MODULE-1 COMPUTER NETWORKS

Network: A network is the interconnection of a set of devices capable of communication. In this definition, a device can be a host such as a large computer, desktop, laptop, workstation, cellular phone, or security system.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance

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

Reliability

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

Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery .

Physical Structures

Before discussing networks, we need to define some network attributes.

Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another.

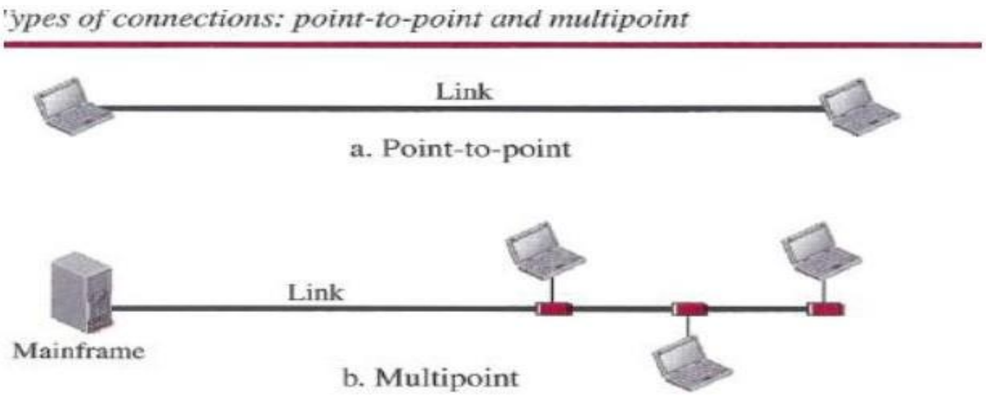
There are two possible types of connections: point-to-point and multipoint.

Point-to-Point

A point-to-point connection provides a dedicated link between two devices.

Multipoint

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.



In a multipoint environment, the capacity of the channel is shared.

Networks Types:

Local Area Networks:

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometres in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size,
(2) Their transmission technology, and
(3) Their topology.

LANs may use a transmission technology consisting of a cable to which all the machines are attached, Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay , and make very few errors.. Figure1 shows two of them. In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending.

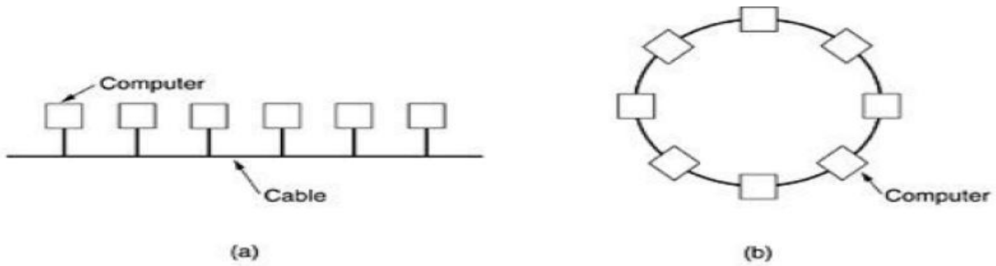
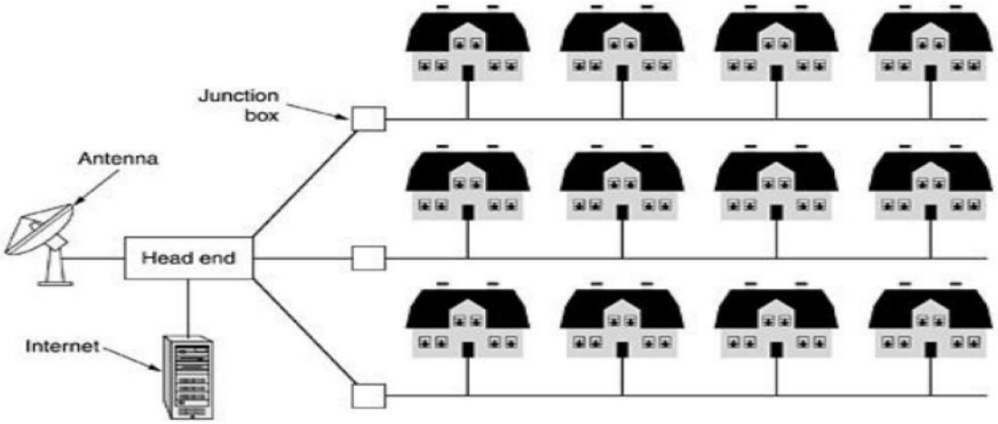


Fig.1: Two broadcast networks . (a) Bus. (b) Ring.

A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs.

Metropolitan Area Network (MAN).

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities.

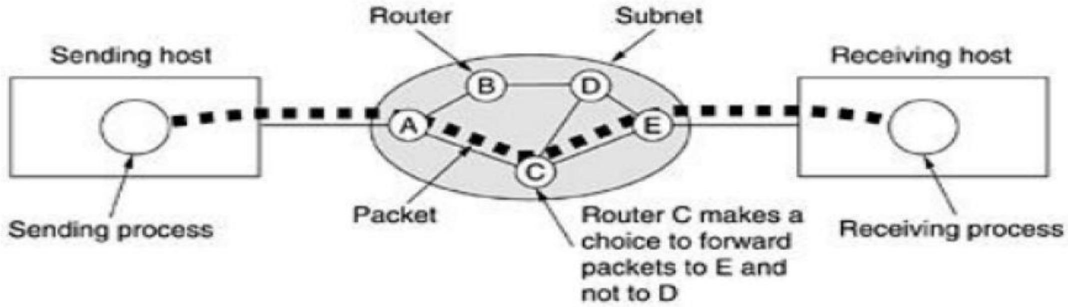


A MAN is implemented by a standard called DQDB (Distributed Queue Dual Bus) or IEEE

802.16. DQDB has two unidirectional buses (or cables) to which all the computers are attached.

Wide Area Network (WAN).

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user programs.

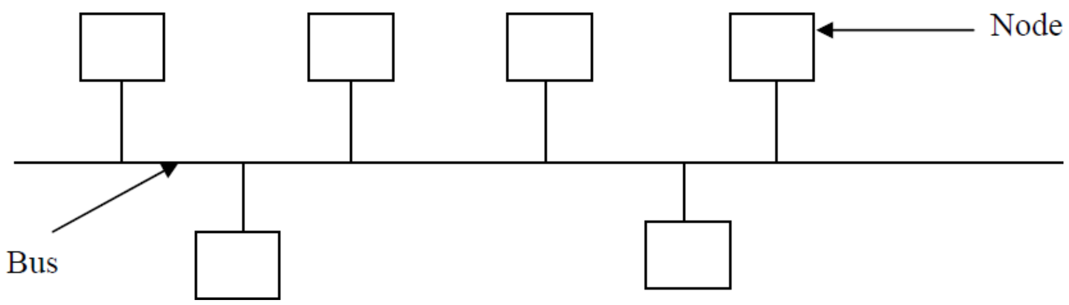


Network topologies:

Network topology defined as the logical connection of various computers in the network.
The six basic network topologies are: bus, ring, star, tree, mesh and hybrid.

1. Bus Topology:

In bus topology all the computers are connected to a long cable called a bus. A node that wants to send data puts the data on the bus which carries it to the destination node. In this topology any computer can data over the bus at any time. Since, the bus is shared among all the computers. When two or more computers to send data at the same time, an arbitration mechanism is needed to prevent simultaneous access to the bus.

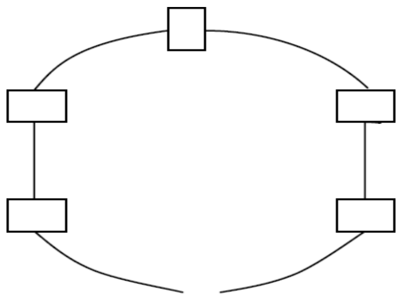


Bus Topology

A bus topology is easy to install but is not flexible i.e., it is difficult to add a new node to bus. In addition to this the bus stops functioning even if a portion of the bus breaks down. It is also very difficult to isolate fault.

2. Ring Topology:

In ring topology, the computers are connected in the form of a ring. Each node has exactly two adjacent neighbors. To send data to a distant node on a ring it passes through many intermediate nodes to reach to its ultimate destination.

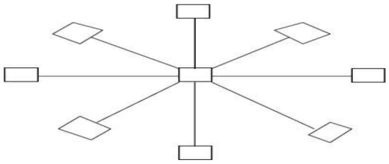


R**ing Topology**

A ring topology is as to install and reconfigure. In this topology, fault isolation is easy because a signal that circulates all the time in a ring helps in identifying a faulty node.
The data transmission takes place in only one direction. When a node fails in ring, it breaks down the whole ring. To overcome this drawback some ring topologies use dual rings.
The topology is not useful to connect large number of computers.

3. Star Topology:

In star topology all the nodes are connected to a central node called a hub. A node that wants to send some six data to some other node on the network, send data to a hub which in turn sends it the destination node. A hub plays a major role in such networks.

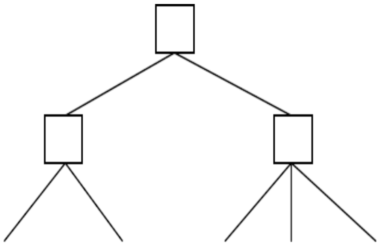


Star topology

Star topology is easy to install and reconfigure. If a link fails then it separates the node connected to link from the network and the network continues to function. However, if the hub goes down, the entire network collapses.

4. Tree Topology:

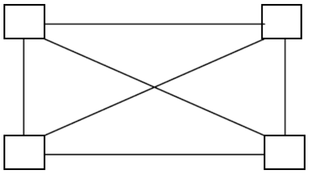
Tree topology is a hierarchy of various hubs. The entire nodes are connected to one hub or the other. There is a central hub to which only a few nodes are connected directly.



The central hub, also called active hub, looks at the incoming bits and regenerates them so that they can traverse over longer distances. The secondary hubs in tree topology may be active hubs or passive hubs. The failure of a transmission line separates a node from the network.

5. Mesh Topology:

A mesh topology is also called complete topology. In this topology, each node is connected directly to every oilier node in the network. That is if there are n nodes then there would be n(n — 1)/2 physical links in the network.

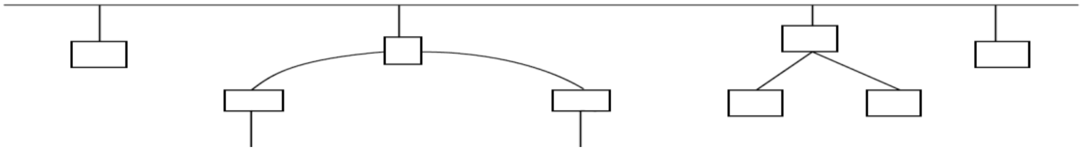


Mesh Topology

As there are dedicated links, the topology does not have congestion problems.

6. Hybrid Topology:

Hybrid topology is formed by connecting two or more topologies together. For example, hybrid topology can be created by using the bus, star and ring topologies,



PROTOCOL LAYERING

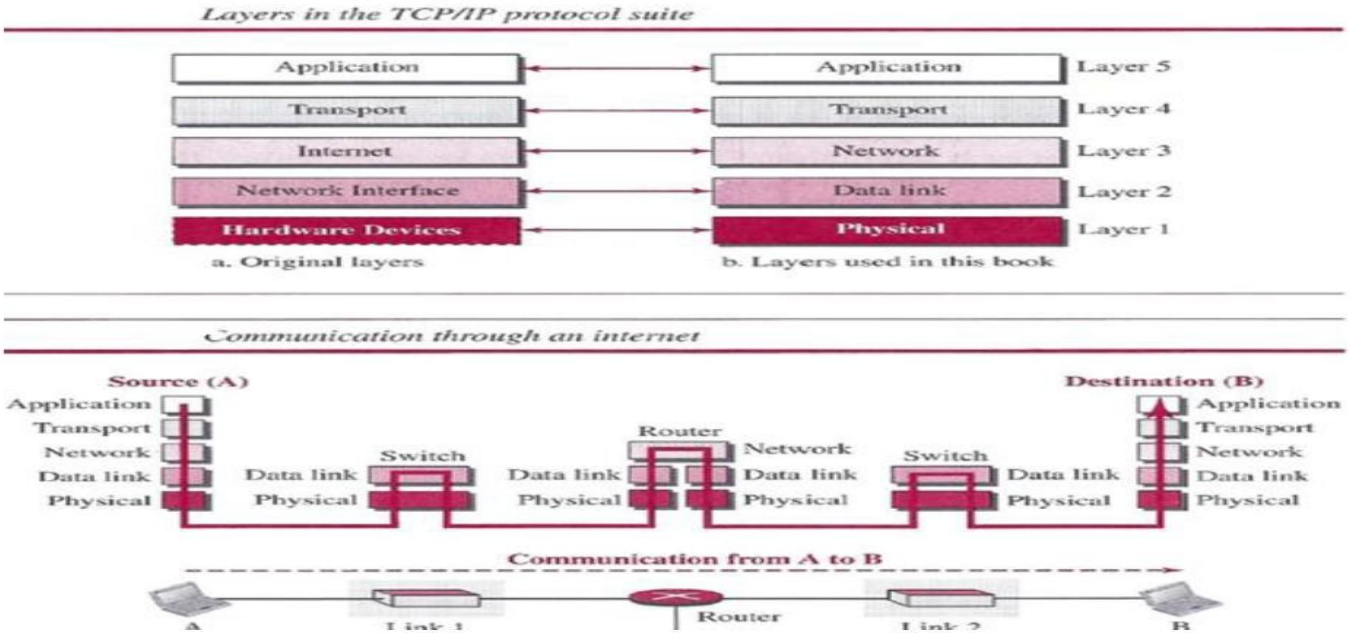
In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or protocol layering.

TCP/IP PROTOCOL SUITE

TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term *hierarchical* means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original *TCP/IP* protocol suite was defined as four software layers built upon the hardware. Today, however, *TCP/IP* is thought of as a five-layer model. Following figure shows both configurations.

Layered Architecture

To show how the layers in the *TCP/IP* protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch. We also assume that the links are connected by one router, as shown in below Figure.

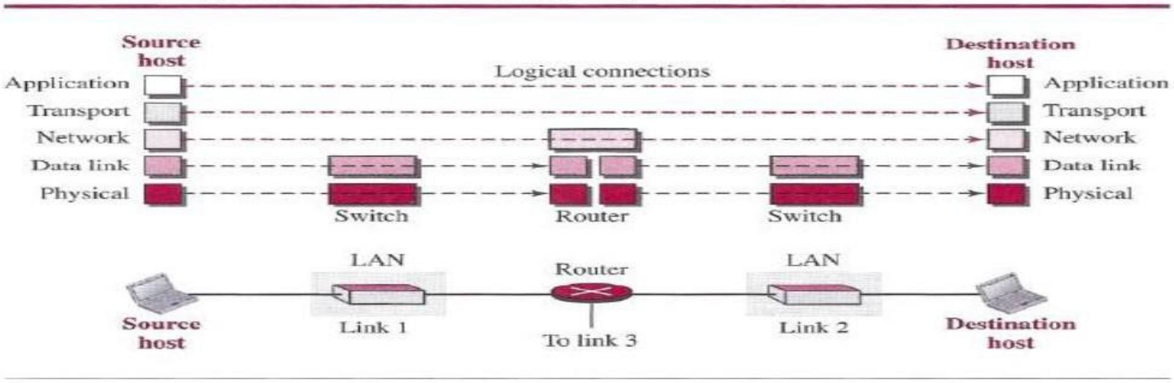


.

Layers in the TCP/IP Protocol Suite

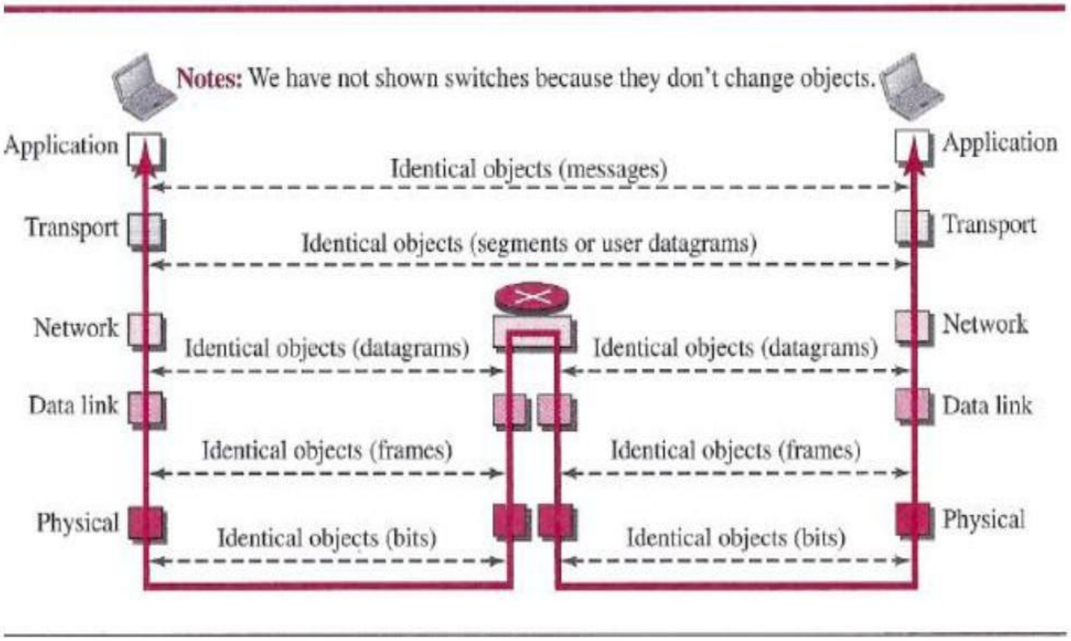
. To better understand the duties of each layer, need to think about the logical connections between layers. Below figure shows logical connections in our simple internet.
Using logical connections makes it easier for us to think about the duty of each layer. As the figure shows, the duty of the application, transport, and network layers is end-to-end.
However,the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router.

Logical connections between layers of the TCP/IP protocol suite



In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link. Another way of thinking of the logical connections is to think about the data unit created from each layer.

Identical objects in the TCP/IP protocol suite


Notes: We have not shown switches because they don't change objects.
Application
Application
Identical objects (messages)
Transport
Transport
Identical objects (segments or user datagrams)
Network
Network
Identical objects (datagrams)
Identical objects (datagrams)
Data link
Data link
Identical objects (frames)
Identical objects (frames)
Physical
Physical
Identical objects (bits)
Identical objects (bits)

.

.

Description of Each Layer

Physical Layer

The physical layer is responsible for carrying individual bits in a frame across the link. Although the physical layer is the lowest level in the TCPIIP protocol suite, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer. Two devices are connected by a transmission medium (cable or air). The bits received in a frame from the data-link layer are transformed and sent through the transmission media, but the logical unit between two physical layers in two devices is a *bit.* There are several protocols that transform a bit to a signal.

Data-link Layer

Internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the destination. The routers are responsible for choosing the *best* links. However, when the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link. In each case, the data-link layer is responsible for moving the packet through the link. *TCP/IP* does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols. Any protocol that can take the datagram and carry it through the link suffices for the network layer. The data-link layer takes a datagram and encapsulates it in a packet called *«frame.* Each link-layer protocol may provide a different service. Some link-layer protocols provide complete error detection and correction, some provide only error correction.

Network Layer

The network layer is responsible for creating a connection between the source computer and the destination computer. The communication at the network layer is host-to-host. However, since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet. The network layer is responsible for host-to-host communication and routing the packet through possible routes.

Transport Layer

The logical connection at the transport layer is also end-to-end. The transport layer at the source host gets the message from the application layer, encapsulates it in a transport layer packet (called a *segment* or a *user datagram* in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host. In other words, the transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host.

Application Layer

The logical connection between the two application layers is end to-end. The two application layers exchange *messages* between each other as though there were a bridge between the two layers. However, the communication is done through all the layers. Communication at the application layer is between two *processes* (two programs running at this layer). To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer.

ETHERNET

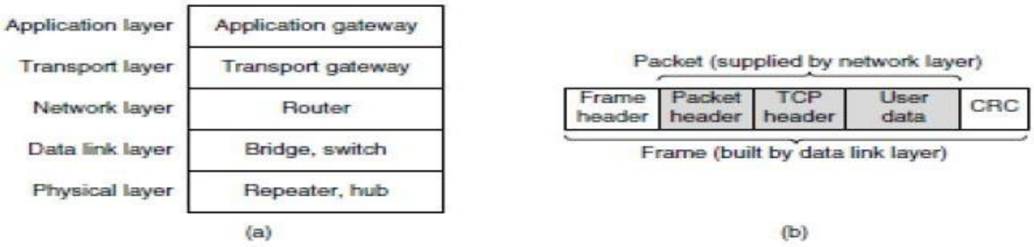
IEEE Project 802

In 1985, the Computer Society of the IEEE started a project, called *Project 802,* to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI model or TCPIIP protocol suite. Instead, it is a way of specifying functions of the physical layer and the data-link layer of major LAN protocols.

Connecting Devices

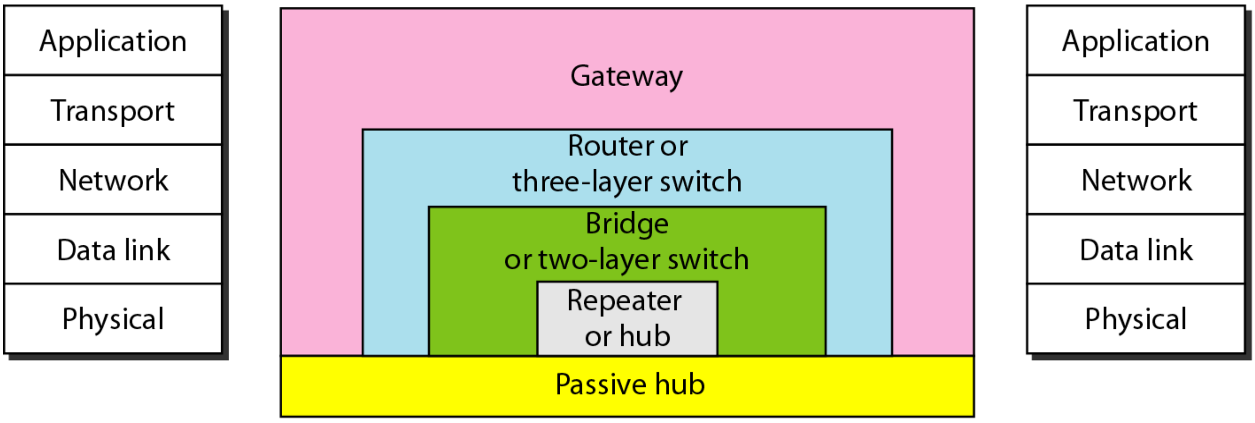
Repeaters, Hubs, Bridges, Switches, Routers, and Gateways

The user generates some data to be sent to a remote machine. Those data are passed to the transport layer, which then adds a header and passes the resulting unit down to the network layer. The network layer adds its own header to form a network layer packet . In Fig. we see the IP packet shaded in gray. Then the packet goes to the data link layer, which adds its own header and checksum (CRC) and gives the resulting frame to the physical layer for transmission, for example, over a LAN.



(a) Which device is in which layer. (b) Frames, packets, and headers.

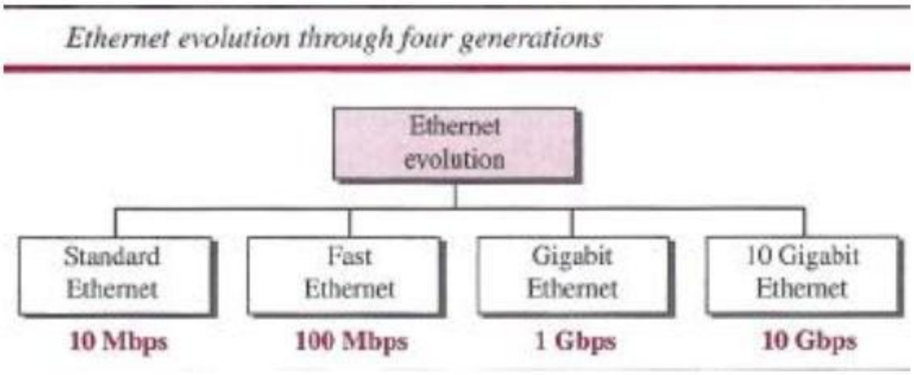
Five categories of Connecting devices



A repeater connects segments of a LAN.
A repeater forwards every frame; it has no filtering capability.
A bridge has a table used in filtering decisions.

Ethernet Evolution

The Ethernet LAN has gone through four generations: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and 10 Gigabit Ethernet.



Ethernet evolution through four generations

STANDARD ETHERNET

The original Ethernet technology with the data rate of 10 Mbps as the *Standard Ethernetis referred* . Although most implementations have moved to other technologies in the Ethernet evolution, there are some features of the Standard Ethernet that have not changed during the evolution.

Characteristics

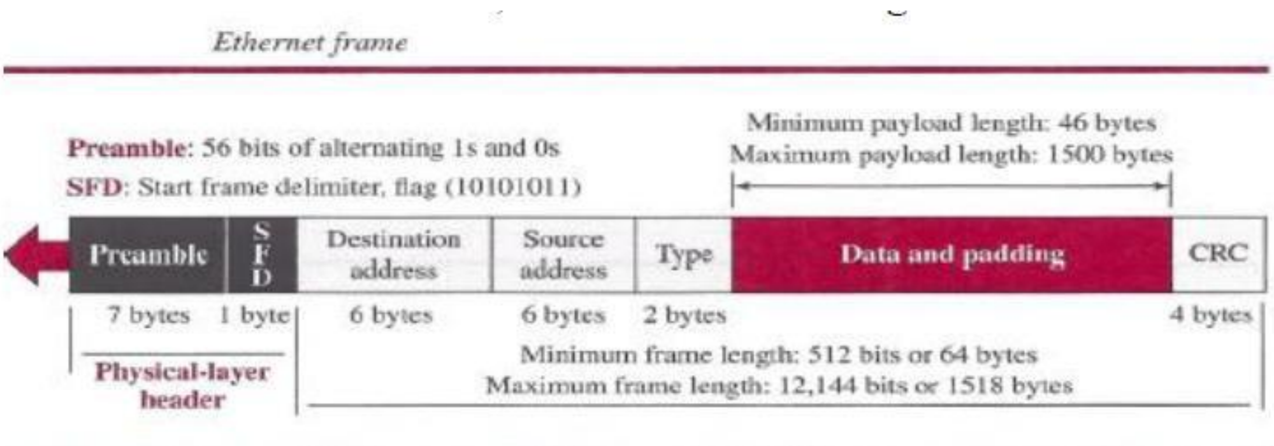
Let us first discuss some characteristics of the Standard Ethernet.

Connectionless and Unreliable Service

Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame. Ethernet has no connection establishment or connection termination phases. The sender sends a frame whenever it has it; the receiver mayor may not be ready for it. The sender may overwhelm the receiver with frames, which may result in dropping frames. If a frame drops, the sender will not know about it. Since IP, which is using the service of Ethernet, is also connectionless, it will not know about it either. If the transport layer is also a connectionless protocol, such as UDP, the frame is lost and salvation may only come from the application layer. However, if the transport layer is TCP, the sender TCP does not receive acknowledgment for its segment and sends it again. Ethernet is also unreliable like IP and UDP

Frame Format

The Ethernet frame contains seven fields, as shown in below figure.


Ethernet frame
Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
Type
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

Preamble This field contains 7 bytes (56 bits) of alternating Os and Is that alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization. The *preamble* is actually added at the physical layer and is not (formally) part of the frame.
Start frame delimiter (SFD) This 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. It needs a flag to define the beginning of the frame. The SFD field is also added at the physical layer.
Destination address (DA) This field is six bytes (48 bits) and contains the linklayer address of the destination station or stations to receive the packet.
Source address (SA) This field is also six bytes and contains the link-layer address of the sender of the packet.
Type This field defines the upper-layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF, and so on. It is used for multiplexing and demultiplexing.
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. The CRC is calculated over the addresses, types, and data field. If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame.

Frame Length

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame. The minimum length restriction is required for the correct operation of CSMAlCD. 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.
The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes.

Minimum frame length: 64 bytes Minimum data length: 46 bytes
Maximum frame length: 1518 bytes Maximum data length: 1500 bytes

Addressing

Each station on an Ethernet network has its own network interface card (NIC). The NIC fits inside the station and provides the station with a link-layer address. The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes. For example, the following shows an Ethernet MAC address: 4A:30:10:21:10:1A

Transmission of Address Bits

The way the addresses are sent out online is different from the way they are written in hexadecimal notation. The transmission is left to right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last.

Distinguish Between Unicast, Multicast, and Broadcast Transmission

Standard Ethernet uses a coaxial cable (bus topology) or a set of twisted-pair cables with a hub (star topology)

- ➢ In a unicast transmission, all stations will receive the frame, the intended recipient keeps and handles the frame; the rest discard it.
- ➢ In a multicast transmission, all stations will receive the frame, the stations that are members of the group keep and handle it; the rest discard it.

In a broadcast transmission, all stations (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

IEEE 802.11

Architecture

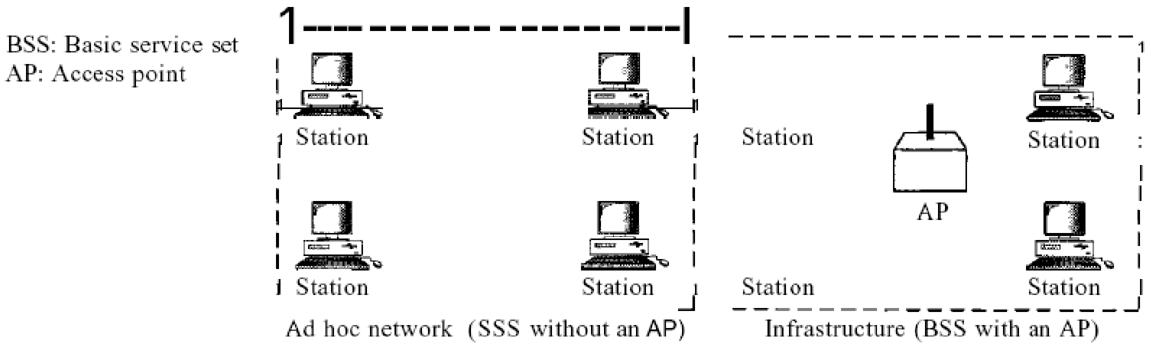
The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure 9 shows two sets in this standard.

The BSS without anAP is a stand-alone network and cannot send data to other BSSs. It is called an *ad hoc architecture.*

AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an *infrastructure* network.



Ad hoc network (SSS without an AP)

Infrastructure (BSS with an AP)

Figure. 9 *Basic service sets (BSSs)*

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a *distribution system,* which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure 10 shows an ESS.

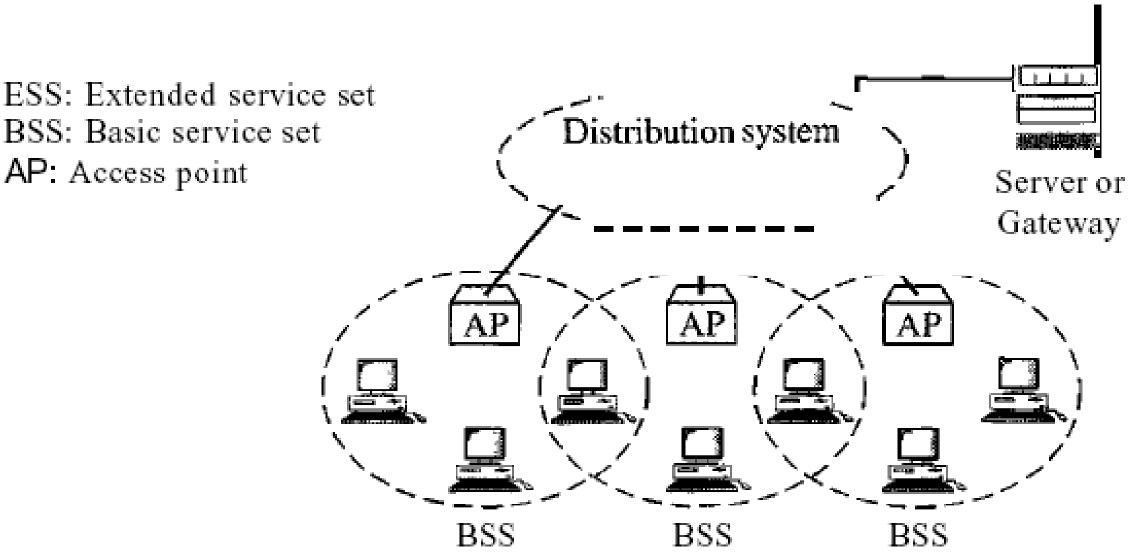


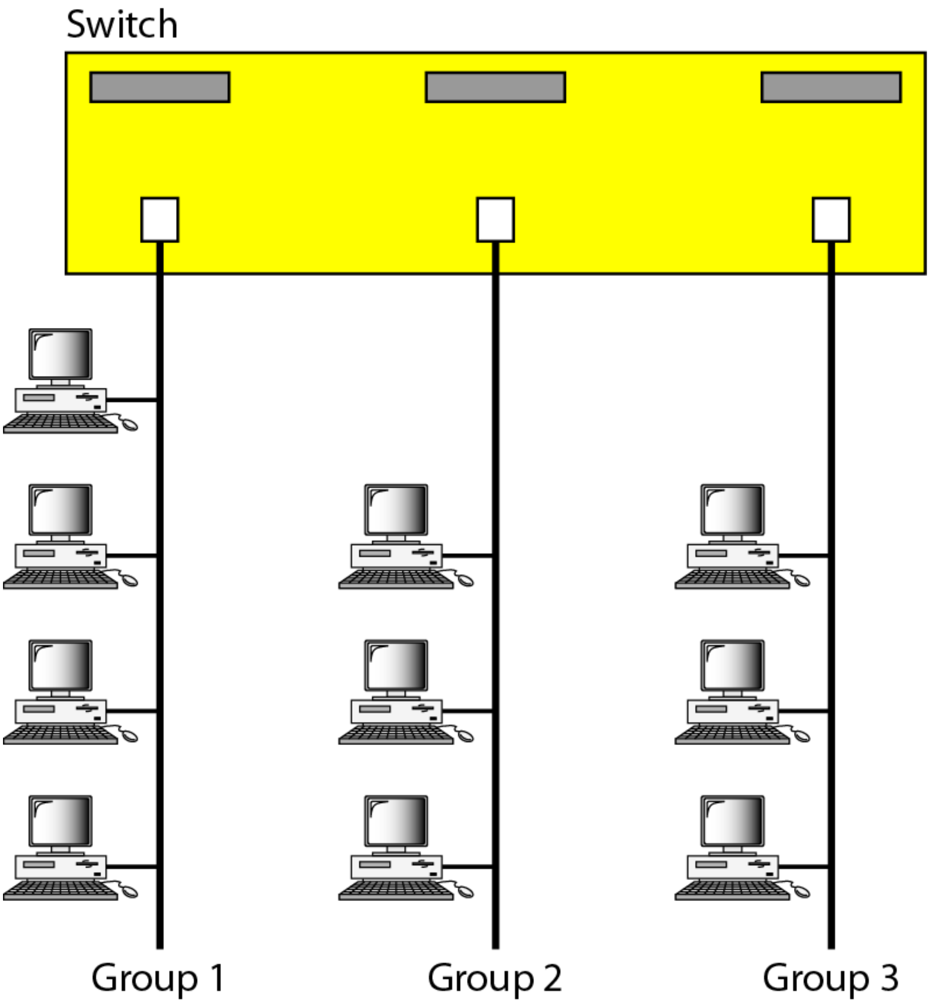
Figure 10 *Extended service sets (ESSs)*

<u>Virtual LANs</u>

A virtual local area network (VLAN) is a local area network configured by software, not by physical wiring**.**

A station is considered part of a LAN if it physically belongs to that LAN. The criterion of membership is geographic. What happens if we need a virtual connection between two stations belonging to two different physical LANs? a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

A Switch connecting 3 LANS

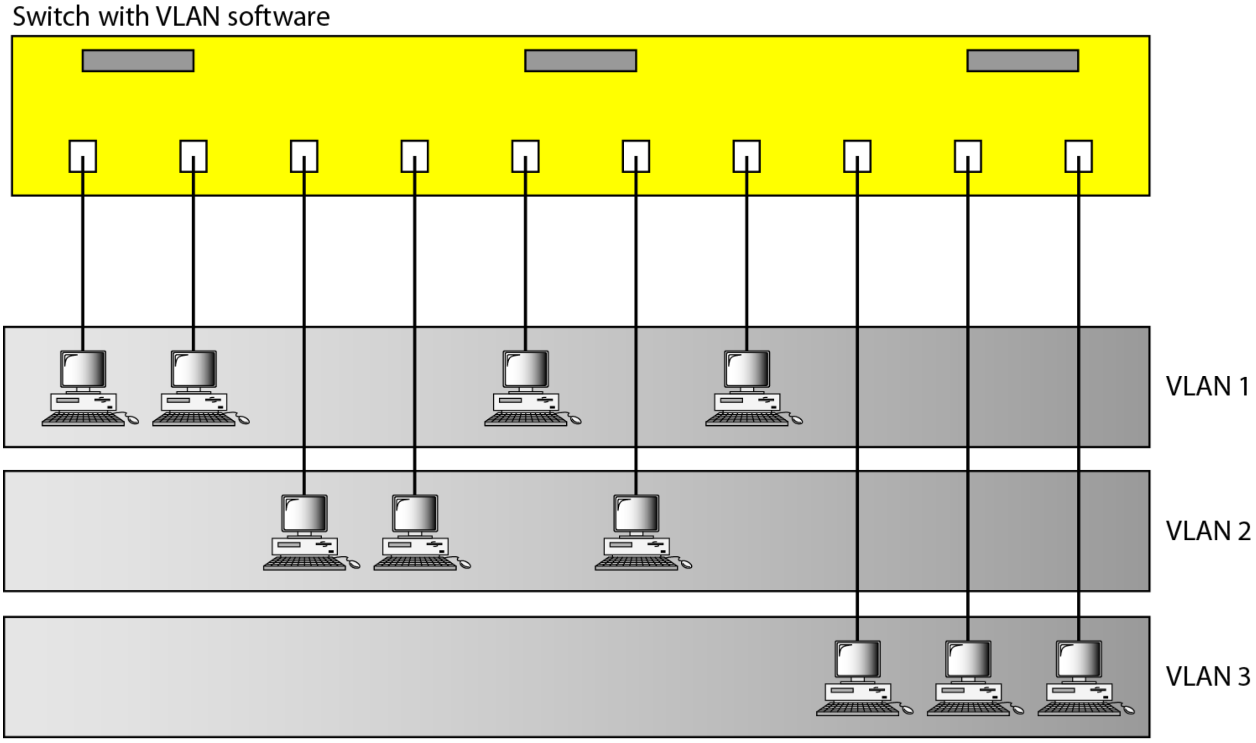


Let us use an example to elaborate on this definition. Figure shows a switched LAN in an engineering firm in which 10 stations are grouped into three LANs that are connected by a switch. The first four engineers work together as the first group, the next three engineers work together as the second group, and the last three engineers work together as the third group. The LAN is configured to allow this arrangement.

But what would happen if the administrators needed to move two engineers from the first group to the third group, to speed up the project being done by the third group?

The LAN configuration would need to be changed. The network technician must rewire. The problem is repeated if, in another week, the two engineers move back to their previous group. In a switched LAN, changes in the work group mean physical changes in the network configuration. These difficulties can be solved by using Virtual LAN as shown below.

A Switch using VLAN


Switch with VLAN software
VLAN 1
VLAN 2
VLAN 3