communicate.

The mobile wireless sensor networks are much more versatile than the static sensor networks. The advantages of MWSN over the static wireless sensor networks include better and improved coverage, better energy efficiency, superior channel capacity, and so on.

### Limitations of Wireless Sensor Networks

1. Possess very little storage capacity – a few hundred kilobytes
2. Possess modest processing power-8MHz
3. Works in short communication range – consumes a lot of power
4. Requires minimal energy – constrains protocols
5. Have batteries with a finite life time
6. Passive devices provide little energy

## UMTS Architecture

The UMTS architecture is required to provide a greater level of performance to that of the original GSM network. However as many networks had migrated through the use of GPRS and EDGE, they already had the ability to carry data. Accordingly many of the elements required for the WCDMA / UMTS network architecture were seen as a migration. This considerably reduced the cost of implementing the UMTS network as many elements were in place or needed upgrading.

With one of the major aims of UMTS being to be able to carry data, the UMTS network architecture was designed to enable a considerable improvement in data performance over that provided for GSM.

UMTS network constituents

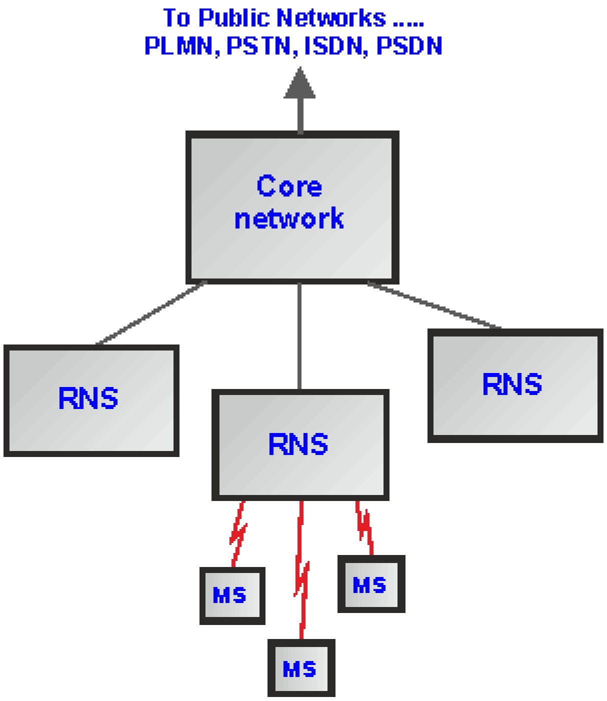
The UMTS network architecture can be divided into three main elements:

1. ***User Equipment (UE):*** The User Equipment or UE is the name given to what was previous termed the mobile, or cellphone. The new name was chosen because the

considerably greater functionality that the UE could have. It could also be anything between a mobile phone used for talking to a data terminal attached to a computer with no voice capability.

2. ***Radio Network Subsystem (RNS):*** The RNS also known as the UMTS Radio Access Network, UTRAN, is the equivalent of the previous Base Station Subsystem or BSS in GSM. It provides and manages the air interface for the overall network.
3. ***Core Network:*** The core network provides all the central processing and management for the system. It is the equivalent of the GSM Network Switching Subsystem or NSS.

The core network is then the overall entity that interfaces to external networks including the public phone network and other cellular telecommunications networks.



**UMTS Network Architecture Overview**

User Equipment, UE

The USER Equipment or UE is a major element of the overall 3G UMTS network architecture. It forms the final interface with the user. In view of the far greater number of applications and facilities that it can perform, the decision was made to call it a user equipment rather than a mobile. However it is essentially the handset (in the broadest terminology), although having access to much higher speed data communications, it can be much more versatile, containing many more applications. It consists of a variety of different elements including RF circuitry, processing, antenna, battery, etc.

There are a number of elements within the UE that can be described separately:

- ***UE RF circuitry:*** The RF areas handle all elements of the signal, both for the receiver and for the transmitter. One of the major challenges for the RF power amplifier was to reduce the power consumption. The form of modulation used for W-CDMA requires the use of a linear amplifier. These inherently take more current than non linear amplifiers which can be used for the form of modulation used on GSM. Accordingly to maintain battery life, measures were introduced into many of the designs to ensure the optimum efficiency.
- ***Baseband processing:*** The base-band signal processing consists mainly of digital circuitry. This is considerably more complicated than that used in phones for previous generations. Again this has been optimised to reduce the current consumption as far as possible.
- ***Battery:*** While current consumption has been minimised as far as possible within the circuitry of the phone, there has been an increase in current drain on the battery. With users expecting the same lifetime between charging batteries as experienced on the previous generation phones, this has necessitated the use of new and improved battery technology. Now Lithium Ion (Li-ion) batteries are used. These phones to remain small and relatively light while still retaining or even improving the overall life between charges.
- ***Universal Subscriber Identity Module, USIM:*** The UE also contains a SIM card, although in the case of UMTS it is termed a USIM (Universal Subscriber Identity Module). This is a more advanced version of the SIM card used in GSM and other systems, but embodies the same types of information. It contains the International Mobile Subscriber Identity number (IMSI) as well as the Mobile Station International ISDN Number (MSISDN). Other information that the USIM holds includes the preferred language to enable the correct language information to be displayed, especially when roaming, and a list of preferred and prohibited Public Land Mobile Networks (PLMN).

  The USIM also contains a short message storage area that allows messages to stay with the user even when the phone is changed. Similarly "phone book" numbers and call information of the numbers of incoming and outgoing calls are stored.

The UE can take a variety of forms, although the most common format is still a version of a "mobile phone" although having many data capabilities. Other broadband dongles are also being widely used.

## UMTS Radio Network Subsystem

This is the section of the 3G UMTS / WCDMA network that interfaces to both the UE and the core network. The overall radio access network, i.e. collectively all the Radio Network Subsystem is known as the UTRAN UMTS Radio Access Network.

The radio network subsystem is also known as the UMTS Radio Access Network or UTRAN.

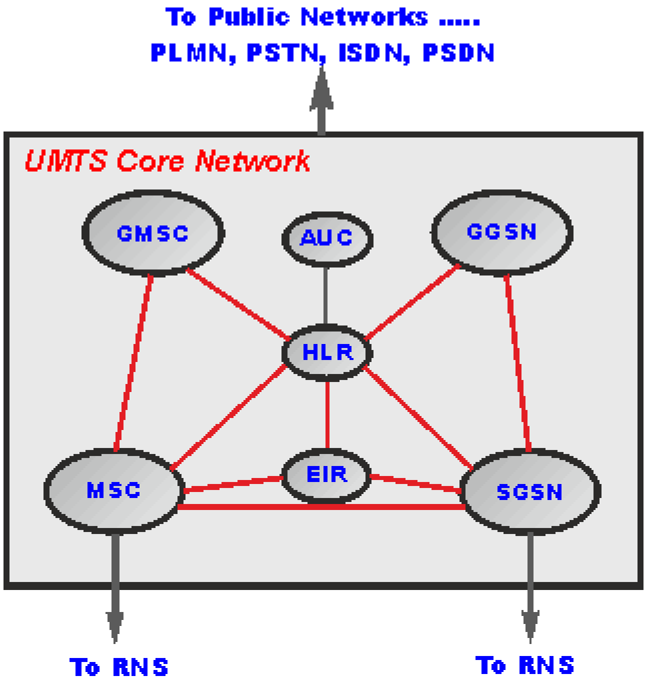
## 3G UMTS Core Network

The 3G UMTS core network architecture is a migration of that used for GSM with further elements overlaid to enable the additional functionality demanded by UMTS.

In view of the different ways in which data may be carried, the UMTS core network may be split into two different areas:

- ***Circuit switched elements:*** These elements are primarily based on the GSM network entities and carry data in a circuit switched manner, i.e. a permanent channel for the duration of the call.
- ***Packet switched elements:*** These network entities are designed to carry packet data. This enables much higher network usage as the capacity can be shared and data is carried as packets which are routed according to their destination.

Some network elements, particularly those that are associated with registration are shared by both domains and operate in the same way that they did with GSM.



**UMTS Core Network**

### Circuitswitchedelements

The circuit switched elements of the UMTS core network architecture include the following network entities:

- ***Mobile switching centre (MSC):*** This is essentially the same as that within GSM, and it manages the circuit switched calls under way.
- ***Gateway MSC (GMSC):*** This is effectively the interface to the external networks.

### Packet switched elements

The packet switched elements of the 3G UMTS core network architecture include the following network entities:

- ***Serving GPRS Support Node (SGSN):*** As the name implies, this entity was first developed when GPRS was introduced, and its use has been carried over into the UMTS network architecture. The SGSN provides a number of functions within the UMTS network architecture.
    - Mobility management When a UE attaches to the Packet Switched domain of the UMTS Core Network, the SGSN generates MM information based on the mobile's current location.
    - Session management: The SGSN manages the data sessions providing the required quality of service and also managing what are termed the PDP (Packet data Protocol) contexts, i.e. the pipes over which the data is sent.
    - Interaction with other areas of the network: The SGSN is able to manage its elements within the network only by communicating with other areas of the network, e.g. MSC and other circuit switched areas.
    - Billing: The SGSN is also responsible billing. It achieves this by monitoring the flow of user data across the GPRS network. CDRs (Call Detail Records) are generated by the SGSN before being transferred to the charging entities (Charging Gateway Function, CGF).
- ***Gateway GPRS Support Node (GGSN):*** Like the SGSN, this entity was also first introduced into the GPRS network. The Gateway GPRS Support Node (GGSN) is the central element within the UMTS packet switched network. It handles inter-working between the UMTS packet switched network and external packet switched networks, and can be considered as a very sophisticated router. In operation, when the GGSN receives data addressed to a specific user, it checks if the user is active and then forwards the data to the SGSN serving the particular UE.

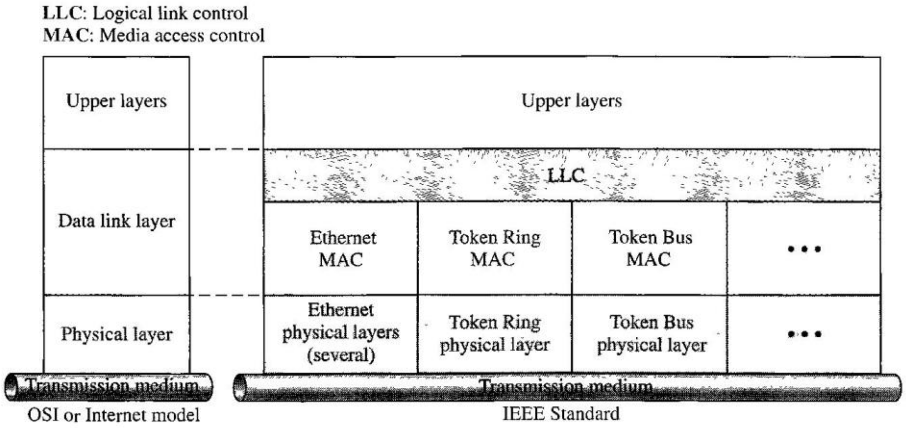
**Sharedelements**

The shared elements of the UMTS core network architecture include the following network entities:

- **Home location register (HLR):** This database contains all the administrative information about each subscriber along with their last known location. In this way, the UMTS network is able to route calls to the relevant RNC / Node B. When a user switches on their UE, it registers with the network and from this it is possible to determine which Node B it communicates with so that incoming calls can be routed appropriately. Even when the UE is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position with their current or last known location on the network.
- **Equipment identity register (EIR):** The EIR is the entity that decides whether a given UE equipment may be allowed onto the network. Each UE equipment has a number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration.
- **Authentication centre (AuC) :** The AuC is a protected database that contains the secret key also contained in the user's USIM card.

## IEEE STANDARDS

The relationship of the 802 Standard to the traditional OSI model is shown in the figure. The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.



### Data Link Layer

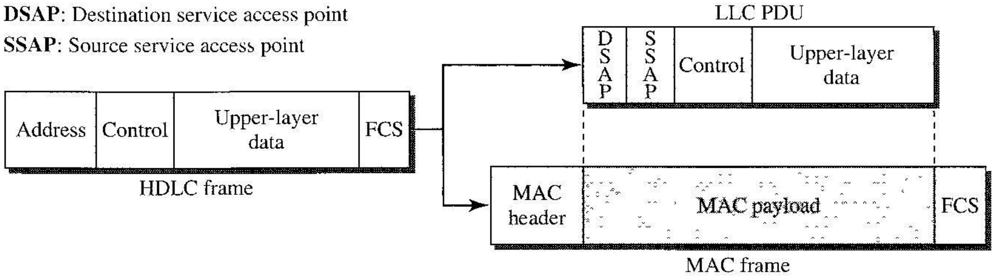
The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

### *Logical Link Control (LLC)*

In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MACsublayer.

The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

**Framing** LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC. The header contains a control field like the one in HDLC; this field is used for flow and error control. The two other header fields define the upper-layer protocol at the source and destination that uses LLC. These fields are called the destination service access point (DSAP) and the source service access point (SSAP). The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer. In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer, as shown in figure.



**Need for LLC** The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols. However, most upper-layer protocols such as IP, do not use the services of LLC.

***Media Access Control (MAC)***

IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token-passing method for Token Ring and Token Bus LANs. Part of the framing function is also handled by the MAC layer.

In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

**Physical Layer**

The physical layer is dependent on the implementation and type of physical media used. IEEE defines detailed specifications for each LAN implementation. For example, although there

is only one MAC sublayer for Standard Ethernet, there is a different physical layer specification for each Ethernet implementations.

**Key features of LANs are summarized below**:

□ Limited geographical area – which is usually less than 10 Km and more than 1 m.
□ High Speed – 10 Mbps to 1000 Mbps (1 Gbps) and more
□ High Reliability – 1 bit error in $10^{11}$ bits.
□ Transmission Media – Guided and unguided media, mainly guided media is used; except in a situation where infrared is used to make a wireless LAN in a room.

□ Topology – It refers to the ways in which the nodes are connected. There are various topologies used.

□ Medium-Access Control Techniques –Some access control mechanism is needed

to decide which station will use the shared medium at a particular point in time. In this lesson we shall discuss various LAN standards proposed by the IEEE 8.2 committee with the following goals in mind:

□ To promote compatibility

- Implementation with minimum efforts
- Accommodate the need for diverse applications

For the fulfillment of the abovementioned goals, the committee came up with a bunch of LAN standards collectively known as IEEE 802 LANs as shown in Fig. 5.3.1. To satisfy diverse requirements, the standard includes CSMA/CD, Token bus, Token

Ring medium access control techniques along with different topologies. All these standards differ at the physical layer and MAC sublayer, but are compatible at the data link layer.

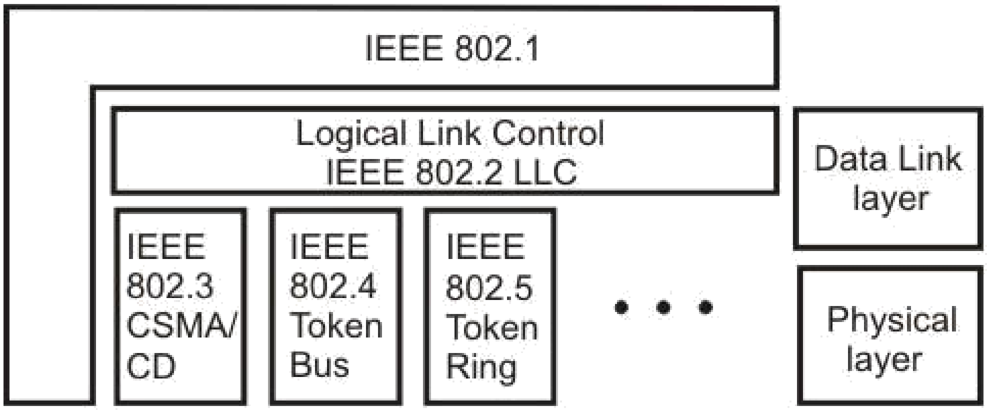


Figure 5.3.1 IEEE 802 Legacy LANs

The **802.1** sublayer gives an introduction to set of standards and gives the details of the interface primitives. It provides relationship between the OSI model and the 802 standards. The **802.2** sublayer describes the **LLC** (logical link layer), which is the upper part of the data link layer. LLC facilitate error control and flow control for reliable communication. It appends a header containing sequence number and acknowledgement number. And offers the following three types of services:

- Unreliable datagram service
- Acknowledged datagram service
- Reliable connection oriental service

The standards 802.3, 802.4 and 802.5 describe three LAN standards based on the CSMA/CD, token bus and token ring, respectively. Each standard covers the physical layer and MAC sublayer protocols. In the following sections we shall focus on these three LAN standards.

*IEEE 802.3 and Ethernet*

## Ethernet - A Brief History

The original Ethernet was developed as an experimental coaxial cable network in the 1970s by Xerox Corporation to operate with a data rate of 3 Mbps using a carrier sense multiple access collision detection (CSMA/CD) protocol for LANs with sporadic traffic requirements. Success with that project attracted early attention and led to the 1980 joint development of the 10-Mbps Ethernet Version 1.0 specification by the three-company consortium: Digital Equipment Corporation, Intel Corporation, and Xerox Corporation.

The original IEEE 802.3 standard was based on, and was very similar to, the Ethernet Version 1.0 specification. The draft standard was approved by the 802.3 working group in 1983 and was subsequently published as an official standard in 1985 (ANSI/IEEE Std.

802.3-1985). Since then, a number of supplements to the standard have been defined to take advantage of improvements in the technologies and to support additional network media and higher data rate capabilities, plus several new optional network access control features. From then onwards, the term *Ethernet* refers to the family of local-area network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fiber and twisted-pair cables:

□ 10 Mbps—10Base-T Ethernet□
□ 100 Mbps—Fast Ethernet□
□ 1000 Mbps—Gigabit Ethernet□

Ethernet has survived as the major LAN technology (it is currently used for approximately 85 percent of the world's LAN-connected PCs and workstations) because its protocol has the following characteristics:

□ It is easy to understand, implement, manage, and maintain□
□ It allows low-cost network implementations□
□ It provides extensive topological flexibility for network installation□

□ It guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer□

## Ethernet Architecture

Ethernet architecture can be divided into two layers:

➢ **Physical layer:** this layer takes care of following functions.
□ Encoding and decoding

□ Collision detection
□ Carrier sensing
□ Transmission and receipt

➢ **Data link layer:** Following are the major functions of this layer.

□ Station interface

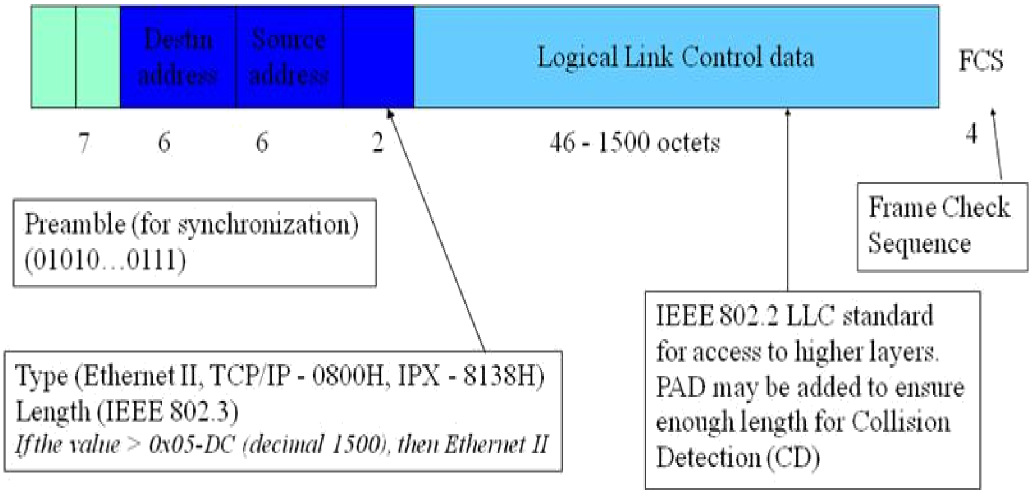
□ Data Encapsulation /Decapsulation

□ Link management

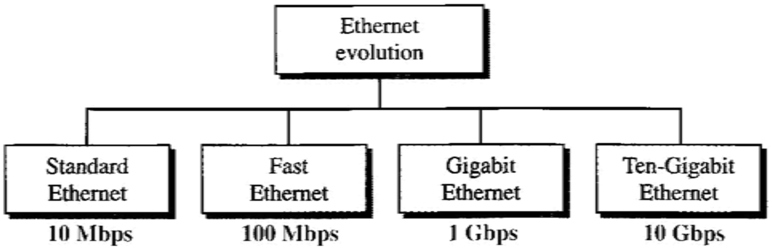
□ Collision Management

## STANDARD ETHERNET

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: Standard Ethernet (10 t Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and Ten-Gigabit Ethernet (10 Gbps), as shown in the figure:



Destn address
Source address
Logical Link Control data
FCS
7
6
6
2
46 - 1500 octets
4
Preamble (for synchronization) (01010…0111)
Frame Check Sequence
Type (Ethernet II, TCP/IP - 0800H, IPX - 8138H)
Length (IEEE 802.3)
If the value > 0x05-DC (decimal 1500), then Ethernet II
IEEE 802.2 LLC standard for access to higher layers. PAD may be added to ensure enough length for Collision Detection (CD)



## MAC Sublayer

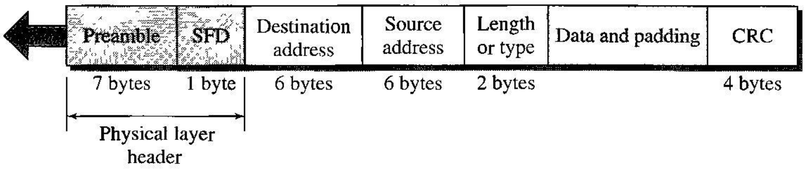
In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

### *Frame Format*

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers. The format of the MAC frame is shown in the figure.

**Preamble**: 56 bits of alternating 1s and 0s.

**SFD**: Start frame delimiter, flag (10101011)



- **Preamble**. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.

- **Start frame delimiter (SFD).** The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

- **Destination address (DA)**. The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.

- **Source address (SA)**. The SA field is also 6 bytes and contains the physical address of the sender of the packet.

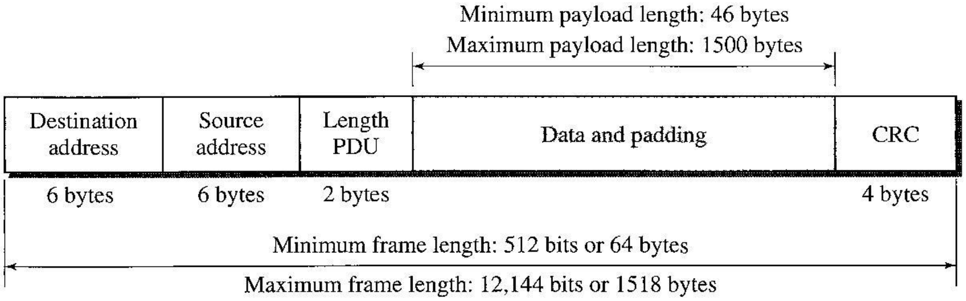
- **Length or type**. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field.

- **Data**. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.

- **CRC**. The last field contains error detection information, in this case a CRC-32.

### *Frame Length*

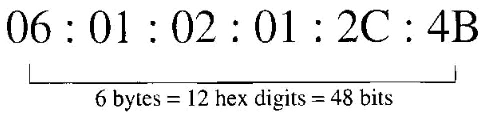
Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame, as shown in figure.


Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

The minimum length restriction is required for the correct operation of CSMA/CD. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

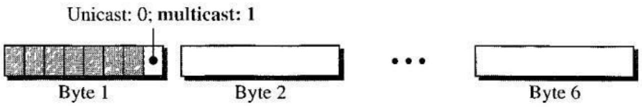
The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons. First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer. Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

### *Addressing*


06 : 01 : 02 : 01 : 2C : 4B
6 bytes = 12 hex digits = 48 bits

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6- byte physical address. As shown in the figure, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

**Unicast, Multicast, and Broadcast Addresses** A source address is always a unicast address--the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. The following figure shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.



A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one4o-many. The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight ls.

### *Access Method: CSMA/CD*

Standard Ethernet uses 1-persistent CSMA/CD

**Slot Time** In an Ethernet network, the round-trip time required for a frame to travel from one end of a maximum-length network to the other plus the time needed to send the jam sequence is called the slot time.
**Slot time = round-trip time + time required to send the jam sequence**

The slot time in Ethernet is defined in bits. It is the time required for a station to send 512 bits. This means that the actual slot time depends on the data rate; for traditional 10-Mbps Ethernet it is 51.2µs.

**Slot Time and Collision** The choice of a 512-bit slot time was not accidental. It was chosen to allow the proper functioning of CSMA/CD. To understand the situation, let us consider two cases.

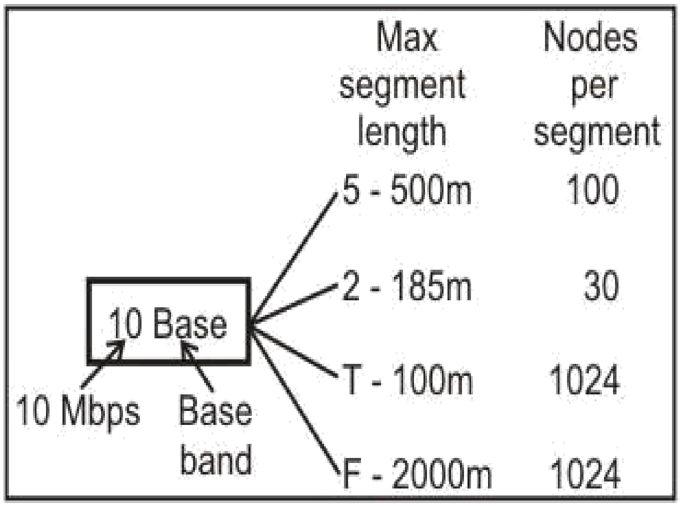
In the first case, we assume that the sender sends a minimum-size packet of 512 bits. Before the sender can send the entire packet out, the signal travels through the network and reaches the end of the network. If there is another signal at the end of the network (worst case), a collision occurs. The sender has the opportunity to abort the sending of the frame and to send a jam sequence to inform other stations of the collision. The roundtrip time plus the time required to send the jam sequence should be less than the time needed for the sender to send the minimum frame, 512 bits. The sender needs to be aware of the collision before it is too late, that is, before it has sent the entire frame.

In the second case, the sender sends a frame larger than the minimum size (between 512 and 1518 bits). In this case, if the station has sent out the first 512 bits and has not heard a

$$\text{MaxLength} = \text{PropagationSpeed} \times \frac{\text{SlotTime}}{2}$$

$$\text{MaxLength} = (2 \times 10^{8}) \times (51.2 \times 10^{-6} / 2) = 5120\text{ m}$$

collision, it is guaranteed that collision will never occur during the transmission of this frame. The reason is that the signal will reach the end of the network in less than one-half the slot time. If all stations follow the CSMA/CD protocol, they have already sensed the existence of the signal (carrier) on the line and have refrained from sending. If they sent a signal on the line before one-half of the slot time expired, a collision has occurred and the sender has sensed the collision. In other words, collision can only occur during the first half of the slot time, and if it does, it can be sensed by the sender during the slot time. This means that after the sender sends the first 512 bits, it is guaranteed that collision will not occur during the transmission of this frame. The medium belongs to the sender, and no other station will use it. In other words, the sender needs to listen for a collision only during the time the first 512 bits are sent.



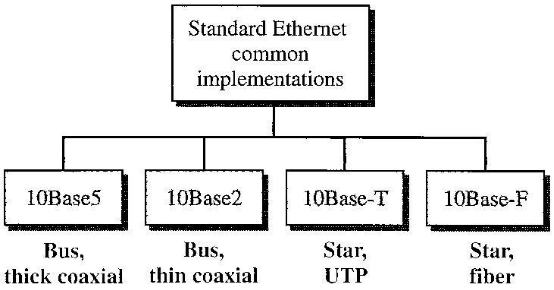
**Slot Time and Maximum Network Length** There is a relationship between the slot time and the maximum length of the network (collision domain). It is dependent on the propagation speed of the signal in the particular medium. In most transmission media, the signal propagates at 2 x 108 m/s (two-thirds of the rate for propagation in air). For traditional Ethernet, we calculate Of course, we need to consider the delay times in repeaters and interfaces, and the time required to send the jam sequen

ce. These reduce the maximum-length of a traditional Ethernet network to 2500 m, just 48 percent of the theoretical calculation.

MaxLength = 2500 m

## Physical Layer

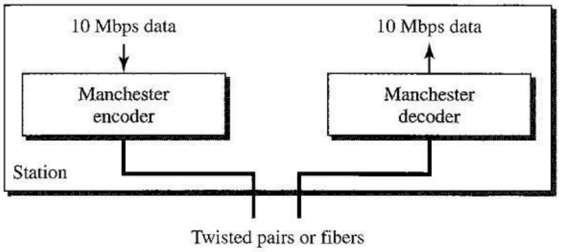
The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in figure.



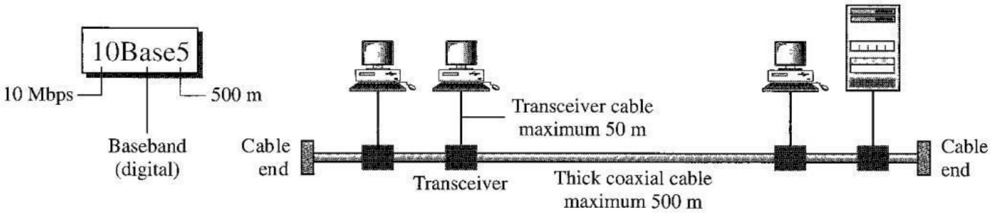
Because Ethernet devices implement only the bottom two layers of the OSI protocol stack, they are typically implemented as network interface cards (NICs) that plug into the host device's motherboard, or presently built-in in the motherboard. Various types cabling supported by the standard are shown in Fig. 5.3.2. The naming convention is a concatenation of three terms indicating the transmission rate, the transmission method, and the media type/signal encoding. Consider for example, 10Base-T. where 10 implies transmission rate of 10 Mbps, Base represents that it uses baseband signaling, and T refers to twisted-pair cables as transmission media. Various standards are discussed below:

### *Encoding and Decoding*

All standard implementations use digital signaling (baseband) at 10 Mbps. At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data. The figure shows the encoding scheme for Standard Ethernet.



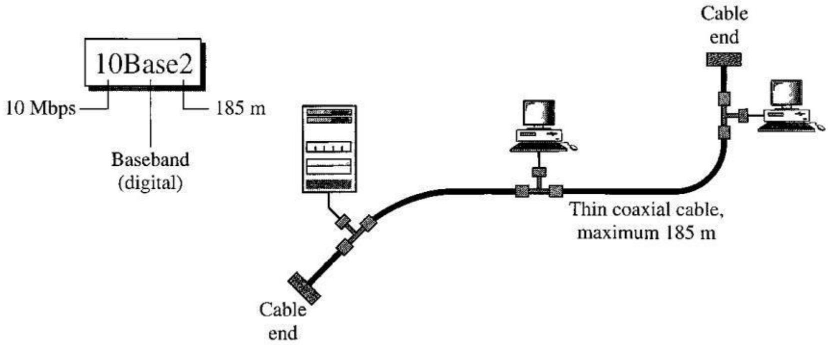
### *10Base5: Thick Ethernet*



10Base5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable. The transceiver is responsible for transmitting, receiving, and detecting collisions.

The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.
The maximum length of the coaxial cable must not exceed 500 m, otherwise, there is excessive degradation of the signal. If a length of more than 500 m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.

***10Base2: Thin Ethernet***

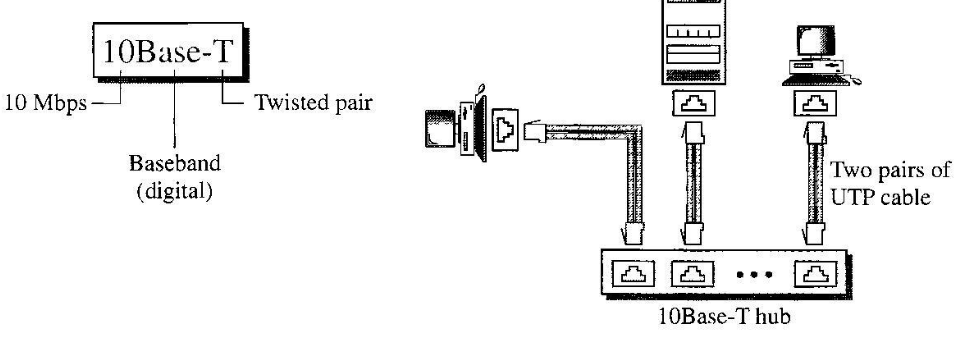


10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

***10Base- T: Twisted-Pair Ethernet***

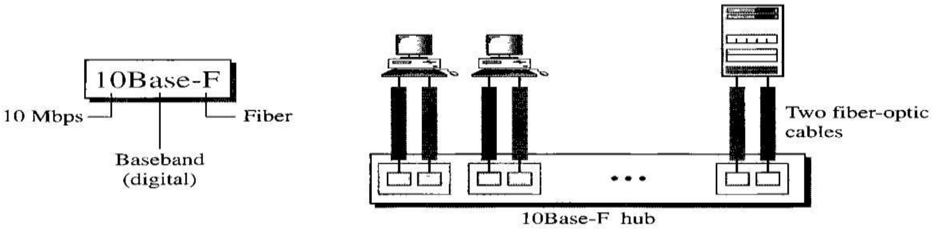
The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable.



Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

### *10Base-F: Fiber Ethernet*

10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables.



### *No Need for CSMA/CD*

In full-duplex switched Ethernet, there is no need for the CSMA/CD method. In a full- duplex switched Ethernet, each station is connected to the switch via two separate links. Each station or switch can send and receive independently without worrying about collision. Each link is a point-to-point dedicated path between the station and the switch. There is no longer a need for carrier sensing; there is no longer a need for collision detection. The job of the MAC layer becomes much easier. The carrier sensing and collision detection functionalities of the MAC sublayer can be turned off.

### *MAC Control Layer*

Standard Ethernet was designed as a connectionless protocol at the MAC sublayer. There is no explicit flow control or error control to inform the sender that the
frame has arrived at the destination without error. When the receiver receives the frame, it does not send any positive or negative acknowledgment.

To provide for flow and error control in full-duplex switched Ethernet, a new sublayer, called the MAC control, is added between the LLC sublayer and the MAC sublayer.

□ ***Introduction***

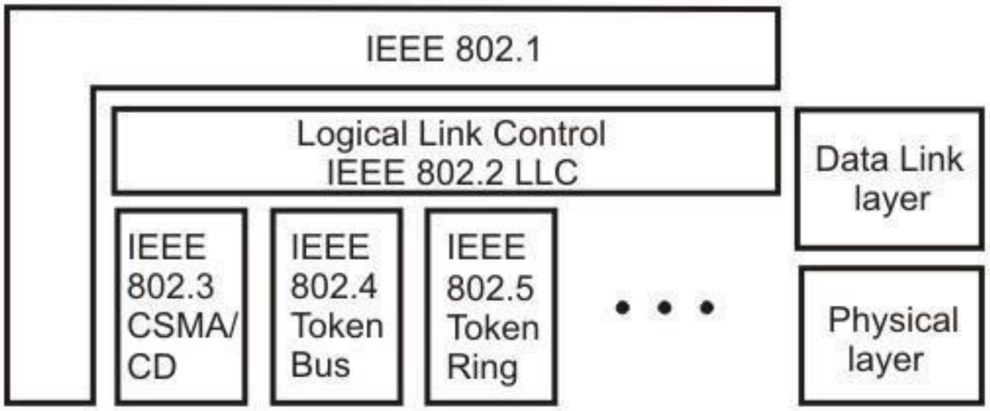


Figure  IEEE 802 Legacy LANs

***Token Ring (IEEE 802.5)***

**Token Ring: A Brief History**

Originally, IBM developed Token Ring network in the 1970s. It is still IBM's primary local-area network (LAN) technology. The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and on the same lines. The term *Token Ring* is generally used to refer to both IBM's Token Ring network and IEEE 802.5 networks.

Before going into the details of the Token Ring protocol, let’s first discuss the motivation behind it. As already discussed, the medium access mechanism used by Ethernet (CSMA/CD) may results in collision. Nodes attempt to a number of times before they can actually transmit, and even when they start transmitting there are chances to encounter collisions and entire transmission need to be repeated. And all this become worse one the traffic is heavy i.e. all nodes have some data to transmit. Apart from this there is no way to predict either the occurrence of collision or delays produced by multiple stations attempting to capture the link at the same time. So all these problems with the Ethernet gives way to an alternate LAN technology, Token Ring.

Token Ring and IEEE802.5 are based on token passing MAC protocol with ring topology. They resolve the uncertainty by giving each station a turn on by one. Each node takes turns sending the data; each station may transmit data during its turn. The technique that coordinates this turn mechanism is called Token passing; as a Token is passed in the network and the station that gets the token can only transmit. As one node transmits at a time, there is no chance of collision. We shall discuss the detailed operation in next section.

Stations are connected by point-to-point links using repeaters. Mainly these links are of shielded twisted-pair cables. The repeaters function in two basic modes: Listen mode, Transmit mode. A disadvantage of this topology is that it is vulnerable to link or station failure. But a few measures can be taken to take care of it.

**COMPARISON AMONG STANDARDS**

| Parameters | FDDI | IEEE 802.3 | IEEE 802.5 |
|---|---|---|---|
| □ BANDWIDTH | 100Mb/s | 10Mb/s | 4 or 16Mb/s |
| □ NUMBER OF STATIONS | 500 | 1024 | 250 |
| □ MAX. DISTANCE BETWEEN STATIONS | 2Km (MMF)<br>20Km (SMF) | 2.8Km | 300m (4Mb/s)<br>100m (RECO.) |
| □ MAX. NETWORK EXTENT | 100Km | 2.8Km | VARIED WITH CONFIGURATION |
| □ LOGICAL TOPOLOGY | DUAL RING,<br>DUAL RING OF TREES | BUS | SINGLE RING |
| □ PHYSICAL TOPOLOGY | RING, STAR<br>HIERARCHICAL STAR | BUS, STAR | RING BUS<br>HIERARCHICAL STAR |
| □ MEDIA | OPTICAL FIBER | OPTICAL FIBRE,<br>TWISTED-WIRE,<br>COAXIAL CABLE | TWISTED-WIRE<br>OPTICAL FIBER |
| □ ACCESS METHOD | TIMED-TOKEN PASSING | CSMA/CD | TOKEN PASSING |
| □ TOKEN | CAPTURES THE TOKEN | - | BY SETTING A STATUS BIT |

| | | | |
|---|---|---|---|
| ACQUISITION | | | |
| □ TOKEN RELEASE | AFTER TRANSMIT | - | AFTER STRIPPING OR AFTER TRANSMIT (16) |
| □ FRAMES ON LAN | MULTIPLE | SINGLE | SINGLE |
| □ FRAMES TRANSMITTED PER ACCESS | MULTIPLE | SINGLE | SINGLE |
| MAX. FRAME SIZE | 4500 BYTES | 1518 BYTES | 4500 BYTES (4)<br>17,800 BYTES (16) |

# COMMUNICATION AND NETWORKING

## UNIT 3

## PHYSICAL LAYER AND DATALINK LAYER.

**The Physical layer - Media - Twisted pair - coaxial cable - microwave - infrared - millimetre wave - PSTN - The local loop modem - ADSL - Switching - Internet over cable - cable modems The Data link layer - design issues - Error detection and control - data link protocols - HDLC - PPP - IEEE standards for data link layer.**

### Design Factors forTransmission Media

**Bandwidth**: All other factors remaining constant, the greater the band-width of a signal, the higher the data rate that can be achieved.

**Transmission impairments**: Limit the distance a signal can travel.

**Interference**: Competing signals in overlapping frequency bands can distort or wipe out a signal.

**Number of receivers**: Each attachment introduces some attenuation and distortion, limiting distance and/or data rate.

### TYPES OF TRANSMISSION MEDIA

1.**Conducted or Guided Media** :

Use a conductor such as a wire or a fiber optic cable to move the signal from sender to receiver.

2.**Wireless or Unguided Media**:

Use radio waves of different frequencies and do notneed a wire or cable conductor to transmit signals.

### Guided Transmission Media

Guided media includes everything that ‘guides’ the transmission. That usually takes the form of some sort of a wire. Usually copper, but can also be an optical fibre.

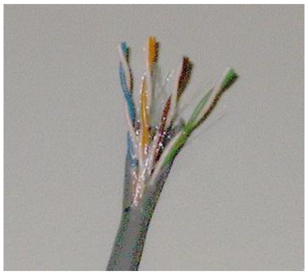
Transmission capacity depends on the distance and on whether the medium is point-to-point or multipoint. Ex:

- twisted pair wires
- coaxial cables
- optical fiber

### Twisted Pair Wires

A transmission medium consisting of pairs of twisted copper wires arranged in a regular spiral pattern to minimize the electromagnetic interference between adjacent pairs .Often used at customer facilities and also over distances to carry voice as well as data communications .Low frequency transmission medium .

We can transmit 1 Mbps over short distances (less than 100m). They are mainly used to transmit analog signals, but they can be used for digital signals.



**Twisted Pair Advantages**

Inexpensive and readily available

Flexible and light weight

Easy to work with and install

**Twisted Pair Disadvantages**

Susceptibility to interference and noise

Attenuation problem
For analog, repeaters needed every 5-6km
For digital, repeaters needed every 2-3km Relatively low bandwidth
(3000Hz)

**Applications**
They are used in telephone lines to provide voice and data channels. Local area networks, such as 10 Base-T and 100 Base-T also use twisted-pair cables.

**Coaxial Cable (or Coax)**

- In its simplest form, coaxial consists of a core made of solid copper surrounded by insulation, a braided metal shielding, and an outer cover.

- A transmission medium consisting of thickly insulated copper wire, which can transmit a large volume of data than twisted wire.

**Coax Advantages**

Higher bandwidth

□ 400 to 600Mhz

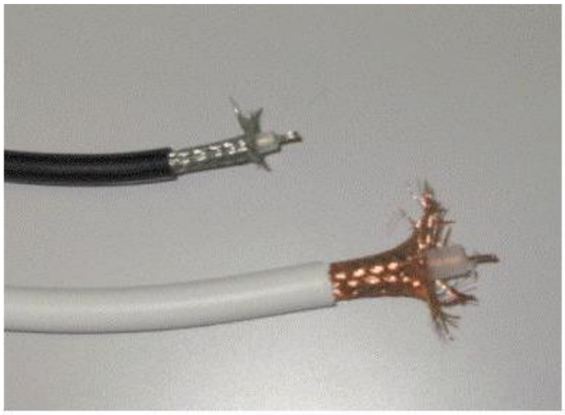
□ up to 10,800 voice conversations

Much less susceptible to interference than twisted pair

**Coax Disadvantages**

High attenuation rate makes it expensive over long distance

Bulky



**Applications**

□ It is used in cable TV networks

□ It is used in traditional Ethernet LANs.

**Fiber Optic Cable**

Relatively new transmission medium used by telephone companies in place of long-distance trunk lines

Also used by private companies in implementing local data communications networks

Require a light source with injection laser diode (ILD) or light-emitting diodes (LED)

Optical fiber consists of a glass core, surrounded by a glass cladding with slightly lower refractive index.

In most networks fiber-optic cable is used as the high-speed backbone, and twisted wire and coaxial cable are used to connect the backbone to individual devices.

**Fiber Optic Advantages**

Greater capacity (bandwidth of up to 2 Gbps).

Smaller size and lighter weight.

Lower attenuation.

immunity to environmental interference.

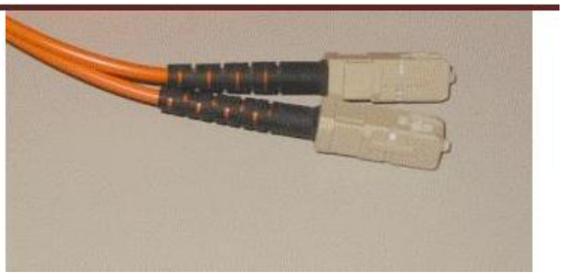
highly secure due to tap difficulty and lack of signal radiation.

**Fiber Optic Disadvantages**

expensive over short distance

requires highly skilled installers

adding additional nodes is difficult



**Applications**

- The fiber optic cable is often found in backbone networks because its bandwidth is cost effective.
- Used in TV companies.
- LAN such as 100 Base-FX Network

**Wireless (Unguided Media) Transmission**

Transmission and reception are achieved by means of an antenna directional

- transmitting antenna puts out focused beam
- transmitter and receiver must be aligned omni directional
- signal spreads out in all directions
- can be received by many antennas

**Wireless Examples**

Terrestrial microwave, satellite microwave ,broadcast radio ,infrared

**Microwaves**

Electromagnetic waves having frequency between 1 and 300 GHz are called as Micro waves.

- Micro waves are unidirectional.
- Microwave propagation is line of sight.
- Very high frequency Micro waves cannot penetrate walls.
- The microwave band is relatively wide, almost 299 GHz

**Terrestrial Microwave**

- Used for long-distance telephone service.
- Uses radio frequency spectrum, from 2 to 40 Ghz.
- Parabolic dish transmitter, mounted high.
- Used by common carriers as well as private networks.
- Requires unobstructed line of sight between source and receiver.
- Curvature of the earth requires stations (repeaters) ~30 miles apart.

**Satellite Microwave**

a microwave relay station in space can relay signals over long distances geostationary satellites

- remain above the equator at a height of 22,300 miles (geosynchronous orbit)

- travel around the earth in exactly the time the earth takes to rotate

**Applications**

They are used in Cellular phones.

They are used in satellite networks.

They are used in wireless LANs.

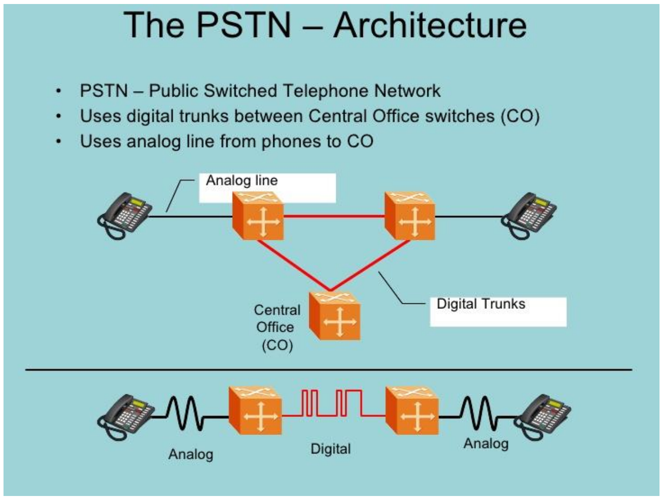
**Radio waves**

**Application**

1. The omnidirectional characteristics of Radio waves make them useful for multicasting, in which there is one sender but many receivers.
2. AM and FM Radio, television, maritime radio, cordless phone, and paging are examples of multicasting.

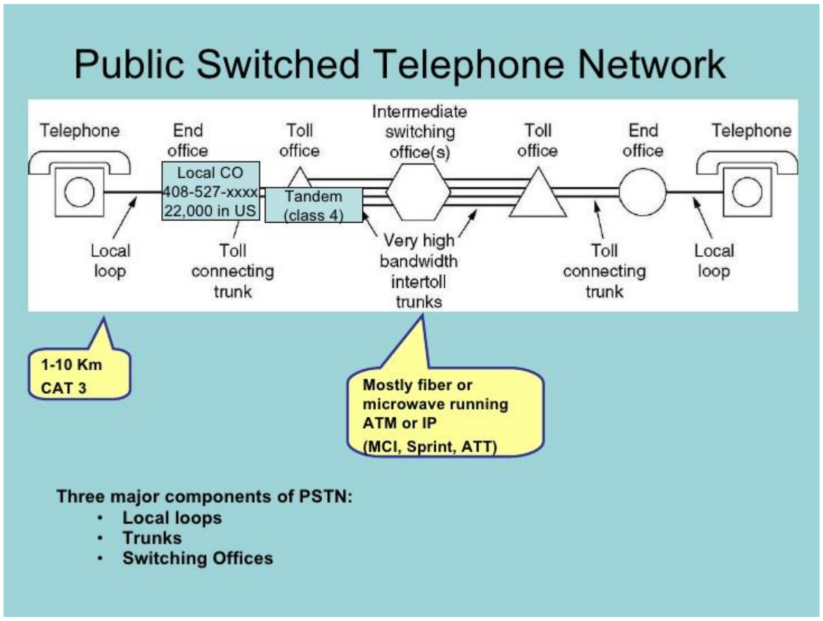
**PSTN**

The public switched telephone network (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing most telephones to communicate with each other. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core network and includes mobile and other networks, as well as fixed telephones.The technical operation of the PSTN adheres to the standards created by the ITU-T. These standards allow different networks in different countries to interconnect seamlessly. The E.163 and E.164 standards provide a single global address space for telephone numbers. The combination of the interconnected networks and the single numbering plan allow telephones around the world to dial each other.



The PSTN – Architecture

- PSTN – Public Switched Telephone Network
- Uses digital trunks between Central Office switches (CO)
- Uses analog line from phones to CO



Three major components of PSTN:

- Local loops
- Trunks
- Switching Offices

**Data-Link Protocols**

**Data-Link Protocol Functions**

**Line discipline** – coordinates hop-to-hop data delivery where a hop is a computer, a network controller, or some type of network-connecting device, such as router.It determines which device is transmitting and which is receiving at any point in time

**Flow control** – the rate at which data is transported over a link.

- It provides an acknowledgement mechanism that data is received at the destination .
- It regulate flow of data from sender to receiver

**Error control** – detects and corrects transmission errors

**Framing** – recognizing beginning and end of frames (blocks, packets).Communications requires at least two devices, one to send and one to receive. If both devices are ready to send some information and put their signals on the link then the two signals collides each other and became nothing. To avoid such a situation the data link layer use a mechanism called line discipline.

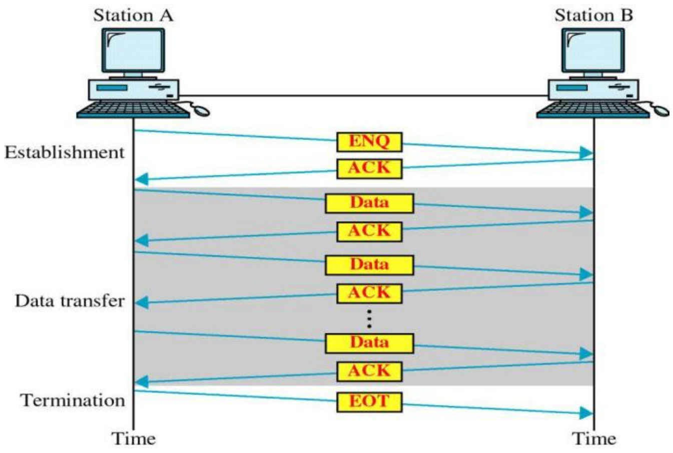
Line discipline coordinates the link system. It determines which device can send and when it can send. It answers then question, who should send now? Line discipline can serve in two ways:

1. enquiry / acknowledgement (ENQ / ACK)
2. poll / select (POLL / SELECT)

**ENQ / ACK:**

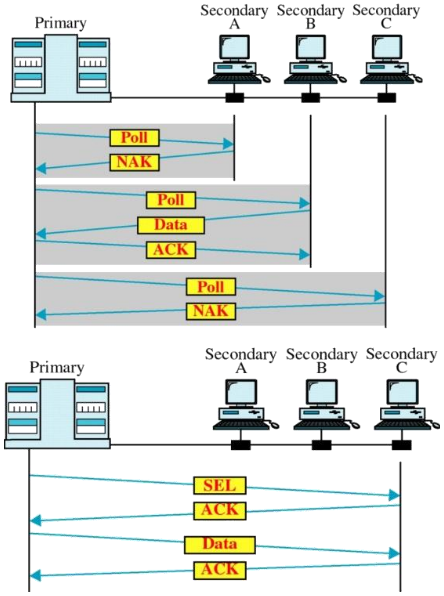
This method is used in peer to peer communications. That is where there is a dedicated link between two devices. The initiator first transmits a frame called an enquiry (ENQ) asking I the receiver is available to receive data. The receiver must answer either with an acknowledgement (ACK) frame if it ready to accept or with a negative acknowledgement (NAK) frame if it is not ready. If the response is positive, the initiator is free to send its data. Otherwise it waits, and try again. Once all its data have been transmitted, the sending system finishes with an end of transmission (EOT) frame.

**<u>Line discipline</u>**



Example of ENQ/ACK line discipline

**<u>POLL/SELECT:</u>**



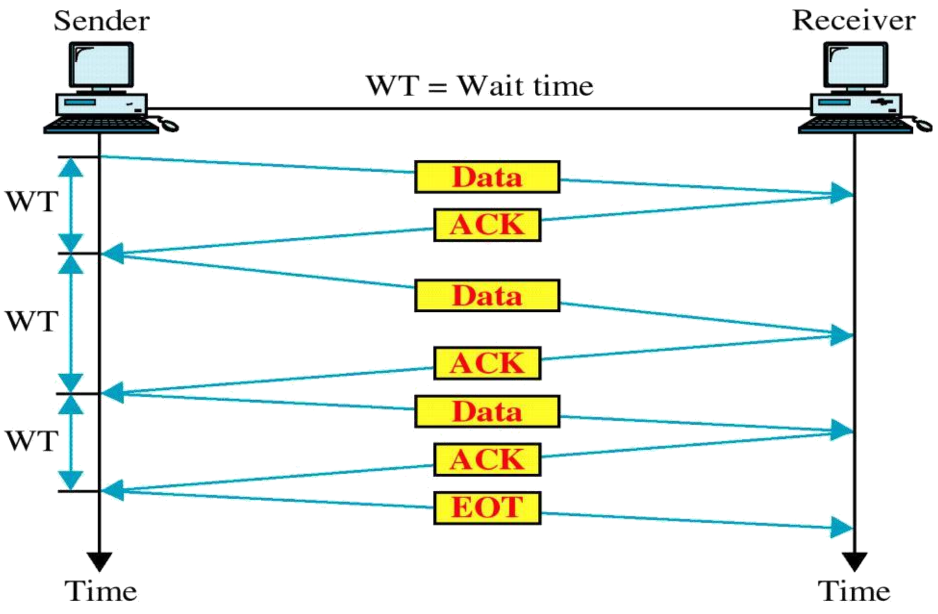
Example of poll/select line discipline

**Flow control**

**Stop-and-Wait flow control**

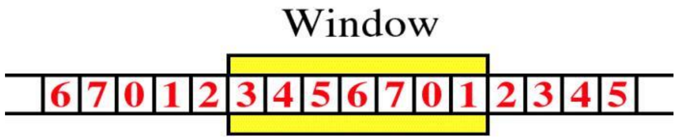
- Source transmits frame

- Destination receives frame and replies with acknowledgement
- Source waits for ACK before sending next frame
- Destination can stop flow by not send ACK
- Works well for a few large frames



Example of Stop-and-Wait flow control

**Sliding Window flow control**



**Error Control**

Detection and correction of errors

Lost frames

Damaged frames

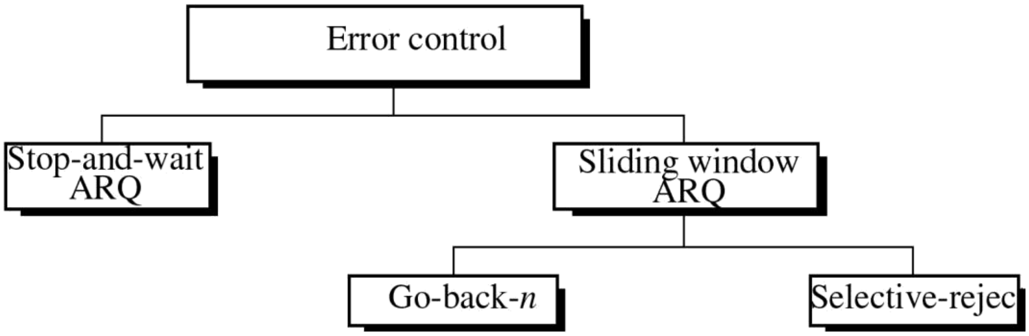
Techniques for error control (Automatic repeat request)

--Error detection

--Positive acknowledgment

--Retransmission after timeout

--Negative acknowledgement and retransmission



## FLOW CONTROL AND ERROR CONTROL

### FLOW CONTROL

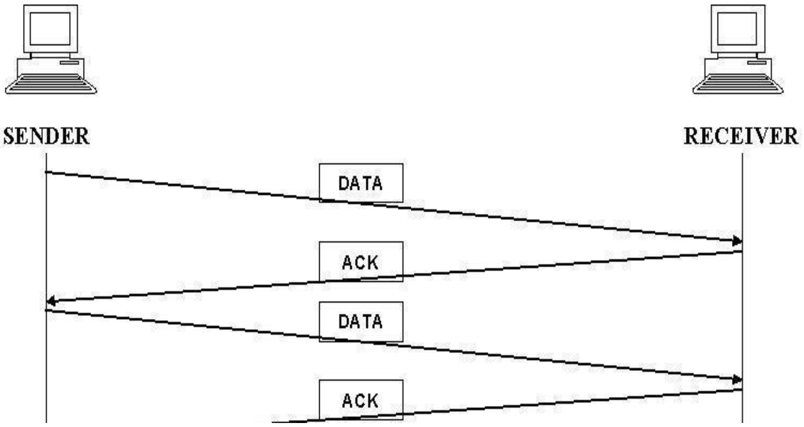
It refers to a set of procedures used to restrict the amount of data flow between sending and receiving stations. It tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.There are two methods are used. They are,

1. stop and wait
2. sliding window

**STOP AND WAIT**:

In this method the sender waits for acknowledgment after every frame it sends.

Only after an acknowledgment has been received, then the sender sends the next frame.

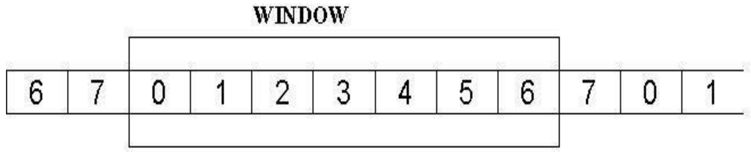


The advantage is simplicity. The disadvantage is inefficiency

**SLIDING WINDOW:**

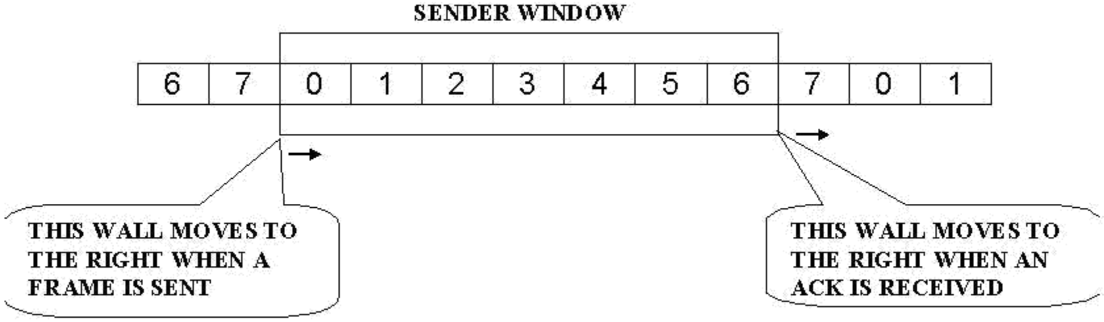
In this method, the sender can transmit several frames before needing an acknowledgment. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.

The sliding window refers to imaginary boxes at both the sender and receiver. This window provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement. To identify each frame the sliding window scheme introduces the sequence number. The frames are numbered as 0 to n-1. And the size of the window is n-1. Here the size of the window is 7 and the frames are numbered as 0,1,2,3,4,5,6,7.

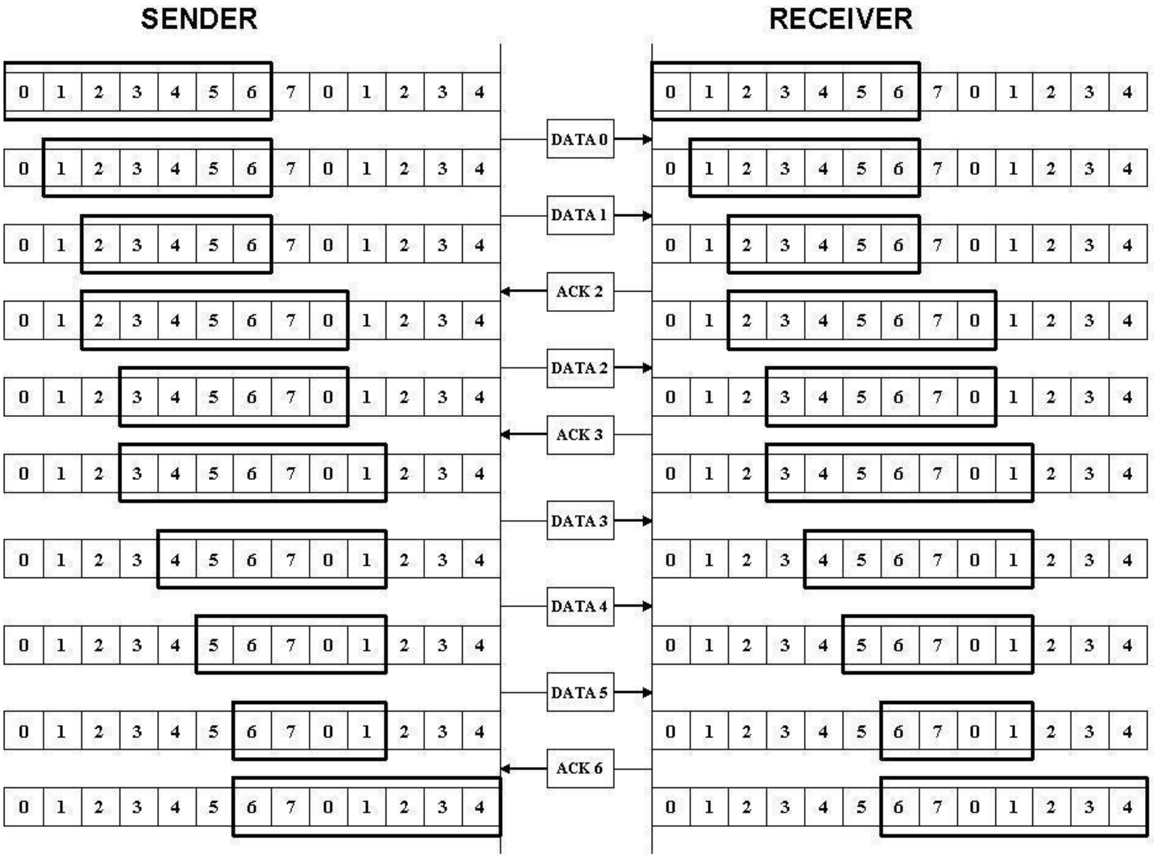


**SENDER WINDOW:**

At the beginning 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. Once an ACK receives the window expands at the right side boundary to allow in a number of new frames equal to number of frames acknowledged by that ACK.


SENDER WINDOW
6
7
0
1
2
3
4
5
6
7
0
1
THIS WALL MOVES TO THE RIGHT WHEN A FRAME IS SENT
THIS WALL MOVES TO THE RIGHT WHEN AN ACK IS RECEIVED

**EXAMPLE:**



## ERROR CONTROL

Error control is implemented in such a way that every time an error is detected, a negative acknowledgement is returned and the specified frame is retransmitted. This process is called **automatic repeat request (ARQ).**The error control is implemented with the flow control mechanism. So there are two types in error control. They are,

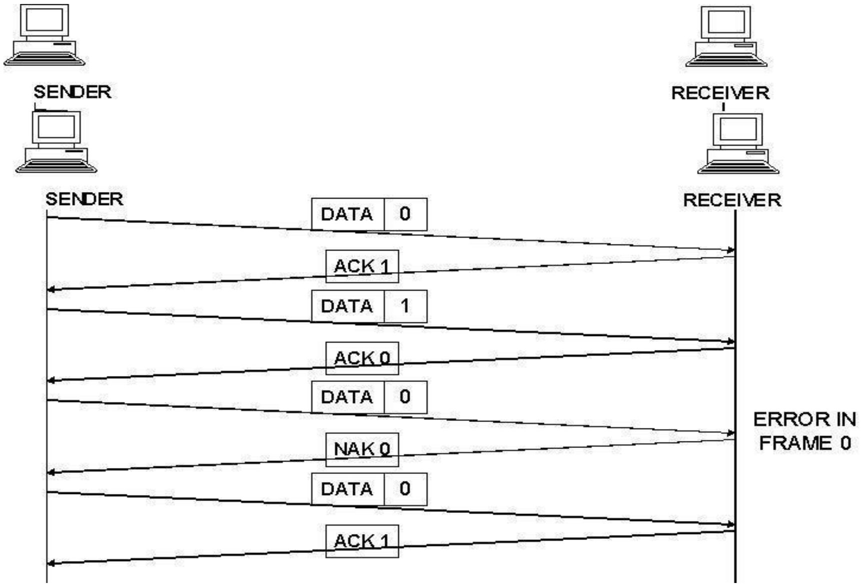
1. stop and wait ARQ
2. sliding window ARQ

**STOP AND WAIT ARQ:**

It is a form of stop and wait flow control, extended to include retransmission of data in case of lost or damaged frames.

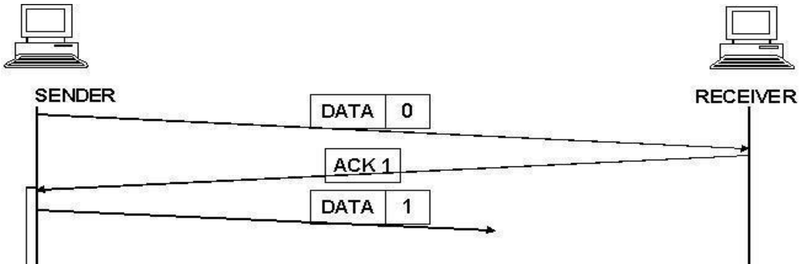
**DAMAGED FRAME:**

When a frame is discovered by the receiver to contain an error, it returns a NAK frame and the sender retransmits the last frame.



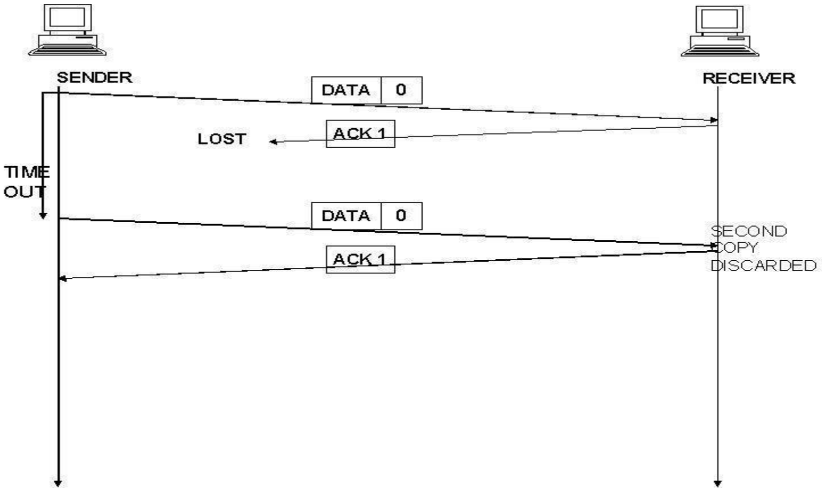
**LOST DATA FRAME:**

The sender is equipped with a timer that starts every time a data frame is transmitted. If the frame lost in transmission the receiver can never acknowledge it. The sending device waits for an ACK or NAK frame until its timer goes off, then it tries again. It retransmits the last data frame.



**LOST ACKNOWLEDGEMENT:**

The data frame was received by the receiver but the acknowledgement was lost in transmission. The sender waits until the timer goes off, then it retransmits the data frame. The receiver gets a duplicated copy of the data frame. So it knows the acknowledgement was lost so it discards the second copy.



**SLIDING WINDOW ARQ**

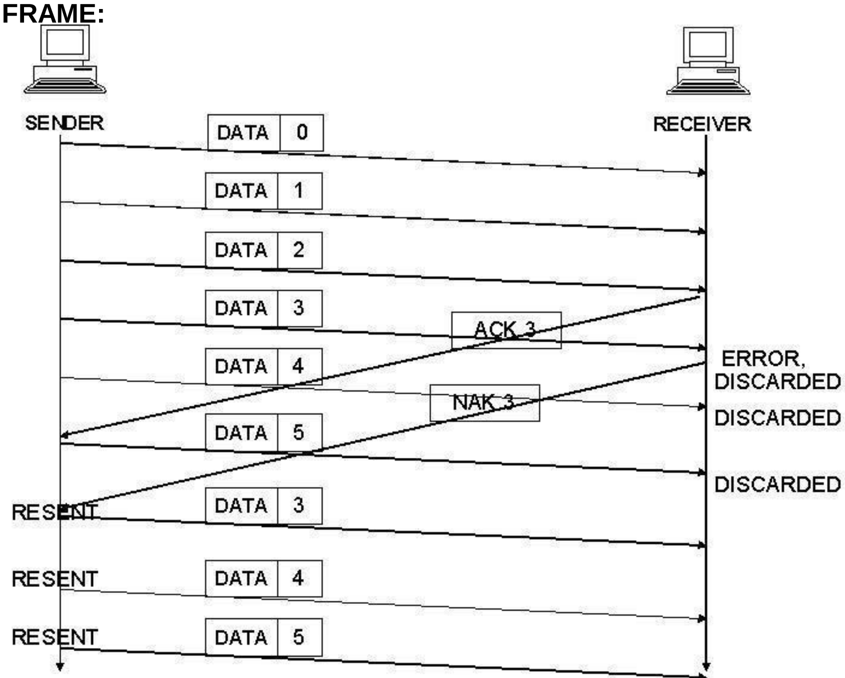
It is used to send multiple frames per time. The number of frame is according to the window size. The sliding window is an imaginary box which is reside on both sender and receiver side. It has two types. They are,

1. go-back-n ARQ
2. selective reject ARQ

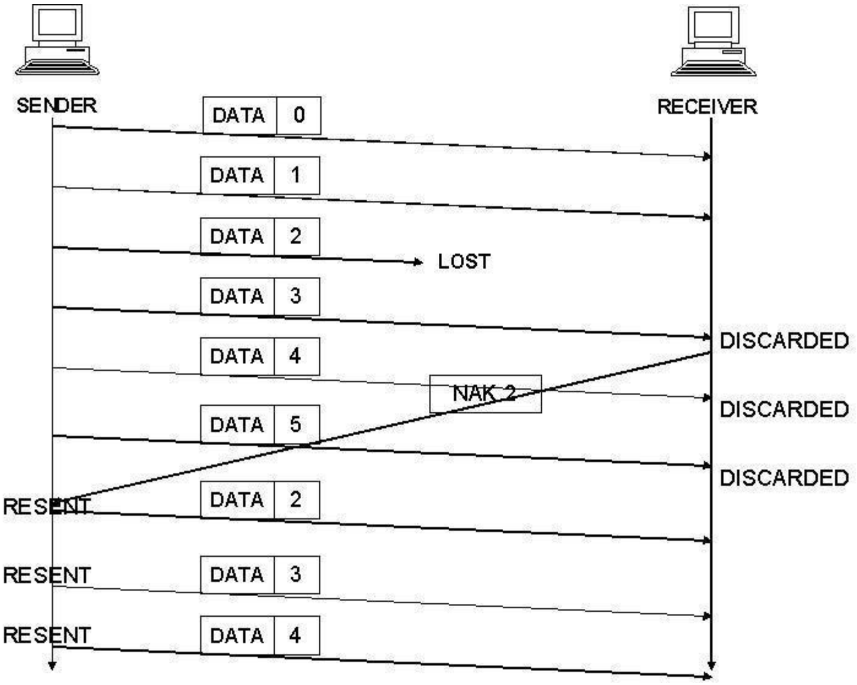
**GO-BACK-N ARQ:**

In this method, if one frame is lost or damaged, all frames sent since the last frame acknowledged or retransmitted.

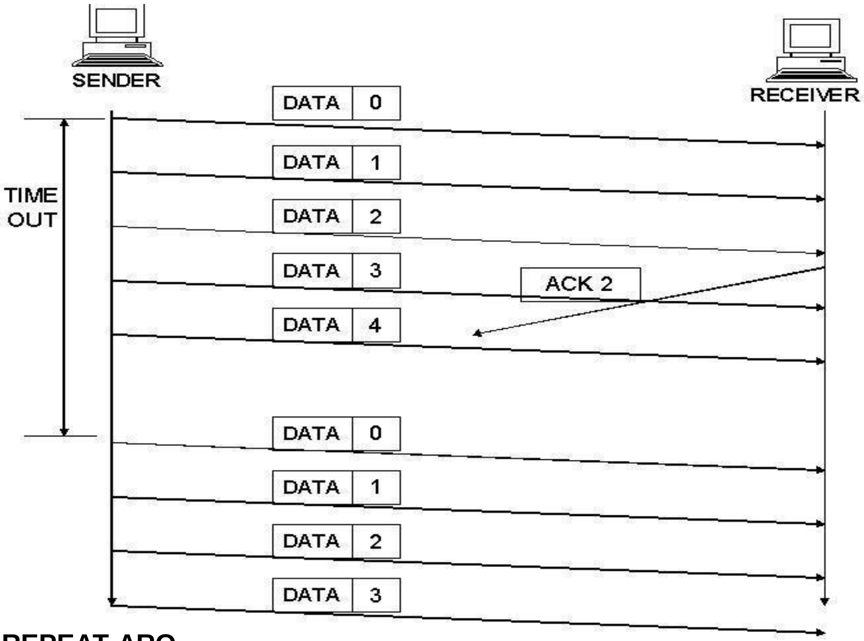
**DAMAGED FRAME:**



**LOST FRAME:**



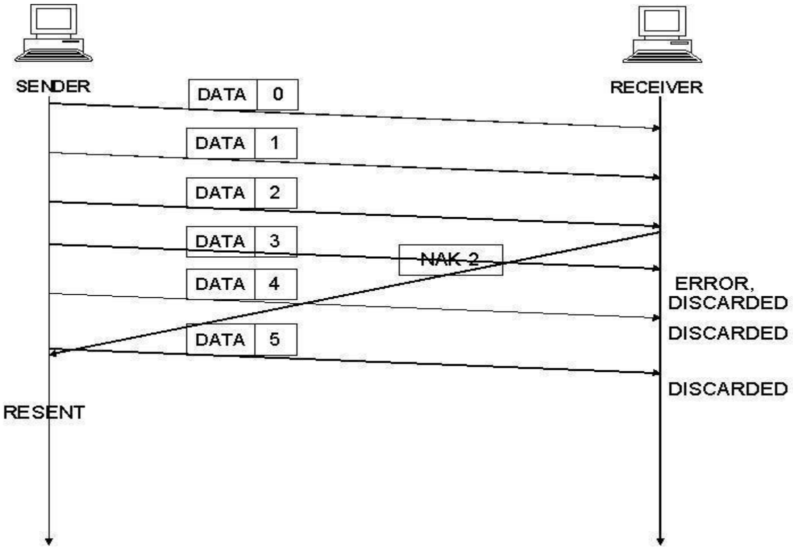
**LOST ACK:**



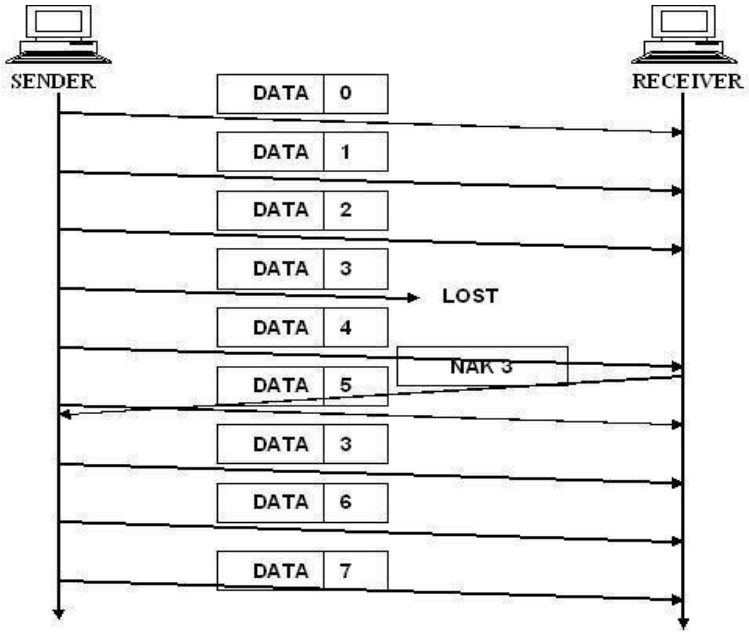
**SELECTIVE REPEAT ARQ**

Selective repeat ARQ re transmits only the damaged or lost frames instead of sending multiple frames. The selective transmission increases the efficiency of transmission and is more suitable for noisy link. The receiver should have sorting mechanism.

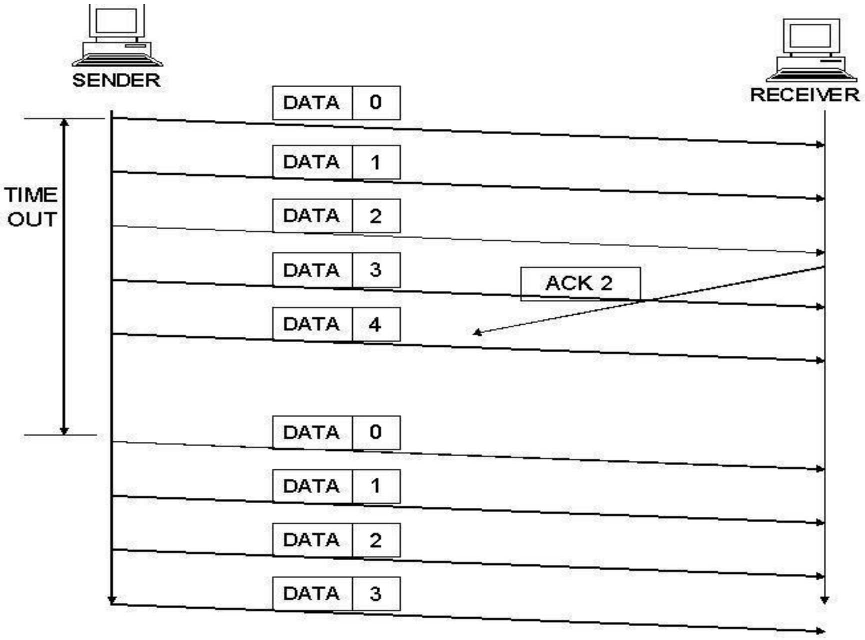
## DAMAGED FRAME



## LOST FRAME



## LOST ACK



**HDLC**

HDLC is a bit-oriented protocol. It was developed by the International Organization for Standardization (ISO). It falls under the ISO standards ISO 3309 and ISO 4335. It specifies a packitization standard for serial links. It has found itself being used throughout the world. It has been so widely implemented because it supports both half-duplex and full-duplex communication lines, point-to-point (peer to peer) and multi-point networks, and switched or non-switched channels. HDLC supports several modes of operation, including a simple sliding-window mode for reliable delivery. Since Internet provides retransmission at higher levels (i.e., TCP), most Internet applications use HDLC's unreliable delivery mode, Unnumbered Information.

Other benefits of HDLC are that the control information is always in the same position, and specific bit patterns used for control differ dramatically from those in representing data, which reduces the chance of errors. It has also led to many subsets. Two subsets widely in use are Synchronous Data Link Control (SDLC) and Link Access Procedure-Balanced (LAP-B).

HDLC Stations and Configurations

HDLC specifies the following three types of stations for data link control:

- Primary Station
- Secondary Station
- Combined Station

**Primary Station**

Within a network using HDLC as its data link protocol, if a configuration is used in which there is a primary station, it is used as the controlling station on the link. It has the responsibility of controlling all other stations on the link (usually secondary stations). A primary issues *commands* and secondary issues *responses*. Despite this important aspect of being on the link, the primary station is also responsible for the organization of data flow on the link. It also takes care of error recovery at the data link level (layer 2 of the OSI model).

**Secondary Station**

If the data link protocol being used is HDLC, and a primary station is present, a secondary station must also be present on the data link. The secondary station is under the control of the primary station. It has no ability, or direct responsibility for controlling the link. It is only activated when requested by the primary station. It only responds to the primary station. The secondary station's frames are called responses. It can only send response frames when requested by the primary station. A primary station maintains a separate logical link with each secondary station.

**Combined Station**

A combined station is a combination of a primary and secondary station. On the link, all combined stations are able to send and receive commands and responses without any permission from any other stations on the link. Each combined station is in full control of itself, and does not rely on any other stations on the link. No other stations can control any combined station. May issue both commands and responses.HDLC also defines three types of configurations for the three types of stations. The word configuration refers to the relationship between the hardware devices on a link. Following are the three configurations defined by HDLC:

- Unbalanced Configuration
- Balanced Configuration
- Symmetrical Configuration

**Unbalanced Configuration**

The unbalanced configuration in an HDLC link consists of a primary station and one or more secondary stations. The unbalanced condition arises because one station controls the other stations. In an unbalanced configuration, any of the following can be used:

- Full-Duplex or Half-Duplex operation
- Point to Point or Multi-point networks

An example of an unbalanced configuration can be found below

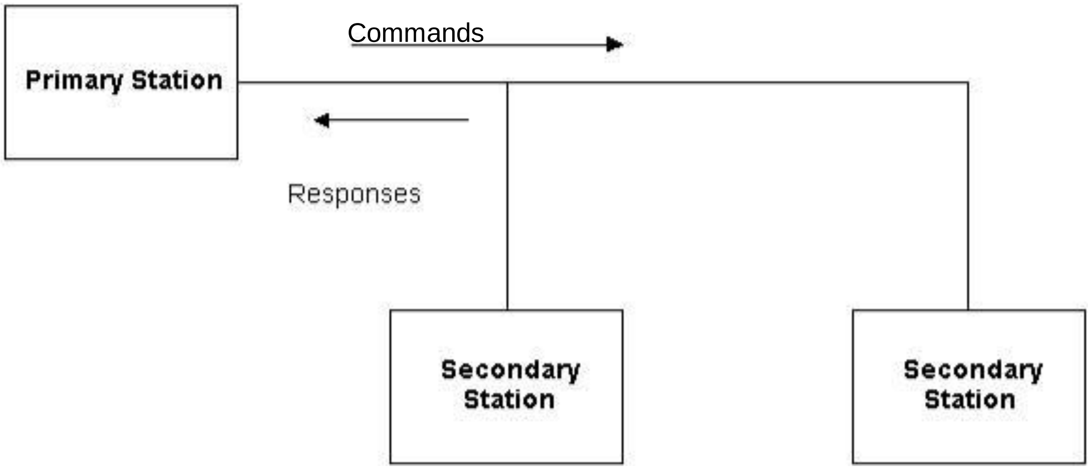


Figure .Unbalanced configuration

**Balanced Configuration**

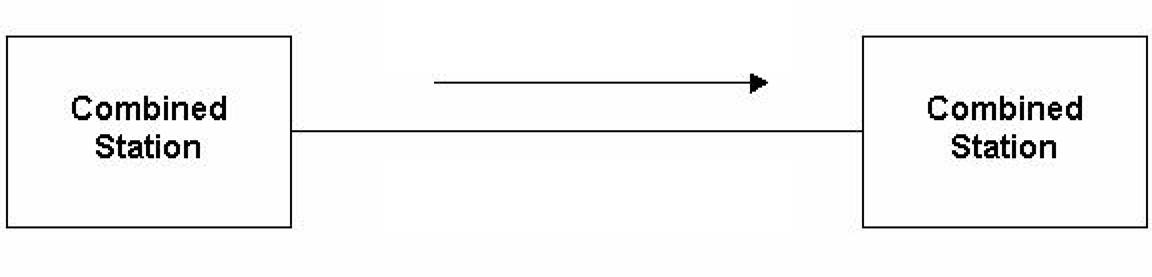
The balanced configuration in an HDLC link consists of two or more combined stations.Each of the stations has equal and complimentary responsibility compared to each other.Balanced configurations can use only the following:

- Full - Duplex or Half - Duplex operation

- Point to Point networks

An example of a balanced configuration can be found below.

**Commands/ responses**



**Commands/ responses**

Figure .Balanced configuration

### Symmetrical Configuration

This third type of configuration is not widely in use today. It consists of two independent point-to-point, unbalanced station configurations as shown in Figure. In this configuration, each station has a primary and secondary status. Each station is logically considered as two stations.

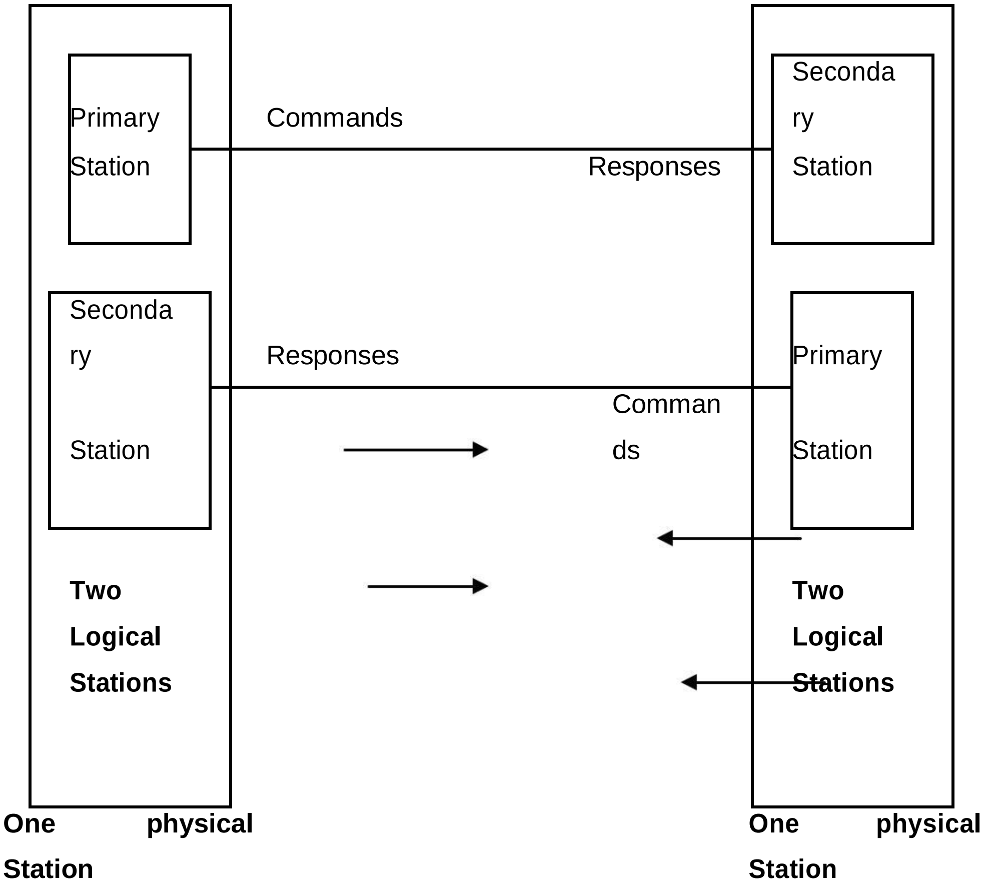


Figure. Symmetric configuration

### HDLC Operational Modes

A mode in HDLC is the relationship between two devices involved in an exchange; the mode describes who controls the link. Exchanges over unbalanced configurations are always conducted in normal response mode. Exchanges over symmetric or balanced configurations can be set to specific mode using a frame design to deliver the command. HDLC offers three different modes of operation. These three modes of operations are:

- Normal Response Mode (NRM)
- Asynchronous Response Mode (ARM)
- Asynchronous Balanced Mode (ABM)

**Normal Response Mode**

This is the mode in which the primary station initiates transfers to the secondary station. The secondary station can only transmit a response when, and only when, it is instructed to do so by the primary station. In other words, the secondary station must receive explicit permission from the primary station to transfer a response. After receiving permission from the primary station, the secondary station initiates its transmission. This transmission from the secondary station to the primary station may be much more than just an acknowledgment of a frame. It may in fact be more than one information frame. Once the last frame is transmitted by the secondary station, it must wait once again from explicit permission to transfer anything, from the primary station. Normal Response Mode is only used within an unbalanced configuration.

**Asynchronous Response Mode**

In this mode, the primary station doesn't initiate transfers to the secondary station. In fact, the secondary station does not have to wait to receive explicit permission from the primary station to transfer any frames. The frames may be more than just acknowledgment frames. They may contain data, or control information regarding the status of the secondary station. This mode can reduce overhead on the link, as no frames need to be transferred in order to give the secondary station permission to initiate a transfer. However, some limitations do exist. Due to the fact that this mode is asynchronous, the secondary station must wait until it detects and idle channel before it can transfer any frames. This is when the ARM link is operating at half-duplex. If the ARM link is operating at full duplex, the secondary station can transmit at any time. In this mode, the primary station still retains responsibility for error recovery, link setup, and link disconnection.

**Synchronous Balanced Mode**

This mode is used in case of combined stations. There is no need for permission on the part of any station in this mode. This is because combined stations do not require any sort of instructions to perform any task on the link.Normal Response Mode is used most frequently in multi- point lines, where the primary station controls the link. Asynchronous Response Mode is better for point-to-point links, as it reduces overhead. Asynchronous Balanced Mode is not used widely today. The "asynchronous" in both ARM and ABM does not refer to the format of the data on the link. It refers to the fact that any given station can transfer frames without explicit permission or instruction from any other station.

HDLC Non-Operational Modes

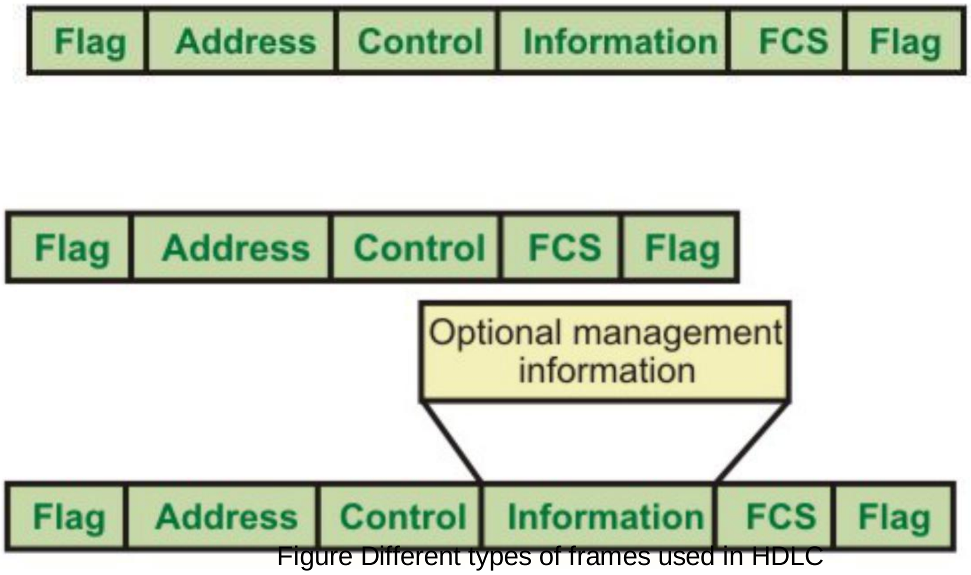
HDLC also defines three non-operational modes. These three non-operational modes are:

- Normal Disconnected Mode (NDM)
- Asynchronous Disconnected Mode (ADM)
- Initialization Mode (IM)

The two disconnected modes (NDM and ADM) differ from the operational modes in that the secondary station is logically disconnected from the link (note the secondary station is not physically disconnected from the link). The IM mode is different from the operations modes in that the secondary station's data link control program is in need of regeneration or it is in need of an exchange of parameters to be used in an operational mode.

HDLC Frame Structure

There are three different types of frames as shown in Fig. and the size of different fields are shown Table



**I-Frame**

**S-Frame**

**U-Frame**

Figure Different types of frames used in HDLC

**Table** Size of different fields

| **Field Name** | **Size(in bits)** |
|---|---|
| [redacted] | [redacted] |
| Flag Field( F ) | 8 bits |
| Address Field( A ) | 8 bits |
| Control Field( C ) | 8 or 16 bits |
| Information Field( I ) OR Data | Variable; Not used in some frames |
| Frame Check Sequence( FCS ) | 16 or 32 bits |
| Closing Flag Field( F ) | 8 bits |

**The Flag field**

Every frame on the link must begin and end with a flag sequence field (F). Stations attached to the data link must continually listen for a flag sequence. The flag sequence is an octet looking like 01111110. Flags are continuously transmitted on the link between frames to keep the link active. Two other bit sequences are used in HDLC as signals for the stations on the link. These two bit sequences are:

- Seven 1's, but less than 15 signal an abort signal. The stations on the link know there is a problem on the link.
- 15 or more 1's indicate that the channel is in an idle state.

The time between the transmissions of actual frames is called the **interframe time fill**. The interframe time fill is accomplished by transmitting continuous flags between frames. The flags may be in 8 bit multiples.

HDLC is a code-transparent protocol. It does not rely on a specific code for interpretation of line control. This means that if a bit at position N in an octet has a specific meaning, regardless of the other bits in the same octet. If an octet has a bit sequence of 01111110, but is not a flag field, HLDC uses a technique called bit-stuffing to differentiate this bit sequence from a flag field as we have discussed in the previous lesson.

At the receiving end, the receiving station inspects the incoming frame. If it detects 5 consecutive 1's it looks at the next bit. If it is a 0, it pulls it out. If it is a 1, it looks at the 8th bit. If the 8th bit is a 0, it knows an abort or idle signal has been sent. It then proceeds to inspect the following bits to determine appropriate action. This is the manner in which HDLC achieves code-transparency. HDLC is not concerned with any specific bit code inside the data stream. It is only concerned with keeping flags unique.

**The Address field**

The address field (A) identifies the primary or secondary stations involvement in the frame transmission or reception. Each station on the link has a unique address. In an unbalanced configuration, the A field in both commands and responses refer to the secondary station. In a balanced configuration, the command frame contains the destination station address and the response frame has the sending station's address.

**The Control field**

HDLC uses the control field (C) to determine how to control the communications process. This field contains the commands, responses and sequences numbers used to maintain the data flow accountability of the link, defines the functions of the frame and initiates the logic to control the movement of traffic between sending and receiving stations. There three control field formats:

- **Information Transfer Format**: The frame is used to transmit end-user data between two devices.
- **Supervisory Format**: The control field performs control functions such as acknowledgment of frames, requests for re-transmission, and requests for temporary suspension of frames being transmitted. Its use depends on the operational mode being used.

- **Unnumbered Format**: This control field format is also used for control purposes. It is used to perform link initialization, link disconnection and other link control functions.

**The Poll/Final Bit (P/F)**

The 5th bit position in the control field is called the **poll/final bit, or P/F bit**. It can only be recognized when it is set to 1. If it is set to 0, it is ignored. The poll/final bit is used to provide dialogue between the primary station and secondary station. The primary station uses P=1 to acquire a status response from the secondary station. The P bit signifies a poll. The secondary station responds to the P bit by transmitting a data or status frame to the primary station with the P/F bit set to F=1. The F bit can also be used to signal the end of a transmission from the secondary station under Normal Response Mode.

**The Information field or Data field**

This field is not always present in a HDLC frame. It is only present when the Information Transfer Format is being used in the control field. The information field contains the actually data the sender is transmitting to the receiver in an I-Frame and network management information in U-Frame.

**The Frame check Sequence field**

This field contains a 16-bit, or 32-bit cyclic redundancy check bits. It is used for error detection as discussed in the previous lesson.

**Error Detecting Codes**

Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.

Some popular techniques for error detection are:

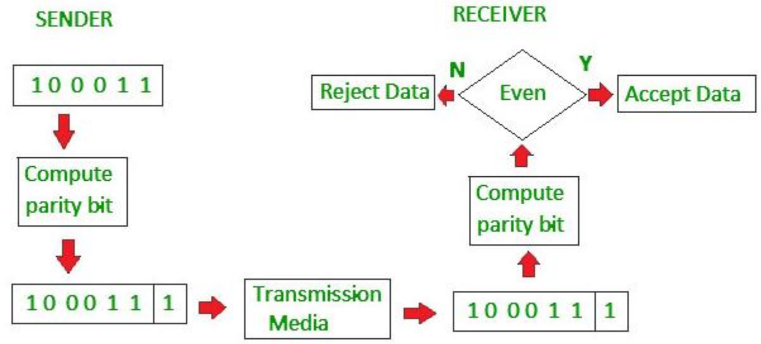
1. Vertical Redundancy Check(VRC)
2. Longitudinal Redundancy Check(VRC)
3. Checksum
4. Cyclic redundancy check

### 1. Vertical Redundancy Check(VRC)

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

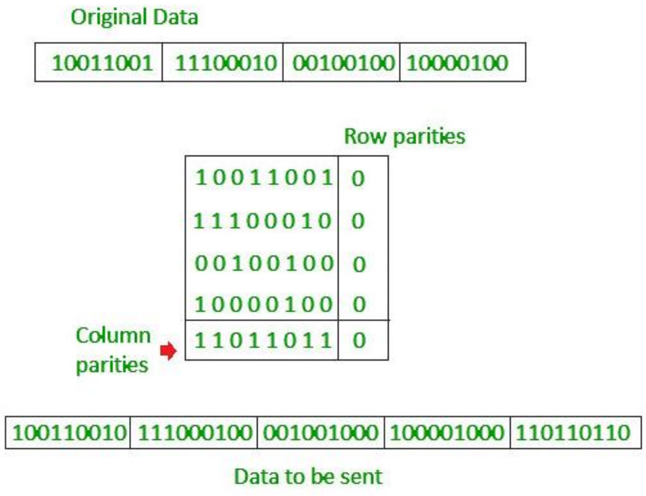
- 1 is added to the block if it contains odd number of 1’s, and
- 0 is added if it contains even number of 1’s

This scheme makes the total number of 1’s even, that is why it is called even parity checking.



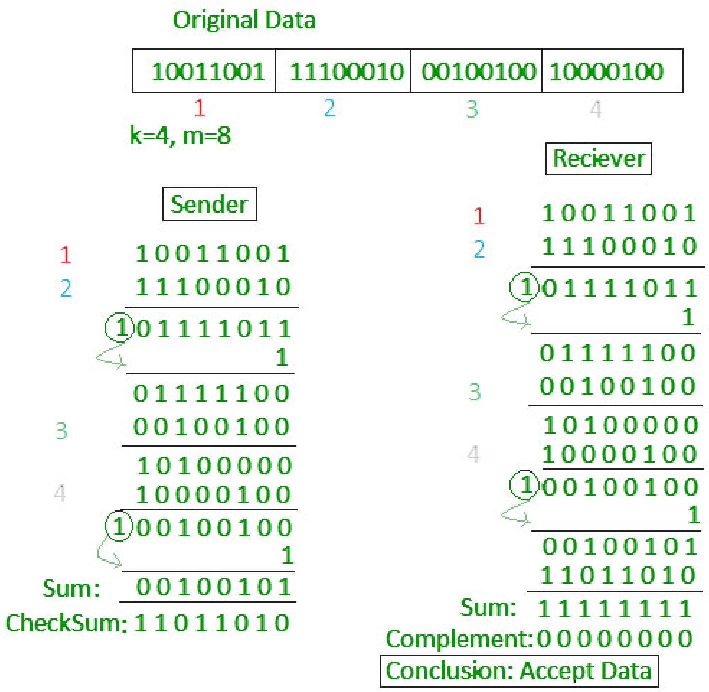
### 2. Longitudinal Redundancy Check(VRC)

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.



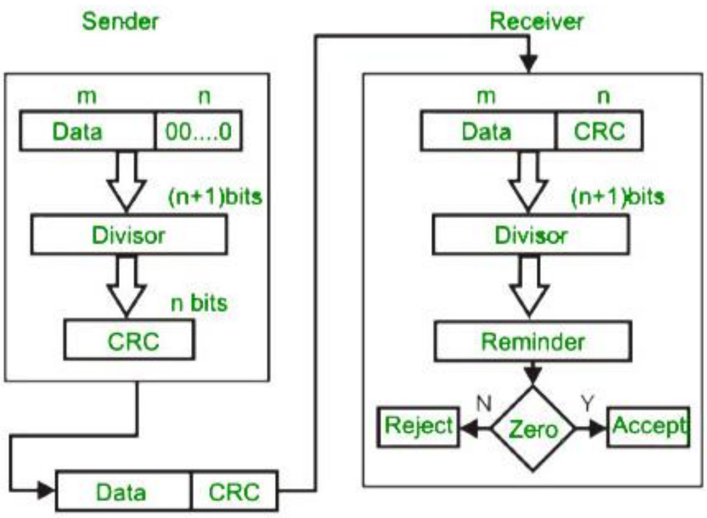
### 3. Checksum

- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender’s end the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

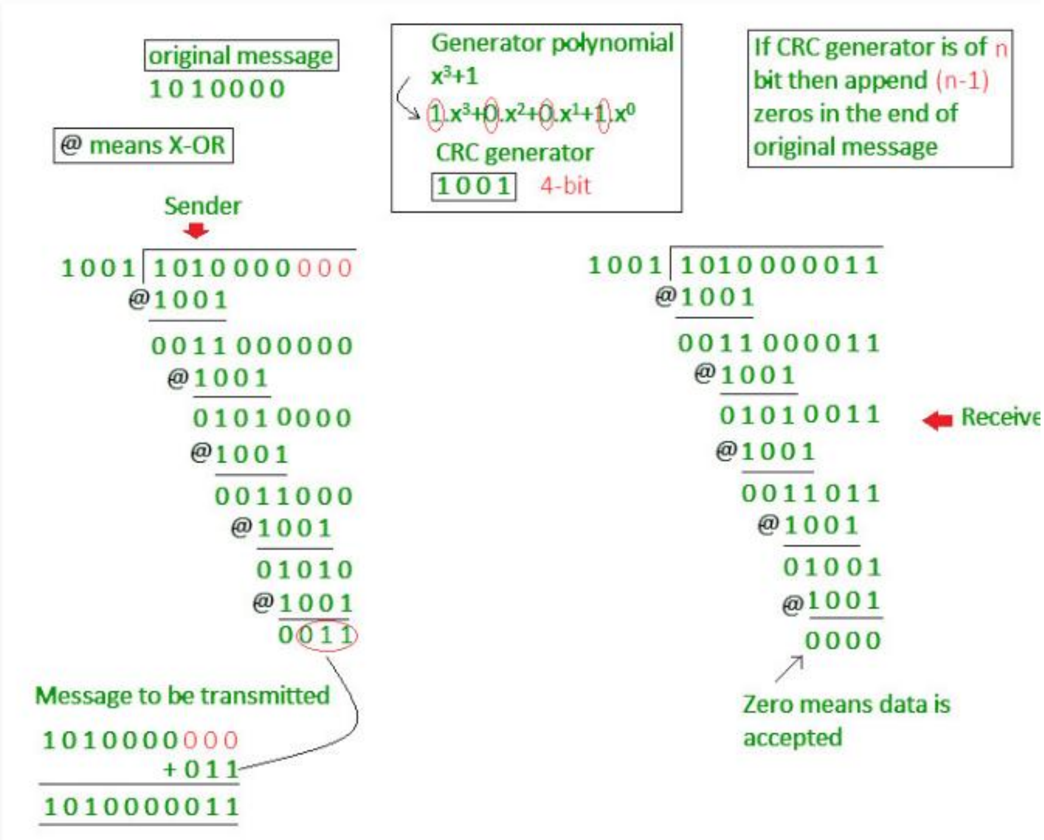


### 4. Cyclic redundancy check (CRC)

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the 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 correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



**Example :**


original message
1010000
@ means X-OR
Generator polynomial
x3+1
1.x3+0.x2+0.x1+1.x0
CRC generator
1001 4-bit
If CRC generator is of n bit then append (n-1) zeros in the end of original message
Sender
1001 | 1010000000
@1001
0011000000
@1001
01010000
@1001
0011000
@1001
01010
@1001
0011
Message to be transmitted
1010000000
+011
1010000011
1001 | 1010000011
@1001
0011000011
@1001
01010011
@1001
0011011
@1001
01001
@1001
0000
Receive
Zero means data is accepted

# SEC1306 DATA COMMUNICATION AND NETWORKING

## UNIT 4

**MAC SUB LAYER AND NETWORK LAYER.**

**MAC sub layer for Standard Ethernet, Fast Ethernet, Wireless LAN and broadband wireless. Design issues of network layer - Routing algorithm - shortest path routing - Distance vector routing - Broadcast routing - Congestion control algorithm - Congestion control in virtual circuit and datagram switches - The network layer in the internet - The IP protocol - IP Addresses - Mobile IP - IPv6.**

### 4.1 MAC sub layer for Standard

Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards. Ethernet supports data bandwidths of:

- 10 Mb/s
- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10,000 Mb/s (10 Gb/s)
- 40,000 Mb/s (40 Gb/s)
- 100,000 Mb/s (100 Gb/s)

Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. For the Layer 2 protocols, as with all 802 IEEE standards, Ethernet relies on the two separate sublayers of the data link layer to operate, the Logical Link Control (LLC) and the MAC sublayers.

### LLC sublayer

The Ethernet LLC sublayer handles the communication between the upper layers and the lower layers. This is typically between the networking software and the device hardware. The LLC sublayer takes the network protocol data, which is typically an IPv4 packet, and adds control information to help deliver the packet to the destination node. The LLC is used to communicate with the upper layers of the application, and transition the packet to the lower layers for delivery.

LLC is implemented in software, and its implementation is independent of the hardware. In a computer, the LLC can be considered the driver software for the NIC. The NIC driver is a program that interacts directly with the hardware on the NIC to pass the data between the MAC sublayer and the physical media.

### MAC sublayer

MAC constitutes the lower sublayer of the data link layer. MAC is implemented by hardware, typically in the computer NIC. The specifics are specified in the IEEE 802.3 standards. Figure 4.1 lists common IEEE Ethernet standards.

### IEEE 802.3 and Ethernet

- Very popular LAN standard.
- Ethernet and IEEE 802.3 are distinct standards but as they are very similar to one another these words are used interchangeably.
- A standard for a 1-persistent CSMA/CD LAN.
- It covers the physical layer and MAC sublayer protocol.

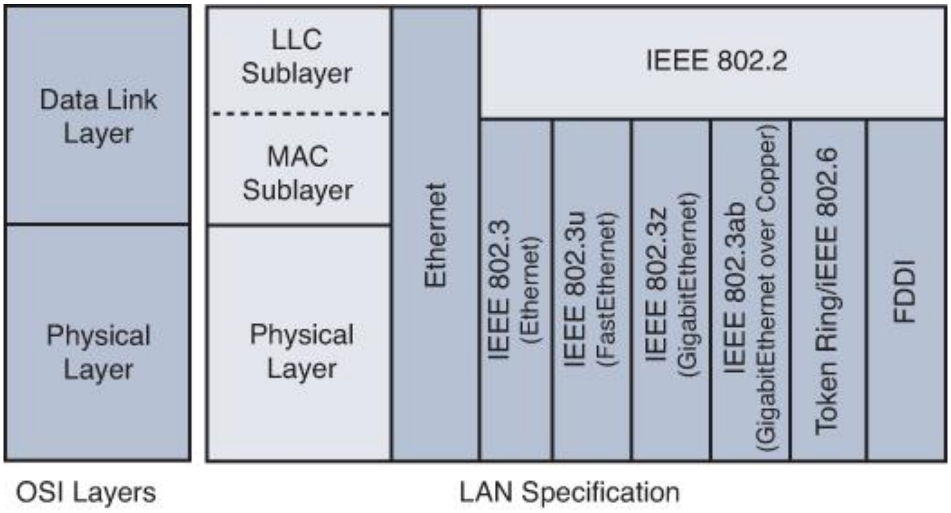


Figure 4.1 Common IEEE Ethernet Standards

### 4.2 Fast Ethernet

Fast Ethernet is a collective term for a number of Ethernet standards that carry traffic at the nominal rate of 100 Mbit/s (the earlier Ethernet speed was 10 Mbit/s). Of the Fast Ethernet standards, 100BASE-TX is by far the most common.

Fast Ethernet was introduced in 1995 as the IEEE 802.3u standard and remained the fastest version of Ethernet for three years before the introduction of Gigabit Ethernet.

### 4.3 wireless local area network (WLAN)

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using wireless communication within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

**4.3.1 Wireless broadband** is technology that provides high-speed wireless Internet access or computer networking access over a wide area.

broadband means "having instantaneous bandwidths greater than 1 MHz and supporting data rates greater than about 1.5 Mbit/s.

### 4.4 The network layer design issues :

**1)** Store and formed packet switching.

**2)** Service provided to the transport layer.

**3)** Implementation of connectionless service.

**4)** Implementation of connection-oriented source.

**5)** Comparison of virtual circuit and datagram submits.

**1) Store and formed packet switching :**

Store and forward operation : -

**i)** Host transmits packet to router across LAN or oval point to point link.

**ii)** Packet is stored on router until fully arrived and processed.

**iii)** Packet is forward to next router.

**2) Service provide to transport layer :**

The network layer services have been designed with the goals : -

**i)** The advice should independent of router telenet

**ii)** The transport layer should be shilded from the number type and topology of the router present.

**iii)** The network addresses maid arailable to transport

**3) Implementation of connectionless service :**

Connectionless service is offered packets are injected into the subnet individually and routed idependently of each other. Each packet is transmitted idenpendently.

Connectionless service used in network layer ID and transport layer.

Packet are frequently called datagram connectionless service is largly for data communication the internet.

**4) Implementation of connection-oriented service : -**

Connection-oriented service is used a path from the source router to the destination router must be established before any data packet can be sent.

Connection oriented service also called virtual circuit service. This service used network layer for ATM. It also used in transport layer for TCP.

A connection must be established before any can be sent packets order preserved logical connection is also established here.

### 4.5 Routing Algorithm

A **Routing Algorithm** is a method for determining the routing of packets in a node. For each node of a network, the algorithm determines a routing table, which in each destination, matches an output line. The algorithm should lead to a consistent routing, that is to say without loop. This means that you should not route a packet a node to another node that could send back the package.

**There are three main types of routing algorithms:**

- Distance Vector (distance-vector routing);

- To link state (link state routing);
- Path to vector (path-vector routing).

**4.6 Shortest path routing** refers to the process of finding paths through a network that have a minimum of distance or other cost metric.

Use Dijkstra's algorithm to compute the shortest paths from a given source node to all other nodes in a network. Links are bi-directional, with the same distance in either direction. Distance can be any measure of cost.

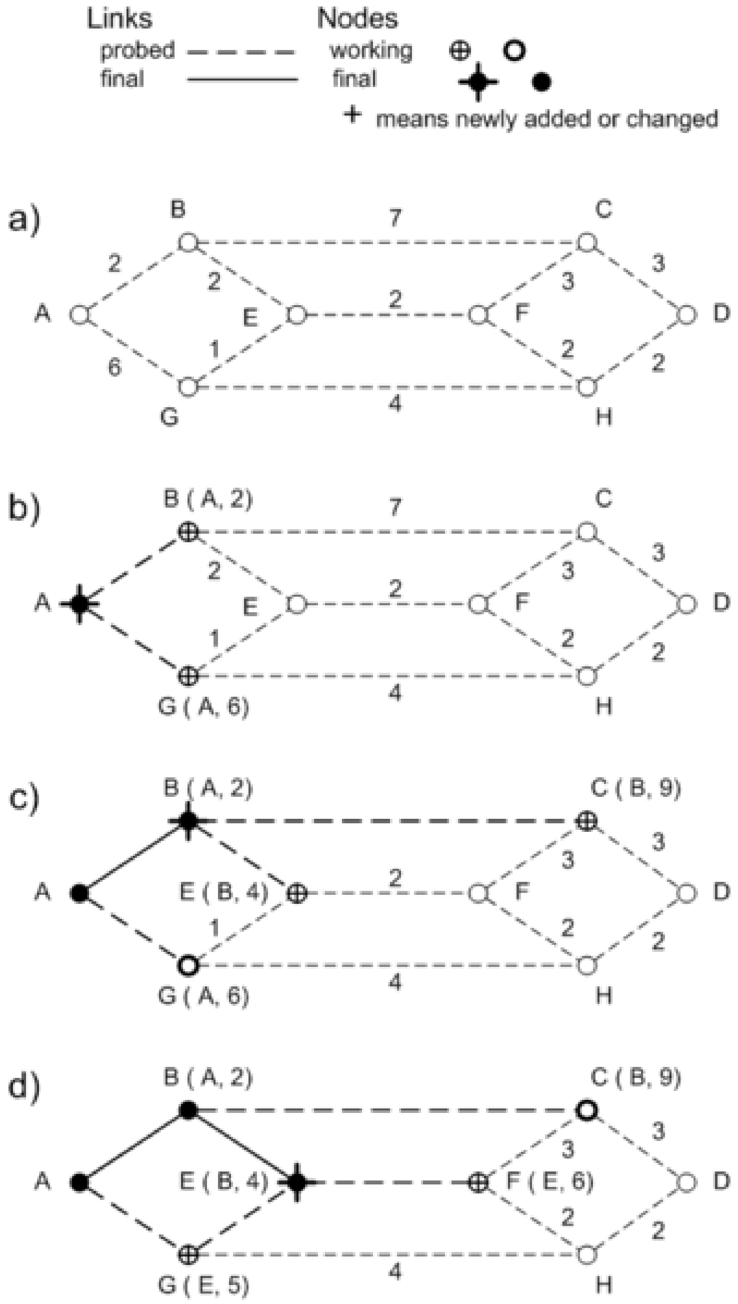
Example from Figure 1 (8 nodes, 11 links)

```
nodeset = {'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H'}

linklist = [('A', 'B', 2), ('B', 'C', 7), ('C', 'D', 3), # (node,node,distance)

        ('B', 'E', 2), ('E', 'F', 2), ('F', 'C', 3),

        ('A', 'G', 6), ('G', 'E', 1), ('G', 'H', 4),

        ('F', 'H', 2), ('H', 'D', 2),
```

The strategy is to start at the source node, send probes to each of its adjacent nodes, pick the node with the shortest path from the source, and make that the new working node. Send probes from the new working node, pick the next shortest path, and make that the next working node. Continue selecting the shortest possible path until every every node in the network has been selected.

Figure 4.2 shows the first few steps in our example network. Labels on each node show its distance from the source, and the previous node on the path from which that distance was computed. As new nodes are first probed, they are added to a working set, shown with a darkened open circle. After each probe cycle, we look at the entire set of working nodes. The node with the shortest path is moved to a final set, shown with a solid circle.

The light dotted lines are links not used in any shortest path from node A. They might be used in another tree, however. Each node in a network can compute its own shortest path tree, given the linklist for the entire network.


Links
probed
final
Nodes
working
final
+ means newly added or changed
a)
A
B
C
D
E
F
G
H
2
6
7
2
1
2
4
3
2
3
2
b)
B ( A, 2)
G ( A, 6)
c)
C ( B, 9)
E ( B, 4)
d)
F ( E, 6)
G ( E, 5)

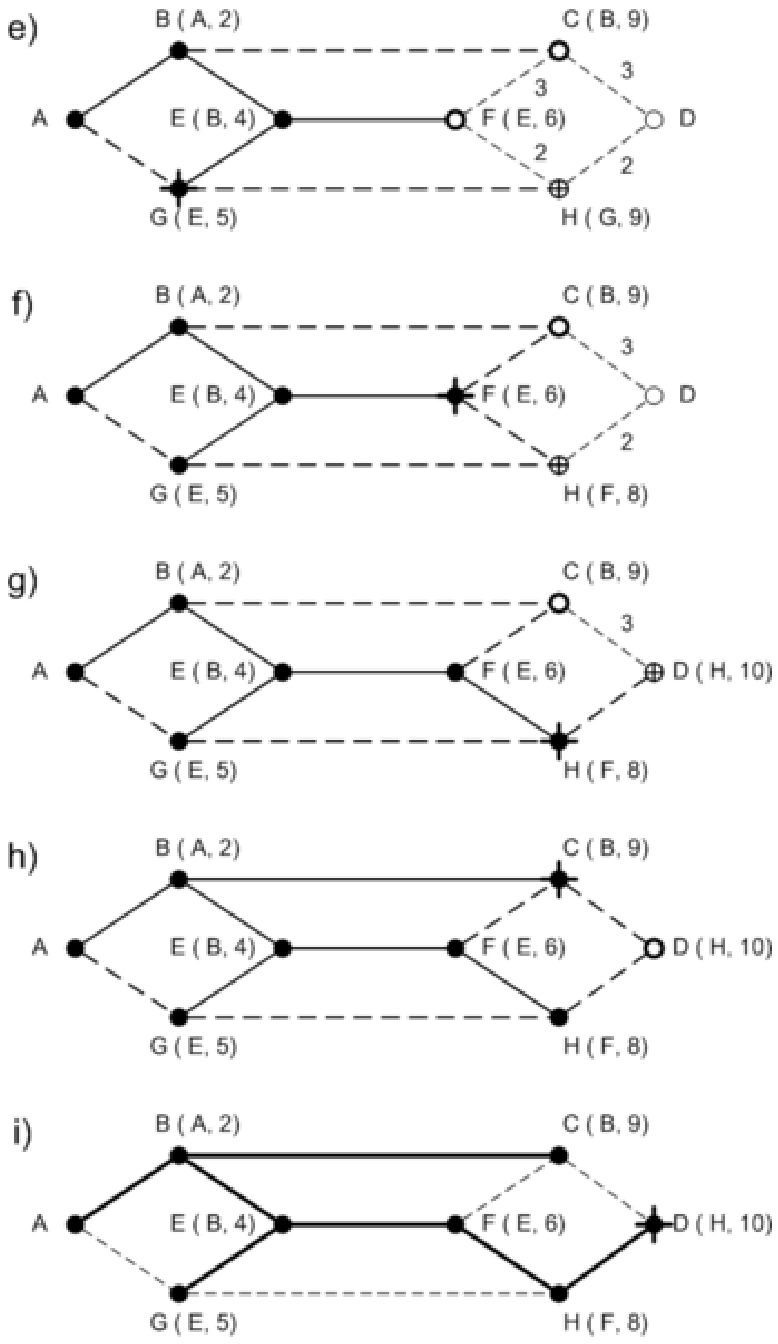


Figure 4.2 Dijkstra's algorithm

### 4.7 Distance-Vector Routing

: Each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.

1. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.

2. A link that is down is assigned an infinite cost.

Example.

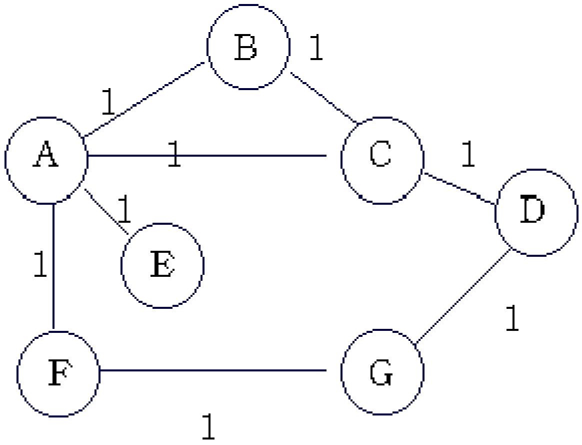


Figure 4.3 Distance-Vector Routing

| **Information Stored at Node** | **Distance to Reach Node** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **A** | **B** | **C** | **D** | **E** | **F** | **G** |
| **A** | 0 | 1 | 1 | � | 1 | 1 | � |
| **B** | 1 | 0 | 1 | � | � | � | � |
| **C** | 1 | 1 | 0 | 1 | � | � | � |
| **D** | � | � | 1 | 0 | � | � | 1 |
| **E** | 1 | � | � | � | 0 | � | � |
| **F** | 1 | � | � | � | � | 0 | 1 |
| **G** | � | � | � | 1 | � | 1 | 0 |

**Table 1. Initial distances stored at each node(global view)**

We can represent each node's knowledge about the distances to all other nodes as a table like the one given in Table 1.

Note that each node only knows the information in one row of the table.

1. Every node sends a message to its directly connected neighbors containing its personal list of distance. ( for example, **A** sends its information to its neighbors **B,C,E**, and **F**. )

2. **I**f any of the recipients of the information from **A** find that **A** is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through **A**. ( node **B** learns from **A** that node **E** can be reached at a cost of 1; **B** also knows it can reach **A** at a cost of 1, so it adds these to get the cost of reaching **E** by means of **A**. **B** records that it can reach **E** at a cost of 2 by going through **A**.)

3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.

4. **I**n addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table. ( for example, **B** knows that it was **A** who said " **I** can reach **E** in one hop" and so **B** puts an entry in its table that says " To reach **E**, use the link to **A**.)

| **Information**<br>**Stored at Node** | **Distance to Reach Node** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **A** | **B** | **C** | **D** | **E** | **F** | **G** |
| **A** | 0 | 1 | 1 | 2 | 1 | 1 | 2 |
| **B** | 1 | 0 | 1 | 2 | 2 | 2 | 3 |
| **C** | 1 | 1 | 0 | 1 | 2 | 2 | 2 |
| **D** | 2 | 2 | 1 | 0 | 3 | 2 | 1 |
| **E** | 1 | 2 | 2 | 3 | 0 | 2 | 3 |
| **F** | 1 | 2 | 2 | 2 | 2 | 0 | 1 |
| **G** | 2 | 3 | 2 | 1 | 3 | 1 | 0 |

**Table 2. final distances stored at each node ( global view).**

In practice, each node's forwarding table consists of a set of triples of the form:

( Destination, Cost, NextHop).

For example, Table 3 shows the complete routing table maintained at node B for the network in figure 4.3.

| **Destination** | **Cost** | **NextHop** |
|---|---|---|
| **A** | 1 | A |
| **C** | 1 | C |
| **D** | 2 | C |
| **E** | 2 | A |
| **F** | 2 | A |
| **G** | 3 | A |

**Table 3. Routing table maintained at node B.**

### 4.8 Broadcast routing

Broadcast Routing

Broadcasting: sending a packet to all N receivers

. routing updates in LS routing

. service/request advertisement in application layer (e.g., Novell)

Broadcast algorithm 1: N point-to-point sends

. send packet to every destination, point-to-point

. wasteful of bandwidth

. requires knowledge of all destinations

Broadcast algorithm 2: flooding

. when node receives a broadcast packet, send it out on every link

. node may receive many copies of broadcast packet, hence must be able to detect duplicates

Broadcast Routing: Reverse Path Forwarding

Goal: avoid flooding duplicates Assumptions:

. A wants to broadcast .

all nodes know predecessor node on shortest path back to A

Reverse path forwarding: if node receives a broadcast packet

. if packet arrived on p ed on predecessor on shortest path to A, then flood to all neighbors

. otherwise ignore broadcast packet - either already arrived

Reverse Path Forwarding

. flood if packet arrives from source on link that router would use to send packets to source

. otherwise discard

. rule avoids flooding loops

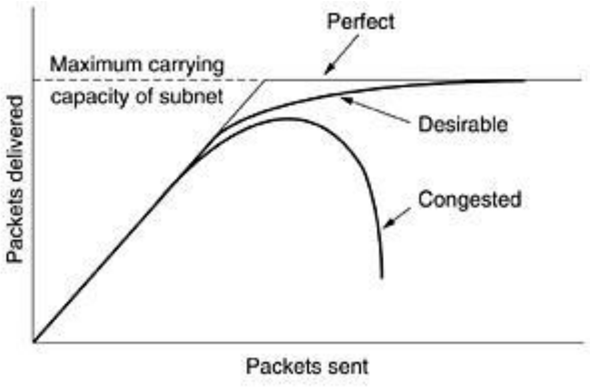
. uses shortest path tree from destinations to source (reverse tree)

**4.9 Congestion control algorithms**

What is **congestion**?

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

**Effects** of Congestion



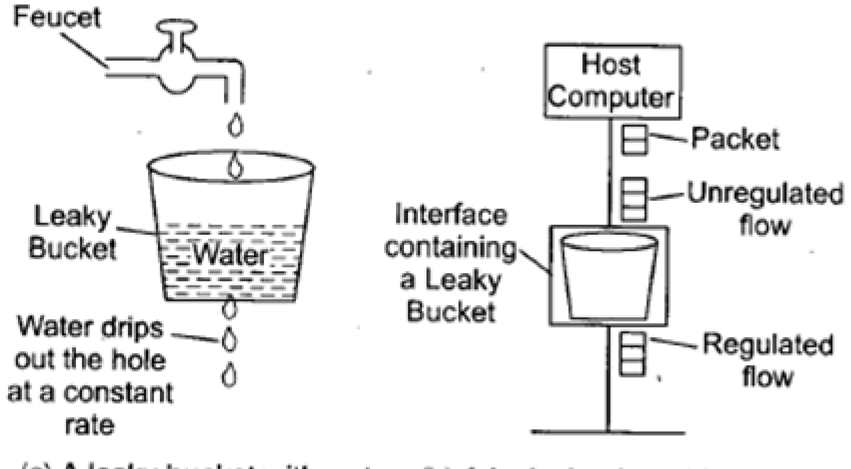
- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

**Congestion control algorithms**

### 4.9.1 Leaky Bucket Algorithm

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.


Feucet
Leaky Bucket
Water
Water drips out the hole at a constant rate
Host Computer
Packet
Unregulated flow
Interface containing a Leaky Bucket
Regulated flow

(a) A leaky bucket with water (b) A leaky bucket with packets

Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

### 4.9.2 Token bucket Algorithm

**Need** of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

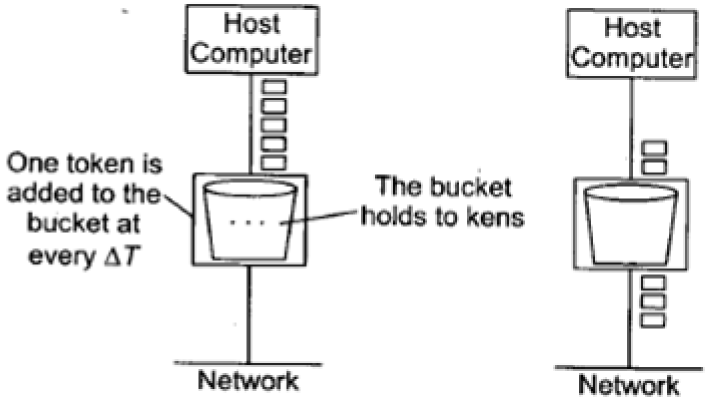
**Steps** of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket. ƒ
2. The bucket has a maximum capacity. ƒ
3. If there is a ready packet, a token is removed from the bucket, and the packet is send.
4. If there is no token in the bucket, the packet cannot be send.

Let’s understand with an example,

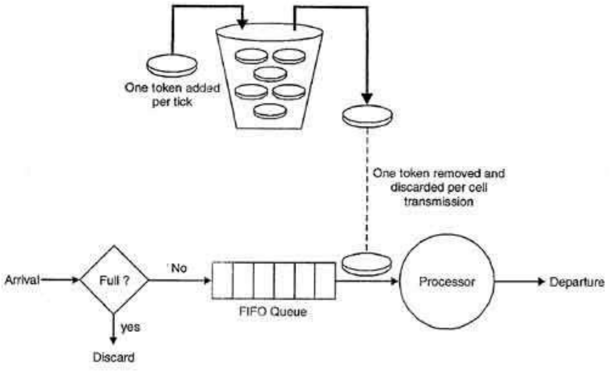
In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted.For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

Let’s understand with an example,



(a) Before

(b) After



Token bucket algorithm

### 4.9.3 Congestion control in virtual Circuit

Different approaches are used to control the congestion in virtual-circuit network. Some of them are as follows:

Admission control: In this approach, once the congestion is signaled, no• new connections are set up until the problem is solved. This type of approach is often used in normal telephone networks. When the exchange is overloaded, then no new calls are established.

Allow new virtual connections other than the congested area.

- Negotiate an agreement between the host and the network when the• connection is setup. This agreement specifies the volume and shape of traffic, quality of service, maximum delay and other parameters. The network will reserve resources (Buffer space, Bandwidth and CPU cycle) along the path when the connection is set up. Now congestion is unlikely to occur on the new connections because all the necessary resources are guaranteed to be available. The disadvantage of this approach is that it may leads to wasted bandwidth because of the some idle connection.

### 4.9.4 Congestion control in Datagram Subnets

Congestion control in Datagram Subnets is achieved by sending warning to sender in advance. Each router can easily monitor the utilization of its output lines. If utilization is greater than threshold value then output line may be congested in future so mark it as warning state. Each newly arriving packet is checked to see if its output line is in warning state. If it is, some action is taken.

The actions are:

1. The warning bit
2. Choke packets
3. Hop-by-hop choke packet

**The warning bit**

When a new packet is to be transmitted on the output line marked as warning state, a special bit is added in header to signal this state. At the destination, this information is sent back with ACK to the sender so that it could cut the traffic. When warning bit is absent, sender increases its transmitting rate.

Note: It uses a whole trip (source to destination to source) to tell the source to slow down

**Choke Packet Technique**

In this approach, the router sends a choke packet back to the source host. The original packet is marked so that it would not generate any more choke packets further along the path and is then forwarded in the usual way. When the source gets the choke packet, it is required to reduce the traffic by X packets.

Choke Packet Technique

In this approach, the router sends a choke packet back to the source host. The original packet is marked so that it would not generate any more choke packets further along the path and is then forwarded in the usual way. When the source gets the choke packet, it is required to reduce the traffic by X packets.

Hop-by Hop Choke Packets In this approach, unlike choke packet, reduction of flow starts from intermediate node rather than source node. To understand this, let us refer the figure 2. When the choke packet reaches the nearest router (say R) from router Q, it reduces the flow. However, router R now requires devoting more buffers to the flow since the source is still sending at full blast but it gives router Q immediate relief. In the next step, the choke packet reaches P and flow genuinely slow down. The net effect of hop-by-hop scheme is to provide quick relief at the point of congestion at the price of using up more buffers upstream.

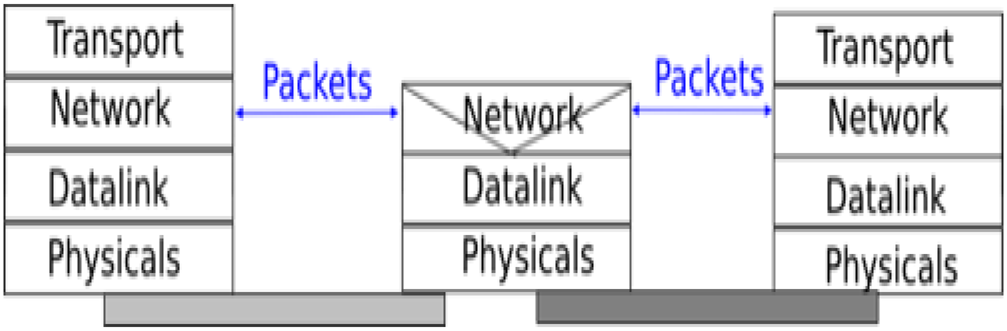
## 4.10 The network layer in the internet

### The network layer

The transport layer enables the applications to efficiently and reliably exchange data. Transport layer entities expect to be able to send segment to any destination without having to understand anything about the underlying subnetwork technologies. Many subnetwork technologies exist. Most of them differ in subtle details (frame size, addressing, ...). The network layer is the glue between these subnetworks and the transport layer. It hides to the transport layer all the complexity of the underlying subnetworks and ensures that information can be exchanged between hosts connected to different types of subnetworks.

### Principles

The main objective of the network layer is to allow endsystems, connected to different networks, to exchange information through intermediate systems called **router**. The unit of information in the network layer is called a **packet**.



An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.[1] An IP address serves two principal functions: host or network interface identification and location addressing.

**Mobile IP** (or **MIP**) is an Internet Engineering Task Force (IETF) standard communications **protocol** that is designed to allow **mobile** device users to move from one network to another while maintaining a permanent **IP address**. **Mobile IP**for **IPv4** is described in IETF RFC 5944, and extensions are defined in IETF RFC 4721.

**In IPv6**, the address size was increased from 32 bits in IPv4 to 128 bits or 16 octets, thus providing up to $2^{128}$ (approximately $3.403\times10^{38}$) addresses. This is deemed sufficient for the foreseeable future.

**Internet Protocol version 6** (**IPv6**) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.

Internet Protocol Version 6 (IPv6) is an Internet Protocol (IP) used for carrying data in packets from a source to a destination over various networks. IPv6 is the enhanced version of IPv4 and can support very large numbers of nodes as compared to IPv4. It allows for 2128 possible node, or address, combinations.

IPv6 is also known as Internet Protocol Next Generation (IPng).

# UNIT V

## Transport Layer

The Transport layer (also known as the Host-to-Host Transport layer) provides the Application layer with session and datagram communication services. The Transport layer encompasses the responsibilities of the OSI Transport layer. The core protocols of the Transport layer are TCP and UDP.

TCP provides a one-to-one, connection-oriented, reliable communications service. TCP establishes connections, sequences and acknowledges packets sent, and recovers packets lost during transmission.

In contrast to TCP, UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when an application developer does not want the overhead associated with TCP connections, or when the applications or upper-layer protocols provide reliable delivery.

TCP and UDP operate over both IPv4 and IPv6 Internet layers.

**Note** The Internet Protocol (TCP/IP) component of Windows contains separate versions of the TCP and UDP protocols than the Microsoft TCP/IP Version 6 component does. The versions in the Microsoft TCP/IP Version 6 component are functionally equivalent to those provided with the Microsoft Windows NT® 4.0 operating systems and contain all the most recent security updates. The existence of separate protocol components with their own versions of TCP and UDP is known as a dual stack architecture. The ideal architecture is known as a dual IP layer, in which the same versions of TCP and UDP operate over both IPv4 and IPv6 (as Figure 2-1 shows). Windows Vista has a dual IP layer architecture for the TCP/IP protocol components.

## Application Layer

The Application layer allows applications to access the services of the other layers, and it defines the protocols that applications use to exchange data. The Application layer contains many protocols, and more are always being developed.

The most widely known Application layer protocols help users exchange information:

- The Hypertext Transfer Protocol (HTTP) transfers files that make up pages on the World Wide Web.
- The File Transfer Protocol (FTP) transfers individual files, typically for an interactive user session.

□ The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments. Additionally, the following Application layer protocols help you use and manage TCP/IP networks:

□ The Domain Name System (DNS) protocol resolves a host name, such as www.microsoft.com, to an IP address and copies name information between DNS servers.

□ The Routing Information Protocol (RIP) is a protocol that routers use to exchange routing information on an IP network.

□ The Simple Network Management Protocol (SNMP) collects and exchanges network management information between a network management console and network devices
such as routers, bridges, and servers.

Windows Sockets and NetBIOS are examples of Application layer interfaces for TCP/IP applications.

## IP Protocol

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

## IP addressing

The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.

Host-to-host communications – IP determines the path a packet must take, based on the□

receiving system's IP address.

## ARP Protocol

The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers.□

□ ARP assists IP in directing datagram's to the appropriate receiving system by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

ICMP

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

Dropped packets – Packets that arrive too fast to be processed-Connectivity failure – A destination system cannot be reached

**Transport Layer**

The TCP/IP transport layer ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets.

This type of communication is known as end-to-end. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service.

UDP provides unreliable datagram service.

**TCP Protocol**

TCP enables applications to communicate with each other as though they were connected by a physical circuit.

TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets. This transmission consists of the following:

**SCTP Protocol**

It is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP. Moreover, SCTP can support connections between systems that have more than one address, or multihued.

The SCTP connection between sending and receiving system is called an association.

## Application Layer

The application layer defines standard Internet services and network applications that anyone can use.

These services work with the transport layer to send and receive data. Many application layer protocols exist.

The following list shows examples of application layer protocols:

1.Standard TCP/IP services such as the ftp, tftp, and telnet commands

- **Node-to-node delivery**: At the data-link level, delivery of frames take place between two nodes connected by a point-to-point link or a LAN, by using the data-link layers address, say MAC address.
- **Host-to-host delivery**: At the network level, delivery of datagrams can take place between two hosts by using IP address.

From user's point of view, the TCP/IP-based internet can be considered as a set of application programs that use the internet to carry out useful communication tasks. Most popular internet applications include Electronic mail, File transfer, and Remote login. IP allows transfer of IP datagrams among a number of stations or hosts, where the datagram is routed through the internet based on the IP address of the destination. But, in this case, several application programs (processes) simultaneously running on a source host has to communicate with the corresponding processes running on a remote destination host through the internet. This requires an additional mechanism called *process-to-process delivery,* which is implemented with the help of a transport -level protocol. The transport level protocol will require an additional address, known as *port number*, to select a particular process among multiple processes running on the destination host. So, there is a requirement of the following third type of delivery system.

- **Process-to-process delivery**: At the transport level, communication can take place between processes or application programs by using port addresses

Basic communication mechanism is shown in Fig. 6.3.1. The additional mechanism needed to facilitate multiple application programs in different stations to communicate with each other simultaneously can be provided by a transport level protocol such as UDP or TCP, which are discussed in this lesson.

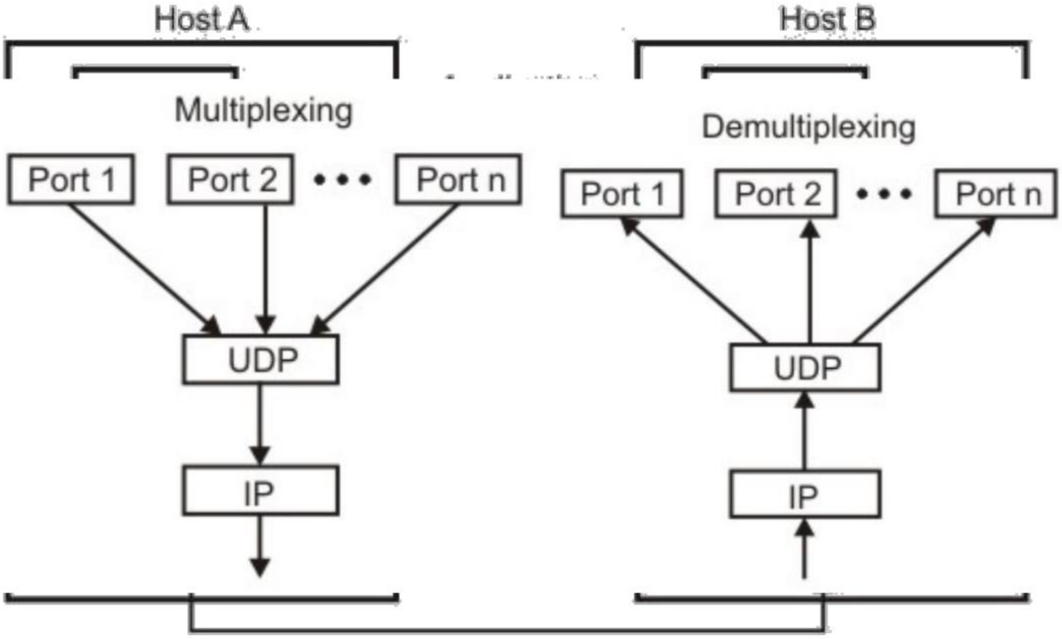


Figure .Communication mechanism through the internet

**User Datagram protocol (UDP)**

UDP is responsible for differentiating among multiple source and destination processes within one host. Multiplexing and demultiplexing operations are performed using the port mechanism as depicted in Fig

## UDP Datagram

A brief description of different fields of the datagram are given below:

- Source port (16 bits): It defines the port number of the application program in the host of the sender
- Destination port (16 bits): It defines the port number of the application program in the host of the receiver
- Length: It provides a count of octets in the UDP datagram, minimum length = 8
- Checksum: It is optional, 0 in case it is not in use

## Characteristics of the UDP

Key characteristics of UDP are given below:

- UDP provides an unreliable connectionless delivery service using IP to transport messages between two processes
- UDP messages can be lost, duplicated, delayed and can be delivered out of order
- UDP is a thin protocol, which does not add significantly to the functionality of IP
- It cannot provide reliable stream transport service

The above limitations can be overcome by using connection-oriented transport layer protocol known as *Transmission Control Protocol* (TCP), which is presented in the following section.

## Transmission Control Protocol (TCP)

TCP provides a connection-oriented, full -duplex, reliable, streamed delivery service using IP to transport messages between two processes.

Reliability is ensured by:

- Connection-oriented service
- Flow control using sliding window protocol
- Error detection using checksum
- Error control using go-back-N ARQ technique
- Congestion avoidance algorithms; multiplicative decrease and slow-start

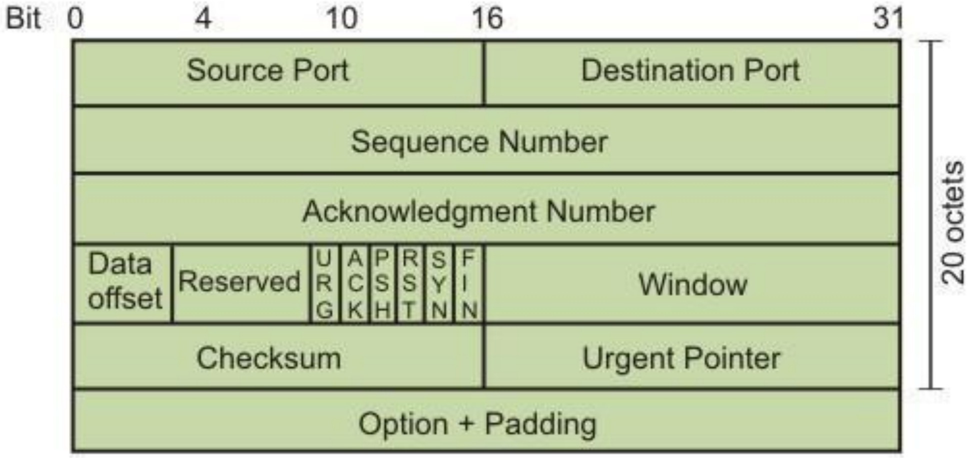
TCP Datagram

The TCP datagram format is shown in Figure. A brief explanation of the functions of different fields are given below:

- Source port (16 bits): It defines the port number of the application program in the host of the sender
- Destination port (16 bits): It defines the port number of the application program in the host of the receiver
- Sequence number (32 bits): It conveys the receiving host which octet in this sequence comprises the first byte in the segment
- Acknowledgement number (32 bits): This specifies the sequence number of the next octet that receiver expects to receive
- HLEN (4 bits): This field specifies the number of 32-bit words present in the TCP header
- Control flag bits (6 bits): URG: Urgent pointer
- ACK: Indicates whether acknowledge field is valid
- PSH: Push the data without buffering
- RST: Resent the connection
- SYN: Synchronize sequence numbers during connection establishment
- FIN: Terminate the connection
- Window (16 bits): Specifies the size of window
- Checksum (16 bits): Checksum used for error detection.

- User pointer (16 bits): Used only when URG flag is valid
- Options: Optional 40 bytes of information

The well-known ports used by TCP are given in Table 6.3.2 and the three types of addresses used in TCP/IP are shown in Fig. 6.3.5. TCP establishes a virtual path between the source and destination processes before any data communication by using two procedures, *connection establishment* to start reliably and *connection termination* to terminate gracefully, as discussed in the following subsection.



The TCP datagram format

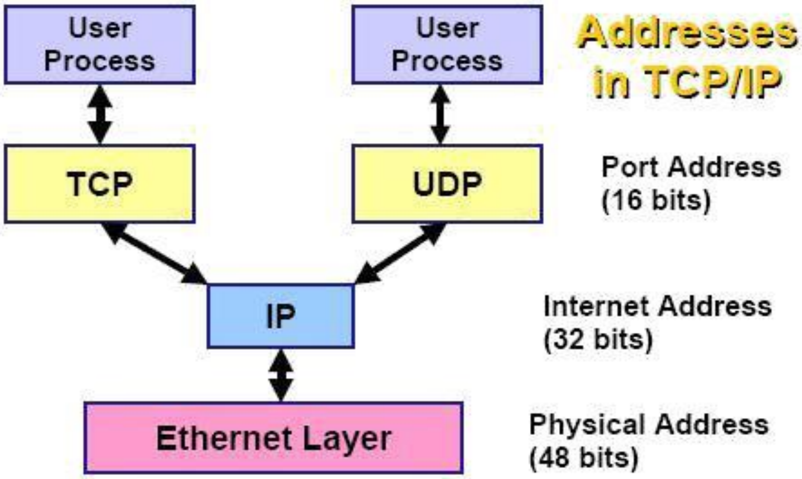
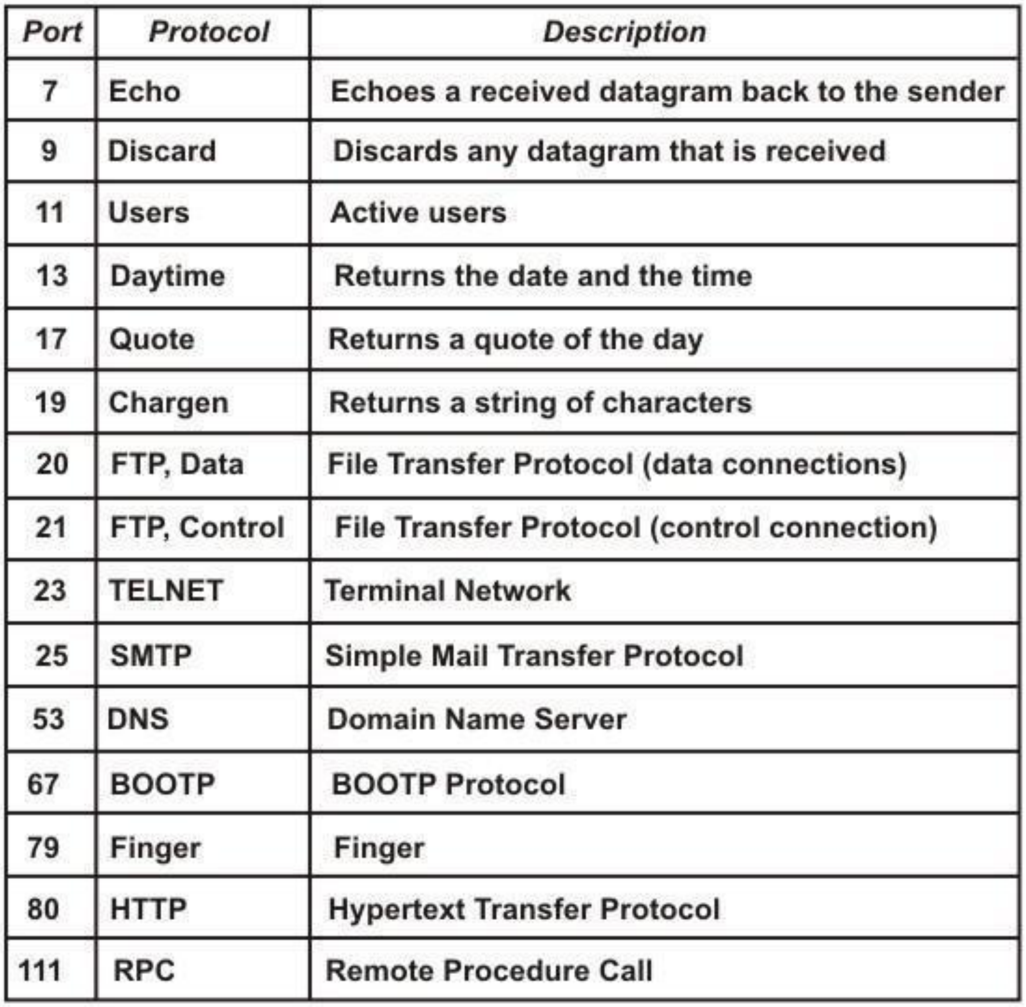


Figure  Three types of addresses used in TCP/IP

Table 6.3.2 Well-known ports used by TCP



| Port | Protocol | Description |
|---|---|---|
| 7 | Echo | Echoes a received datagram back to the sender |
| 9 | Discard | Discards any datagram that is received |
| 11 | Users | Active users |
| 13 | Daytime | Returns the date and the time |
| 17 | Quote | Returns a quote of the day |
| 19 | Chargen | Returns a string of characters |
| 20 | FTP, Data | File Transfer Protocol (data connections) |
| 21 | FTP, Control | File Transfer Protocol (control connection) |
| 23 | TELNET | Terminal Network |
| 25 | SMTP | Simple Mail Transfer Protocol |
| 53 | DNS | Domain Name Server |
| 67 | BOOTP | BOOTP Protocol |
| 79 | Finger | Finger |
| 80 | HTTP | Hypertext Transfer Protocol |
| 111 | RPC | Remote Procedure Call |

## Electronic Mail

**Simple Mail Transfer Protocol** (**SMTP**) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

SMTP is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel, typically a Transmission Control Protocol (TCP) connection. An SMTP session consists of commands originated by an SMTP client (the initiating agent, sender, or transmitter) and corresponding responses from the SMTP server (the listening agent, or receiver) so that the session is opened, and session parameters are exchanged. A session may include zero or more SMTP transactions. An SMTP transaction consists of three command/reply sequences (see example below.) They are:

1. MAIL command, to establish the return address, a.k.a. Return-Path, 5321.From, mfrom, or

envelope sender. This is the address for bounce messages.

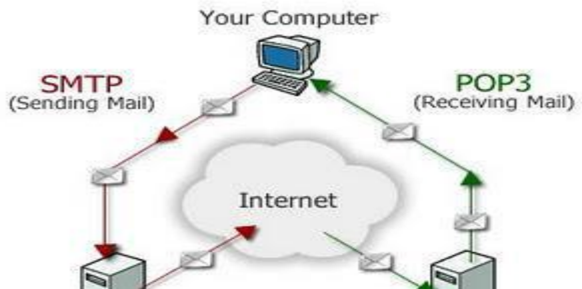
2. RCPT command, to establish a recipient of this message. This command can be issued multiple

times, one for each recipient. These addresses are also part of the envelope.

3. DATA to send the message text. This is the content of the message, as opposed to its envelope.

It consists of a message header and a message body separated by an empty line. DATA is

actually a group of commands, and the server replies twice: once to the DATA command proper, to acknowledge that it is ready to receive the text, and the second time after the end-of-data sequence, to either accept or reject the entire message.



Electronic mail is among the most widely available application services. Each user, who intends to participate in email communication, is assigned a mailbox, where out-going and incoming messages are buffered, allowing the transfer to take place in thebackground. The message contains a header that specifies the sender, recipients, and subject, followed by a body that contains message. The TCP/IP protocol that supports electronic mail on the internet is called *Simple Mail Transfer Protocol* (SMTP), which supports the following:

- Sending a message to one or more recipients
- Sending messages that include text, voice, video, or graphics

A software package, known as *User Agent*, is used to compose, read, reply or forward emails and handle mailboxes. The email address consists of two parts divided by a @ character. The first part is the local name that identifies mailbox and the second part is a domain name.

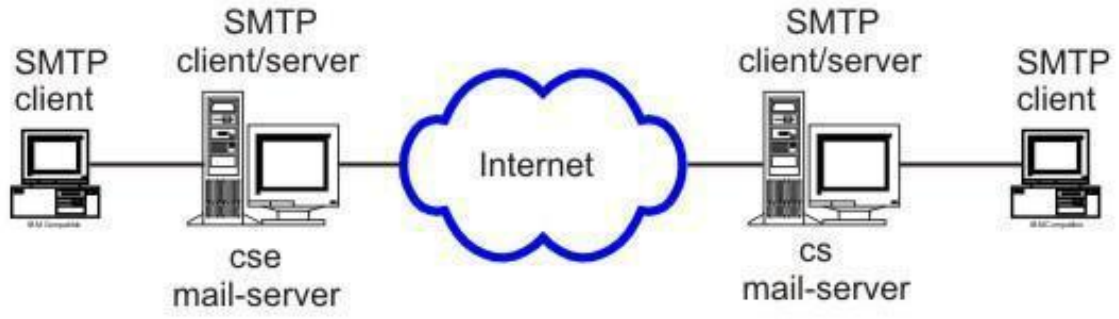


Figure  Simple Mail Transfer Protocol (SMTP)

Telnet

Telnet is a simple remote terminal protocol that provides a remote log-on capability, which enables a user to log on to a remote computer and behaves as if it is directly connected to it. The following three basic services are offered by TELNET:

- It defines a network virtual terminal that provides a standard interface to remote systems

- It includes a mechanism that allows the client and server to negotiate options from a standard set
- It treats both ends symmetrically

## File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a TCP/IP client -server application for transfer files between two remote machines through internet. A TCP connection is set up before file transfer and it persists throughout the session. It is possible to send more than one file before disconnecting the link. A control connection is established first with a remote host before any file can be transferred. Two connections required are shown in Fig. 6.3.15. Users view FTP as an interactive system

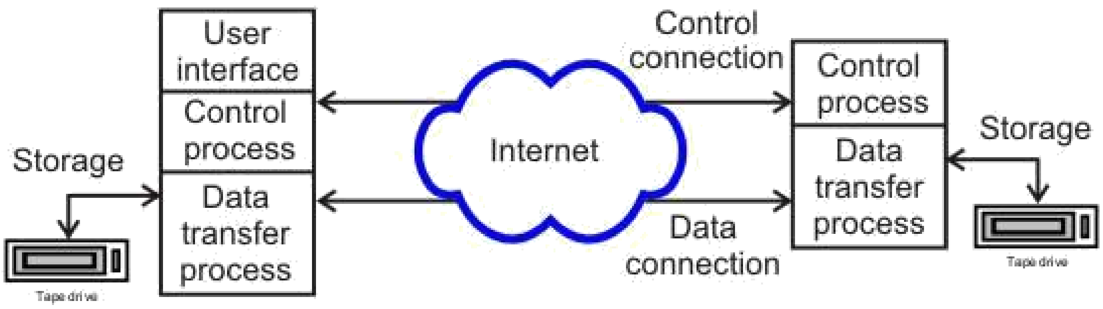


Figure File Transfer Protocol (FTP)

**Simple Network Management Protocol (SNMP)**

Network managers use network management software that help them to locate, diagnose and rectify problems. Simple Network Management Protocol (SMTP) provides a systematic way for managing network resources. It uses transport layer protocol for communication. It allows them to monitor switches, routers and hosts. There are four components of the protocol:

- Management of systems
- Management of nodes; hosts, routers, switches
- Management of Information Base; specifies data items a host or a router must keep and the operations allowed on each (eight categories)
- Management of Protocol; specifies communication between network management client program a manager invokes and a network management server running on a host or router

**HTTP (HyperText Transfer Protocol)**
**The WEB**

Internet (or The Web) is a massive distributed client/server information system as depicted in the following diagram.

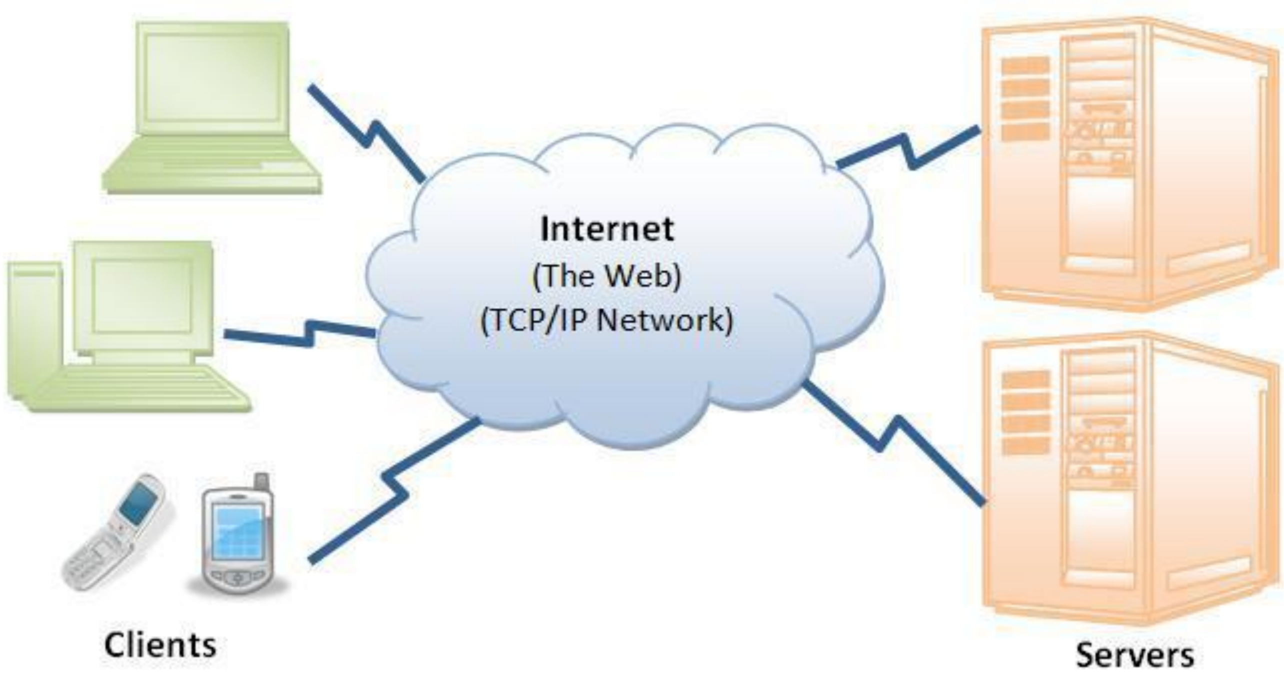
Many applications are running concurrently over the Web, such as web browsing/surfing, e-mail, file transfer, audio & video streaming, and so on. In order for proper communication to take place between the client and the server, these applications must agree on a specific application-level protocol such as HTTP, FTP, SMTP, POP, and etc.

## HyperText Transfer Protocol (HTTP)

HTTP (Hypertext Transfer Protocol) is perhaps the most popular application protocol used in the Internet (or The WEB).

## The WEB

Internet (or The Web) is a massive distributed client/server information system as depicted in the following diagram.



Many applications are running concurrently over the Web, such as web browsing/surfing, e-mail, file transfer, audio & video streaming, and so on. In order for proper communication to take place between the client and the server, these applications must agree on a specific application-level protocol such as HTTP, FTP, SMTP, POP, and etc.

## Hyper Text Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) is communications protocol of the TCP/IP Suit. It is used for retrieving inter-linked text documents (hypertext). HTTP led to the establishment of the World Wide Web.

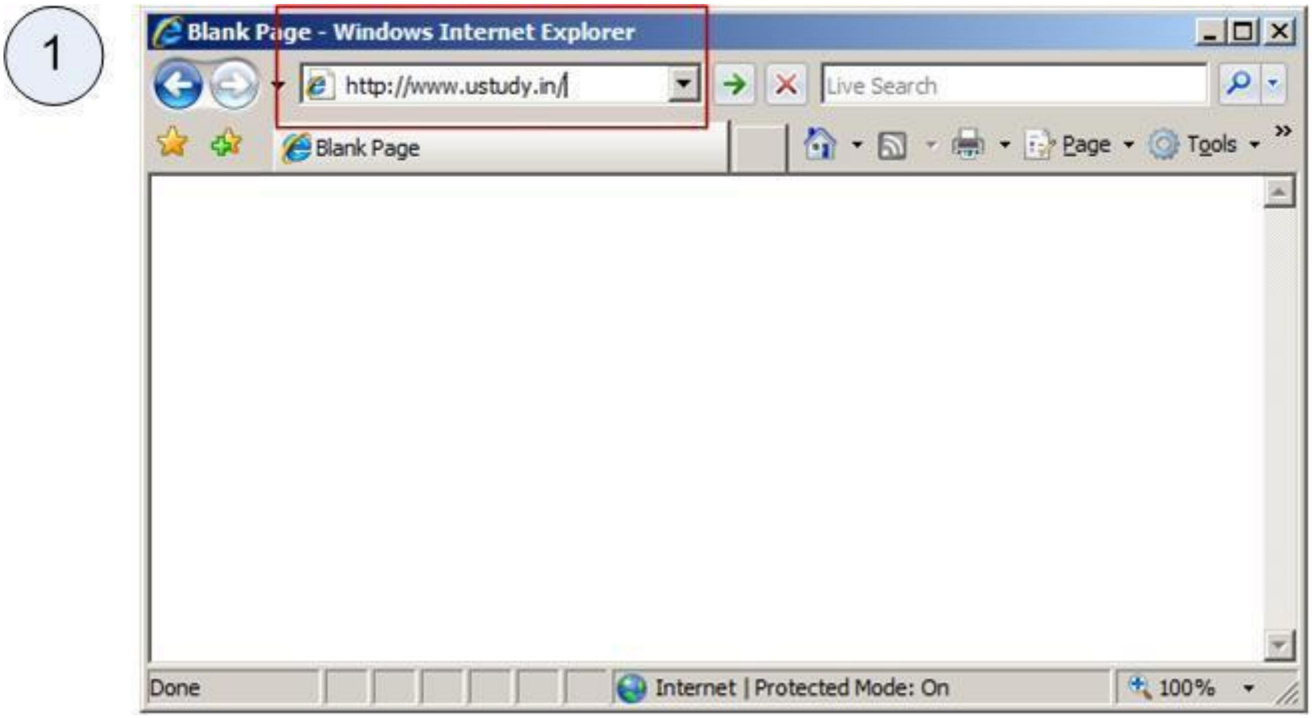
HTTP's development was coordinated by the World Wide Web Consortium and the Internet Engineering Task Force (IETF), resulting in the publication of a series of Request for Comments (RFCs), most notably RFC 2616 (June 1999), which defines HTTP/1.1, the version of HTTP in common use.

HTTP is a request/response standard between a client and a server. The end-user client making a HTTP request—using a web browser typically—is referred to as the **user agent**. The responding server—which serves resources such as HTML files and images—is called the **origin server**.

Typically, an HTTP client initiates a request. It establishes a Transmission Control Protocol (TCP) connection to a particular port on a host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message. Upon receiving the request, the server sends back the requested resource. Resources to be accessed by HTTP are identified using Uniform Resource Identifiers (URIs) (or, more specifically, Uniform Resource Locators (URLs)) using the http: or https: URI schemes.

**Here is how HTTP works:**

1. You type a website's URL, for example, www.ustudy.in in your favorite browser (IE, Firefox, Opera, Safari)



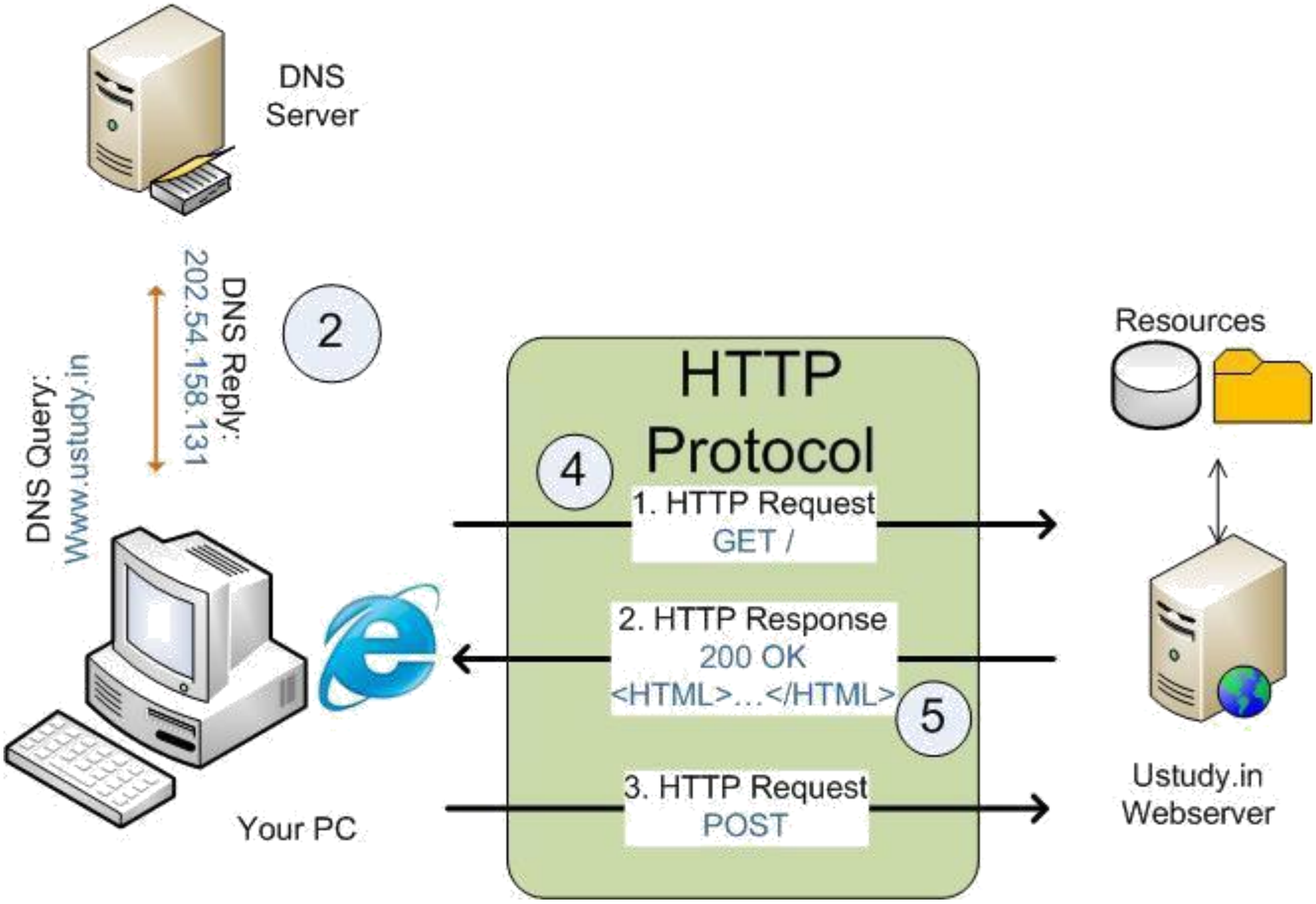
http://www.ustudy.in/

1
Blank Page - Windows Internet Explorer
Live Search
Blank Page
Page
Tools
Done
Internet | Protected Mode: On
100%

2. Your web browser looks up the IP address of www.ustudy.in using DNS services - it is resolved as 202.54.158.131.

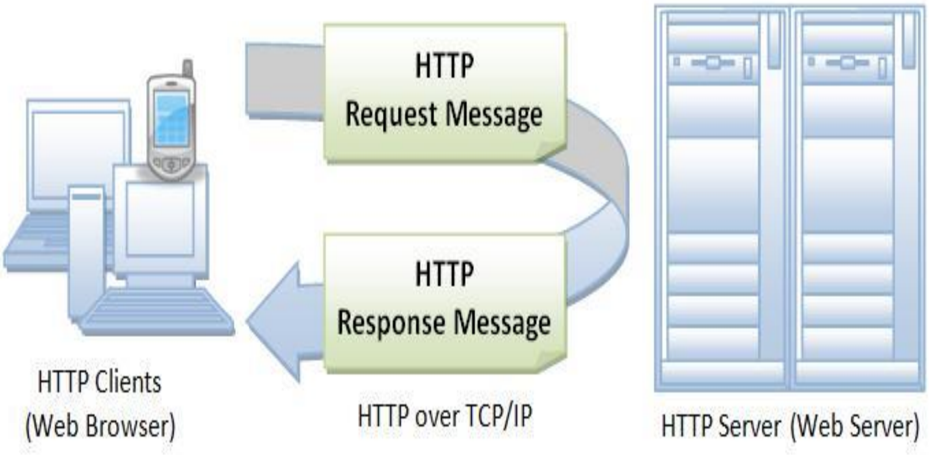
3. Your web browser then establishes a TCP connection to the IP address 202.54.158.131 on port

80. The web browser's packets are transported to the Ustudy.in server over the internet using IP. The server for UStudy.in successfully receives the packet and acknowledges a connection. On seeing it is for port 80, delivers it to the web server software (apache, IIS etc.).



HTTP (Hypertext Transfer Protocol) is perhaps the most popular application protocol used in the Internet (or The WEB).

HTTP is an *asymmetric request-response client-server* protocol as illustrated. An HTTP client sends a request message to an HTTP server. The server, in turn, returns a response message. In other words, HTTP is a*pull protocol*, the client *pulls* information from the server (instead of server *pushes* information down to the



client).

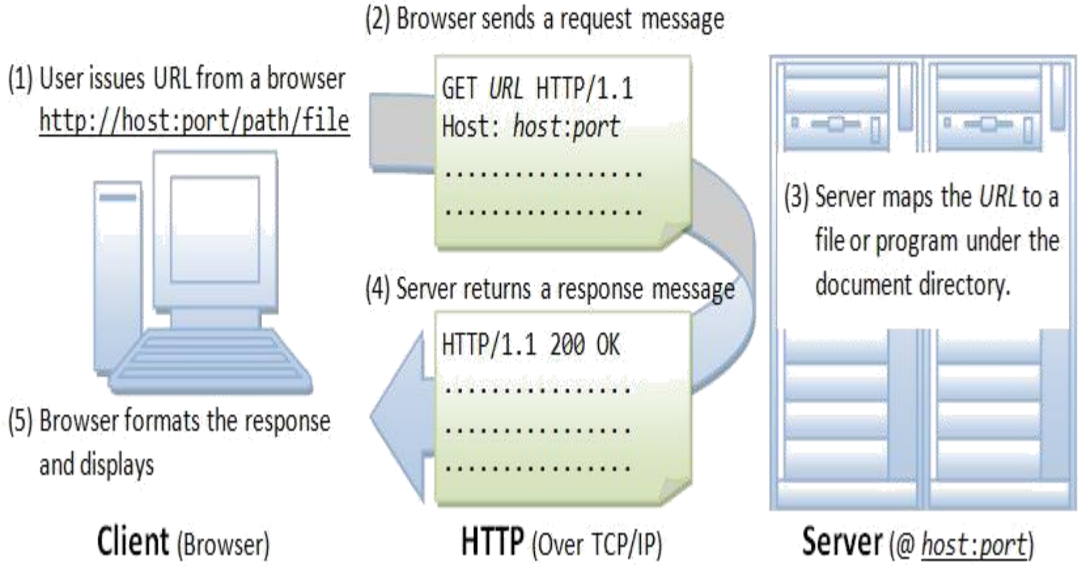
HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests.

HTTP permits negotiating of data type and representation, so as to allow systems to be built independently of the data being transferred.

Quoting from the RFC2616: "The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers."

### Browser

Whenever you issue a URL from your browser to get a web resource using HTTP, e.g. http://www.nowhere123.com/index.html, the browser turns the URL into a *request* *message* and sends it to the HTTP server. The HTTP server interprets the request message, and returns you an appropriate response message, which is either the resource you requested or an error message. This process is illustrated below:


(2) Browser sends a request message
(1) User issues URL from a browser
http://host:port/path/file
GET URL HTTP/1.1
Host: host:port
................
................
(3) Server maps the URL to a file or program under the document directory.
(4) Server returns a response message
HTTP/1.1 200 OK
...............
...............
...............
(5) Browser formats the response and displays
Client (Browser)
HTTP (Over TCP/IP)
Server (@ host:port)

## Uniform Resource Locator (URL)

A URL (Uniform Resource Locator) is used to uniquely identify a resource over the web. URL has the following syntax:

*protocol*://*hostname*:*port*/*path-and-file-name*

There are 4 parts in a URL:

1. *Protocol*: The application-level protocol used by the client and server, e.g., HTTP, FTP, and telnet.
2. *Hostname*: The DNS domain name (e.g., www.nowhere123.com) or IP address (e.g., 192.128.1.2) of the server.
3. *Port*: The TCP port number that the server is listening for incoming requests from the clients.
4. *Path-and-file-name*: The name and location of the requested resource, under the server document base directory.

- HTTP is an *asymmetric request-response client-server* protocol as illustrated. An HTTP client sends a request message to an HTTP server. The server, in turn, returns a response message. In other words, HTTP is a*pull protocol*, the client *pulls* information from the server (instead of

  server *pushes* information down to the client).
- HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests.
- HTTP permits negotiating of data type and representation, so as to allow systems to be built independently of the data being transferred.

- Quoting from the RFC2616: "The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers."

**World Wide Web** (WWW)

- The **World Wide Web** (WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.

- Each site holds one or more documents, referred to as *Web pages*. Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browsers.

**Client (Browser)**

A variety of vendors offer commercial browsers that interpret and display a Web document, and all use nearly the same architecture. Each browser usually consists of three parts: a controller, client protocol, and interpreters. The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols described previously such as FTP or HTTP (described later in the chapter). The interpreter can be HTML, Java, or JavaScript, depending on the type of document.

**Server**

The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk. A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time.