COMPUTER NETWORKS

UNIT –I

Uses of computer networks - Network hardware - Network software - Reference models - Example networks.

DEFINITION

A set of autonomous computers interconnected via wired or wireless medium is called as Computer Network.

USES OF COMPUTER NETWORK

1. BUSINESS APPLICATIONS

Business Applications of network are many and more. Some of its applications are, Resource Sharing, E-mail, Report Writing, Video Conferencing and E-Commerce

Resource Sharing

Make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user. A group of workers sharing a common printer is an example of resource sharing. In this scenario no individual need a private printer, and a high-volume networked printer is often cheaper, faster, and easier to maintain than a large collection of individual printers.

E-mail

A computer network can provide a powerful communication among employees through e-mail (electronic mail), which employees generally use for daily communication.

Advantages

- Fastest communication without regard to distance
- Lower cost
- Convenience

Report writing

With a network, it is easy for two or more people who work far apart to write a report together. When one worker makes a change to an online document, the others can see the change immediately, instead of waiting several days for a letter.

AADHAVAN COLLEGE

Videoconferencing

Using this technology, employees at distant locations can held a meeting, seeing and hearing each other and even writing on a shared virtual blackboard. Videoconferencing is a powerful tool for eliminating the cost and time previously devoted to travel.

E-commerce

Many companies are doing business electronically with other companies, especially suppliers and customers.

2. HOME APPLICATIONS

Access to remote information

It can be surfing the World Wide Web for information or just for fun. Information available includes the arts, business, cooking, government, health, history, hobbies, recreation, science, sports, travel, and many others. Many newspapers have gone on-line and can be personalized. Access to on-line digital libraries like ACM and IEEE are also possible. already have many journals and conference proceedings on-line.

Person-to-person communication

- **E-mail**
- **Instant messaging** - allows two people to type messages at each other in real time.
- **Chat room** - A multiperson version of instant messaging is the chat room, in which a group of people can type messages for all to see.

Access to Newsgroups

A newsgroup is an Internet-based discussion about a particular topic. These topics range from sports, cars, investing, teen problems, etc. Users post messages to a newsserver which then sends them to a bunch of other participating servers. Then other users can access the newsgroup and read the postings.

The groups can be either "moderated," where a person or group decides which postings will become part of the discussion, or "unmoderated," where everything posted is included in the discussion.

To participate in a newsgroup, user must subscribe to it. It typically doesn't cost anything, but some groups can be hard to get into unless you know people in the group. There were nearly more than 13,000 newsgroups.

NAVAN COLLEGE

Programs called newsreaders are used to read and post messages to one or more newsgroups. Some of Usenet newsreaders are Louts notes, Netscape communicator, Windows live mail, Opera mail, Mozilla Thunderbird, etc. Newsgroup access has also been integrated into Netscape and Internet Explorer. Unlike chat rooms, newsgroups are not real time and messages are saved waiting for reading.

Peer-to-Peer communication

Individuals who form a group can communicate with others in the group. Every person can communicate with one or more other people; there is no fixed division into clients and servers.

Ex: Social networks, E-mail, etc.

Entertainment

- **Video on demand**

  It may be possible for a user to select any movie or television program ever made, in any country, and have it displayed on their screen instantly. New films may become interactive, where the user is occasionally prompted for the story direction with alternative scenarios provided for all cases.

- **Interactive TV**

  Live television may also become interactive, with the audience participating in quiz shows, choosing among contestants, and so on.

- **Network games:** Single person and multi-person games are available. **M**ultiperson real-time simulation games, like hide-and-seek in a virtual dungeon, and flight simulators with the players on one team trying to shoot down the players on the opposing team.

Electronic commerce and Electronic flea markets (e-flea). On-line auctions of second-hand goods have become a massive industry.

Telelearning and **Telemedicine** are only now starting to catch on (e.g., remote patient monitoring) but may become much more important.

3. MOBILE USERS APPLICATIONS

Mobile computers, such as notebook computers and personal digital assistants (PDAs), are one of the fastest-growing segments of the computer industry. Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless networks.

Colleges and universities

AADHAVAN COLLEGE

At computer conferences these days, the organizers often set up a wireless network in the conference area. Anyone with a notebook computer and a wireless modem can just turn the computer on and be connected to the Internet, as though the computer were plugged into a wired network.

Similarly, some universities have installed wireless networks on campus so students can sit under the trees and consult the library's card catalog or read their e-mail.

Trucks, taxis, delivery vehicles

Wireless networks are of great value to fleets (navy) of trucks, taxis, delivery vehicles, and repair persons for keeping in contact with home. For example, in many cities, taxi drivers are independent businessmen, rather than being employees of a taxi company.

In some of these cities, the taxis have a display the driver can see. When a customer calls up, a central dispatcher, types in the pickup and destination points. This information is displayed on the drivers' displays and a beep sounds. The first driver to hit a button on the display gets the call.

Military

Wireless networks are also important to the military.

Airports

At many busy airports, car rental return clerks work in the parking lot with wireless portable computers. They type in the license plate number of returning cars, and their portable, which has a built-in printer, calls the main computer, gets the rental information, and prints out the bill on the spot.

Wireless parking meters

The meters could accept credit or debit cards with instant verification over the wireless link. When a meter expires, it could check for the presence of a car (by bouncing a signal off it) and report the expiration to the police. They have advantages for both users and city governments to enforce better parking.

Food, drink, and other vending machines

In these machines periodically, someone comes by with a truck to fill them. If the vending machines issued a wireless report once a day announcing their current inventories, the truck

AADHAVAN COLLEGE

driver would know which machines needed servicing and how much of which product to bring. This information could lead to more efficient route planning.

Utility meter reading

If electricity, gas, water, and other meters in people's homes were to report usage over a wireless network, there would be no need to send out meter readers.

Wireless smoke detectors

It could call the fire department instead of making a big noise (which has little value if no one is home). As the cost of both the radio devices and the air time drops, more and more measurement and reporting will be done with wireless networks.

M-commerce: Buying and selling of goods and services through wireless handheld devices such as cellphones and PDAs.

Personal area networks and wearable computers: IBM has developed a watch that runs Linux (including the X11 windowing system) and has wireless connectivity to the Internet for sending and receiving e-mail.

SOCIAL ISSUES OF NETWORK

Newsgroups

Popular features of many networks are newsgroups or bulletin boards whereby people can exchange messages with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

The trouble comes when newsgroups are set up on topics that people actually care about, like politics, religion, or sex.

Employee rights versus employer rights

Many people read and write e-mail at work. Many employers have claimed the right to read and possibly censor employee messages, including messages sent from a home computer after work. Not all employees agree with this.

Anonymous messages

Computer networks offer the potential for sending anonymous messages. In some situations, this capability may be desirable. For example, it provides a way for students, soldiers, employees,

ADHAVAN COLLEGE

and citizens to blow the whistle on illegal behavior on the part of professors, officers, superiors, and politicians without fear of punishment. Anonymous accusation cannot be used as evidence.

Ill-informed, misleading, or downright messages

It can't be assured that all information available in internet is 100% correct. For example, the medical advice published in Internet may have come from a Nobel Prize winner or from a high school dropout.

Electronic junk mail

Electronic junk mail (spam) has become a part of life because many people have collected millions of e-mail addresses and sell them on CD-ROMs to marketers. E-mail messages containing active content can contain viruses that cause destruction.

Copyright violations

Being able to transmit music and video digitally has opened the door to massive copyright violations that are hard to catch.

NETWORK HARDWARE

The two important dimensions into which all computer networks fit are: transmission technology and scale. There are two types of transmission technology such as,

1. Broadcasting
2. Point-to-Point

Broadcast network

- Single communication channel, shared by all machines on a network
- Short messages called packets sent by any computer are received by all others.
- An address field within the packet specifies the intended recipient. Upon 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.
- The two types of data transfer mode are broadcasting and multicasting.
- **Broadcasting : Sending a packet to all machines in the network**
- **Multicasting : Transmission to a subset of machines**

AADHAVAN COLLEGE

- Both broadcasting and multicasting is achieved by setting a special bit in address field of the packet.

This works well in a small network of 2-5 computers, but as the number of computers increases it will increase the network traffic, decrease the performance and available bandwidth of the network.

If the single communication channel is damaged anywhere in its path, it will collapse the entire network.

Point-to-Point Network

- It consists of many connections between individual pair of machines. Hence multiple routes of different length are possible. So finding a good one is important in point-to-point networks.
- A packet on this type of network may have to visit one or more intermediate machines.
- As a general rule, smaller geographically localized networks use broadcasting network technique and larger networks use Point-to-Point networking technique.

TYPES OF NETWORKS

Based on the scale i.e., size networks are classified into following categories. They are

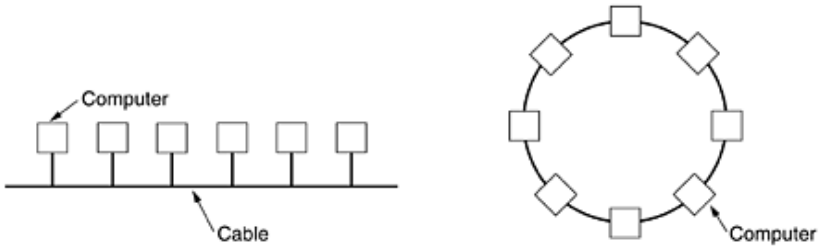
1. **Personal area network**
   - Networks that are meant for one person.
   - A wireless network connecting a computer with its mouse, keyboard, and printer is a personal area network.
2. **LAN (Local Area Network)**
3. **MAN (Metropolitan area Network)**
4. **WAN (Wide Area Network)**

Local Area Network

- Privately-owned networks
- It covers a single building or campus of up to a few kilometers in size.
- It is used to share resources (e.g., printers) and exchange information.

ADHAVAN COLLEGE

- LANs may use broadcasting 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 (microseconds or nanoseconds), and make very few errors.
- Newer LANs operate at up to 10 Gbps.
- Various topologies are possible for broadcast LANs. Two of them are bus and Ring (i.e., a linear cable) network.



(a) (b)

- At any instant at most one machine is the master and is allowed to transmit. All other machines are required to keep silent from sending.
- An arbitration mechanism is needed to solve conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed.
- In the centralized channel allocation method, there is a single entity, for example, a bus arbitration unit, which determines who goes next. It might do this by accepting requests and making a decision according to some internal algorithm. In the decentralized channel allocation method, there is no central entity; each machine must decide for itself whether to transmit.
- IEEE 802.3, called Ethernet is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps.
- IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.
- Broadcast networks can be further divided into static and dynamic, depending on how the channel is allocatd.

- Static allocation: divide time into discrete intervals and use a round-robin algorithm, allowing each machine to broadcast only when its time slot comes up.
    - Static allocation wastes channel capacity when a machine has nothing to send during its allocated slot.
- Dynamic allocation methods attempt to allocate the channel dynamically (i.e., on demand). Dynamic allocation is either centralized or decentralized.

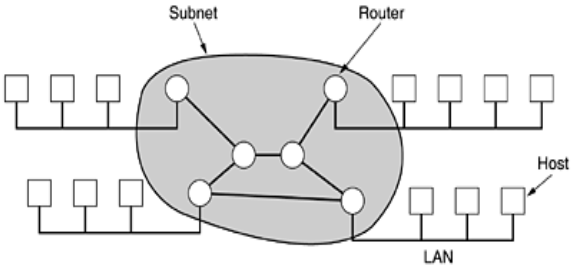
Metropolitan Area Network

A metropolitan area network or MAN is basically a bigger version of a LAN and normally uses similar technology. It might cover a group of nearby corporate offices or a city and might be either private or public. A MAN can support both data and voice, and might even be related to the local cable television network.

Wide Area Network

- WAN covers large geographical area.
- Collection of machines (hosts) connected by a communication subnet is called as WAN.
- The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is owned and operated by a telephone company or Internet service provider.
- The subnet consists of two components
    1. Transmission lines
    2. 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 as router.

ADHAVAN COLLEGE



Store-and-forward or packet-switched subnet

In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. 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. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet.

When a process on some host has a message to be sent to a process on some other host,

- Sending host first cuts the message into packets; each one has its number in the sequence.
- These packets are then injected into the network one at a time.
- The packets are transported individually and at the receiving host, they are reassembled into the original message and delivered to the receiving process.

Wireless Networks

Wireless networks can be divided into three main categories

1. System interconnection.
2. Wireless LANs.
3. Wireless WANs.

System interconnection

It is all about design a short-range wireless network called Bluetooth to connect these components of a computer without wires. Bluetooth also allows digital cameras, headsets, scanners, and other devices to connect to a computer by merely being brought within range. No cables, no driver installation, just put them down, turn them on, and they work.

ADHAVAN COLLEGE

Wireless LAN

- Wireless LANs are becoming increasingly common in small offices and homes, where installing Ethernet is considered too much trouble.
- These are systems in which every computer has a radio modem and antenna with which it can communicate with other systems.
- If the systems are close enough, they can communicate directly with one another in a peer-to-peer configuration.
- There is a standard for wireless LANs, called IEEE 802.11, which most systems implement and which is becoming very widespread.
- Wireless LANs can operate at rates up to about 50 Mbps over distances of tens of meters.

Wireless WAN

The third kind of wireless network is used in wide area systems. The radio network used for cellular telephones is an example of a low-bandwidth wireless system. This system has already gone through three generations. The first generation was analog and for voice only. The second generation was digital and for voice only. The third generation is digital and is for both voice and data.

Home Networks

Every device in the home will be capable of communicating with every other device, and all of them will be accessible over the Internet. Many devices are capable of being networked. Some of the more obvious categories (with examples) are as follows

1. Computers (desktop PC, notebook PC, PDA, shared peripherals).
2. Entertainment (TV, DVD, VCR, camcorder, camera, stereo, MP3).
3. Telecommunications (telephone, mobile telephone, intercom, fax).
4. Appliances (microwave, refrigerator, clock, furnace, airco, lights).
5. Telemetry (utility meter, smoke/burglar alarm, thermostat, babycam).

AADHAVAN COLLEGE

Internetworks

An internetwork is formed when distinct networks are interconnected. Many networks exist in the world, often with different hardware and software.

People connected to one network often want to communicate with people attached to a different one. A special kind of machine called **gateway** is used to make the connection and to provide the necessary translation, both in terms of hardware and software.

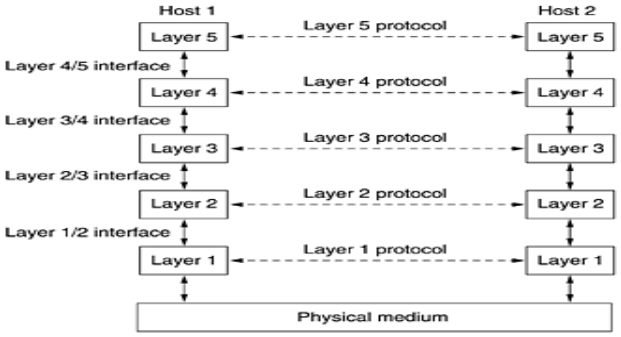
A collection of interconnected networks is called an **internetwork or internet**.

NETWORK SOFTWARE

Protocol Hierarchies

- To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- 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, shielding those layers from the details of how the offered services are actually implemented.
- Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer n protocol.
- Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.
- The entities comprising the corresponding layers on different machines are called **peers**.

Figure 1-13. Layers, protocols, and interfaces.



DHAVAN COLLEGE

No data are directly transferred from layer n on one machine to layer n on another machine. Instead, 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.

Between each pair of adjacent layers is an **interface**. When network designers decide how many layers to include in a network and what each one should do, one of the most important considerations is defining clean interfaces between the layers. The interface defines

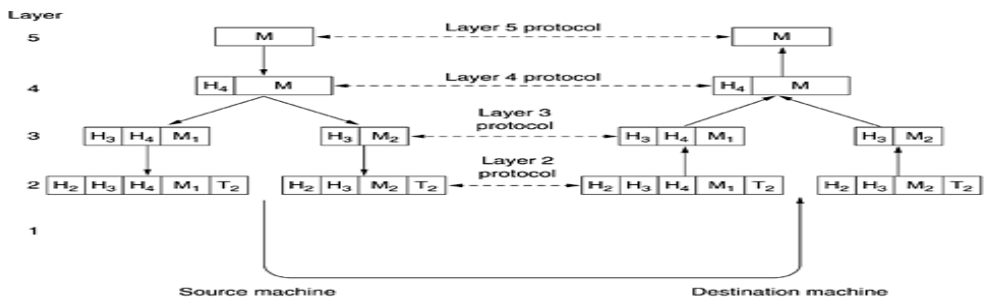
- The primitive operations and services the lower layer makes available to the upper one.
- Minimizing the amount of information that must be passed between layers
- Easy to replace the implementation of one layer with a completely different implementation.

A set of layers and protocols is called **network architecture**. A list of protocols used by a certain system, one protocol per layer, is called a protocol stack.

Information flow in five layer architecture is

- A message, M, is produced by an application process running in layer 5 and given to layer 4 for transmission.
- Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3. The header includes control information, such as sequence numbers, to allow layer 4 on the destination machine to deliver messages in the right order if the lower layers do not maintain sequence.

Figure 1-15. Example information flow supporting virtual communication in layer 5.



ADHAVAN COLLEGE

- In many networks, there is no limit to the size of messages transmitted in the layer 4 protocol, but there is nearly always a limit imposed by the layer 3 protocols.
- Consequently, layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 headers to each packet. In this example, M is split into two parts, M_1 and M_2.
- Layer 3 decides which of the outgoing lines to use and passes the packets to layer 2. Layer 2 adds not only a header to each piece, but also a trailer, and gives the resulting unit to layer 1 for physical transmission.
- At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses.

Design Issues for the Layers

Addressing

Since a network has many computers, some of which have multiple processes, a means is needed for a process on one machine to specify with whom it wants to talk. Every layer needs a mechanism for identifying senders and receivers.

Rules of data transfer

In some systems, data only travel in one direction; in others, data can go both ways. The protocol must also determine how many logical channels the connection corresponds to and what their priorities are. Many networks provide at least two logical channels per connection, one for normal data and one for urgent data.

Error control

Since physical communication circuits are not at all perfect error control is important to implement. Many error-detecting and error-correcting codes are known, but both ends of the connection must agree on which one is being used.

In error control,

- The receiver must have some way of telling the sender which messages have been correctly received and which have not
- Since not all communication channels preserve the order of messages the protocol must make provision for the receiver to allow the pieces to be reassembled properly.

ADHAVAN COLLEGE

Flow control

An issue that occurs at every level is how to keep a fast sender from swamping a slow receiver with data. This is where flow control is employed. Some flow control techniques involve a kind of **feedback** from the receiver to the sender, either directly or indirectly, about the receiver's current situation.

Fragmentation

It is a mechanism for disassembling, transmitting, and then reassembling messages. This is essential to solve problem of inability to accept arbitrarily long messages and too small messages that sending each one separately is inefficient.

Here the solution is to gather several small messages (split if the message is large) heading toward a common destination into a single large message and dismember the large message at the other side.

Multiplexing and De-Multiplexing

Use the same connection for multiple, unrelated conversations is called as multiplexing. Since it is inconvenient or expensive to set up a separate connection for each pair of communicating processes, multiplexing is used.

Multiplexing is needed in the physical layer, for example, where all the traffic for all connections has to be sent over at most a few physical circuits.

Routing

When there are multiple paths between source and destination, a route must be chosen. Sometimes this decision must be split over two or more layers. This topic is called routing.

Connection-Oriented and Connectionless Services

- Layers can offer two different types of service to the layers above them: connection-oriented and connectionless.

Connection-oriented service

- To use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- The essential aspect of a connection is that the order is preserved so that the bits arrive in the order they were sent.

ADHAVAN COLLEGE

- In some cases when a connection is established, the sender, receiver, and subnet conduct a negotiation about parameters to be used, such as maximum message size, quality of service required, and other issues.

Connectionless service

- Each message (letter) carries the full destination address, and each one is routed through the system independent of all the others.
- Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive. However, it is possible that the first one sent can be delayed so that the second one arrives first.

Each service can be characterized by a quality of service. Two types of QOS are reliable and unreliable

- Reliable services never lose data.
- In reliable service receiver acknowledge the receipt of each message so the sender is sure that it arrived.
- In file transfer reliable connection-oriented service is appropriate. (To be sure that all the bits arrive correctly and in the same order they were sent).
- For some applications, the transit delays introduced by acknowledgements are unacceptable. One such application is digitized voice traffic and video conferencing.

Reason for unreliable

- Reliable communication may not be available. (Ex: Ethernet). Packets can occasionally be damaged in transit. It is up to higher protocol levels to deal with this problem.
- The delays inherent in providing a reliable service may be unacceptable, especially in real-time applications such as multimedia.

Unreliable connectionless service

Not all applications require connections, for example electronic junk mail. Unreliable (meaning not acknowledged) connectionless service is often called **datagram service**, which does not return an acknowledgement to the sender.

ADHAVAN COLLEGE

In other situations, the convenience of not having to establish a connection to send one short message is desired, but reliability is essential. The acknowledged datagram service can be provided for these applications.

Still another service is the **request-reply service**. In this service the sender transmits a single datagram containing a request; the reply contains the answer. Request-reply is commonly used to implement communication in the client-server model: the client issues a request and the server responds to it.

	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

Reference models

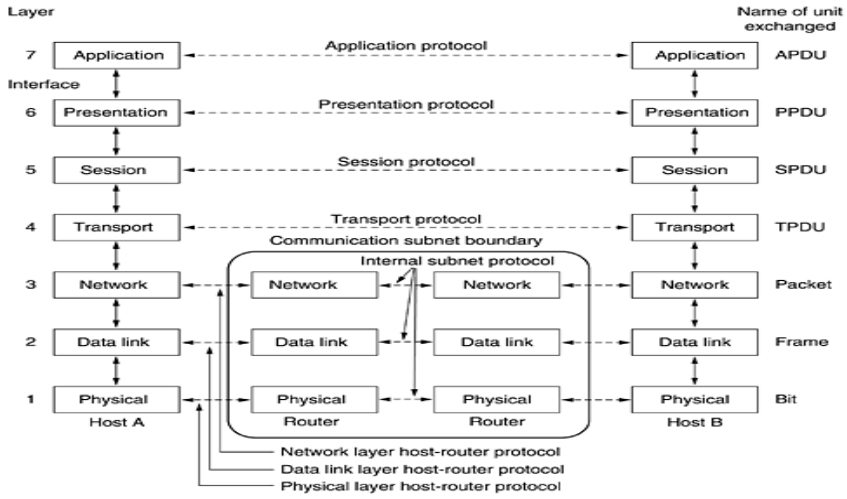
The OSI Reference Model

The OSI model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers. The model 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.

- Layers should be created where abstraction is needed.
- Each layer should perform a well-defined function.
- The function of the layer should be chosen while defining protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- There should not be too many or too few layers.

ADHAVAN COLLEGE

Figure 1-20. The OSI reference model.



Physical layer

- The physical layer is concerned with transmitting raw bits over a Communication channel.
- The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.

Data link layer

- Transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer.
- **Framing**

  Break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmit the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.
- **Flow control**

  Keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment.
- **Error control**

ADHAVAN COLLEGE

- **Medium access control** in Broadcast networks: It is how to control access to the shared channel. A special sub layer of the data link layer, the medium access control sub layer, deals with this problem.

Network layer

The network layer controls the operation of the subnet. Various functions of the network are,

- **Routing:** Determining how to route packets from source to destination. Two types of routing are, *Static routing* (Wont consider current state of network, it is fixed routing) and *Dynamic routing* (consider current state of network)
- **Congestion control**: When too many packets are present in a subnet, it may lead to the state of congestion because of which packets may collide and data may loss. The control of such congestion also belongs to the network layer.
- **Providing Quality of service** (reducing delay, transit time, jitter, etc.) is also a network layer issue.
- **Heterogeneous networks communication** - to allow heterogeneous networks to be interconnected. The factors in which networks differ are packet size, addressing, protocols, architecture, etc.

The Transport Layer

- Accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.
- Determines the type of service to provide to the session layer and to the users of the network.

The Session Layer

- The session layer allows users on different machines to establish sessions between them. Session layer offer various services
  - Dialog control (keeping track of whose turn it is to transmit)
  - Token management (preventing two parties from attempting the same critical operation at the same time),
  - Synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

ADHAVAN COLLEGE

The Presentation Layer

- Concerned with the syntax and semantics of the information transmitted.
- To make computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire."

Application Layer

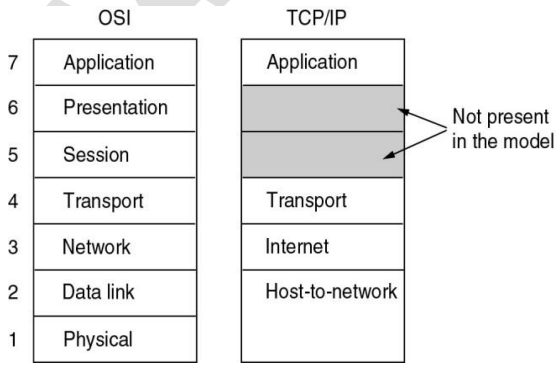
It contains a variety of protocols. Ex: HTTP (Hypertext Transfer Protocol) - the basis for the World Wide Web. Some other protocols are,

- FTP - file transfer.
- SMTP - electronic mail
- NNTP - network news transfer protocol

TCP/IP MODEL

The ARPANET was a research network sponsored by the DoD (U.S. Department of Defense). It eventually connected hundreds of universities and government installations, using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so new reference architecture was needed. This architecture later became known as the TCP/IP Reference Model, after its two primary protocols.

- Host-to-network Layer
- Internet Layer
- Transport Layer
- Application Layer



ADHAVAN COLLEGE

- The host-to-network layer is undefined in the TCP/IP model.
- They leave out all of the underlying layers, leaving the implementation up to whoever creates the network.

Internet layer

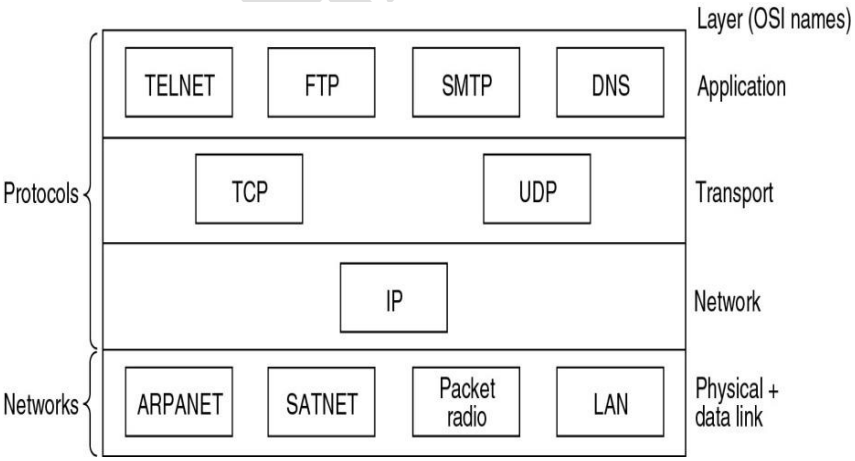
- Functionality to the OSI network layer.
- Responsible for injecting packets into any network and have they travel to their destination.
- Order of arrival is not important
- The internet layer defines an official packet format and protocol called **Internet Protocol (IP).**

Transport layer

- The transport layer is intended to allow two machines to carry on a conversation, just like the OSI transport layer.
- There are two protocols defined for this
  - ✓ TCP (Transmission Control Protocol) -reliable, connection-oriented
  - ✓ UDP (User Datagram Protocol) - unreliable, connectionless
- Flow control

Application layer

This layer contains all of the higher-level protocols as telnet, FTP, SMTP, DNS, NNTP and HTTP



HAVAN COLLEGE

A Critique of the OSI Model

1. Bad timing - Arrived late on the scene
2. Bad technology - Model was too complex and the protocols were flawed (some stuff appears in multiple levels)
3. Bad Implementation - Poor implementation
4. Bad Politics - Poorly marketed

Critiques of TCP/IP reference model

- Does not clearly distinguish the concepts of service, interface, and protocol.
- Not much of a guide for designing new networks using new technologies.
- Not at all general and is poorly suited to describing any protocol stack other than TCP/IP. Example: Trying to use the TCP/IP model to describe Bluetooth, for example, is completely impossible.
- The host-to-network layer is not really a layer. It is an interface (between the network and data link layers).
- Does not distinguish (or even mention) the physical and data link layers. A proper model should include both as separate layers.
- Although the IP and TCP protocols were carefully thought out and well implemented, many of the other protocols were ad hoc

HAVAN COLLEGE

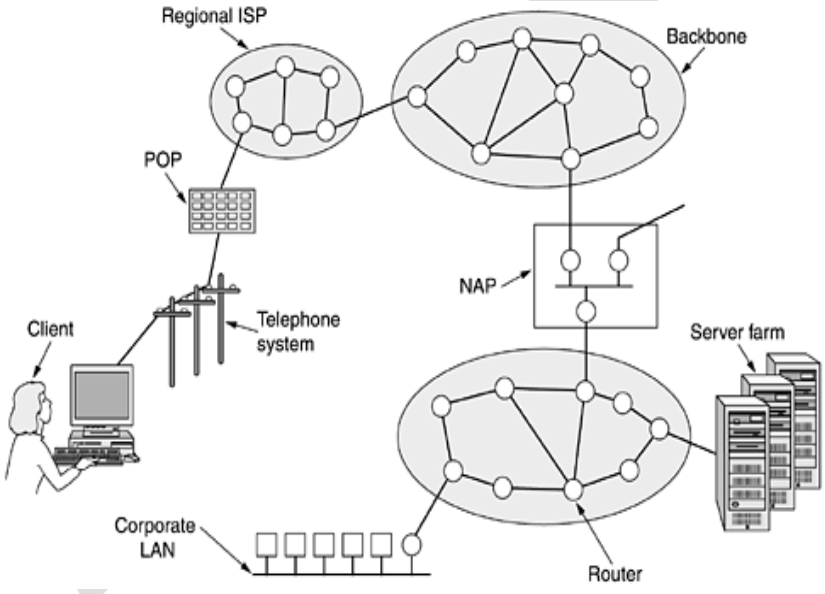
S.No	OSI model	TCP/IP
1	Clearly defined the distinction between services, interfaces and protocols,	TCP/IP model does not.
2	Protocols can easily be replaced	Not easy

3	Supports connectionless and connection-oriented in the network layer, only connection-oriented in the transport layer.	Supports only connectionless in the network layer, both in the transport layer.
4	Developed before invention of protocols (no good idea of which functionality to put in which layer)	Protocols came first, so no problem with protocol fitting the model. But not fit with other protocol stacks.
5	7 layers	4 layers

Note: Service- what the layer does, but not how the layer works. Interface – how to access the services (to layers above)

EXAMPLE NETWORKS

Architecture of internet



- Client calls his or her ISP over a dial-up telephone line.

(The modem is a card within the PC that converts the digital signals the computer produces to analog signals that can pass unhindered over the telephone system).

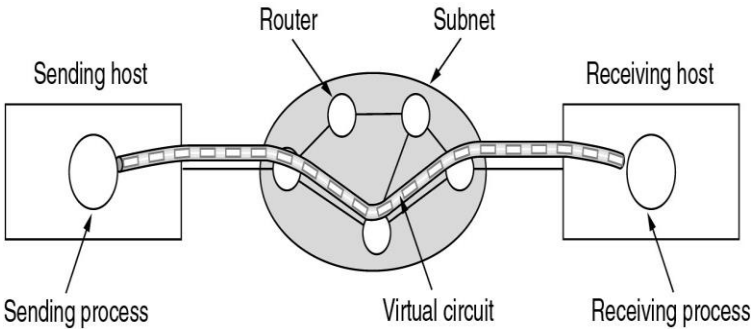
- These signals are transferred to the ISP's POP (Point of Presence), where they are removed from the telephone system and injected into the ISP's regional network**.** From now the system is fully digital and packet switched.
- The ISP's regional network consists of interconnected routers in the various 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.
- Backbone operators companies (AT&T and Sprint) operate large international backbone networks, with thousands of routers connected by high-bandwidth fiber optics.
- Large corporations and hosting services that run server farms (machines that can serve thousands of Web pages per second) often connect directly to the backbone.
  - If a packet given to the backbone is destined for an ISP or company served by the backbone, it is sent to the closest router and handed off there.
  - However, many backbones, of varying sizes, exist in the world, so a packet may have to go to a competing backbone.
  - To allow packets to hop between backbones, all the major backbones connect at the NAPs(Network Access Point)
  - NAP is a room full of routers, at least one per backbone.
  - A LAN in the room connects all the routers, so packets can be forwarded from any backbone to any other backbone.
  - In addition to being interconnected at NAPs, the larger backbones have numerous direct connections between their routers, a technique known as private peering

ATM Network and Reference model

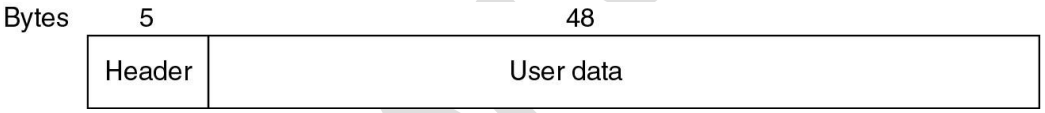
- ATM networks are connection-oriented.
- Sending data requires first sending a packet to set up the connection.
- As the setup packet wends its way through the subnet, all the routers on the path make an entry in their internal tables noting the existence of the connection and reserving whatever resources are needed for it.

ADHAVAN COLLEGE

- Connections are often called **virtual circuits**. Most ATM networks also support permanent virtual circuits, which are permanent connections between two (distant) hosts.
- Each connection, temporary or permanent, has a unique connection identifier.



- Once a connection has been established, either side can begin transmitting data.
- ATM transmits all information in small, fixed-size packets called cells. The cells are 53 bytes long, of which 5 bytes are header and 48 bytes are payload.



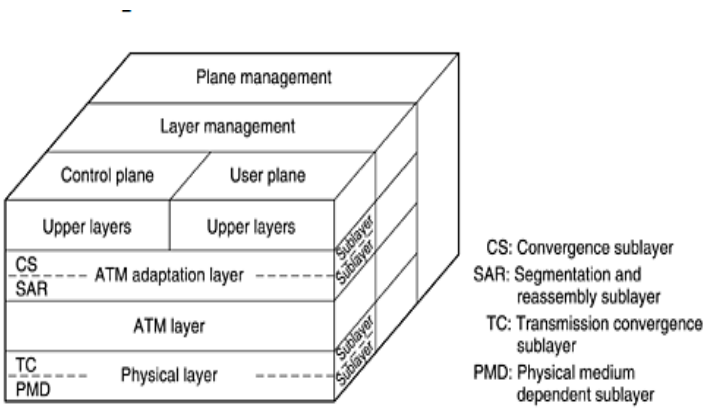
- Part of the header is the connection identifier, so the sending and receiving hosts and all the intermediate routers can tell which cells belong to which connections.
- This information allows each router to know how to route each incoming cell

Reasons for dividing message into cell

- It is easy to build hardware routers to handle short, fixed-length cells at high speed.
- Variable-length IP packets have to be routed by software, which is a slower process.
- The hardware can be set up to copy one incoming cell to multiple output lines (need to broadcast to many receivers).
- Small cells do not block any line for very long, which makes guaranteeing quality of service easier.
- All cells follow the same route to the destination ATM, guarantees to deliver cells in order.

ADHIYAMAN COLLEGE

- The most common speeds for ATM networks are 155 Mbps and 622 Mbps, although higher speeds are also supported.
- The 155-Mbps speed was chosen because this is about what is needed to transmit high definition television.
- The 622 Mbps speed was chosen so that four 155-Mbps channels could be sent over it.



Physical layer

- The physical layer deals with the physical medium: voltages, bit timing, and various other issues. ATM has been designed to be independent of the transmission medium.

ATM layer

- The ATM layer deals with cells and cell transport.
- It defines the layout of a cell and tells what the header fields mean.
- It also deals with establishment and release of virtual circuits.
- Congestion control is also located here.

ATM Adaptation layer

- Because most applications do not want to work directly with cells,
- The AAL layer interface segments the packets, transmits the cells individually, and reassembles them at the other end.
- Thus AAL allow users to send packets larger than a cell.

AADHAVAN COLLEGE

- The user plane

  It deals with data transport, flow control, error correction, and other user functions.
- The control plane

  It deals with connection management.
- The layer and plane management functions relate to resource management and interlayer coordination.

Sublayers

- The physical and AAL layers are each divided into two sublayers
- Convergence sublayer on top that provides the proper interface to the layer above it.
- The PMD (Physical Medium Dependent) sublayer interfaces to the actual cable.

  It moves the bits on and off and handles the bit timing. For different carriers and cables, this layer will be different.

TC (Transmission Convergence) sublayer

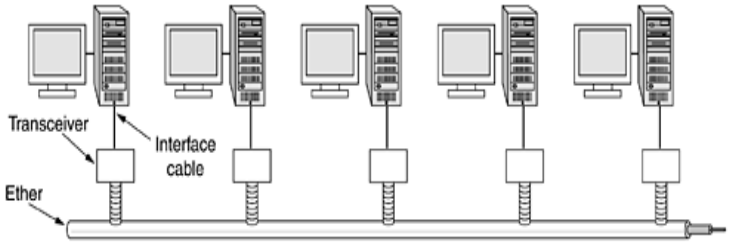
- To convert this bit stream into a cell stream for the ATM layer.
- When cells are transmitted, the TC layer sends them as a string of bits to the PMD layer.
- At the other end, the TC sublayer gets a pure incoming bit stream from the PMD sublayer.
- It handles all the issues related to telling where cells begin and end in the bit stream.

The AAL layer is split into a SAR (Segmentation And Reassembly) sublayer and a CS (Convergence Sublayer).

- The lower sublayer (SAR) breaks up packets into cells on the transmission side and puts them back together again at the destination.
- The upper sublayer (CS) makes it possible to have ATM systems offer different kinds of services to different applications
- (e.g., file transfer and video on demand have different requirements concerning error handling, timing, etc.).

ADHIYAMAN COLLEGE

Ethernet



- The transmission medium is a thick coaxial cable (the ether) up to 2.5 km long (with repeaters every 500 meters).
- 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 multi-drop cable. The system ran at 2.94 Mbps.
- Before transmitting, a computer first listened to the cable to see if someone else was already transmitting. If so, the computer held back until the current transmission finished. Doing so avoided interfering with existing transmissions, giving a much higher efficiency.
- Ethernet continued to develop and is still developing.
- New versions at 100 Mbps, 1000 Mbps, and still higher have come out. Also the cabling has improved, and switching and other features have been added.
- Ethernet (IEEE 802.3) is not the only LAN standard. The committee also standardized a token bus (802.4) and a token ring (802.5).

Token bus

LAN in which the topology was the same as Ethernet (a linear cable) but computers took turns in transmitting by passing a short packet called a token from computer to computer. A computer could only send if it possessed the token, thus avoiding collisions.

This, 802.4 has basically vanished from sight.

Token ring

ADHAVAN COLLEGE

The token was passed around the ring and whichever computer held the token was allowed to transmit before putting the token back on the ring. Unlike 802.4, this scheme, standardized as 802.5, is still in use at some IBM sites, but virtually nowhere outside of IBM sites.

Wireless LAN 802.11

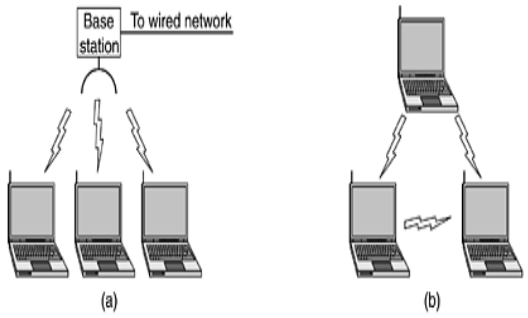
- Finally, the industry decided that a wireless LAN standard.
- The standard it came up with was named 802.11. A common slang name for it is WiFi.

The proposed standard had to work in two modes:

- In the presence of a base station.
- In the absence of a base station.

1. All communication was to go through the base station, called an access point in 802.11 terminology.
2. The computers would just send to one another directly. This mode is now sometimes called ad hoc networking.

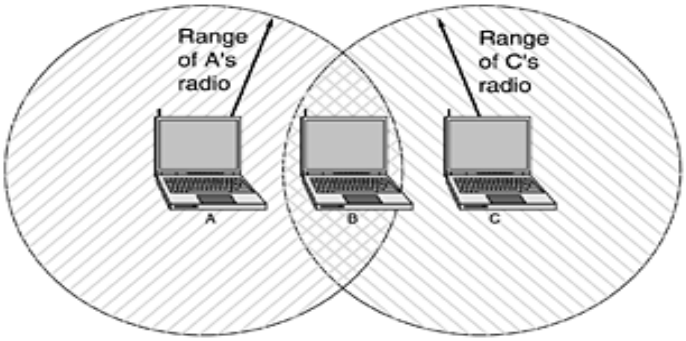
(a) Wireless networking with a base station. (b) Ad hoc networking.



Problems of 802.11

1. A computer on Ethernet always listens to the ether before transmitting. With wireless LANs, that idea does not work so well.

A. COLLEGE



2. 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.

3. The third problem is that a great deal of software is not aware of mobility.

4. If a notebook computer is moved away from the ceiling-mounted base station it is using and into the range of a different base station, some way of handing it off is needed.

AADHAVAN COLLEGE