COMPUTER NETWORKS

Unit I - Introduction: Uses of Computer Networks - Network Hardware - Network Software -Reference Models - Example Networks.

1. Computer Network

- A computer network is a set of computers connected together for the purpose of sharing resources.
- The most common resource shared today is connection to the internet.

2. Goals of networking:

- Resource sharing
- High reliability
- Save money
- Scalability
- Powerful communication medium

3.Uses of computer Networks

3.1Business Applications

- The aim of networking is to make all programs, equipment's, and data available to anyone on the network without regard to the physical location of the resource and the user.
- A company has separate computers to monitor production, keep track of inventories, and do the payroll.
- Each computer has worked in isolation from the others, but at some point.
- They are connected to extract and correlate information about the entire company.
- Client server
- Email
- Desktop Sharing

3.2Home Applications

The main usage of networks in home is internet. Some popular uses of the Internet for home users are:

- Access to remote information by surfing the World Wide Web for information or just for fun.
- Person-to-person communication sharing the audio, video, text and pictures among groups of people.
- Interactive entertainment where any movie or television program made in any country can be displayed on the screen instantly.
- Electronic commerce where people do home shopping, pay their bills, manage their bank accounts, and handle their investments electronically.
- Instant Message Ex: Twitter
- Social Networking Ex: Face Book, Watsup
- Wiki
- Ecommerce
- IPTV

3.3 Mobile Users

- Mobile computers, such as notebook computers and personal digital assistants (PDAs) are connected to the office or home even when away from home.
- People on the road use their portable electronic equipment to send and receive telephone calls, faxes, and electronic mail, surf the Web, access remote files, and log on to remote machines.
- People do this from anywhere on land, sea, or air.
- SMS
- M-Commerce
- GPS

3.4 Social Issuses

- Cookies
- Gmail

4. Network hardware

- It depends on transmission technology and scale.

4.1 Transmission Technology

There are two types of transmission technology:

1. Broadcast links.
2. Point-to-point links.

4.1.1Broadcast link

- Broadcast networks have a single communication channel that is shared by all the machines on the network.
- Short messages, called packets sent by any machine are received by all the others.
- An address field within the packet specifies the intended recipient.
- On receiving a packet, a machine checks the address field.
- If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.
- Broadcast systems also allows the possibility of addressing a packet to all destinations by using a special code in the address field.
- Some broadcast systems support transmission to a subset of the machines, called as multicasting.

4.1.2Point-to-point link

- Point-to-point networks consist of many connections between individual pairs of machines.
- Point-to-point transmission with one sender and one receiver is sometimes called unicasting.

4.2 Scale

- An alternative criterion for classifying networks is their scale.
- The table classifies networks according to their scale.

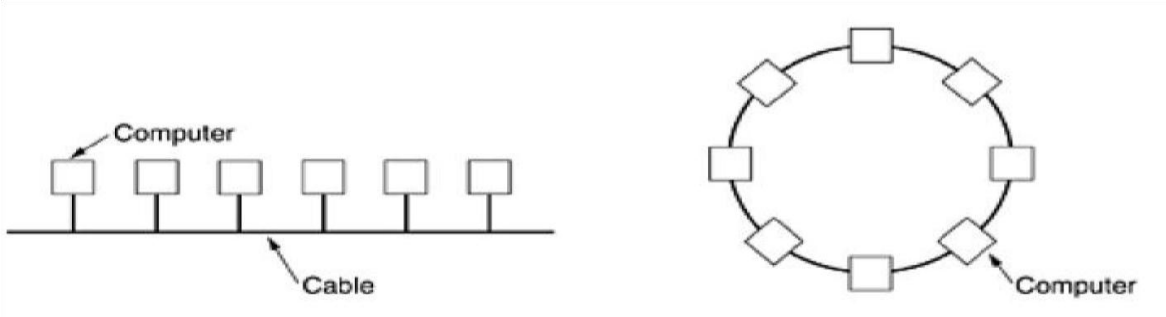
Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

4.2.1 Personal Area Networks

- It communicate over the range of person.
- Its coverage area of the network is within a meter.
- Ex.Bluetooth

4.2.2Local Area Networks

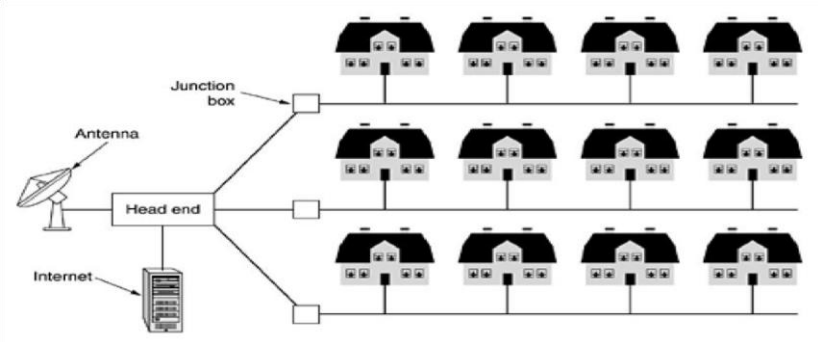
- Local area networks, called LANs, are privately-owned networks within a single building or campus of up to a few kilometres in size.
- They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.
- LANs are distinguished by three characteristics: (1) size, (2) transmission technology (3) topology.
- LANs are restricted in size. LANs use a transmission technology consisting of a cable to which all the machines are attached.
- Various topologies are used for broadcast LANs.



- In a bus 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. Eg: IEEE 802.3(Ethernet).
- In the ring system each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Eg: IEEE 802.5 (the IBM token ring).

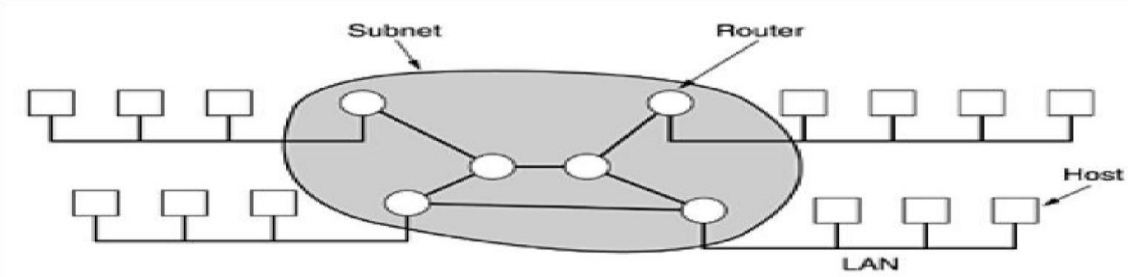
4.2.3 Metropolitan Area Networks

- A metropolitan area network, or MAN, covers a city like cable television network available in many cities.

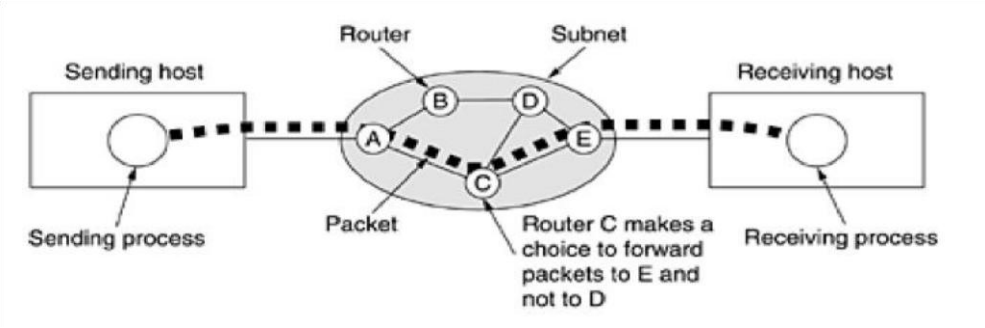


4.2.4 Wide Area Networks

- A wide area network, or WAN,covers large geographical area, often a country or continent.
- It contains a collection of machines intended for running user programs.
- The hosts are connected by a communication subnet.
- The hosts are owned by the customers, whereas the communication subnet is owned and operated by a telephone company or Internet service provider.
- The job of the subnet is to carry messages from host to host.
- In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements.
- Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links.
- Switching elements are specialized computers that connect three or more transmission lines.
- When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them. These switching computers are called router.



- The collection of communication lines and routers that move packets from the source host to the destination host form the subnet.
- When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded.
- This is called store-and-forward or packet-switched subnet.
- If the packets are small and all the same size, they are called cells.
- A process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence.
- These packets are then injected into the network one at a time in quick succession.
- The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process.



4.2.5 Internetworks

- The world collection of computer is called internetworks or internet.
- Gateway: it is used to connection between two or more networks

5. Wireless Networks

Wireless networks can be divided into three main categories:

- System interconnection- It is interconnecting the components of a computer using short-range radio.
- Some short-range wireless networks called Bluetooth are used to connect these components without wires.
- Wireless LANs are systems in which every computer has a radio modem and antenna with which it can communicate with other systems.
- Wireless WANs.

6. Home Networks

Every device in the home is capable of communicating with every other device, and all of them will be accessible over the Internet. Some categories are :

- Computers (desktop PC).
- Entertainment (TV, DVD).
- Telecommunications (telephone, mobile telephone).
- Appliances (microwave, refrigerator).
- Telemetry (utility meter, smoke/burglar alarm).

Home networking has different properties than other network types. These are:

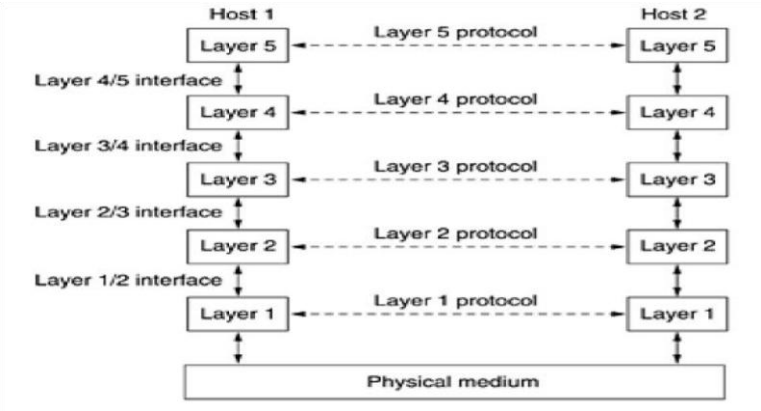
- The network and devices have to be easy to install.
- The network and devices have to be fool proof in operation.
- Low price is essential for success.
- Security and reliability is very important.

7.Network software

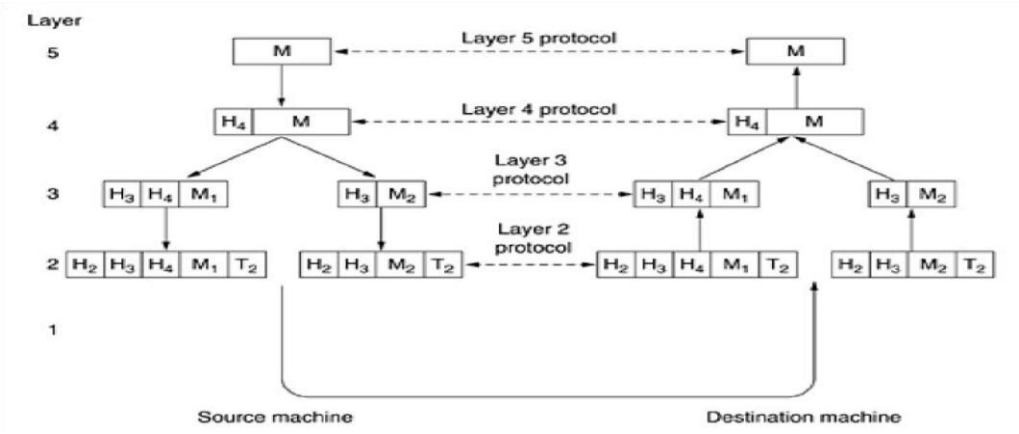
7.1Protocol Hierarchies

- Networks are organized as a stack of layers or levels, each one built upon the other.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers.

A five-layer network is:



- The entities comprising the corresponding layers on different machines are called peers. The peers may be processes, hardware devices, or even human beings.
- No data are directly transferred from layer n on one machine to layer n on another machine. Each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which actual communication occurs.
- A set of layers and protocols is called a network architecture. A list of protocols used by a certain system, one protocol per layer, is called a protocol stack.



7.2 Connection-Oriented and Connectionless Services

- Layers offer two different types of service to the layers above them: connection-oriented and connectionless.
- Connection-oriented service first establishes a connection, uses the connection, and then releases the connection. eg. Telephone system.
- Connectionless service is modelled after the postal system. Each message carries the full destination address, and each one is routed through the system independent of all the others.
- Unreliable connectionless service is called datagram service, which does not return an acknowledgement to the sender.
- In this service the sender transmits a single datagram containing a request; the reply contains the answer.

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

7.3 Service Primitives

A service is specified by a set of primitives available to a user process to access the service. The primitives are normally system calls of an OS.

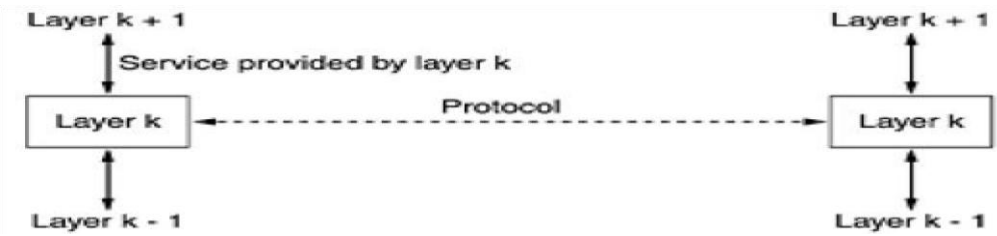
Some of the essential primitives:

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

- The server executes LISTEN to indicate that it is prepared to accept incoming connections. After executing the primitive, the server process is blocked until a request for connection appears.
- The client process executes CONNECT to establish a connection with the server. The CONNECT call needs to specify who to connect to. The operating system sends a packet to the peer asking it to connect.
- When the system sees that the packet is requesting a connection, it checks to see if there is a listener. If so, it does two things: unblocks the listener and sends back an acknowledgement. The arrival of this acknowledgement then releases the client.
- The server executes RECEIVE to prepare to accept the first request. Then the client executes SEND to transmit its request followed by the execution of RECEIVE to get the reply.
- The client use DISCONNECT to terminate the connection. When the server gets the packet, it also issues a DISCONNECT of its own, acknowledging the client and releasing the connection.

7.4 Relationship of Services and Protocols

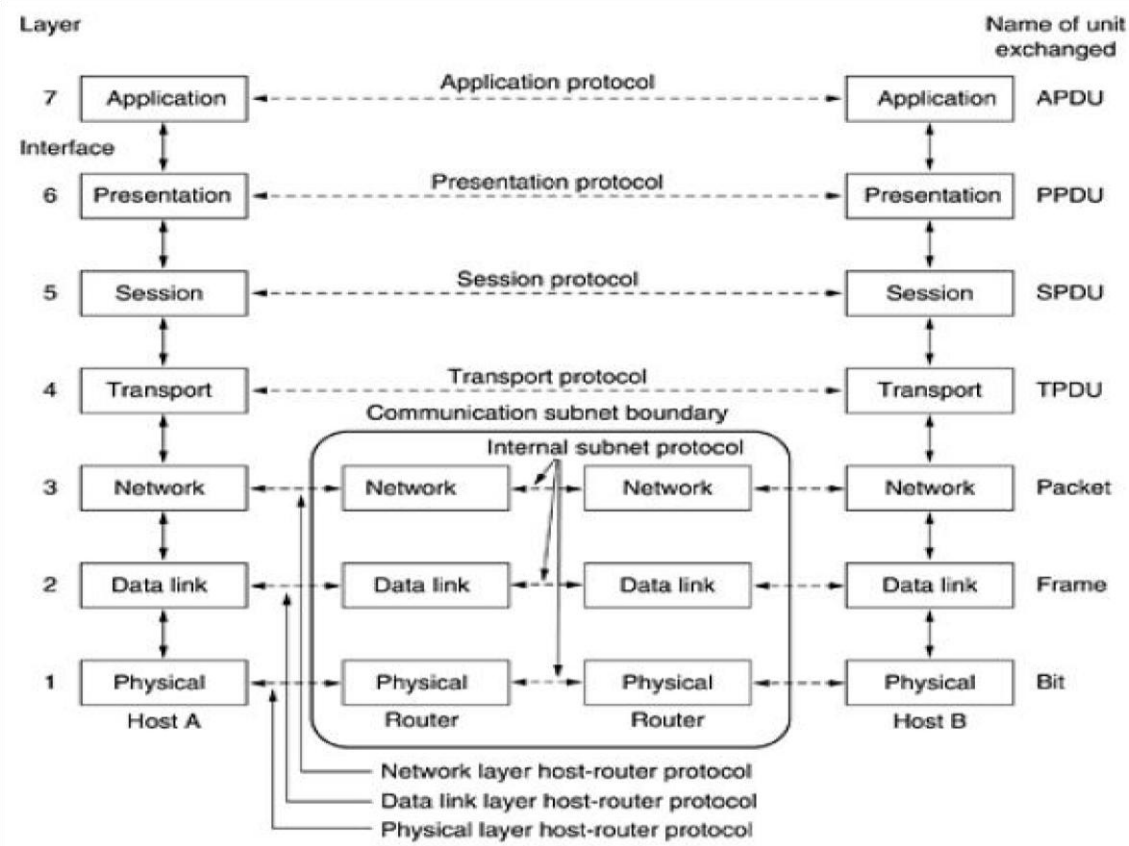
- A service is a set of primitives that a layer provides to the layer above it.
- The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented.
- A service relates as an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.
- A protocol is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer.
- Services relate to the interfaces between layers whereas protocols relate to the packets sent between peer entities on different machines.



8. Reference Models

8.1The OSI Reference Model

- This model is based on a proposal developed by the International Standards Organization (ISO).
- It is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems that is, systems that are open for communication with other systems.



The Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel.

The components of the physical layer are:

- Cabling system components
- Adapters that connect media to physical interfaces
- Hub, repeater, and patch panel specifications
- Network Interface Card (NIC)

The Data Link Layer

- The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer.
- It performs this task by the sender breaking up the input data into data frames and transmit the frames sequentially.
- If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.

This layer provides the following functions:

- Allows a device to access the network to send and receive messages
- Offers a physical address so a device's data can be sent on the network
- Works with a device's networking software when sending and receiving messages

- Provides error-detection capability

The common networking components are :

- Network interface cards
- Ethernet and Token Ring switches
- Bridges

The Network Layer

- The network layer controls the operation of the subnet.
- A key design issue is determining how packets are routed from source to destination. The quality of service provided is also a network layer issue.
- When a packet has to travel from one network to another to get to its destination, many problems can arise.
- Network layer overcomes all these problems to allow heterogeneous networks to be interconnected.

The Transport Layer

- The basic function is to accept data from above, split it up into smaller units , pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.
- The transport layer also determines what type of service to provide to the session layer, and, to the users of the network.

Functions:

- Segmentation of data for network transport
- Control of data flow to prevent memory overruns
- Transmission-error detection

The most common transport layer protocols are the connection-oriented TCP Transmission Control Protocol (TCP) and the connectionless UDP User Datagram Protocol (UDP).

The Session Layer

- The session layer allows users on different machines to establish sessions between them.
- Sessions offer various services like dialog control, token management, and synchronization.

The Presentation Layer

- It is concerned with the syntax and semantics of the information transmitted.
- The presentation layer manages abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

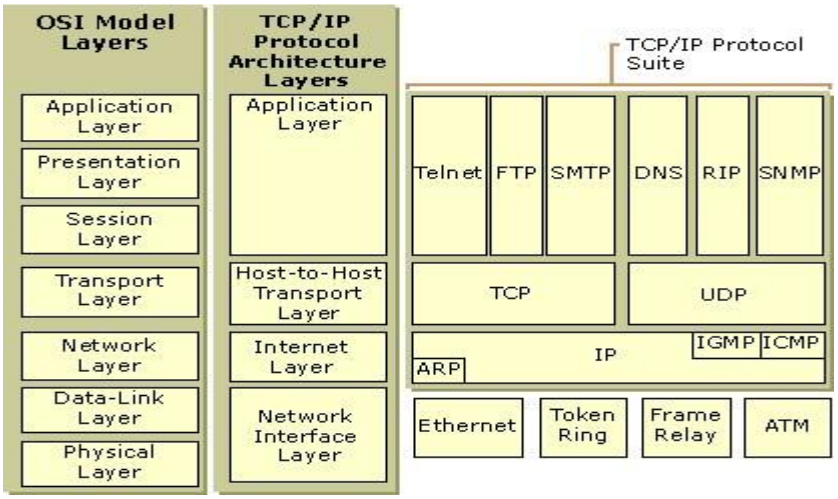
The Application Layer

- The application layer contains a variety of protocols that are commonly needed by users.eg: HTTP (HyperText Transfer Protocol), which is the basis for the World Wide Web.
- When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back.
- Other application protocols are used for file transfer, electronic mail, and network news.

8.2 The TCP/IP Reference Model

- The ARPANET was a research network sponsored by U.S. Department of Defense with a major goal to connect multiple networks.

- This architecture was later known as the TCP/IP Reference Model, after its two primary protocols. The relation between OSI and TCP/IP model is:



The Network Interface Layer

- This is also called as Network Access Layer. This is the first layer of the four layer TCP/IP model.
- Network Access layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices .
- The layer is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium.
- It is used to connect different network types like LAN technologies such as Ethernet and Token Ring.
- The protocols included are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

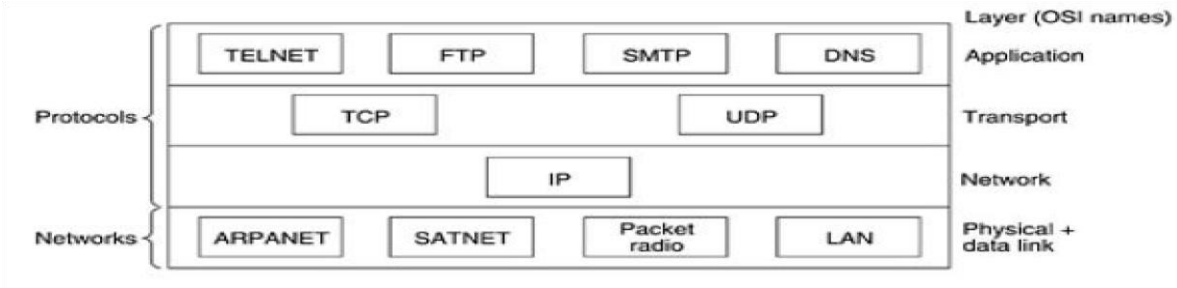
The Internet Layer

- This layer permits hosts to inject packets into any network and have them travel independently to the destination.
- They may even arrive in a different order than they were sent, in which higher layers rearrange them.
- It defines an official packet format and protocol called IP (Internet Protocol).
- The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue.
- The Internet layer is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.
- The Internet Protocol (IP) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The Address Resolution Protocol (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The Internet Control Message Protocol (ICMP) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- The Internet Group Management Protocol (IGMP) is responsible for the management of IP multicast groups.

The Transport Layer

- The layer above the internet layer is called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation.

- TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
- It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer.
- At the destination, the receiving TCP process reassembles the received messages into the output stream.
- UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. The relation of IP, TCP, and UDP is:



The Application Layer

- The Application layer provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data.
- The most widely-known Application layer protocols are those used for the exchange of user information:
    - The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
    - The File Transfer Protocol (FTP) is used for interactive file transfer.
    - The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
    - Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

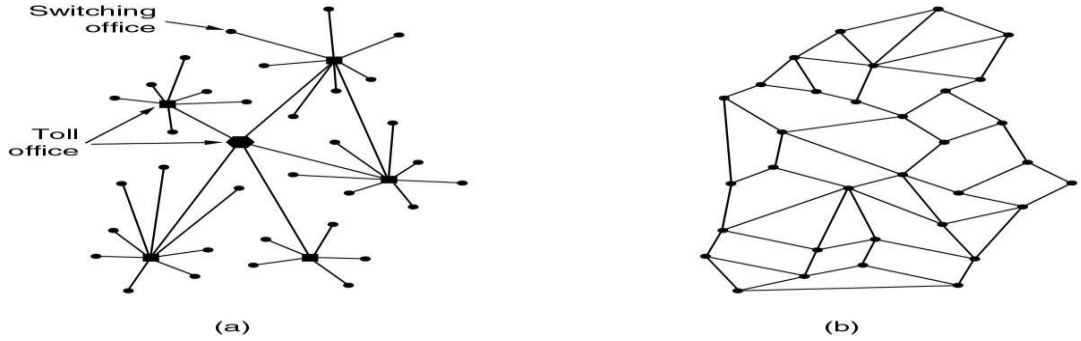
- The Domain Name System (DNS) is used to resolve a host name to an IP address.
- The Routing Information Protocol (RIP) is a routing protocol that routers use to exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (SNMP) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

9. Example Networks

- The ARPANET
- NSFNET
- INTERNET
- Connection-Oriented Networks: X.25, Frame Relay, and ATM
- Ethernet
- Wireless LANs: 802:11

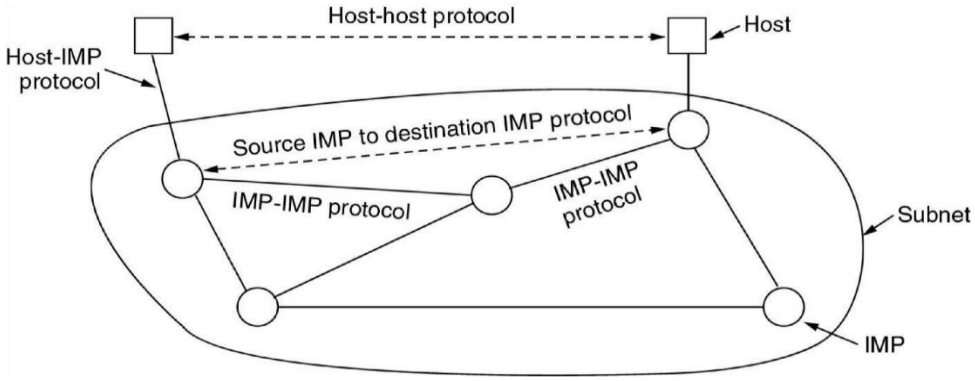
The ARPANET

- The Internet is not a network, but a vast collection of different networks that use certain common protocols and provide certain common services.
- US created a single defence research organization, ARPA, the Advanced Research Projects Agency – it had no scientists or laboratories but did its work by issuing grants and contracts to universities and companies.



- (a) Structure of the telephone system.
- (b) Baran's proposed distributed switching system.

The ARPANET design



DNS

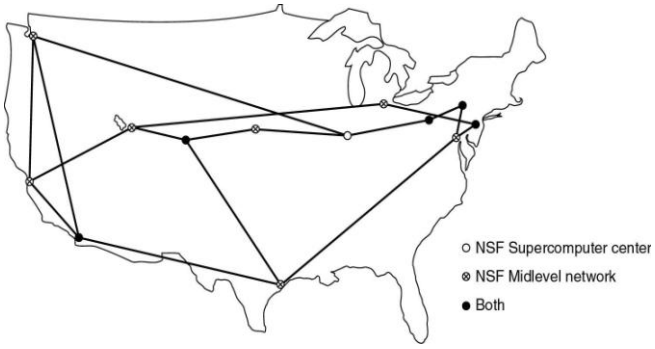
- During the 1980s, additional networks, mainly LANs, were connected to the ARPANET. Finding hosts became increasingly expensive, so DNS (Domain Name System) was created to organize machines into domains and map host names onto IP addresses.
- DNS has become a generalized, distributed database system for storing a variety of information

NSFNET

- In 1970s, NSF (the U.S. National Science Foundation) found the major impact of the ARPANET and designed a successor to the ARPANET that is open to all university research groups
- NSF decided to build a backbone network to connect its six supercomputer centers, in San Diego, Boulder, Champaign, Pittsburgh, Ithaca, and Princeton
- NSF also funded some regional networks that connected to the backbone to allow users at thousands of universities, research labs, libraries, and museums to access any of the supercomputers and to communicate with one another .
- This complete network was called NSFNET

- NSF awarded contracts to four different network operators to establish a NAP (Network Access Point)
- During the 1990s, many other countries and regions also built national research networks, often

- The NSFNET backbone in 1988.

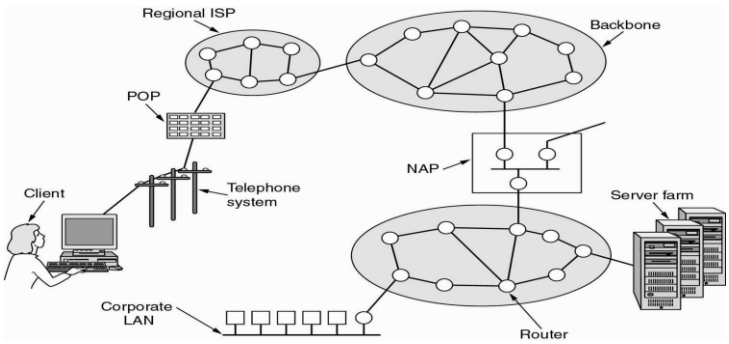


patterned on the ARPANET and NSFNET. They are Europa NET and EBONE in Europe.

Internet

- The number of networks, machines, and users connected to the ARPANET grew rapidly after TCP/IP became the only official protocol on January 1, 1983
- When NSFNET and the ARPANET were interconnected, the growth became exponential. Many regional networks joined up, and connections were made to networks in Canada, Europe, and the Pacific
- The glue that holds the Internet together is the TCP/IP reference model and TCP/IP protocol stack
- To be on the Internet - a machine is on the Internet if it runs the TCP/IP protocol stack, has an IP address, and can send IP packets to all the other machines on the Internet.
- Up to 1990s, the Internet was largely populated by academic, government, and industrial researchers.
- WWW (World Wide Web) changed all that and brought millions of new, non-academic users to the net

Architecture of the Internet

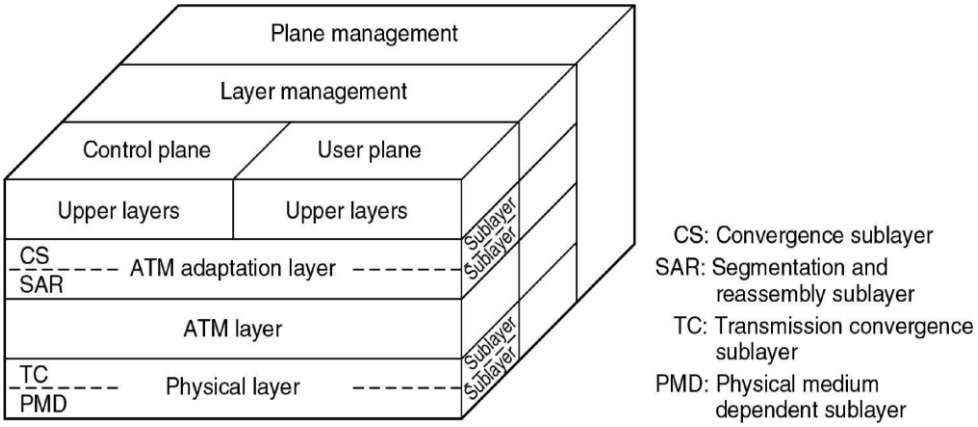


- ISP have POP (Point of Presence), where converted digital signals from the computer to analog signals (by modem) are removed from the telephone system and injected into the ISP's regional network, from this point on, the system is fully digital and packet switched
- The ISP's regional network consists of interconnected routers in the various cities the ISP serves.
- If the packet is destined for a host served directly by the ISP, the packet is delivered to the host.
  - Otherwise, it is handed over to the ISP's backbone operator

Connection-Oriented Networks: X.25, Frame Relay, and ATM

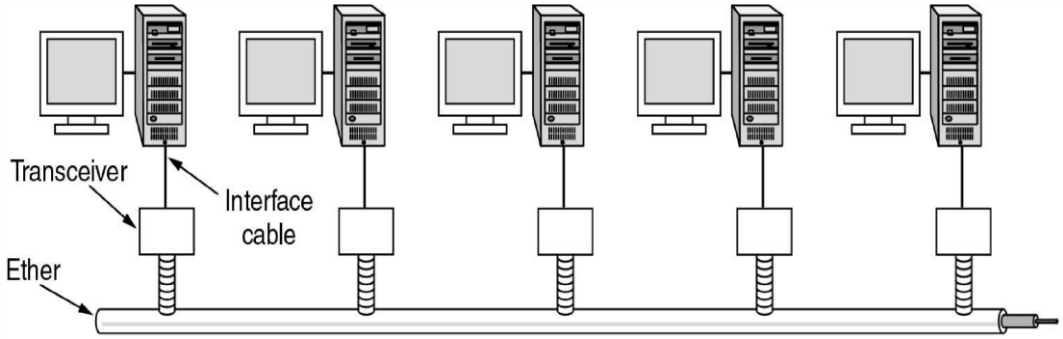
- X.25 is the first public data network, deployed in the 1970s at a time when telephone service was a monopoly
- In the 1980s, X.25 networks were largely replaced by a new kind of network called frame relay.
- The essence of frame relay is that it is a connection-oriented network with no error control and no flow control
- ATM (Asynchronous Transfer Mode) - merging voice, data, cable television, telex, telegraph, etc into a single integrated system that could do everything for everyone .
- ATM transmits all information in small, fixed-size packets called cells - an ATM cell.

The ATM Reference Model



Ethernet

- Internet and ATM are designed for wide area networking
- The most popular LAN is Ethernet
- Up to 256 machines could be attached to the system via transceivers screwed onto the cable.
- A cable with multiple machines attached to it in parallel is called a multidrop cable
- A computer first listened to the cable to see if someone else was already transmitting, the computer held back until the current transmission finished
- Architecture of the original Ethernet.



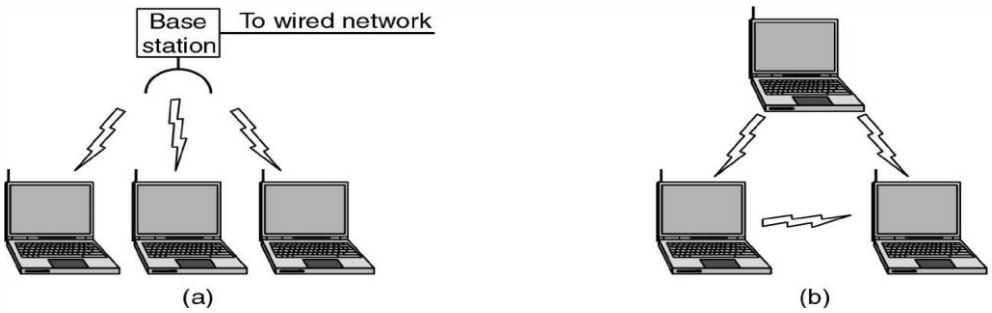
- If two or more computers start transmitting at once each computer listens during its own transmission and if it detects interference, jam the ether to alert all senders
- Then the station/computer backs off and waits a random time before retrying
- If a second collision happens, the random waiting time is doubled, and so on, to spread out the competing transmissions and give one of them a chance to go first
- In 1978 Xerox drew the 10-Mbps Ethernet standard – became IEEE 802.3 standard in 1983

Wireless LANs: 802.11

- IEEE committee that standardized the wired LANs was given the task of creating wireless LAN standard that resulted in 802.11
- Commonly known as WiFi
- The proposed standard had to work in two modes:

  In the presence of a base station

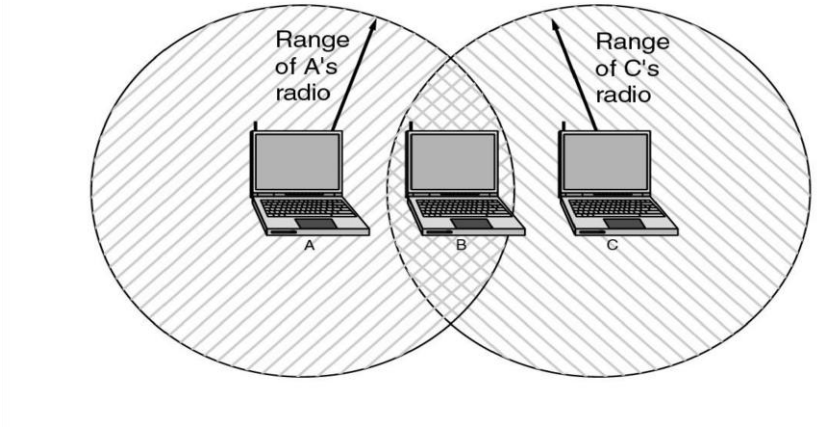
  In the absence of a base station
- In the first case, all communication go through the base station, called an access point
- In the second case, the computers would just send to one another directly - ad hoc networking.



(a) Wireless networking with a base station.(b) Ad hoc networking.

- Ethernet had dominated local area networking, so the committee decided to make 802.11 compatible with Ethernet above the data link layer
- Possible to send an IP packet over the wireless LAN the same way a wired computer sent an IP packet over Ethernet

- Another problem is that a radio signal can be reflected off solid objects, so it may be received multiple times (along multiple paths). This interference results in what is called multipath fading.



- A multicell 802.11 network.