CAP275: Data Communiction and Networking
Unit-I: Networks

Dr. Manmohan Sharma

School of Computer Applications

Lovely Professional University

Distributed Processing

- Most networks use distributed processing, in which a task is divided among multiple computers.
- Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.
- Remote computers cooperate via a network to appear as a local machine, users are given the impression that they are interacting with just one machine.
- Spread computation and storage throughout a network of computers
- Applications are able to execute code on local machines and remote machines and to share data, files and other resources among these machines
- Attributes of distributed systems: Performance, Scalability, Connectivity, Security, Reliability, Fault tolerance.

Network Criteria

A network must meet following criteria:

- Performance
- Reliability
- Energy Efficiency
- Security
- Scalability
- Fairness
- Adaptability
- Channel Utilization
- Throughput

1. Performance

- Performance can be measured in following ways:
  - **Transit Time:** Time taken by the message to travel from one device to another device.
  - **Response Time:** It is the elapsed time between the enquiry and response.
- Performance is often evaluated by two networking metrics:
  - **Throughput:** It refers to how much data can be transferred from source to destination within a given timeframe. Throughput measures how many packets arrive at their destinations successfully and measured in bits per second, but it can also be measured in data per second.
  - **Delay:** It specifies the latency for a bit of data to travel across the network from one communication endpoint to another. It is typically measured in multiples or fractions of a second.

- Performance of a network depends upon:
  - Capability of Software
  - Efficiency of Hardware
  - Number of users
  - Type of transmission media used

2. Reliability

- It is the frequency of network failure. More is the failure less reliable is the network.
- It is the measure of time taken by the network to recover from the failure.
- It also defines the robustness in a catastrophe. (disaster or misfortune)

3. Energy Efficiency

- Energy Efficiency refers to the energy consumed per unit of successful communication.

4. Security

Network security issues include:

- Protecting data from unauthorized user or access.
- Protecting data from damage and implementing policies and procedures for recovery from and data losses.

5. Fairness

- Fairness refers to the ability of different systems to equally share a common transmission channel

6. Adaptability

- Adaptability refers to the ability to accommodate the changes network topology.

7. Channel Utilization

- Channel utilization refers to the bandwidth utilization for effective communication.

8. Throughput

- Throughput refers to the amount of data successfully transferred from a sender to a receiver in a given time.

9. Scalability

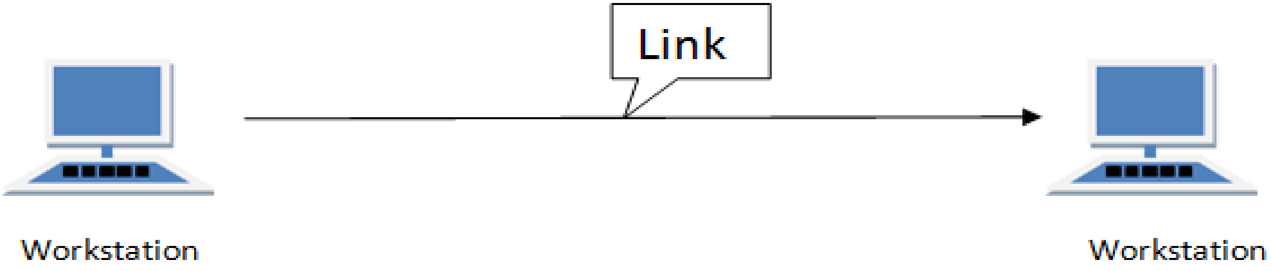
- Scalability refers to the ability to accommodate the change in network size.

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.
- For communication to occur, two devices must be connected in some way to the same link at the same time.
- There are two possible types of connections:
  - Point-to-Point connection
  - Multipoint connection

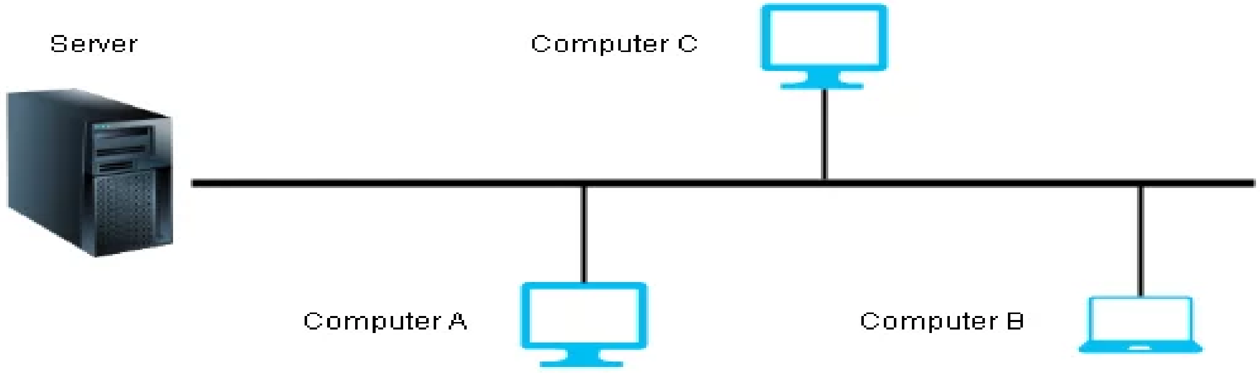
Point-to-Point Connection

- A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.
- Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.
  - When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.



A Multipoint Connection

- 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, either spatially or temporally.
  - **Spatial Sharing:** If several devices can share the link simultaneously, its called Spatially shared line configuration
  - **Temporal (Time) Sharing:** If users must take turns using the link, then its called Temporally shared or Time Shared Line Configuration



Topology

- The term “**Topology**” refers to the way in which the end points or stations/computer systems, attached to the networks, are interconnected.
- A topology is essentially a stable geometric arrangement of computers in a network. If you want to select a topology for doing networking. You have attention to the following points.
  - Application S/W and protocols
  - Types of data communicating devices
  - Geographic scope of the network
  - Cost
  - Reliability

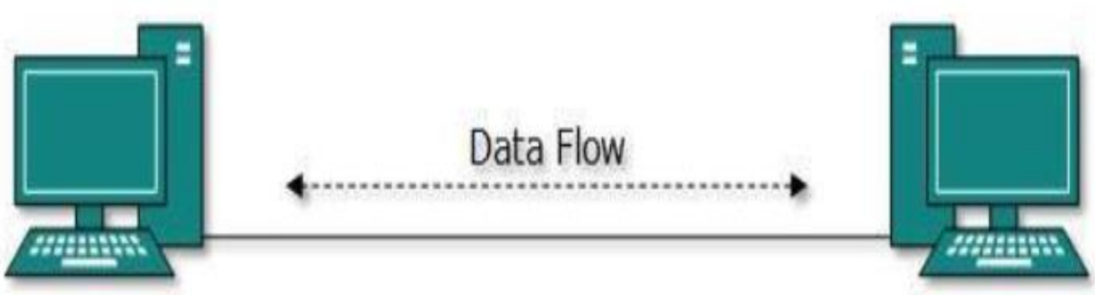
Types of Topologies

Depending on the requirement there are different Topologies to construct a network.

- Point-to-Point topology
- Bus topology
- Star topology
- Ring topology
- Mesh topology
- Tree (Hierarchical) topology
- Daisy Chain
- Cellular topology
- Hybrid Topology

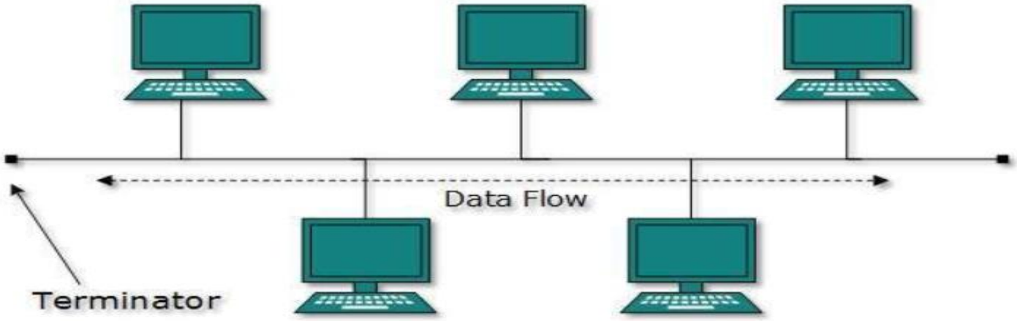
Point to Point Topology

- Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa.
- If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.



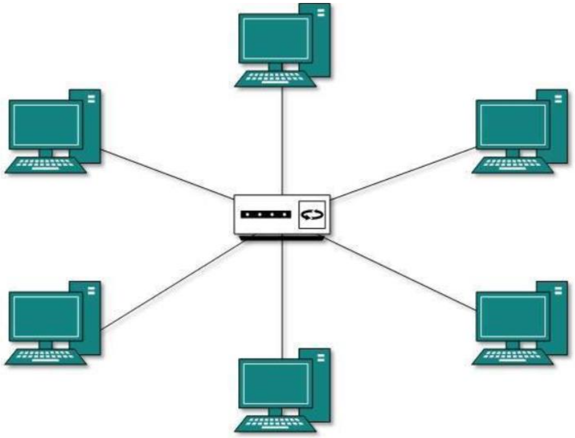
Bus topology

- In case of Bus topology, all devices share single communication line or cable.
- Bus topology may have problem while multiple hosts sending data at the same time.
  - Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue.
- It is one of the simple forms of networking where a failure of a device does not affect the other devices.
  - But failure of the shared communication line can make all other devices stop functioning.
- Both ends of the shared channel have line terminator.
  - The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.



Star topology

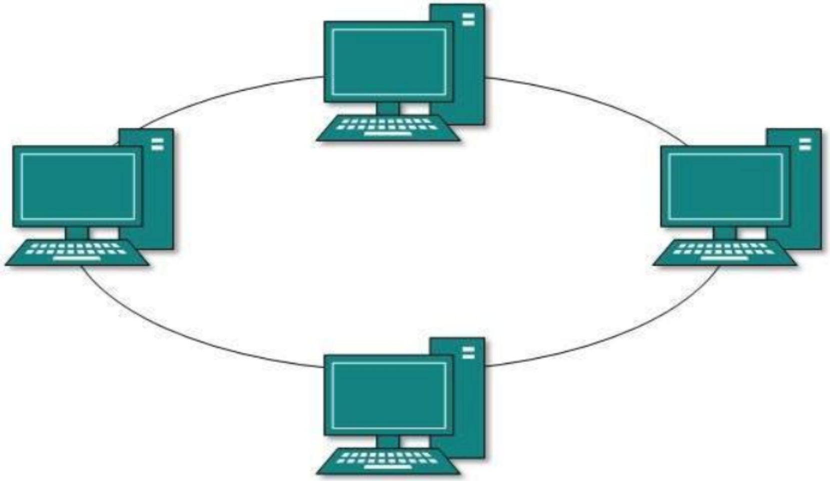
- All hosts in Star topology are connected to a central device using a point-to-point connection. That is, there exists a point to point connection between hosts and central device . The central device can be any of the following:
  - Layer-1 device such as hub or repeater
  - Layer-2 device such as 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.

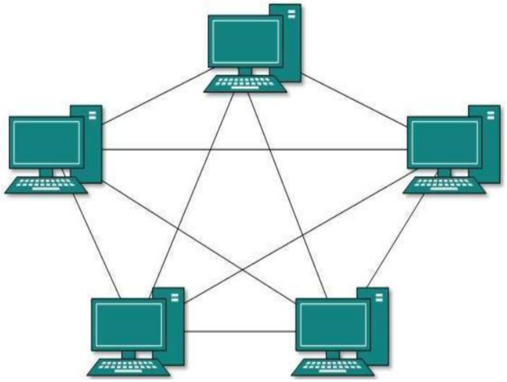
Ring topology

- In ring topology, each host machine connects to exactly two other machines, creating a circular network structure.
- When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.
- To connect one more host in the existing structure, the administrator may need only one more extra cable.
- Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure.



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.

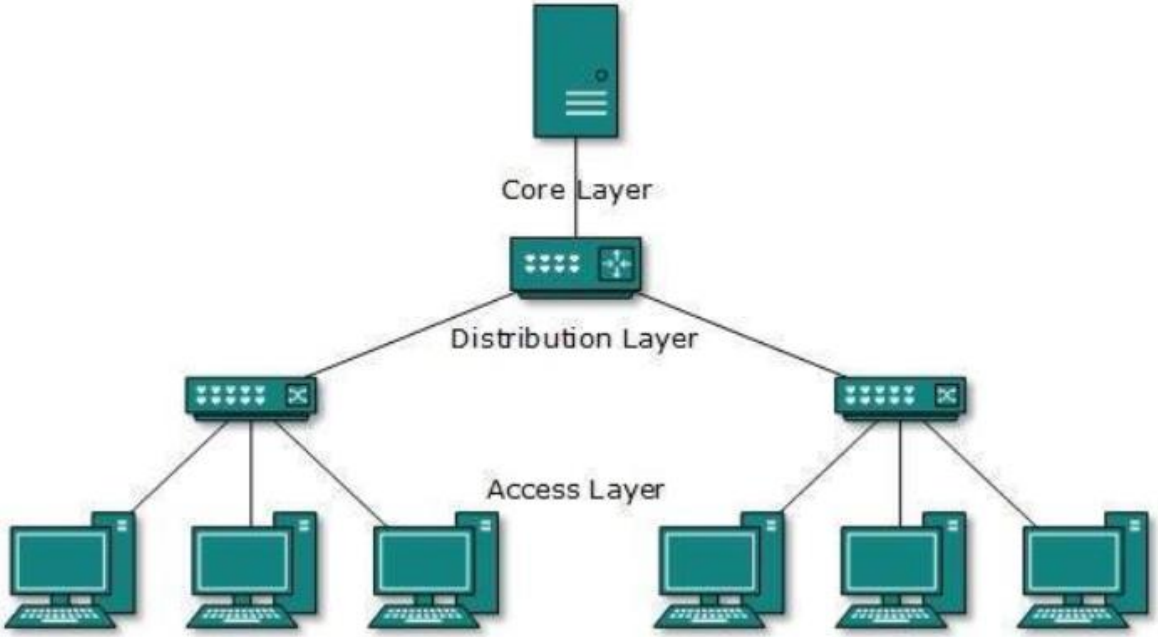


Tree (Hierarchical) topology

- Tree topology also known as Hierarchical Topology, this is the most common form of network topology in use presently.
- This topology imitates as extended Star topology and inherits properties of bus topology.
- This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices.
  - The lowermost is access-layer where computers are attached.
  - The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer.
  - The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.

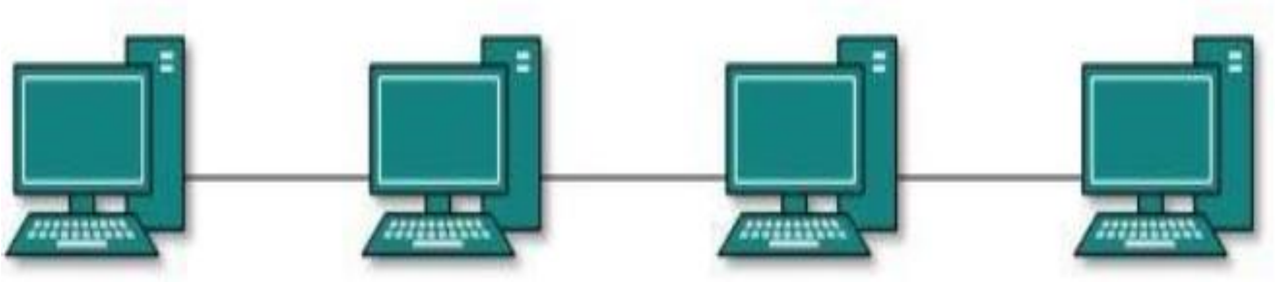
Tree (Hierarchical) topology contd…

- All neighbouring hosts have point-to-point connection between them.
- Similar to the Bus topology, if the root goes down, then the entire network suffers even though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.



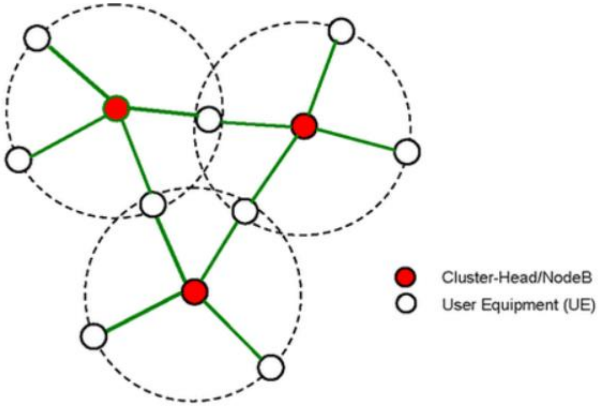
Daisy Chain

- This topology connects all the hosts in a linear fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts. Means, if the end hosts in daisy chain are connected then it represents Ring topology.
- Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments.
- Every intermediate host works as relay for its immediate hosts.



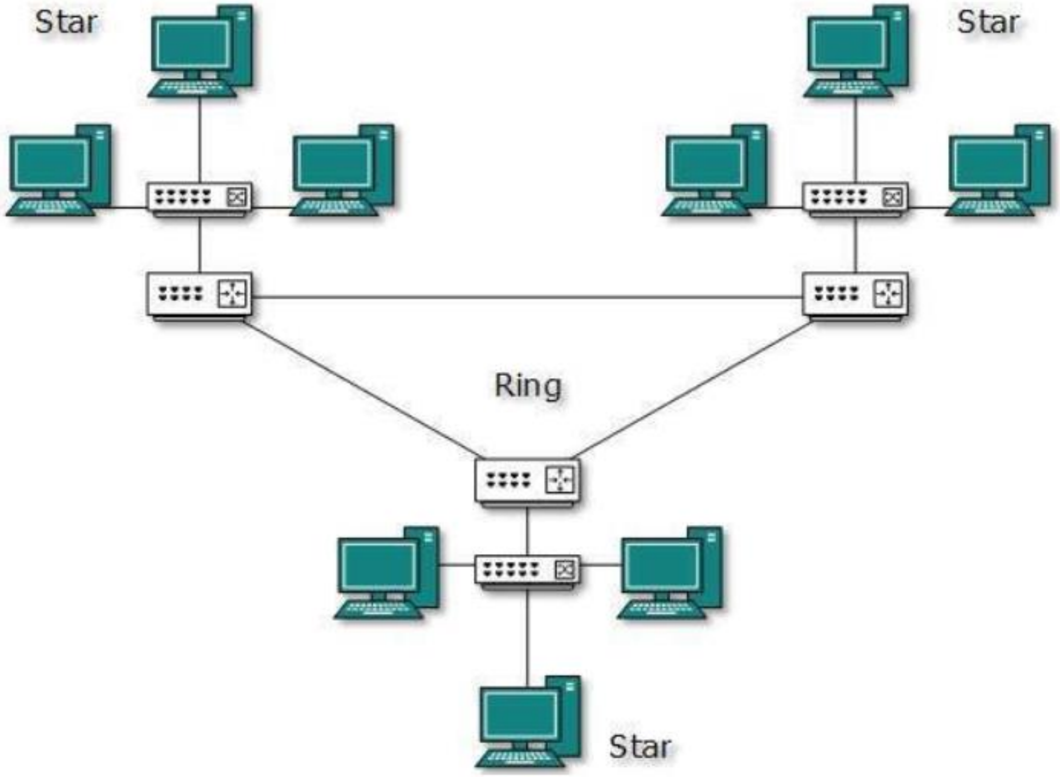
Cellular topology

- The cellular topology is applicable only in case of wireless media that does not require cable connection.
- In wireless media, each point transmits in a certain geographical area called a cell. Each cell represents a portion of the total network area.
- Devices that are in the cell communicate through a central hub. Hubs in different cells are interconnected. They route data across the network and provide a complete network infrastructure.
- The data is transmitted in the cellular digital packet data (CDPD) format.



Hybrid Topology

- A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



Categories of Networks

One way to categorize the different types of computer network designs is by their **geographical scope or scale**. For historical reasons, the networking industry refers to nearly every type of design as some kind of *area network*. Common examples of area network types are:

- PAN – Personal Area Network
- LAN - Local Area Network
- WLAN - Wireless Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network

Distance	Area covered
1 m	Working table
10 m	Room
100 m	Building
1 km	Campus
10 km	City
100 km	Country
1000 km	Continent
10,000 km	Planet

PAN –Personal Area Network

LAN –Local Area Network

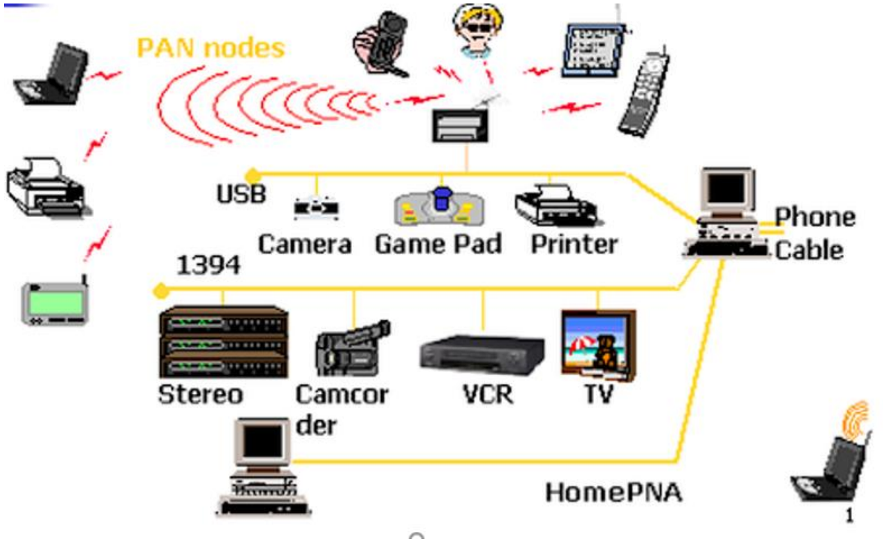
MAN –Metropolitan Area Network

WAN –Wide Area Network

Internet

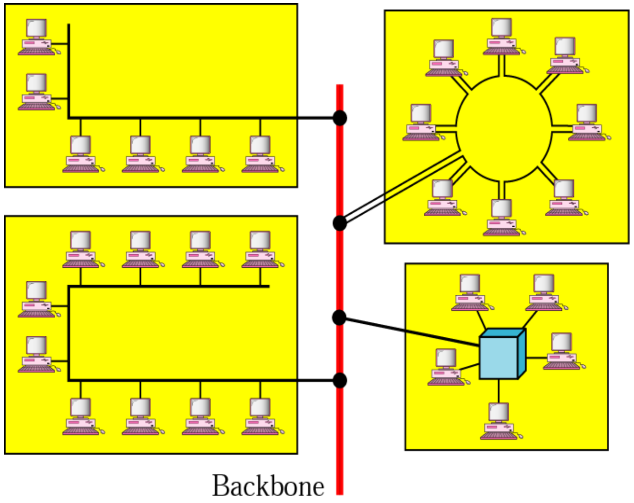
Personal Area Network

- A personal area network is a network concerned with the exchange of information in the vicinity of a person.
- Typically, these systems are wireless and involve the transmission of data between devices such as smartphones, personal computers, tablet computers, etc.
- The purpose of such a network is usually to allow either transmission of data or information between such devices or to server as the network that allows further up link to the Internet.

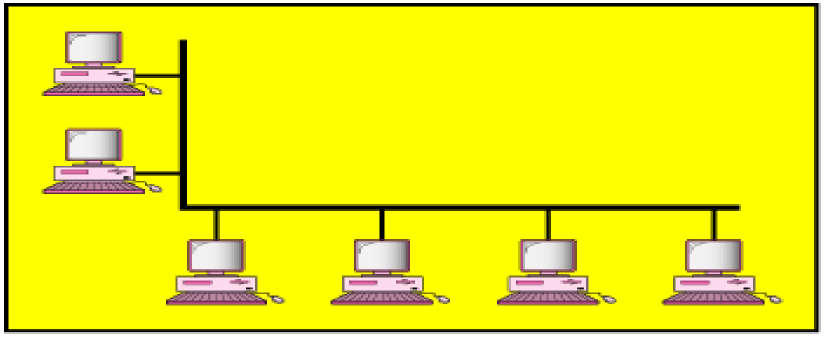


Local Area Network

- A LAN connects network devices over a relatively short distance. LAN is privately owned network that operates in very small geographical area (10 m to a few km) widely used:
  - To connect personal computers and workstations in offices and factories
  - To share hardware (like printers, scanners) and software (application software)
  - To exchange information



b. Multiple-building LAN

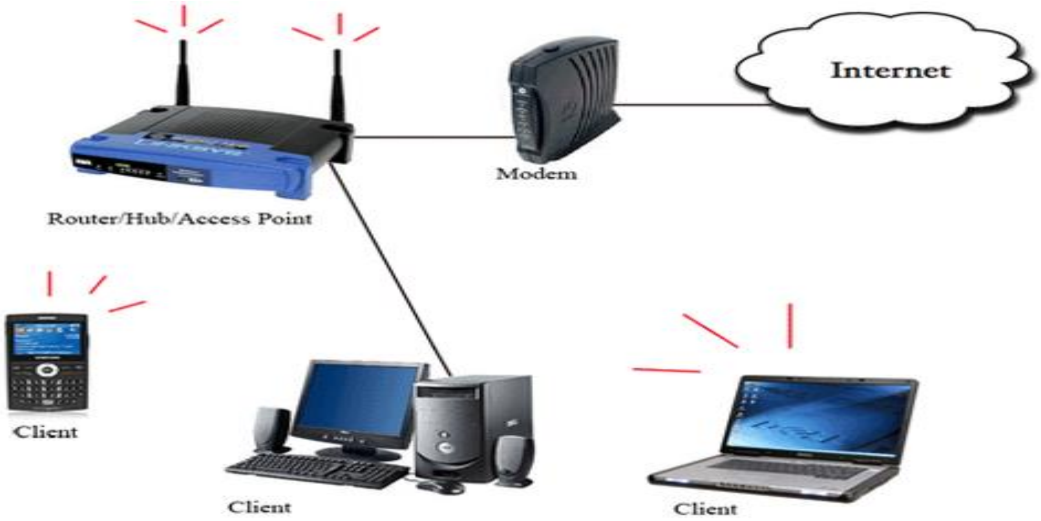


a. Single-building LAN

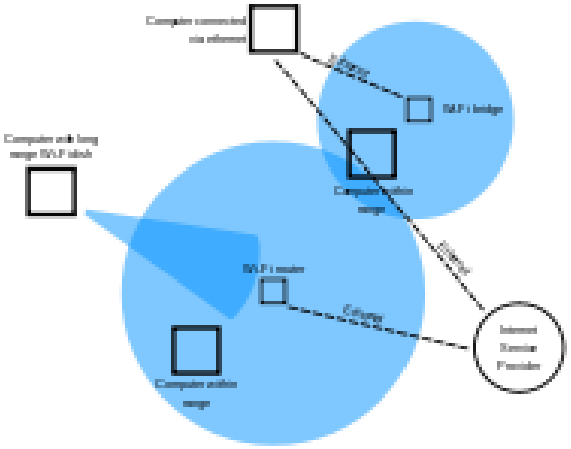
- A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings.
- In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet.
- In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.
- LANs are distinguished from one other by three characteristics:
  - **Size** of LAN is restricted by number of users licensed to access the operating system or application software
  - Transmission technology: LAN consists of single type of cable and all the computers/ communicating devices connected to it.
    - Most local-area networks use a 48-bit physical address
  - Topology used

Wireless Local Area Network (WLAN)

- A WLAN, or wireless LAN, is a network that allows devices to connect and communicate wirelessly. Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a WLAN communicate via Wi-Fi.
- While a WLAN may look different than a traditional LAN, it functions the same way. New devices are typically added and configured using DHCP.

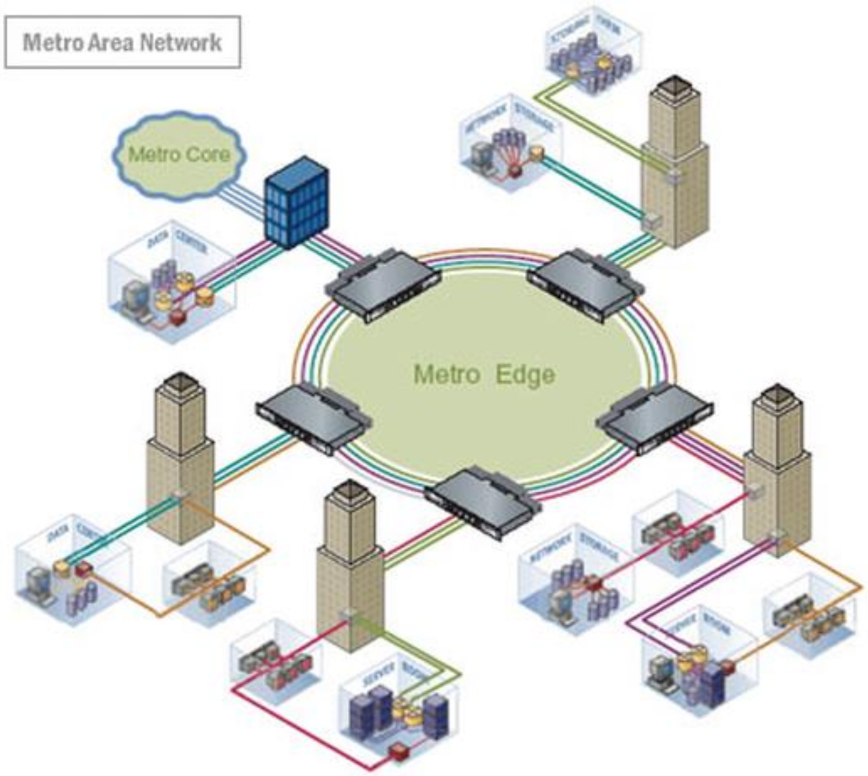


- They can communicate with other devices on the network the same way they would on a wired network.
- The primary difference is how the data is transmitted. In a LAN, data is transmitted over physical cables in a series of Ethernet packets containing. In a WLAN, data is transmitted over the air using one of the IEEE 802.11 protocols.
- Many wireless routers also include Ethernet ports, providing connections for a limited number of wireless devices.


Computer connected via ethernet
Ethernet
Wi-Fi bridge
Computer with long range Wi-Fi dish
Computer within range
Ethernet
Wi-Fi router
Ethernet
Computer within range
Internet Service Provider

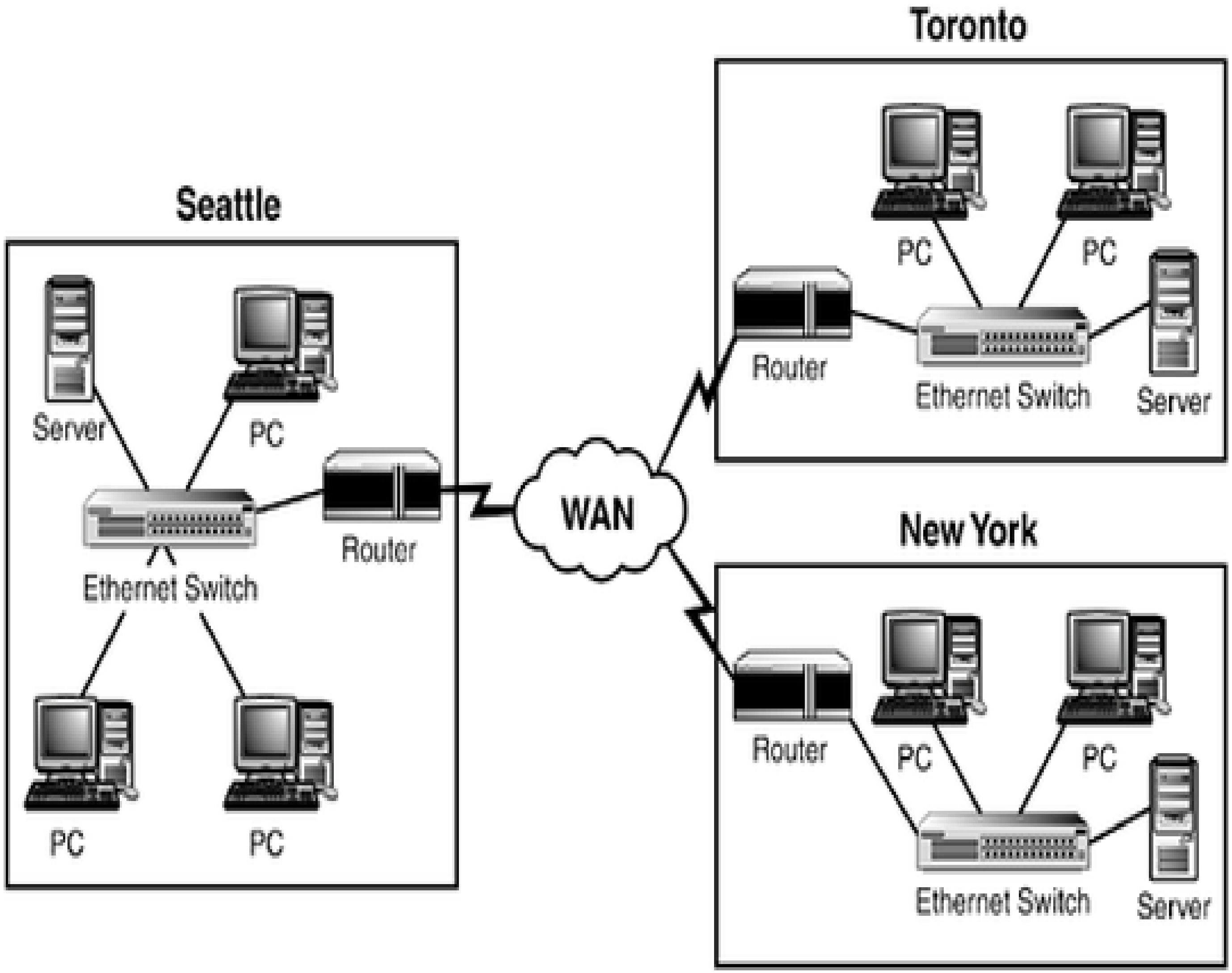
Metropolitan Area Network

- A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city.
- A MAN is typically owned an operated by a single entity such as a government body or large corporation.



Wide Area Network

- A WAN is a network that spans more than one geographical location often connecting separated LANs. A WAN is a geographically-dispersed collection of LANs.
  - As the term implies, a WAN spans a large physical distance.
  - The Internet is the largest WAN, spanning the Earth.
  - A network device called a router connects LANs to a WAN.
  - In IP networking, the router maintains both a LAN address and a WAN address.
- WANs are slower than LANs and often require additional and costly hardware such as routers, dedicated leased lines, and complicated implementation procedures.
- A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management.
- WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.


Toronto
PC
PC
Router
Ethernet Switch
Server
Seattle
Server
PC
Ethernet Switch
Router
PC
PC
WAN
New York
Router
PC
PC
Ethernet Switch
Server

Protocol and its Components

Protocol is a set of rules that governs data communication. It represents an agreement between the communicating devices. Without protocol two devices may be connected but cannot communicate.

The key elements of protocol are:

1. **Syntax:** The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented.
2. **Semantics:** The word *semantics* refers how a particular pattern to be interpreted and what action is to be taken based on that interpretation.
3. **Timing:** Timing refers to when the data should be sent and how fast it should be sent?

The key functions that a protocol performs are:

- **Protocol Data Unit:** It refers to the breaking of data in manageable units called Protocol Data Unit e.g. Segment, Packet, Frame etc.
- **Format of packet:** Format of the packet like which group of bits in the packet constitute data, address, or control bits.
- **Sequencing:** It refers to the breaking long message into smaller units. Sequencing is responsibility protocol.
- **Routing of packets:** Finding the most efficient path between source and destination is responsibility of protocol.
- **Flow control:** It is responsibility of the protocol to prevent fast sender to overwhelm slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data through the shared medium.

- **Error control:** Protocol is responsible to provide method for error detection and correction.
- **Log related information:** Some communication software has features to provide log of usage of network resources.
- **Defining priority:** Different types of packets needs to have different priority while moving on the shared network e.g. network management packets needs to be given higher priority if some congestion occurs.
- **Creating and terminating a connection:** Protocol defines the rules to create and terminate a connection between sender and receiver to communicate among each other.
- **Security of data:** Several communication software has features to prevent data from unauthorized access.

Network Standards

- Networking standards define the rules for data communications that are needed for interoperability of networking technologies and processes.
- Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.

Types of Standards

Standards are of two types

- **De facto –** These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts.
    - For example, the HTTP had started as a de facto standard.
- **De jure –** These standards are the ones which have been adopted through legislation by any officially recognized standards organization.
    - Most of the communication standards that are used today are de jure standards.

Standards Organizations

1. Standards Creation Committees: While many organizations are dedicated to the establishment of standards, some of the noted standards organizations are

- **American National Standards Institute (ANSI):** The official standards organization in the United States. ANSI is pronounced *An-See*.
- **Institute of Electrical and Electronics Engineers (IEEE):** An international organization that publishes several key networking standards; in particular, the official standard for the Ethernet networking system (known officially as IEEE 802.3). IEEE is pronounced *Eye-triple-E*.
- **International Organization for Standardization (ISO):** A federation of more than 100 standards organizations from throughout the world. If I had studied French in high school, I'd probably understand why the acronym for International Organization for Standardization is ISO, and not IOS.
- **Internet Engineering Task Force (IETF):** The organization responsible for the protocols that drive the Internet.
- **World Wide Web Consortium (W3C):** An international organization that handles the development of standards for the World Wide Web.

2. Forums

- Standards committees are procedural bodies and by nature slow-moving.
- To accommodate the need for working models and agreements and to facilitate the standardization process, many special-interest groups have developed **forums** made up of representatives from interested corporations.
- The forums work with universities and users to test, evaluate, and standardize new technologies.
- By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community.
- The forums present their conclusions to the standards bodies.

3. Regulatory Agencies

- All communications technology is subject to regulation by government agencies such as the Telecom Regulatory Authority of India (TRAI).
- The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications.
- TRAI's mission is to create and nurture conditions for growth of telecommunications in the country in a manner and at a pace which will enable India to play a leading role in emerging global information society.
- One of the main objectives of TRAI is to provide a fair and transparent policy environment which promotes a level playing field and facilitates fair competition.

Internet Standards

- An **Internet standard** is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed.
- There is a strict procedure by which a specification attains Internet standard status.
- A specification begins as an Internet draft. An **Internet draft** is a working document (a work in progress) with no official status and a 6-month lifetime.
- Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment** (RFC). Each RFC is edited, assigned a number, and made available to all interested parties.
- RFCs go through maturity levels and are categorized according to their requirement level.