UG –COMPUTER SCIENCE

V -SEMESTER

COMPUTER NETWORK

Unit - I

INTRODUCTION:

A collection of autonomous computer interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information.

USES OF COMPUTER NETWORK

1. Business application:

Every large and medium-sized company and many small companies are vitally dependent on computerized information. Most companies have customer records, inventories, accounts receivable, financial statements, tax information, and much more online. Computer networks is widely used in the following areas.It can be done by

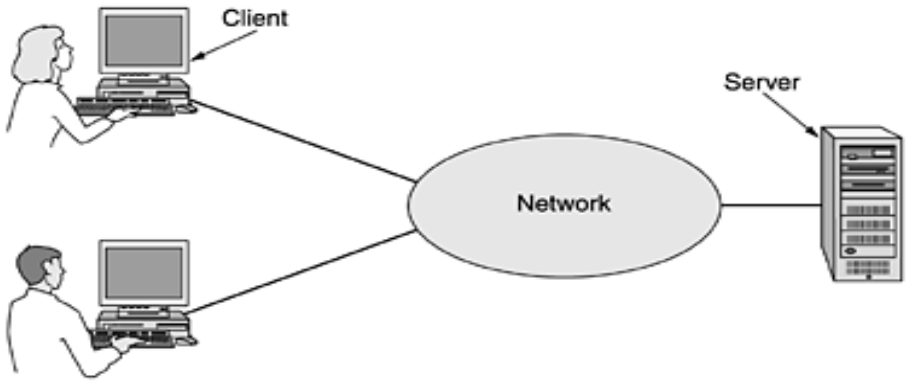
i. Resource sharing
ii. Client server model
iii. Electronic mail

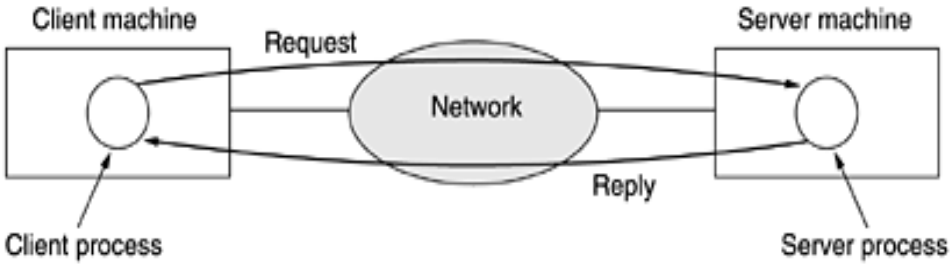
Resource sharing:

The goal is to make all programs, equipment and especially data available to anyone on the network with out regard to the physical location of the resource and the user. The important one is sharing information.

Client server model:

- The simplest of terms one can image a company's information system as consisting of one or more data base and some number of employees who need to access them remotely. In this model, the data are stored on powerful computers called servers.
- Employees have simpler machines called clients on their desk with which they access remote data. This whole arrangement is called client-server model.





Electronic mail:

E-mail which employees generally use for a great deal of daily communication. Many companies provide catalogs of their goals and services online and take orders on line. It is called E-commerce.

2. Home application:

People buy computers for internet access. Some of the more popular uses of the internet for home users are as

i. Access to remote information
ii. Person to Person communication
iii. Entertainment
iv. Electronic commerce

Access to remote information:

It can be surfing the WWW for information. Information available includes the arts, business, working, government, health, history, hobbies, recreation, science, sports, travel and etc…

Person to Person communication:

It is classified in to three ways

*** Instant messaging:**

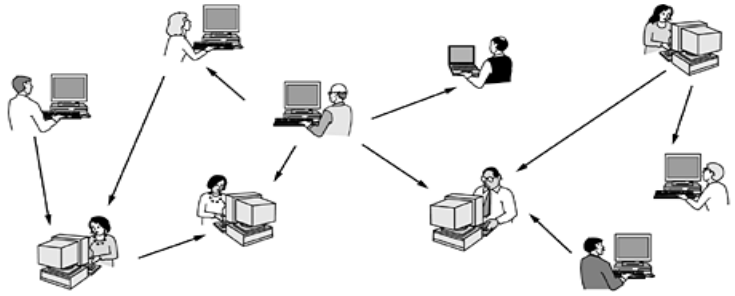
Two people to type messages at each other in real time.

***Chat room:**

A multiperson and a group of people can type messages for all to see.

***Peer-to-Peer communication**:

Each and Every person can in principle communicate with one or more other people, there is no fixed division in to client and servers.



Entertainment:

It is a huge and growing industry. The killer application here is video on demand. On the other hand, may be the killer application will not be video and demand may be it will be game playing.

Electronic commerce:

It is for a home shopping, it is used to pay their bills, manage the bank accounts, and handle their investments electronically.

Tag	Full name	Example
B2C	Business- to- consumer	Ordering books online
B2B	Business- to- business	Car manufacturer ordering tires for supplier
G2C	Government-to- consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on line
P2P	Peer-to-peer	File sharing

3. Mobile users:

Such as notebook computers and personal digital assistance (PDAs), are one of the fastest growing segments of the computer industry. Although wireless networking and mobile computing are often related, they are not identical.

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

4. Social issues:

1. Bulletin boards whereby people can exchange messages with like minded individuals.
2. Another fun area is employee rights verses employer rights.

NETWORK HARDWARE.

There are two types of transmission technology that are in wide spread use. They are

1. Broadcast links

2. Point-to-point links

Broadcast networks:

- It is generally also allow the possibility of addressing a packet to all dimensions by using a special code in the address field. When a packet with this code is transmitted it is received and processed by every machine on the network.
- This mode of operation is called broadcasting. Some broadcast systems also support transmission to a subset of the machines, something known as multicasting.

Point-to-point networks:

- It consists of many connections between individual pairs of machines. To go from the source to the destination, a packet on this type of network may have to first visit one or more intermediate machines. Often multiple routes of different lengths are possible.
- As a general rule, smaller, geographically localized networks tend to use broadcasting, where as layer networks usually are point-to-point. This transmission with one sender and one receiver is sometimes called unicasting.

The types of networks are:

1. Local Area Network (LAN):

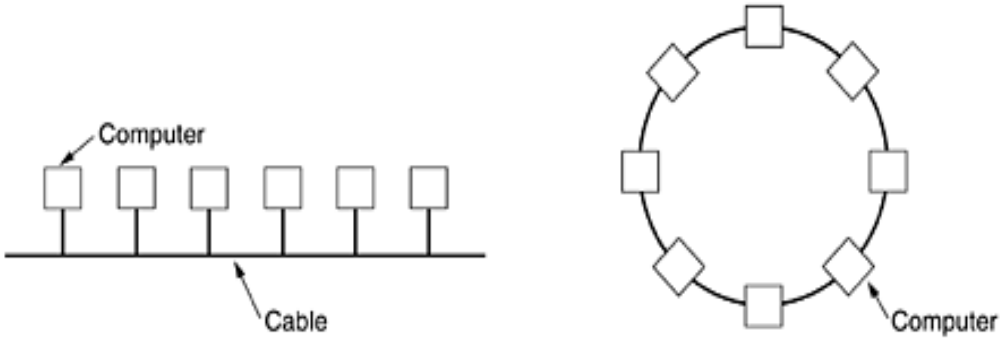
- Local area network generally called LANs are privately owned networks within a single building or campus of upto a few kilometers in size.
- Its widely used to connect personal computers and workstations in company offices and factories to share resources and exchange information.
  LANs are distinguished from other kinds of networks by three characteristics.
  1. Their size
  2. Their transmission technology
  3. Their topology.

Various topologies are possible for broadcast LANs.

Ex:

a. Bus topology
b. Ring topology

- In a bus network, at any instant atmost one machine is the master and is allowed to transmit. It based broadcast network with decentralize control, usually operating at 10 Mbps to 10 Gbps.
- In a ring network, each bit propagates around on its own, not waiting for the rest of the packet to which it belong.

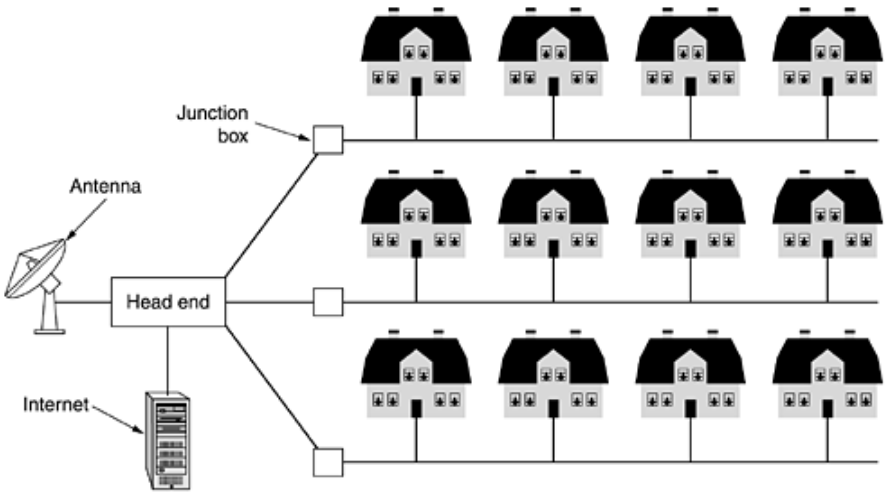


(a) (b)

BUS TOPOLOGY **RING TOPOLOGY**

2. Metropolitan Area Networks (MAN):

A metropolitan area network or MAN covers a city. Ex: cable television network available in many cities. A MAN might look something like the systems shown in the figure.



3. Wide Area Networks (WAN):

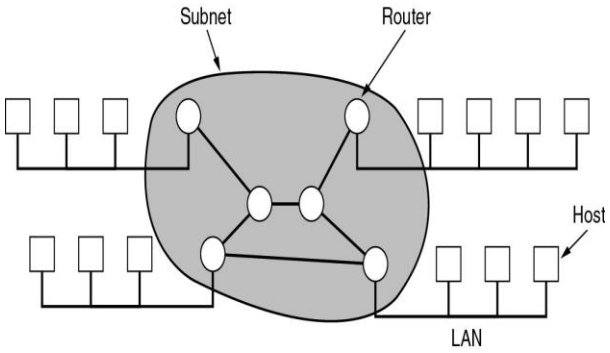
- WAN, spans a large geographical area often a country or continent. It contains a collection of machines intended for running user/application programs. These machines are called as hosts. The hosts are connected by communication subnet or short subnet.

WAN consists of two distinct components:

- Transmission lines:
- Move bits between machines they can be made of copper wire, optical fiber, or even radio links.

Switching elements:

- When data arrive on a incoming line, the switching element must choose an outgoing line on which to forward them. These switching elements are named as router.
- Each host is frequently connected to a LAN on which the router is present. A host can be connected directly to a router. The collection of communication lines and routers from the subnet.



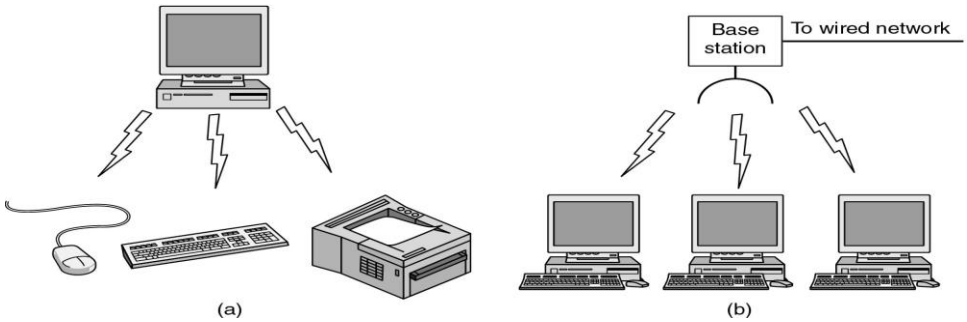
4. Wireless Networks:

It can be divided into three main categories.

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

i) System interconnection:

- It is all about interconnecting the components of a computer using short-range radio. Some companies get together to design a short range of wireless network called Bluetooth to connect these components without wires. No cables, no driver installation.



2) Wireless LAN:

In which every computer has a modem and antenna with which it can communicate with other systems. The system can communicate directly with one another in a peer-to-peer configuration. It becoming common in small offices and homes.

3)Wireless WAN:

- It 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.
  1st → Analog (voice only)
  2nd → Digital (voice only)
  3rd → Digital (voice and data).

5. Home networks:

The fundamental idea is that in the future most homes will be setup in the networking. Every device in the home will be capable of communicating with every other device and all of them will be accessible over the internet.

1. Computers(desktop PC, notebook PC, PDA)
2. Entertainment (TV, DVD, etc…)
3. Telecommunications (telephone, mobile, etc…)
4. Appliances (microwave, clock)
5. Telemetry (utility meter, baby cam)

Properties of Home network:

- Easy to install, Low cost
- The network and devices have to be foolproof in the operation.
- The main application is lightly to involve multimedia, to the network needs sufficient capacity.

- It must be possible to stop with one or more devices and expand the reach of the network gradually.
- Security and reliability

6. Internetworks:

- A collection of interconnected networks is called an internetwork or internet. A common form of internet is a collection of LAN connected by a WAN. If the system with in the gray area contains only routers, it is a subnet, if it contains both routers and hosts it is a WAN.
- Subnets, networks and internetworks are often confused. The combination of the subnet and its host forms a network. In the case of LAN, the cable and the hosts form the network.

NETWORK SOFTWARE

The network software deals with the following

- Protocol hierarchies
- Design issues for the layers
- Connection- oriented and Connectionless services
- Service primitives
- The relationship of services to protocols

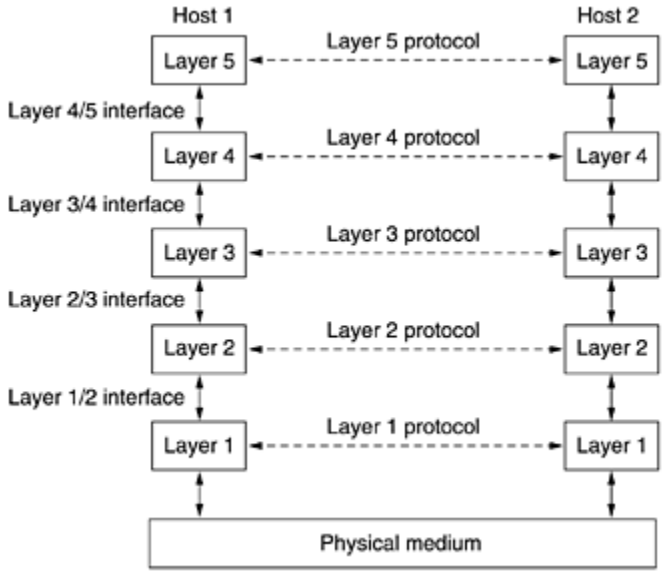
a) Protocol hierarchies:

- To reduce the design complexities, 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.

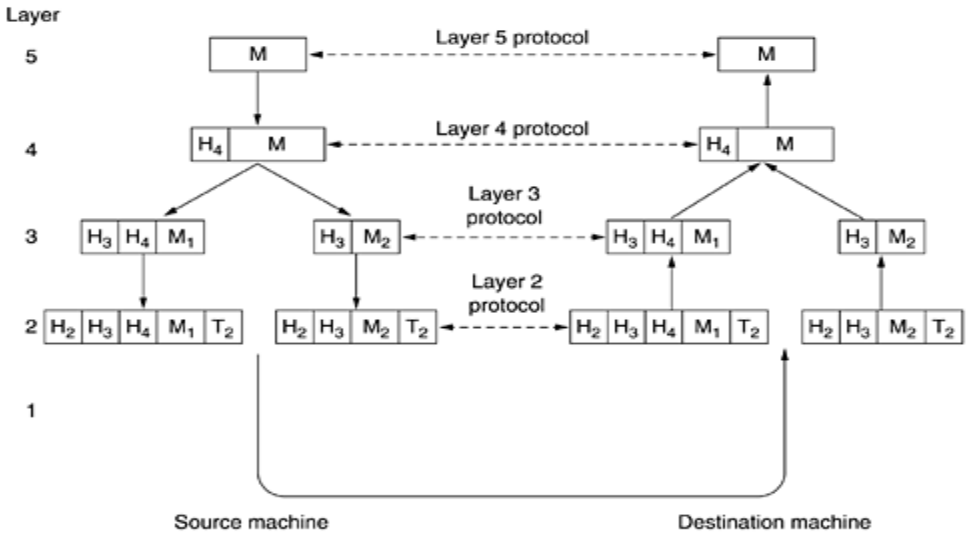
- Each layer is a kind of virtual machine, offering certain services to layer above it.

Protocol:

- It is an agreement between the communicating parties on how communication is to proceed. A five layer network is illustrated in the following figure. The entities comprising the corresponding layers on different machines are called peers.
- The peers may be process hardware devices, or even human beings. Each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below the layer 1 is the physical medium through which actual communication occurs.



- The interface defines which primitive operations and services the lower layer makes available to the upper one. A set of layers and protocols is called network architecture.A list of protocols is used by a certain systems, one protocol per layer is called protocol stack.
- The above fig shows how to provide communication to the top layer of the five layer network as in the figure. 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 the 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



Design issues for the Layers:

- Every layer needs a mechanism for identifying senders and receivers. Since a network normally has many computers, some of which have multiple processes, a means is needed for a process on one machine to specify to with whom it wants to talk.
- Many networks provide at least two logical channels per connection, one for normal data and one for urgent data.

Connection-oriented and connectionless services:

Layers can offer two different types of services to the layers above them

1. Connection-oriented service:

It is modeled after the telephone system. To use a connection oriented network service, first establish a connection, use the connection and then release the connection.

Ex: Telephone

- To talk to someone, you pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- 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. Typically, one side makes a proposal and the other side can accept it, reject it.

2. Connectionless service:

It is modeled after the postal system. Each message carries the full destination address; 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.

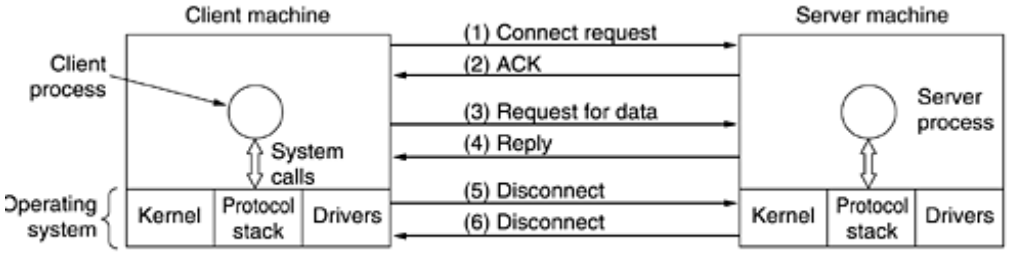
	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Service Primitives:

- A service is formally specified by a set of primitives available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, the primitives are normally system calls.
- The set of primitives available depends on the nature of the service being provided. The primitives for connection- oriented service are different from those of connectionless service.

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. A common way to implement LISTEN is to make it a blocking system call.
- The client process executes CONNECT to establish a connection with the server. The CONNECT call needs to specify who to connect to, so it might have a parameter giving a server's address.

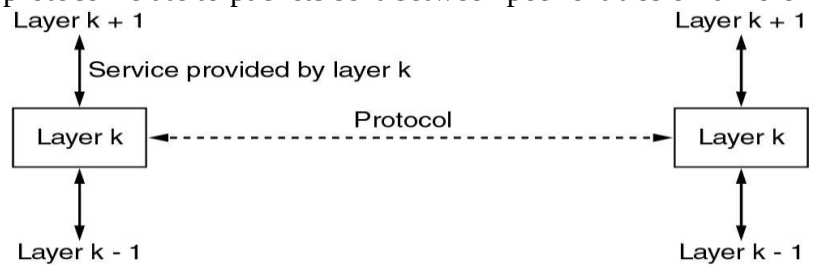


- The operating system sends a packet to the peer asking it to connect, as shown by (1) in fig. The client process is suspended until there is a response. When the packet arrives at the server, it is processed by the OS there.

- When the system sees that the packet is requesting a connection, it checks to see if there is a listener. At this point, the client and server are both running and they have a connection established.
- The next step is to execute RECEIVE to prepare, to accept the first request. Normally the server does this immediately upon being released from the LISTEN, before the acknowledgement can get back to the client. The RECEIVE call blocks the server.
- Then the client executes SEND to transmit its request (3).
- If the client has additional request, it can make them now. If it is done, it can 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.

The Relationships of Services to Protocols:

- A service is a set of primitives that a layer provides to the layer above it. The service defines what operation the layer is prepared to perform on behalf of its users, but it says nothing at all how these operations are implemented.
- 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. In contrast protocol relate to packets sent between peer entities on different machines.



An analogy with programming language is worth making. A service is like an abstract data type or an object in an object-oriented language.

REFERENCE MODELS

Two important network architectures, the OSI reference model and the TCP/IP Reference model.

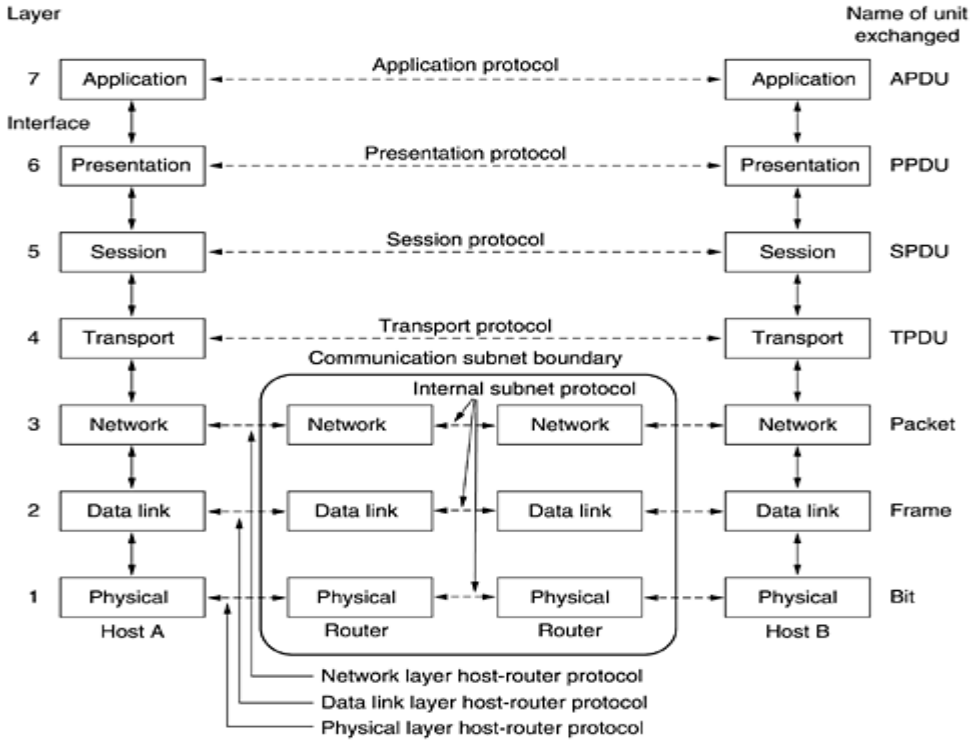
OSI Reference Model.

This model is called the ISO-OSI (Open Systems Interconnection) Reference Model, because it deals with connecting open systems. The OSI model has seven layers.

Principles applied to arrive at the seven layers like

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.

5. The number of layers should be large enough that distinct functions need not be thrown together.



1)The Physical Layer:

- ❖ It 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 1 bit, not as a 0 bit.

The Data Link Layer:

- ❖ The main task of the data link layer is to take a raw transmission facility and transform it into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break the input data into data frames.

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.
- ❖ Routes can be based on static tables that are "wired into" the network and rarely changed.

The Transport Layer:

- ❖ It is to accept data from the session layer, split it upto smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. It determines what type of service to provide the session layer.
- ❖ The most popular type of transport connection is an error free point- to- point channel that delivers messages or bytes in the order in which they were sent.

The Session Layer:

- ❖ It allows users on different machines to establish sessions between them. A session offers various services, including dialog control, token management and synchronization.

The Presentation Layer:

- ❖ It is concerned with the syntax and semantics of the information transmitted. This layer manages this abstract data structures and also higher level data structures to be defined and exchanged.

The Application Layer:

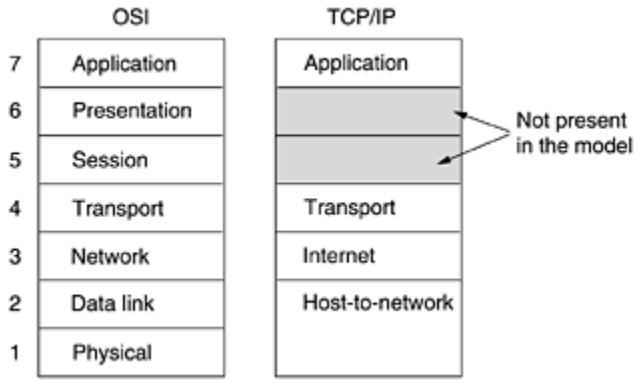
- ❖ It contains a variety of protocols that are commonly needed by users. One widely used application protocol is HTTP, which is the basis for the www. When a browser wants a webpage , it sends a name of the page, it wants to the server using HTTP.
- ❖ The server then sends the page back. Other application protocols are used for file transfer, E-mail and network news.

TCP/IP Reference Model.

- ❖ The ability to connect multiple networks together in a seamless way was one of the major design goals from the very beginning. This architecture later become known as TCP/IP reference model after its two primary protocols.

a) The Internet Layer:

- ❖ All these requirements led to the choice of an packets in which network based on the connectionless internet work layer. This layer called the internet layer is the linchpin that holds the whole architecture together.
- ❖ 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.

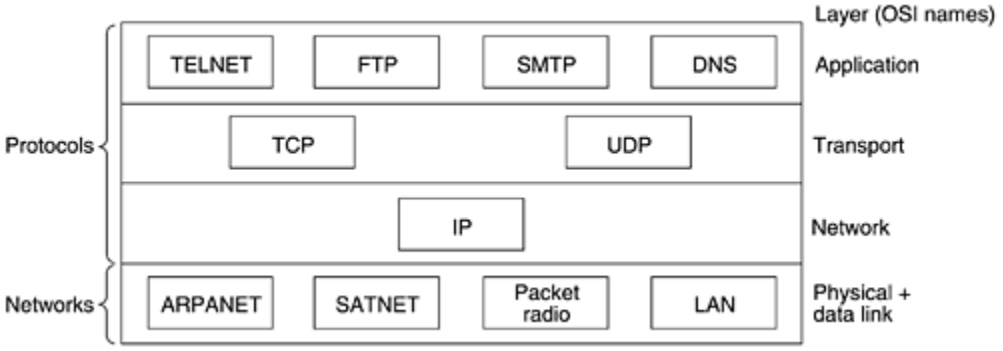


b)The Transport Layer:

- ❖ It is designed to allow peer entities on the source and destination hosts to carry on a conversation, the same as in the OSI transport layer. Two end-to-end protocols have been defined here.

1. 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 the internet layer.

2. UDP (User Datagram Protocol), is unreliable, connectionless protocols for applications that do not want TCP's sequencing or flow control and wish to provide their own.



c) The Application Layer:

- ❖ It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP).
- ❖ The FTP provides a way to move data efficiently from one machine to another.
- ❖ Domain Naming Service (DNS), for mapping host name on to the network addresses.
- ❖ NNTP, the protocol for moving USENET new articles around and HTTP, the protocol for fetching pages on the www and many others.

d) The Host-to-Network Layer:

- ❖ Point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and various from host to host and network to network.

THE PHYSICAL LAYER

- ❖ Three kinds of transmission media: guided (copper wire and fiber optics), wireless (terrestrial radio), and satellite.

THE THEORETICAL BASIS FOR DATA COMMUNICATION

- ❖ Information can be transmitted on wires by varying some physical property such as voltage or current. By representing the value of this voltage or current as a single-valued function of time, f(t),

Fourier Analysis

- ❖ Periodic function, g(t) with period T can be constructed as the sum of a (possibly infinite) number of sines and cosines:

Equation 2

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

- ❖ where f = 1/T is the fundamental frequency, an and bn are the sine and cosine amplitudes of the nth harmonics (terms), and c is a constant. Such a decomposition is called a Fourier series.

- A data signal that has a finite duration (which all of them do) can be handled by just imagining that it repeats the entire pattern over and over forever (i.e., the interval from T to 2T is the same as from 0 to T, etc.).
- The an amplitudes can be computed for any given g(t) by multiplying both sides of Eq. (2-1) by sin(2pkft) and then integrating from 0 to T. Since

$$\int_0^T \sin(2\pi kft)\,\sin(2\pi nft)\,dt \;=\; \begin{cases} 0 \text{ for } k \neq n \\ T/2 \text{ for } k = n \end{cases}$$

- Similarly, by multiplying Eq. (2-1) by cos(2pkft) and integrating between 0 and T, we can derive b.n By just integrating both sides of the equation as it stands, we can find c. The results of performing these operations are as follows:

$$a_n = \frac{2}{T}\int_0^T g(t)\sin(2\pi nft)\,dt \qquad b_n = \frac{2}{T}\int_0^T g(t)\cos(2\pi nft)\,dt \qquad c = \frac{2}{T}\int_0^T g(t)\,dt$$

Bandwidth-Limited Signals

- **Fig. 2-1(a)].** Unfortunately, all transmission facilities diminish different Fourier components by different amounts, thus introducing distortion. The range of frequencies transmitted without being strongly attenuated is called the bandwidth.
- **Figure 2-1(b)** shows the signal that results from a channel that allows only the first harmonic (the fundamental, f) to pass through.
- **Fig. 2-1(c)-(e)** show the spectra and reconstructed functions for higher-bandwidth channels.Given a bit rate of b bits/sec, the time required to send 8 bits .1 bit at a time is 8/b sec

$$a_n = \frac{1}{\pi n}[\cos(\pi n/4) - \cos(3\pi n/4) + \cos(6\pi n/4) - \cos(7\pi n/4)]$$

$$b_n = \frac{1}{\pi n}[\sin(3\pi n/4) - \sin(\pi n/4) + \sin(7\pi n/4) - \sin(6\pi n/4)]$$

$$c = 3/4$$

Figure 2-1. (a) A binary signal and its root-mean-square Fourier amplitudes. (b)-(e) Successive approximations to the original signal.

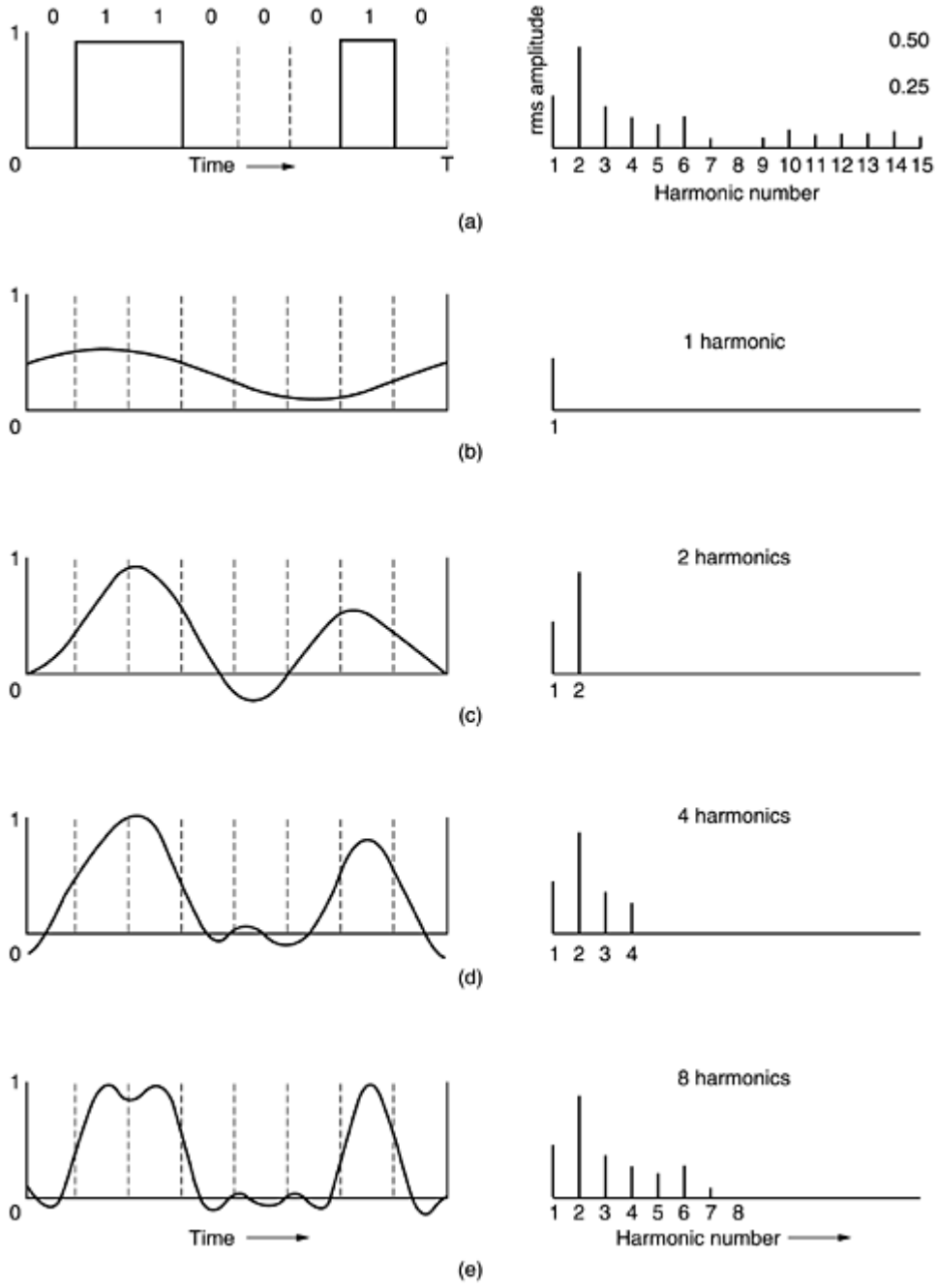


Figure 2-2. Relation between data rate and harmonics.

Bps	T (msec)	First harmonic (Hz)	# Harmonics sent
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
2400	3.33	300	10
4800	1.67	600	5
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0

The Maximum Data Rate of a Channel

maximum data rate = $2H \log_2 V$ bits/sec

maximum number of bits/sec = $H \log_2 (1 + S/N)$

- ❖ the maximum data rate of a noisy channel whose bandwidth is H Hz, and whose signal-to-noise ratio is S/N, is given by
- ❖ noiseless 3-kHz channel cannot transmit binary (i.e., two-level) signals at a rate exceeding 6000 bps.

GUIDED TRANSMISSION MEDIA

- ❖ The purpose of the physical layer is to transport a raw bit stream from one machine to another. Various physical media can be used for the actual transmission.
- ❖ Each one has its own bandwidth, delay, cost, and ease of installation and maintenance. Media are roughly grouped into guided media, such as copper wire and fiber optics, and unguided media.

A) Magnetic Media

- ❖ One of the most common ways to transport data from one computer to another is to write them onto magnetic tape or removable media,physically transport the tape or disks to the destination machine, and read them back in again.

B) Twisted Pair

- ❖ One of the oldest and still most common transmission media is twisted pair. The most common application of the twisted pair is the telephone system.
- ❖ Nearly all telephones are connected to the telephone company office by a twisted pair. Twisted pairs can run several kilometers without amplification, but for longer distances, repeaters are needed.
- ❖ It can be used for transmitting either analog or digital signals. The bandwidth depends on the thickness of the wire and the distance traveled. Twisted pair cabling comes in several varieties, two of which are important for computer networks.

Category 3:

- ❖ It consists of two insulated wires gently twisted together. Four such pairs are typically grouped in a plastic sheath to protect the wires and keep them together.

Category 5:

- ❖ It's more advanced, which results in less crosstalk and a better-quality signal over longer distances, making them more suitable for high-speed computer communication.
- ❖ All of these wiring types are often referred to as UTP (Unshielded Twisted Pair), to contrast them with the bulky, expensive, shielded twisted pair cables.

(a) (b)

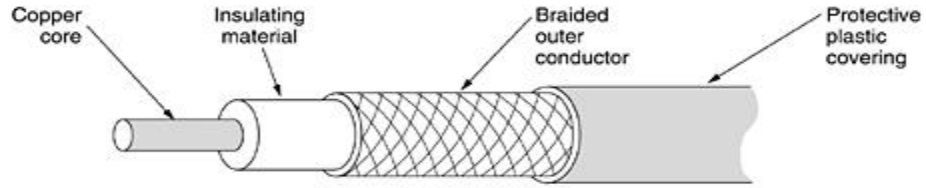
C) Coaxial Cable:

It has better shielding than twisted pairs, so it can span longer distances at higher speeds.

Two kinds of coaxial cable

50-ohm cable → for digital transmission
75-ohm cable → for analog and cable television

- A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely-woven braided mesh.
- The outer conductor is covered in a protective plastic sheath. A cutaway view of a coaxial cable is shown in Fig.

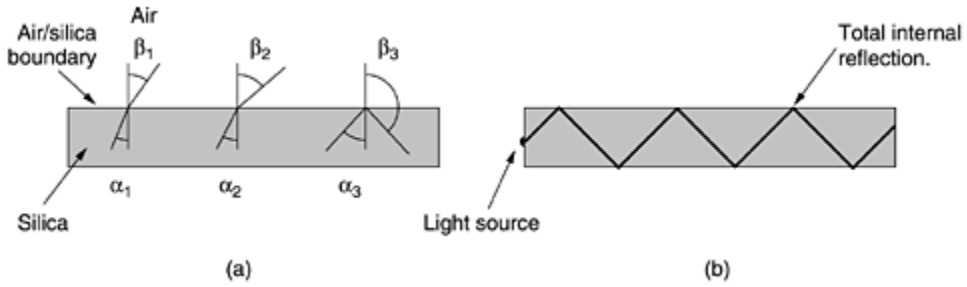


D) Fiber optics:

An optical transmission system has three key components:

1. The light source
2. The transmission medium
3. Detector.

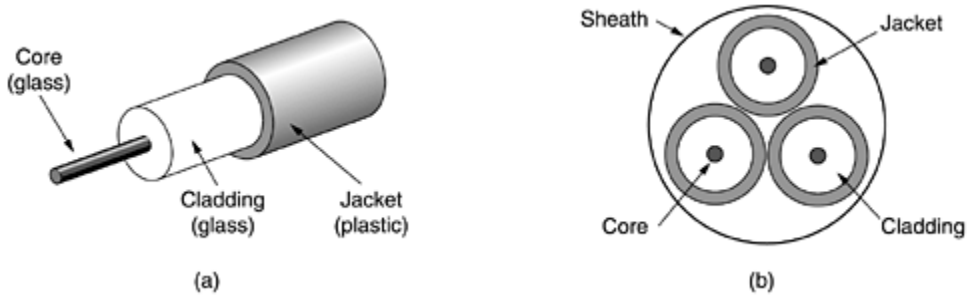
- A pulse of light indicates a 1 bit and the absence of light indicates a 0 bit. The transmission medium is an ultra-thin fiber of glass. The detector generates an electrical pulse when light falls on it.



- Each ray is said to have a different mode, so a fiber having this property is called a multimode fiber.
- However, if the fiber's diameter is reduced to a few wavelengths of light, the fiber acts like a wave guide, and the light can propagate only in a straight line, without bouncing, yielding a single-mode fiber.

E) Fiber Cables:

- It is similar to coax, except without the braid. Fig(a) shows a single fiber viewed from the side. At the center is the glass core through which the light propagates.
- In multimode fibers, the core is typically 50 microns in diameter.

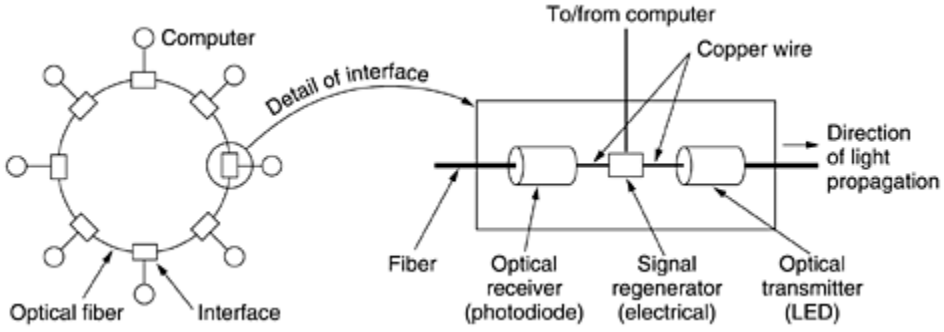


- The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core. Next comes a thin plastic jacket to protect the cladding. Fibers are typically grouped in bundles, protected by an outer sheath.
- Two kinds of light sources are typically used to do the signaling. LEDs and semiconductor lasers. They have different properties

Item	LED	Semiconductor laser
Data rate	Low	High
Fiber type	Multimode	Multimode or single mode
Distance	Short	Long
Lifetime	Long life	Short life
Temperature sensitivity	Minor	Substantial
Cost	Low cost	Expensive

F) Fiber Optic Networks:

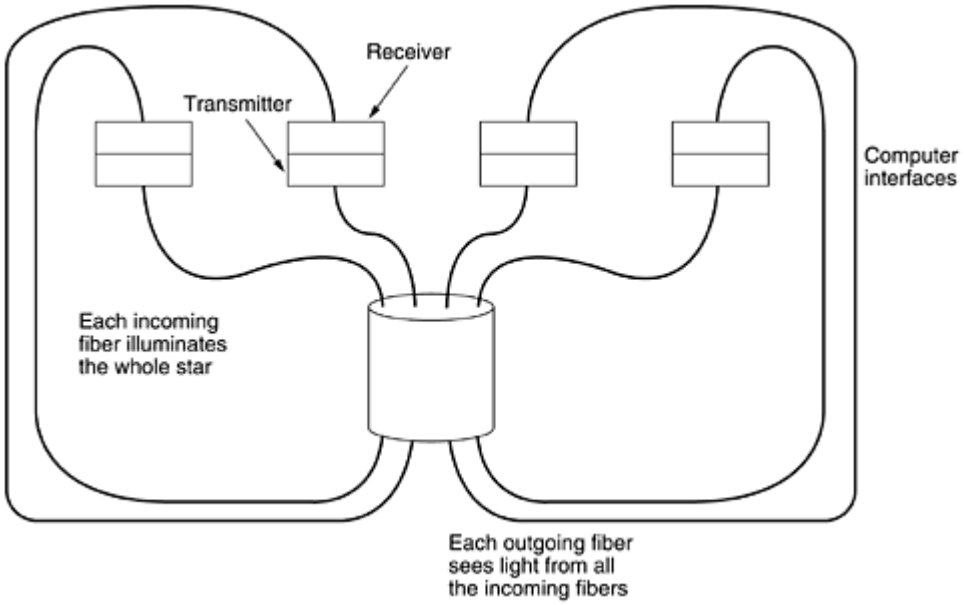
- It can be used for LANs as well as for long-haul transmission, although tapping into it is more complex than connecting to an Ethernet.
- One way around the problem is to realize that a ring network is really just a collection of point-to-point links.



Two types of interfaces are used.

- A passive interface consists of two taps fused onto the main fiber. One tap has an LED or laser diode at the end of it (for transmitting), and the other has a photodiode.

- ❖ The incoming light is converted to an electrical signal, regenerated to full strength if it has been weakened, and retransmitted as light.
- ❖ The interface with the computer is an ordinary copper wire that comes into the signal regenerator.



Comparison of Copper wire and Fiber Optics

1. Fiber has many advantages; it can handle much higher bandwidths than copper.
2. Fiber also has the advantage of not being affected by power surges, electromagnetic interference, or power failures.
3. Fibers do not leak light and are quite difficult to tap.
4. Fiber is a less familiar technology requiring skills not all engineers have, and fibers can be damaged easily by being bent too much.
5. Finally, fiber interfaces cost more than electrical interfaces.

WIRELESS TRANSMISSIONS

Two kinds of communication

(i) Fiber.
(ii) Wireless.

Types of wireless transmission:

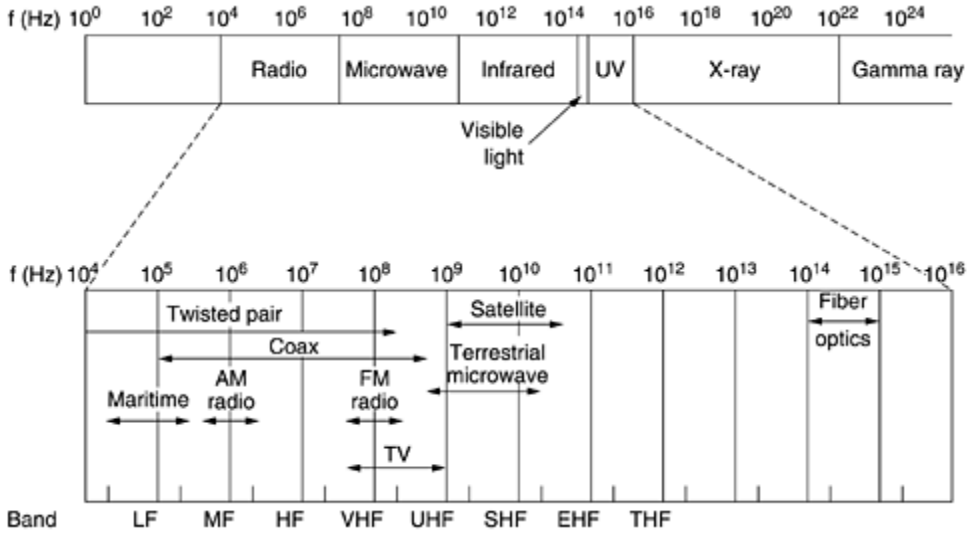
1. The electro magnetic spectrum
2. Radio transmission
3. Microwave transmission
4. Infrared and millimeter waves
5. Light wave transmission.

The Electromagnetic Spectrum:

- In this when electrons move, they create electromagnetic waves that can propagate through space (even in a vacuum). The number of oscillations per second of a wave is called its frequency, f, and is measured in Hz.
- The distance between two consecutive maxima is called the wavelength, which is universally designated by the Greek letter □ (lambda).

The fundamental relation between f, l, and c (in vacuum) is

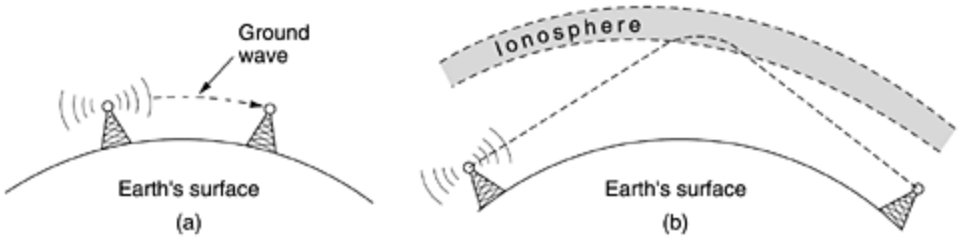
$$\lambda f = c$$



- Since c is a constant, if we know f, we can find □, and vice versa.
- The radio, microwave, infrared, and visible light portions of the spectrum can all be used for transmitting information by modulating the amplitude, frequency, or phase of the waves.
- The terms LF, MF, and HF refer to low, medium, and high frequency, respectively. Higher bands were later named the Very, Ultra, Super, Extremely, and Tremendously High Frequency bands.

Radio Transmission

- It is easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.
- It can travel in all directions from the source. In the VLF, LF, and MF bands, radio waves follow the ground, as in Fig(a). These waves can be detected for perhaps 1000 km at the lower frequencies, less at the higher ones.
- AM radio broadcasting uses the MF band, which is why the ground waves from Boston AM radio stations cannot be heard easily in New York.
- In the HF and VHF bands, the ground waves tend to be absorbed by the earth. However, the waves that reach the ionosphere under certain atmospheric conditions, the signals can bounce several times



Microwave Transmission:

- ❖ It travels in a straight line, if the towers are too far apart; the earth will get in the way unlike radio waves at lower frequencies, microwaves do not pass through buildings well.
- ❖ It is so widely used for long-distance telephone communication, mobile phones, television distribution, and other uses that a severe shortage of spectrum has developed.

Advantages of microwave:

- ❖ No right of way is needed and by buying a small part of ground every 50 km and putting a microwave tower on it, one can bypass the telephone system and communicate directly.
- ❖ It is also relatively inexpensive.
- ❖ It is cheaper than leasing the telephone company's fiber.

Infrared and Millimeter Waves:

- ❖ Both are used for short-range communication. The remote controls used on televisions, VCRs, and stereos all use infrared communication.

Advantages:

a. Directional
b. Cheap
c. Easy to build

Drawback:

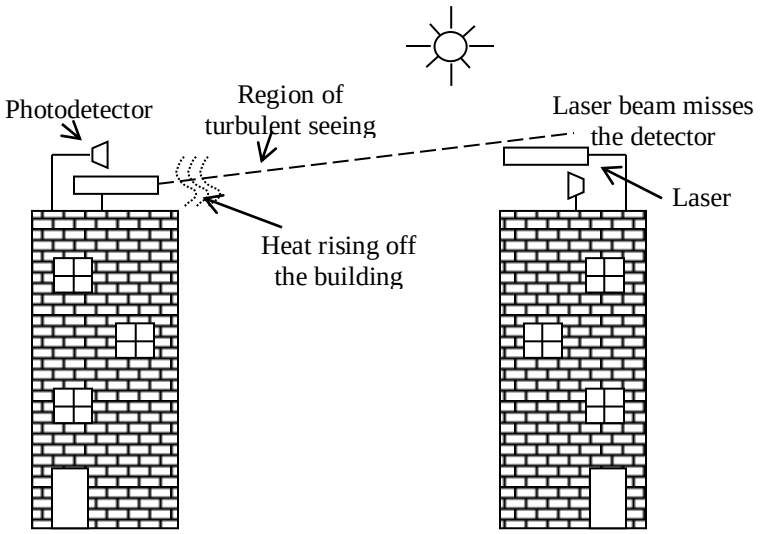
a. They do not pass through solid objects.
b. Infrared waves do not pass through solid walls well is also a plus.

Light wave Transmission:

- ❖ A more modern application is to connect the LANs in two buildings via lasers mounted on their rooftops.
- ❖ Coherent optical signaling using lasers is inherently unidirectional, so each building needs its own laser and its own Photodetector.

Advantages:

- ❖ It offers very high bandwidth
- ❖ Very low cost.
- ❖ Easy to install



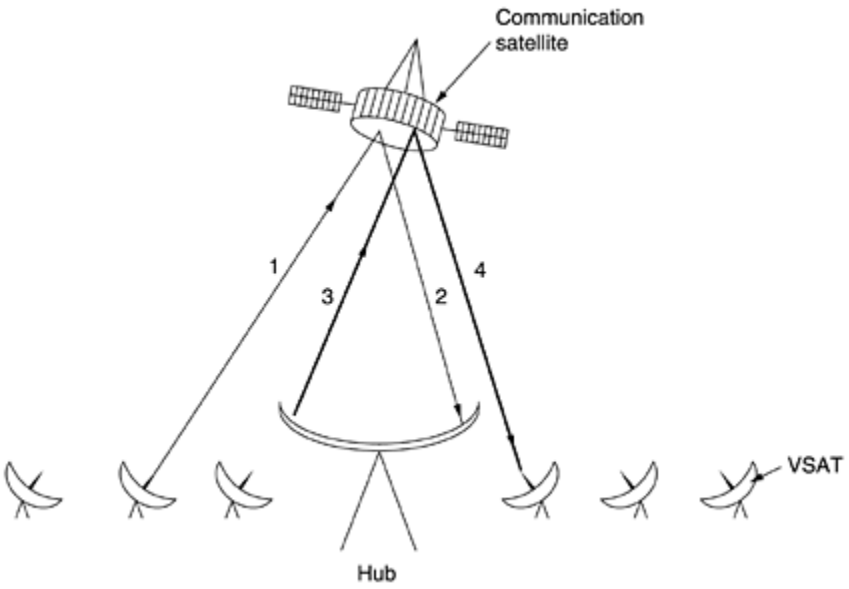
- Unlike microwave, does not require an FCC license.

COMMUNICATION SATELLITES.

- A communication satellite can be thought of as a big microwave repeater in the sky.
- It contains several transponders, each of which listens to some portion of the spectrum, amplifies the incoming signal, and then rebroadcasts it at another frequency to avoid interference with the incoming signal.

A) Geostationary Satellites:

- The first artificial communication satellite, Telstar, was launched in July 1962. Since then, communication satellites have become a multibillion dollar business and the only aspect of outer space that has become highly profitable. These high-flying satellites are often called GEO (Geostationary Earth Orbit) satellites.
- A new modern communication satellite world is the development of low-cost microstations, sometimes called VSATs (Very Small Aperture Terminals). These tiny terminals have 1-meter or smaller antennas (versus 10 m for a standard GEO antenna) and can put out about 1 watt of power.



- In many VSAT systems, the microstations do not have enough power to communicate directly with one another. Instead, a special ground station, the hub, with a large, high-gain antenna is needed to relay traffic between VSATs.

Figure 2-16. The principal satellite bands.

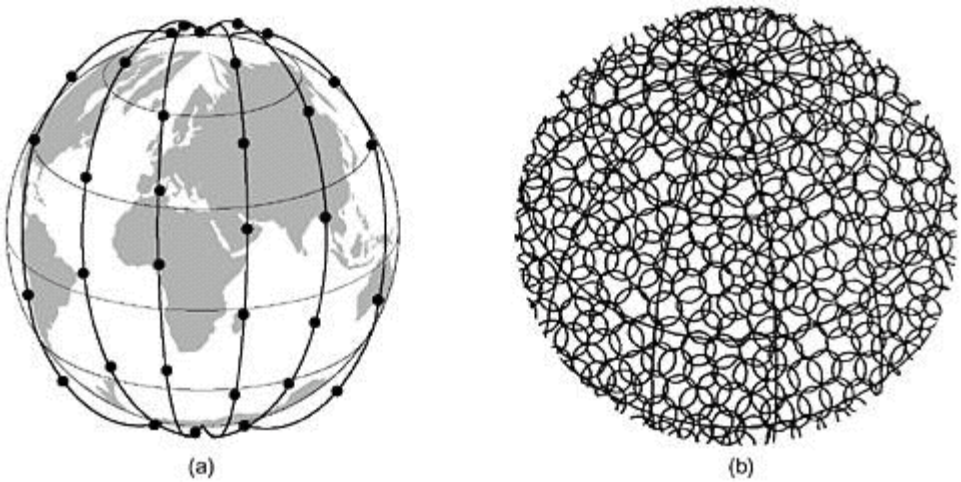
Band	Downlink	Uplink	Bandwidth	Problems
L	1.5 GHz	1.6 GHz	15 MHz	Low bandwidth; crowded
S	1.9 GHz	2.2 GHz	70 MHz	Low bandwidth; crowded
C	4.0 GHz	6.0 GHz	500 MHz	Terrestrial interference
Ku	11 GHz	14 GHz	500 MHz	Rain
Ka	20 GHz	30 GHz	3500 MHz	Rain, equipment cost

B) Medium-Earth Orbit Satellites:

- Moving down in altitude, we come to the LEO (Low-Earth Orbit) satellites. Due to their rapid motion, large numbers of them are needed for a complete system.
- On the other hand, because the satellites are so close to the earth, the ground stations do not need much power, and the round-trip delay is only a few milliseconds.

C) Iridium:

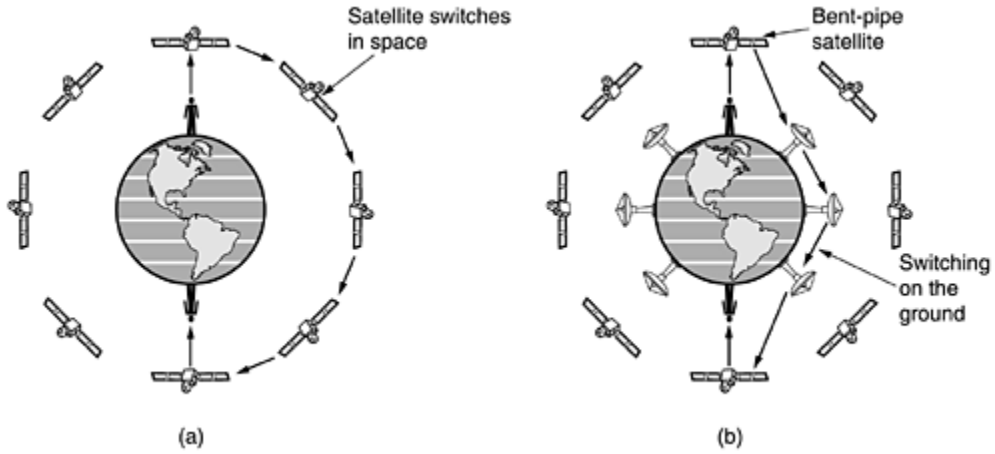
- Iridium's business was providing worldwide telecommunication service using hand-held devices that communicate directly with the Iridium satellites.
- It provides voice, data, paging, fax, and navigation service everywhere on land, sea, and air.



- Each satellite has a maximum of 48 cells with a total of 1628 cells over the surface of the earth. Each satellite has a capacity of 3840 channels, or 253,440 in all. Some of these are used for paging and navigation, while others are used for data and voice.

D) Global star:

- It is based on 48 LEO satellites but uses a different switching scheme than that of Iridium. Global star uses a traditional bent-pipe design.
- The call originating at the North Pole in Fig.(b) is sent back to earth and picked up by the large ground station at Santa's Workshop.
- The call is then routed via a terrestrial network to the ground station nearest the callee and delivered by a bent-pipe connection as shown.



E) Teledesic:

- It is targeted at bandwidth-hungry Internet users all over the world. The goal of the Teledesic system is to provide millions of concurrent Internet users with an uplink of as much as 100 Mbps.

Satellites versus Fiber:

1. While a single fiber has, in principle, more potential bandwidth than all the satellites ever launched, this bandwidth is not available to most users.
2. Mobile communication. Many people nowadays want to communicate while jogging, driving, sailing, and flying.
3. A third niche is for situations in which broadcasting.
4. Communication in places with hostile terrain or a poorly developed terrestrial infrastructure.
5. Market for satellites is to cover areas where obtaining the right of way for laying fiber is difficult or unduly expensive
6. When rapid deployment is critical, as in military communication systems in time of war, satellites win easily.

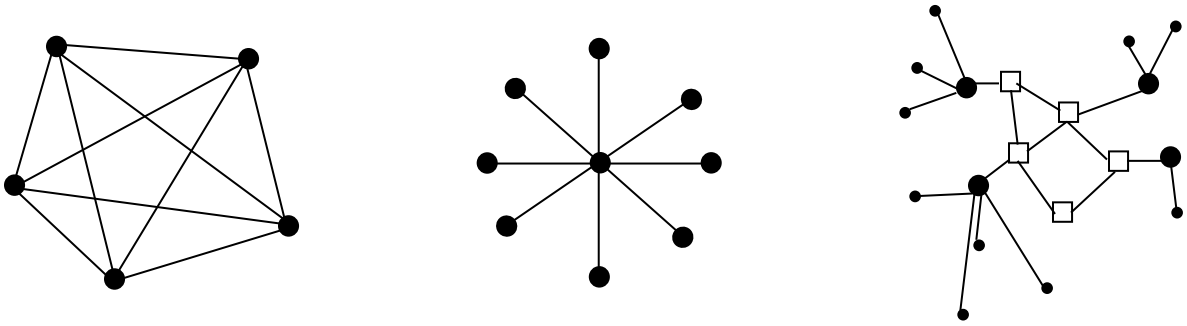
PUBLIC SWITCHED TELEPHONE NETWORK.

- The PSTN (Public Switched Telephone Network), were usually designed many years ago, with a completely different goal in mind: transmitting the human voice in a more-or-less recognizable form.
- In any event, the telephone system is so tightly intertwined with computer networks.

Structure of the Telephone System

- Alexander Graham Bell patented the telephone in 1876 there was an enormous demand for his new invention. The initial market was for the sale of telephones, which came in pairs. It was up to the customer to string a single wire between them.

  Model of connecting every telephone to every other telephone, as shown in



- **Fig 1:**To make a call, the customer would crank the phone to make a ringing sound in the telephone company office to attract the attention of an operator, who would then manually connect the caller to the caller by using a jumper cable.
- The model of a single switching office is illustrated in **Fig.(2)**. to connect every switching office to every other switching office by means of a wire between them quickly became unmanageable, so second-level switching offices were invented. Multiple second-level offices were needed, as illustrated in **Fig.(3).**
- Each telephone has two copper wires coming out of it that go directly to the nearest end office. The two-wire connections between each subscriber's telephone and the end office are known in the trade as the local loop.If the called telephone is attached to another end office, a different procedure has to be used.

- Each end office has a number of outgoing lines to one or more nearby switching centers, called toll offices; these lines are called toll connecting trunks.

- The toll, primary, sectional, and regional exchanges communicate with each other via high-bandwidth intertoll trunks (also called interoffice trunks).Figure shows how a medium-distance connection might be routed.
  The telephone system consists of three major components:

1. Local loops (analog twisted pairs going into houses and businesses).
2. Trunks (digital fiber optics connecting the switching offices).
3. Switching offices (where calls are moved from one trunk to another).

Modems

- The square waves used in digital signals have a wide frequency spectrum and subject to strong attenuation and delay distortion. These effects make base band (DC) signaling unsuitable except at slow speeds and over short distances.
- To get around the problems associated with DC signaling, especially on telephone lines, AC signaling is used.
- A continuous tone in the 1000 to 2000 Hz range called a sine wave carrier is introduced. Its amplitude, frequency, or phase can be modulated to transmit information.
- In amplitude modulation, two different amplitudes are to represent 0 and 1 respectively. In frequency modulation, also known as frequency shift keying, two (or more) different tones are used.
- In the simplest form of phase modulation, the carrier wave is systematically shifted 0 or 180 degrees at uniformly speed intervals.

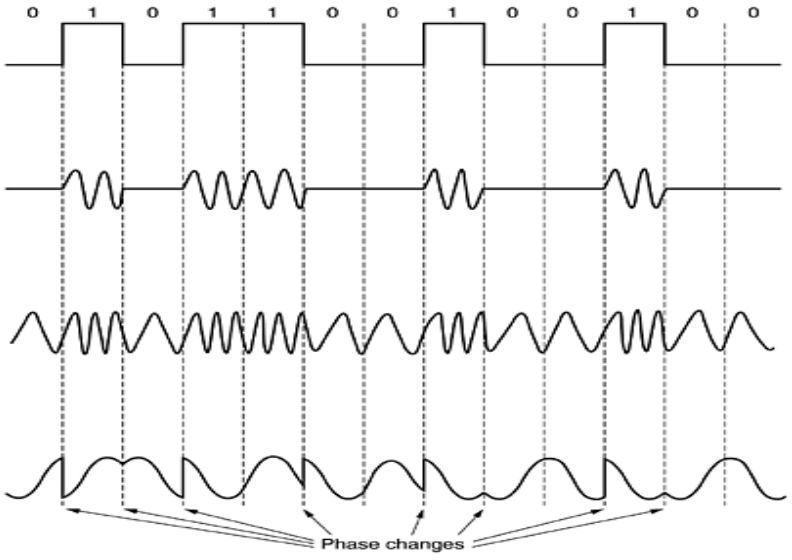
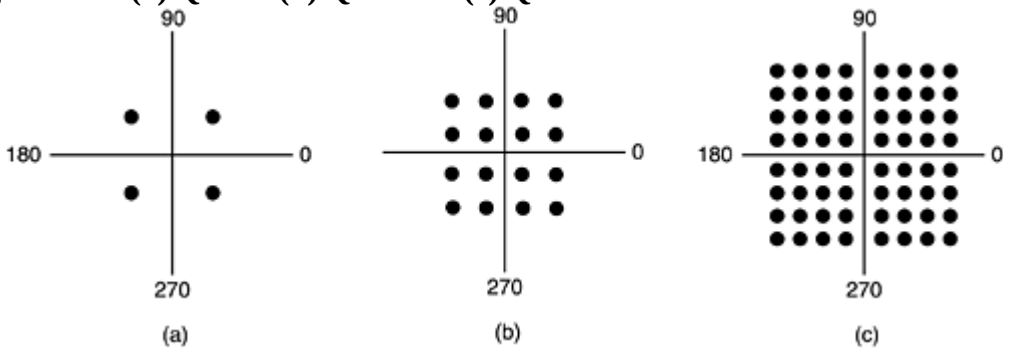


Fig: (a) A binary signal. (b) Amplitude modulation. (c) Frequency modulation. (d) Phase modulation

- A better scheme is to use shifts of 45, 135, 225 or 315 degrees to transmit 2 bits of information per time interval.
- A device that accepts a serial stream of bits as input and produces a carrier modulated by one of these methods is called a modem (for modulation – demodulation).
- The modem is inserted between the (digital) computer and the (analog) telephone system.
- All modern modems allow traffic in both directions at the same time. A connection that allows traffic in both directions simultaneously is called full duplex. A two-lane road is full duplex.
- A connection that allows traffic either way, but only one way at a time is called half duplex.
- A connection that allows traffic only one way is called simplex. A one-way street is simplex.

Figure 2-25. (a) QPSK. (b) QAM-16. (c) QAM-64.



- **Fig. 2-25(a**) has four valid combinations and can be used to transmit 2 bits per symbol. It is QPSK
- This modulation scheme can be used to transmit 4 bits per symbol. It is called QAM-16 (**Quadrature Amplitude Modulation**).
- **In Fig. 2-25(b)** It consists 16 different combinations. This modulation scheme can be used to transmit 4 bits per symbol. It is called QAM-16 **(Quadrature Amplitude Modulation**).
- **Figure 2-25(c)** . It allows 64 different combinations, so 6 bits can be transmitted per symbol. It is called QAM-64. Higher-order QAMs also are used.

Digital Subscriber Lines

- Services with more bandwidth than standard telephone service are sometimes called broadband,

<u>Trunks and Multiplexing</u>

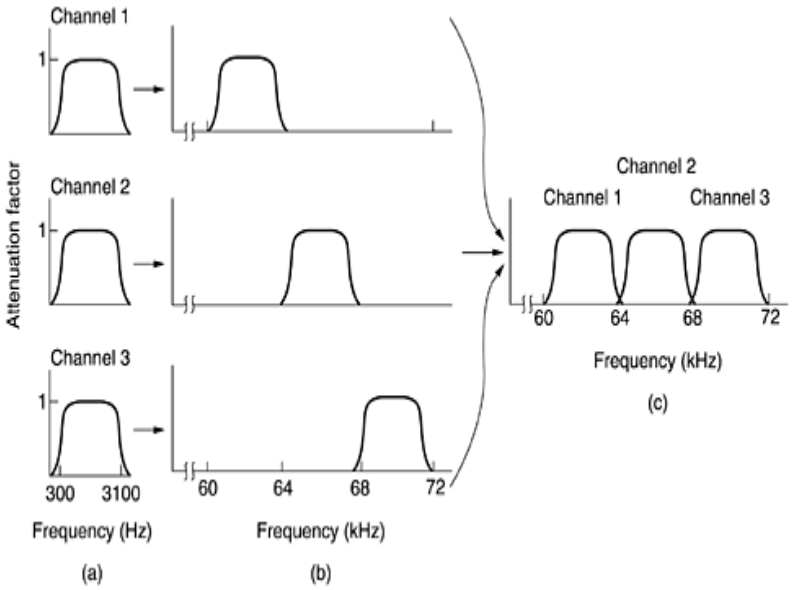
- Telephone companies have developed elaborate schemes for multiplexing many conversations over a single physical trunk.

Multiplexing divided into three categories,

1. FDM (Frequency Division Multiplexing)
2. TDM (Time Division Multiplexing).
3. WDM (Wavelength Division Multiplexing)

1) Frequency Division Multiplexing (FDM):

- In FDM, the frequency spectrum is divided into frequency bands, with each user having exclusive possession of some band.



- Figure shows how three voice-grade telephone channels are multiplexed using FDM. Filters limit the usable bandwidth to about 3100 Hz per voice-grade channel.

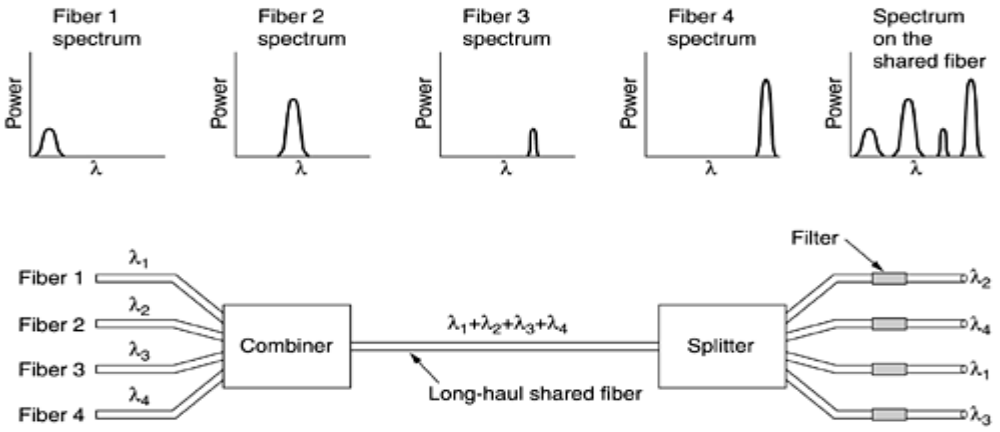
- The FDM schemes used around the world are to some degree standardized. A widespread standard in 400 Hz.
- Voice channels multiplexed in to 60 to 108 KHz. This unit called group, five groups can multiplexed to from a super group, the next unit is called master group, which is five super groups or ten super groups.

2) Wavelength Division Multiplexing:

- For fiber optic channels, a variation of frequency division multiplexing is used. It is called WDM (Wavelength Division Multiplexing).

Basic principle of WDM:

- Here four fibers come together at an optical combiner, each with its energy present at a different wavelength. The four beams are combined onto a single shared fiber for transmission to a distant destination. At the far end, the beam is split up over as many fibers as there were on the input side**.**
- Each output fiber contains a short, specially-constructed core that filters out all but one wavelength. The resulting signals can be routed to their destination or recombined in different ways for additional multiplexed transport.

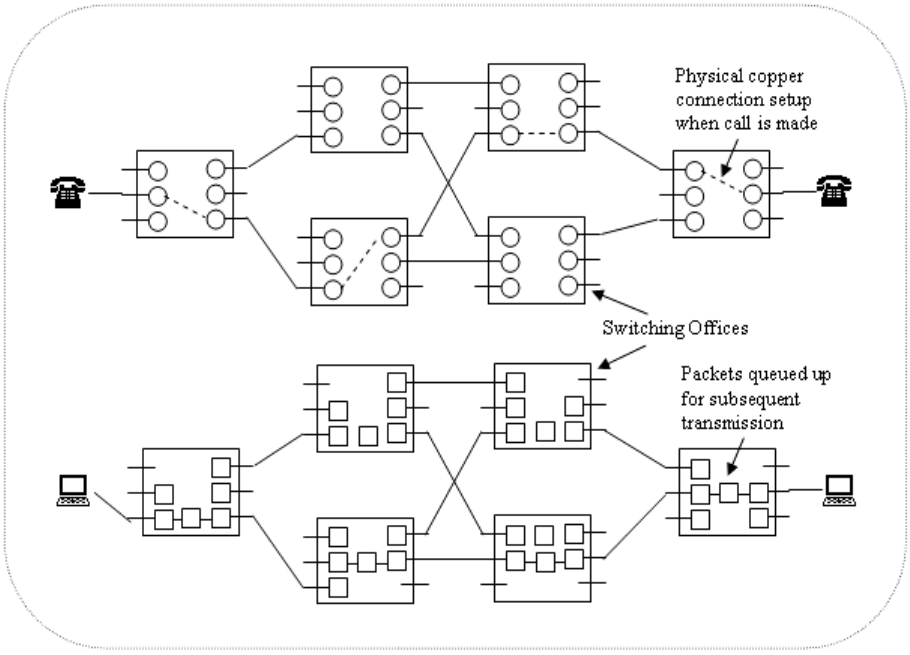


3) Time Division Multiplexing:

- TDM can be handled entirely by digital electronics, so it has become far more widespread in recent years. Unfortunately, it can only be used for digital data. Since the local loops produce analog signals, a conversion is needed from analog to digital in the end office, where all the individual local loops come together to be combined onto outgoing trunks.
- The analog signals are digitized in the end office by a device called a codec (coder-decoder), producing a series of 8-bit numbers.
- At a lower sampling rate, information would be lost; at a higher one, no extra information would be gained. This technique is called PCM (Pulse Code Modulation).
- Once the voice signal has been digitized, it is tempting to try to use statistical techniques to reduce the number of bits needed per channel. These techniques are appropriate not only for encoding speech, but for the digitization of any analog signal
- One method, called differential pulse code modulation, consists of outputting not the digitized amplitude, but the difference between the current value and the previous one

SWITCHING.

- The phone system is divided into two principal parts: outside plant (the local loops and trunks, since they are physically outside the switching offices) and inside plant (the switches), which are inside the switching offices.



.

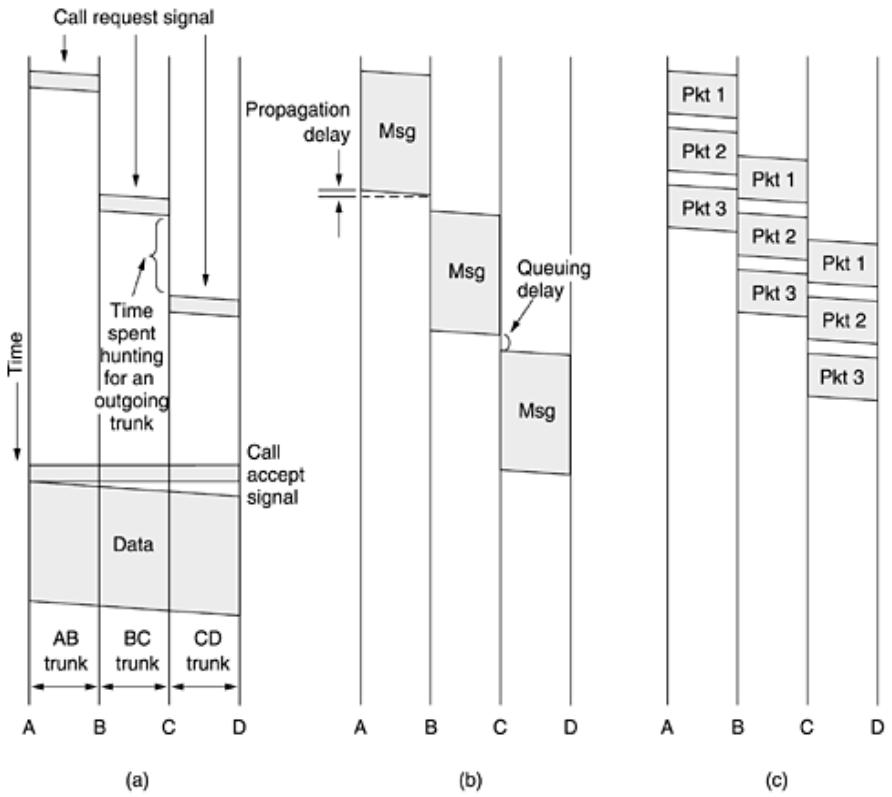
Circuit and Packet switching

Types of switching:

1. Circuit switching.
2. Message switching.
3. Packet switching.

1) Circuit Switching:

- When you or your computer places a telephone call, the switching equipment within the telephone system seeks out a physical path all the way from your telephone to the receiver's telephone. This technique is called **circuit switching**
- In circuit switching each of the six rectangles represent a carrier switching office, in this example each office has three incoming lines and three outgoing lines.
- When a call passes through a switching office a physical connection is established between the line on which the call name in and one of the output lines as shown by the doted lines.



- In fig highlighted simplified of cause because part of the physical path between two telephones way in that microwave or fiber lines on which thousands of calls are multiplexed.

2) Message Switching:

- When this form of switching is used, no physical path is established in advance between sender and receiver. Instead, when the sender has a block of data to be sent, it is stored in the first switching office and then forwarded later, one hop at a time.
- Each block is received in its entirety, inspected for errors, and then retransmitted. A network using this technique is called a store-and-forward network.

3) Packet Switching:

- In a single block can tie up a router-router line for minutes, rendering message switching useless for interactive traffic. To get around these problems, packet switching was invented.
- It places a tight upper limit on block size, allowing packets to be buffered in router main memory instead of on disk. By making sure that no user can monopolize any transmission line very long packet-switching networks are well suited for handling interactive traffic

Comparision (Circuit and Packet switching.)

Item	Circuit switched	Packet switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
Time of possible congestion	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

MOBILE TELEPHONE SYSTEM

Telephones mobile system has two basic varieties: Cordless phones and Mobile phones. Cordless phones are devices consisting of a base station and a handset sold as a set for use within the home. Mobile phones have gone through three distinct generations, with different technologies:

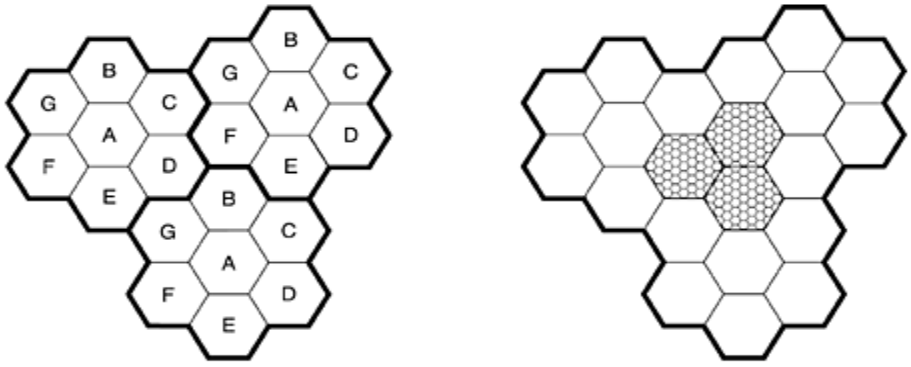
1. Analog voice.
2. 2. Digital voice.
3. 3. Digital voice and data

1)First-Generation: Analog Voice:

- The first system for car-based telephones was set up in St. Louis. This system used a single large transmitter on top of a tall building and had a single channel, used for both sending and receiving.
- It used a high-powered (200-watt) transmitter, on top of a hill, but now had two frequencies, one for sending and one for receiving.

Advanced Mobile Phone System:

- AMPS (Advanced Mobile Phone System), invented by Bell Labs in 1982. In all mobile phone systems, a geographic region is divided up into cells, which is why the devices are sometimes called cell phones.
- In AMPS, the cells are typically 10 to 20 km across; in digital systems, the cells are smaller. The idea of frequency reuse is illustrated in Fig. (a). The cells are normally roughly circular, but theyare easier to model as hexagons.



(a) (b)

- ❖ All the base stations are connected to a single device called an MTSO (Mobile Telephone Switching Office) or MSC (Mobile Switching Center).
- ❖ The telephone is then informed of its new boss, and if a call is in progress, it will be asked to switch to a new channel. This process called handoff.

Handoffs can be done in two ways.

- ❖ In a soft handoff,the telephone is acquired by the new base station before the previous one signs off. In this way there is no loss of continuity.
- ❖ Hard handoff, the old base station drops the telephone before the new one acquires it.

Channels:

The AMPS system uses 832 full-duplex channels, each consisting of a pair of simplex channels.

The 832 channels are divided into four categories:

1. Control to manage the system.
2. Paging to alert mobile users to calls for them.
3. Access for call setup and channel assignment.
4. Data for voice, fax, or data.

Call Management:

- ❖ Each mobile telephone in AMPS has a 32-bit serial number and a 10-digit telephone number in its PROM.

2)Second-Generation Mobile Phones: Digital Voice:

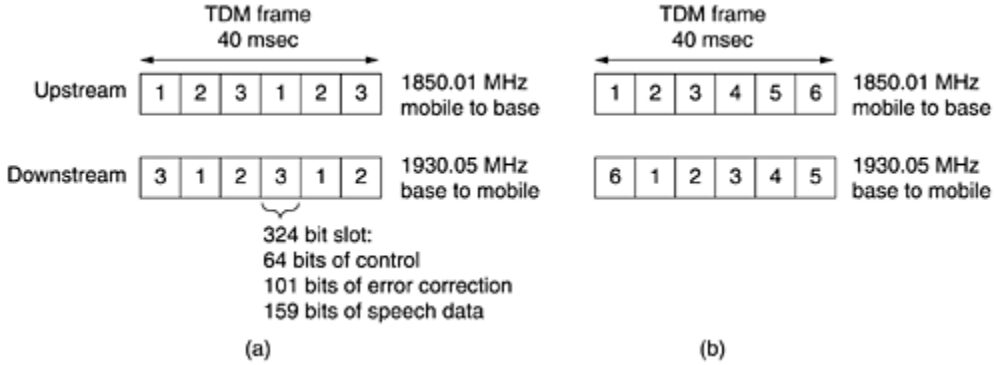
Four systems are in use now:

1. D-AMPS
2. GSM
3. CDMA
4. PDC

a) D-AMPS-The Digital Advanced Mobile Phone System:

- ❖ It is fully digital. When D-AMPS was introduced as a service, a new frequency band was made available to handle the expected increased load.
- ❖ On a D-AMPS mobile phone, the voice signal picked up by the microphone is digitized and compressed using a model that is more sophisticated than the delta modulation and predictive encoding schemes the compression is done by a circuit called a vocoder.

- In D-AMPS, three users can share a single frequency pair using time division multiplexing. Each frequency pair supports 25 frames/sec of 40 msec each. Each frame is divided into six time slots of 6.67 msec each.



b)GSM-The Global System for Mobile Communications:

- GSM (Global System for Mobile communications) is used, To a first approximation, GSM is similar to D-AMPS. Both are cellular systems.
- Frequency division multiplexing is used, with each mobile transmitting on one frequency and receiving on a higher frequency

Each frequency band is 200 kHz wide,

1. A GSM system has 124 pairs of simplex channels. Each currently active station is assigned one time slot on one channel pair.
2. The eight shaded time slots all belong to the same connection, four of them in each direction.
3. Transmitting and receiving does not happen in the same time slot because the GSM radios cannot transmit and receive at the same time and it takes time to switch from one to the other

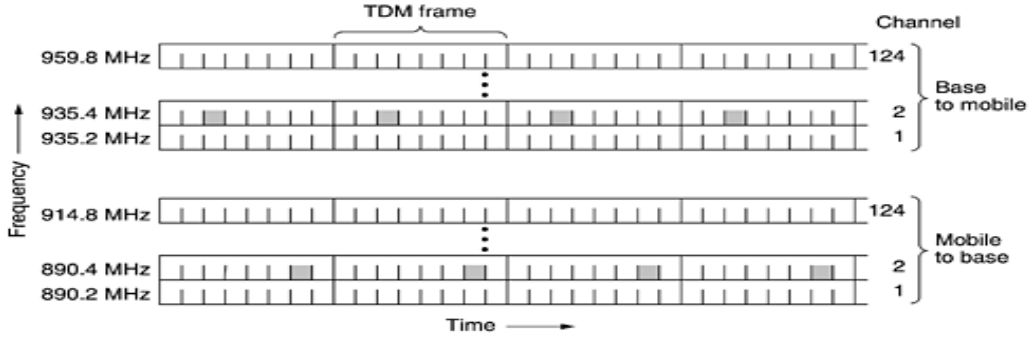
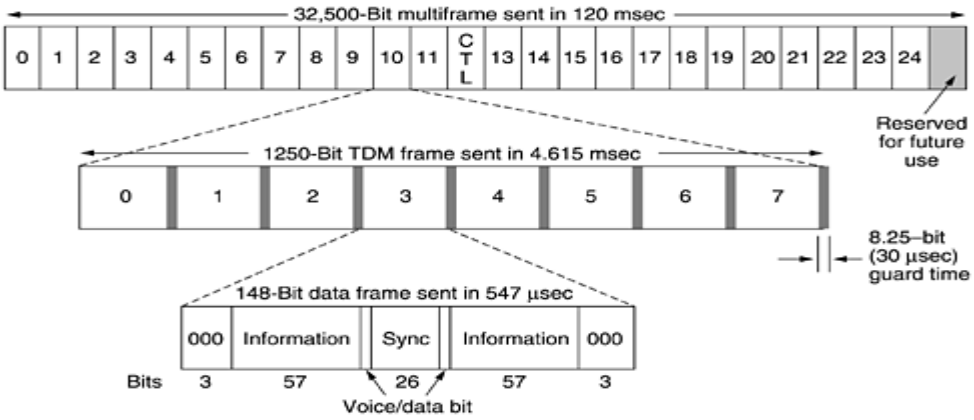


Figure 2-44. A portion of the GSM framing structure.



c) CDMA-Code Division Multiple Access :

- CDMA which works completely differently, CDMA is completely different from AMPS, D-AMPS, and GSM. CDMA allows each station to transmit over the entire frequency spectrum all the time.Multiple simultaneous transmissions are separated using coding theory. CDMA also relaxes the assumption that colliding frames are totally garbled.

3) Third Generation Mobile phones: Digital Voice and Data:

IMT-2000: Where IMT stood for International Mobile Telecommunications. The number 2000 stood for three things:.

(1) The frequency it was supposed to operate at (in MHz).

(3) The bandwidth the service should have (in kHz).

The basic services that the IMT-2000 network is supposed to provide to its users are:

1. High-quality voice transmission.
2. 2. Messaging (replacing e-mail, fax, SMS, chat, etc.).
3. Multimedia (playing music, viewing videos, films, television, etc.).
4. Internet access (Web surfing, including pages with audio and video).

Several proposal were made, and after some winnowing like W-CDMA (Wide band CDMA) and UNITS (Universal Mobile Telecommunication System).

********** **UNIT I COMPLETED** **********

UNIT - II

DATA LINK LAYER:

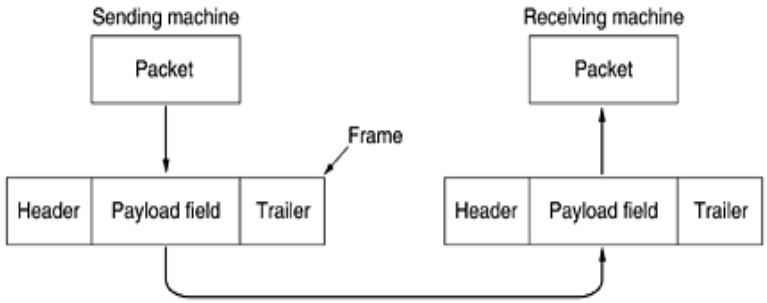
- ❖ It consist algorithms for achieving reliable, efficient communication between two adjacent machines.By adjacent, we mean that the two machines are connected by a communication channel that acts conceptually like a wire (e.g., a coaxial cable, telephone line, or point-to-point wireless channel)

Data Link Layer Functions

a) Providing a well-defined service interface to the network layer.
b) Dealing with transmission errors.
c) Regulating the flow of data so that slow receivers are not swamped by fast senders

- ❖ To accomplish these goals, the data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission.
- ❖ Each frame contains a frame header, a payload field for holding the packet, and a frame trailer, as illustrated in **Fig. 3-1**.

Figure 3-1. **Relationship between packets and frames.**



Data Link Layer Design Issues

(i) Framing
(ii) Error control
(iii) Flow control.

Process of Network layer:

- ❖ The function of the data link layer is to provide services to the network layer. The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine.

Services provided by the data link Layer:

- ❖ Data link layer provide services to the network layer, the actual services offered can vary from system to system. Three reasonable possibilities that are commonly provided are
    1. Unacknowledged connectionless service.
    2. Acknowledged connectionless service.
    3. Acknowledged connection-oriented service.

1)Un Acknowledged connectionless service:

- ❖ This service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.

- No logical connection is established beforehand or released afterward.If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover from it in the data link layer.

2) Acknowledged connectionless service:

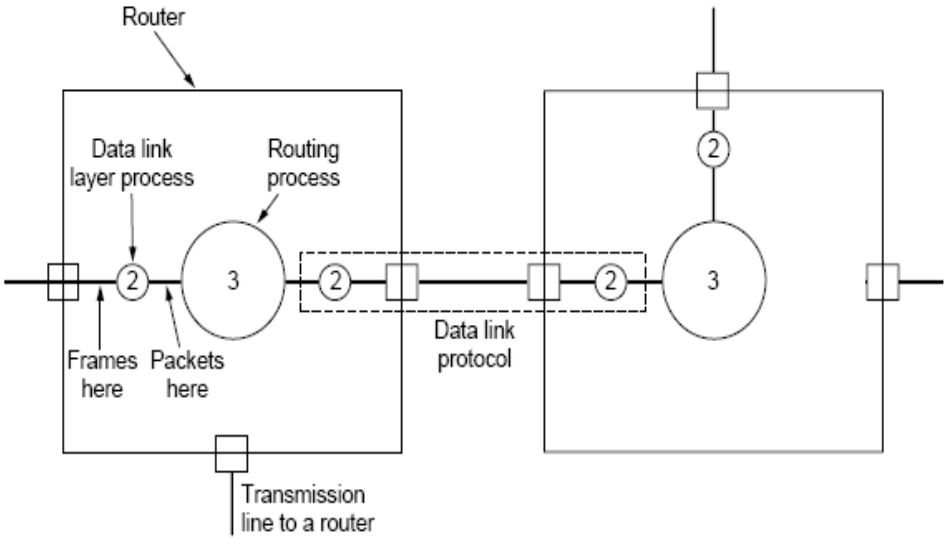
- When this service is offered, there are still no logical connections used, but each frame sent is individually acknowledged. The sender knows whether a frame has arrived correctly. If it has not arrived within a specified time interval, it can be sent again.

3) Connection oriented service:

- The source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received.
- When connection-oriented service is used, transfers go through three distinct
-
- phases.
- In the first phase, the connection is established by having both sides initialize variables and counters needed to keep track of which frames have been received and which ones have not.

Framing:

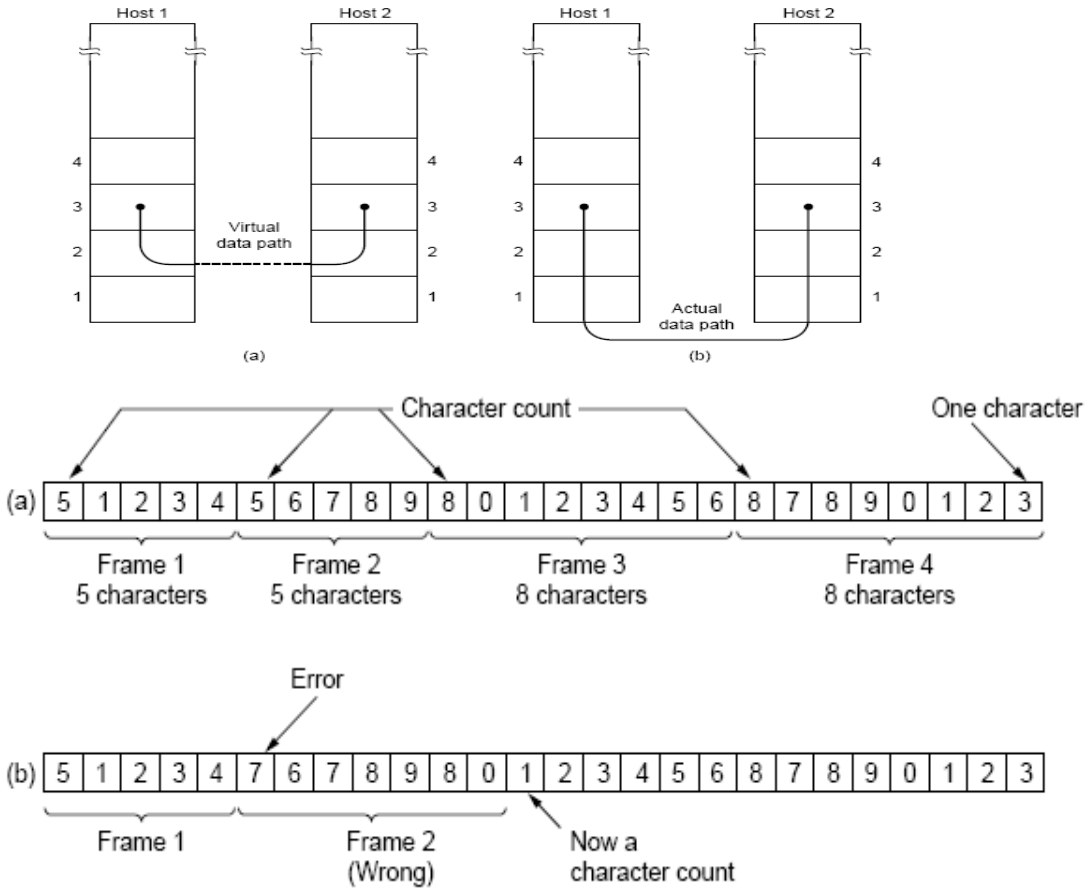
- The physical layer does is accept a raw bit stream and attempt to deliver it to the destination.
- This bit stream is not guaranteed to be error free.
- The usual approach is for the data link layer to break the bit stream up into discrete frames and compute the checksum for each frame.



❖ Newly-computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it.

Methods:

- Character count.



- Flag bytes with byte stuffing.
- Starting and ending flags, with bit stuffing.
- Physical layer coding violations.

❖ The first framing method uses a field in the header to specify the number of characters in the frame.

❖ When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is.

❖ The trouble with this algorithm is that the count can be garbled by a transmission error.

Figure 3-4. A character stream. (a) Without errors. (b) With one error.

❖ The second framing method gets around the problem of resynchronization after an error by having each frame start and end with special bytes.

- In the past, the starting and ending bytes were different, but in recent years most protocols have used the same byte, called a flag byte, as both the starting and ending delimiter, as shown **in Fig. (a) as FLAG**.
- In this way, if the receiver ever loses synchronization, it can just search for the flag byte to find the end of the current frame.
- Two consecutive flag bytes indicate the end of one frame and start of the next one.
- A serious problem occurs with this method when binary data, such as object programs or floating-point numbers, are being transmitted.
- It may easily happen that the flag byte's bit pattern occurs in the data. This situation will usually interfere with the framing.
- One way to solve this problem is to have the sender's data link layer insert a special escape byte (ESC) just before each "accidental" flag byte in the data.
- The data link layer on the receiving end removes the escape byte before the data are given to the network layer.
- This technique is called byte stuffing or character stuffing.
- Each frame begins and ends with a special bit pattern, 01111110 (in fact, a flag byte). Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.
- This bit stuffing is analogous to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.

Figure 3-5.

- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically deletes the 0 bit. Just as byte stuffing is completely transparent to the network layer in both computers, so is bit stuffing.
- If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110. Figure gives an example of bit stuffing.

As a final note on framing, many data link protocols use a combination of a character count with one of the other methods for extra safety. When a frame arrives, the count field is used to locate the end of the frame

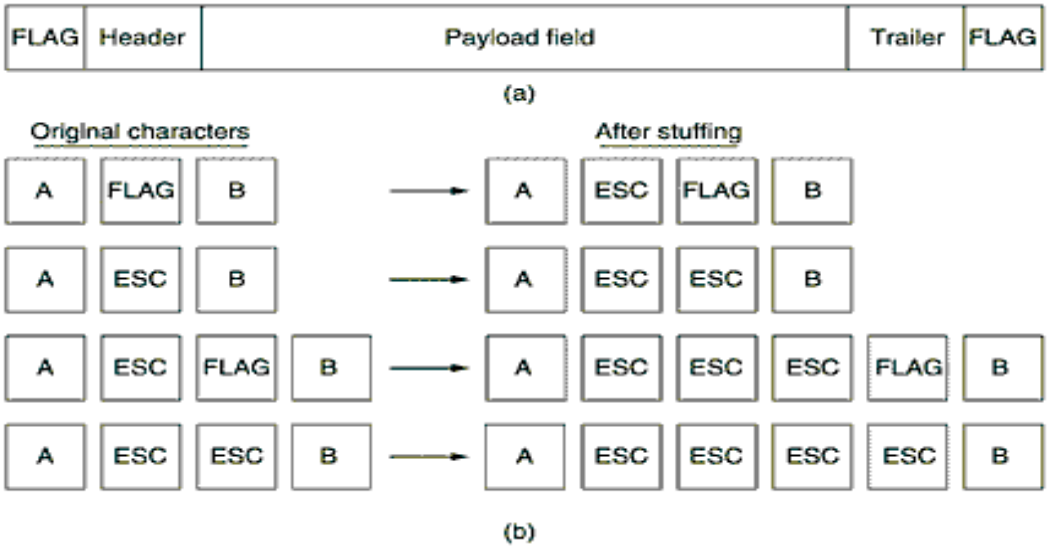


Figure 3-5. (a) A frame delimited by flag bytes. (b) Four examples of byte sequences before and after byte stuffing.

Error control:

- The protocol calls for the receiver to send back special control frames bearing positive or negative acknowledgements about the incoming frames. If the sender receives a positive acknowledgement about a frame, it knows the frame has arrived safely.
- On the other hand, a negative acknowledgement means that something has gone wrong, and the frame must be transmitted again.
- An additional complication comes from the possibility that hardware troubles may cause a frame to vanish completely (e.g., in a noise burst). In this case, the receiver will not react at all, since it has no reason to react.
- It should be clear that a protocol in which the sender transmits a frame and then waits for an acknowledgement, positive or negative.
- When frames may be transmitted multiple times there is a danger that the receiver will accept the same frame two or more times and pass it to the network layer more than once.
- To prevent this from happening, to assign sequence numbers to outgoing frames, so that the receiver can distinguish retransmissions from originals

Flow control:

- Another important design issue that occurs in the data link layer (and higher layers as well) is what to do with a sender that systematically wants to transmit frames faster than the receiver can accept them. This situation can easily occur when the sender is running on a fast computer and the receiver is running on a slow (or heavily loaded) machine.
- The sender keeps pumping the frames out at a high rate until the receiver is completely swamped.
- Even if the transmission is error free, at a certain point the receiver will simply be unable to handle the frames as they arrive and will start to lose some.

Two approaches are commonly used.

1. In the first one, feedback-based flow control, the receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing.
2. In the second one, rate-based flow control, the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver

ERROR DETECTION AND CORRECTION.

- Errors are rare on the digital part; they are still common on the local loops. Furthermore, wireless communication is becoming more common, and the error rates here are orders of magnitude worse than on the interoffice fiber trunks.

Error-Correcting Codes

- Network designers have developed two basic strategies for dealing with errors. One way is to include enough redundant information along with each block of

data sent, to enable the receiver to deduce what the transmitted data must have been.

- The other way is to include only enough redundancy to allow the receiver to deduce that an error occurred, but not which error, and have it request a retransmission.
- The former strategy uses error-correcting codes and the latter uses error-detecting codes. The use of error-correcting codes is often referred to as forward error correction**.**To understand how errors can be handled, it is necessary to look closely at what an error really is.
- Normally, a frame consists of m data (i.e., message) bits and r redundant, or check, bits. Let the total length be n (i.e., n = m + r).
- An n-bit unit containing data and check bits is often referred to as an n-bit codeword.
- Given any two codeword, say, **10001001** and **10110001,** it is possible to determine how many corresponding bits differ. In this case, 3 bits differ.
- To determine how many bits differ, just exclusive OR the two code words and count the number of 1 bits in the result, for **Example:**

10001001
10110001
00111000

- The number of bit positions in which two code words differ is called the Hamming distance. Hamming distance d apart, it will require d single-bit errors to convert one into the other.

Error-Detecting Codes:

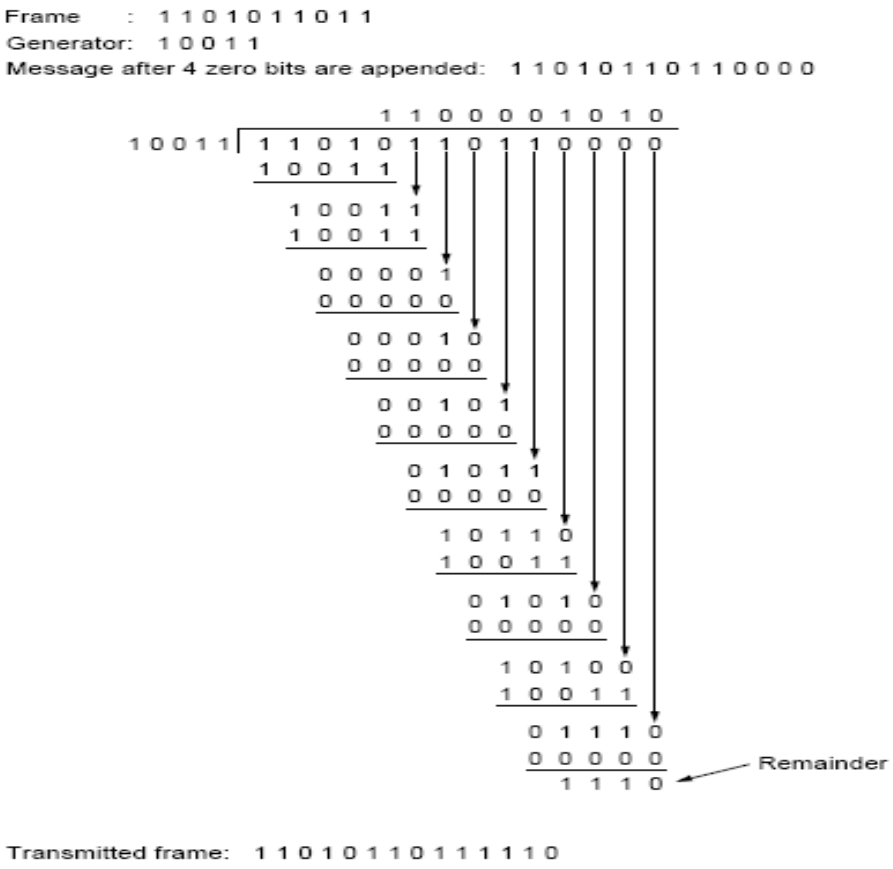
- The polynomial code, also known as a **CRC (Cyclic Redundancy Check)**. Polynomial codes are based upon treating bit strings as representations of polynomials with coefficients of 0 and 1 only. A k-bit frame is regarded as the coefficient list for a polynomial with k terms, ranging from xk - 1 to x0.
- When the polynomial code method is employed, the sender and receiver must agree upon a generator polynomial, G(x), in advance. Both the high- and low-order bits of the generator must be 1.
- To compute the checksum for some frame with m bits, corresponding to the polynomial M(x), the frame must be longer than the generator polynomial. When the receiver gets the checksummed frame, it tries dividing it by G(x). If there is a remainder, there has been a transmission error.

Algorithm for computing the checksum:

1. Let r be the degree of G(x). Append r zero bits to the low-order end of the frame so it now contains m + r bits and corresponds to the polynomial $x^rM(x)$.
2. Divide the bit string corresponding to G(x) into the bit string corresponding to $x^rM(x)$, using modulo 2 division.
3. Subtract the remainder (which is always r or fewer bits) from the bit string corresponding to $x^rM(x)$ using modulo 2 subtraction. The result is the

checksummed frame to be transmitted. Call its polynomial T(x). The fig illustrates the calculation for a frame **1101011011** using the generator

G(x) = x^4 + x + 1.



Elementary data Link Protocols

- The data link layer is concerned; the packet passed across the interface to it from the network layer is pure data, whose every bit is to be delivered to the destination's network layer.
- The fact that the destination's network layer may interpret part of the packet as a header is of no concern to the data link layer. When the data link layer accepts a packet, it encapsulates the packet in a frame by adding a data link header and trailer to it.
- When a frame arrives at the receiver, the hardware computes the checksum. If the checksum is incorrect (i.e., there was a transmission error), the data link layer is so informed (event = cksum_err).
- If the inbound frame arrived undamaged, the data link layer is also informed (event = frame_arrival) so that it can acquire the frame for inspection using from_physical_layer.
- A frame is composed of four fields: kind, seq, ack, and info, the first three of which contain control information and the last of which may contain actual data to be transferred.

- These control fields are collectively called the frame header. The kind field tells whether there are any data in the frame.
- The **seq** and **ack** fields are used for sequence numbers and acknowledgements, respectively

An Unrestricted Simplex Protocol

The protocol consists of two distinct procedures,

1. **Sender.**
2. **2.Receiver**.

- The sender runs in the data link layer of the source machine, and the receiver runs in the data link layer of the destination machine. The sender is in an infinite while loop just pumping data out onto the line as fast as it can. The body of the loop consists of three actions:
  - Go fetch a packet from the (always obliging) network layer
  - Construct an outbound frame using the variable s
  - Send the frame on its way.
- Only the info field of the frame is used by this protocol, because the other fields have to do with error and flow control and there are no errors or flow control restrictions here.

- The receiver is equally simple. Initially, it waits for something to happen, the only possibility being the arrival of an undamaged frame.
- Eventually, the frame arrives and the procedure wait_for_event returns, with event set to frame_arrival (which is ignored anyway).
- The call to from_physical_layer removes the newly arrived frame from the hardware buffer and puts it in the variable r, where the receiver code can get at it.

A Simplex Stop-and-Wait Protocol

- To prevent the sender from flooding the receiver with data faster than the latter is able to process them. It might be possible for the sender to simply insert a delay into protocol 1 to slow it down sufficiently to keep from swamping the receiver.
- A more general solution to this dilemma is to have the receiver provide feedback to the sender.
- After having passed a packet to its network layer, the receiver sends a little dummy frame back to the sender which, in effect, gives the sender permission to transmit the next frame
- Protocols in which the sender sends one frame and then waits for an acknowledgement before proceeding are called stop-and-wait.

Example of a simplex stop-and-wait protocol:

```
/* Protocol 2 (stop-and-wait) also provides for a one-directional flow of data from
   sender to receiver. The communication channel is once again assumed to be error
   free, as in protocol 1. However, this time, the receiver has only a finite buffer
   capacity and a finite processing speed, so the protocol must explicitly prevent
   the sender from flooding the receiver with data faster than it can be handled. */

typedef enum {frame_arrival} event_type;
#include "protocol.h"

void sender2(void)
{
  frame s;                              /* buffer for an outbound frame */
  packet buffer;                        /* buffer for an outbound packet */
  event_type event;                     /* frame_arrival is the only possibility */

  while (true) {
      from_network_layer(&buffer);      /* go get something to send */
      s.info = buffer;                  /* copy it into s for transmission */
      to_physical_layer(&s);            /* bye-bye little frame */
      wait_for_event(&event);           /* do not proceed until given the go ahead */
  }
}

void receiver2(void)
{
  frame r, s;                           /* buffers for frames */
  event_type event;                     /* frame_arrival is the only possibility */
  while (true) {
      wait_for_event(&event);           /* only possibility is frame_arrival */
      from_physical_layer(&r);          /* go get the inbound frame */
      to_network_layer(&r.info);        /* pass the data to the network layer */
      to_physical_layer(&s);            /* send a dummy frame to awaken sender */
  }
}
```

A Simplex Protocol for a Noisy Channel:

- The sender could send a frame, but the receiver would only send an acknowledgement frame if the data were correctly received. If a damaged frame arrived at the receiver, it would be discarded. After a while the sender would time out and sends the frame again. This process would be repeated until the frame finally arrived intact.
- The obvious way to achieve this is to have the sender put a sequence number in the header of each frame it sends. Then the receiver can check the sequence number of each arriving frame to see if it is a new frame or a duplicate to be discarded.

- Protocols in which the sender waits for a positive acknowledgement before advancing to the next data item are often called PAR (Positive Acknowledgement with Retransmission) or ARQ **(Automatic Repeat reQuest).**
- After transmitting a frame, the sender starts the timer running. If it was already running, it will be reset to allow another full timer interval.
- The time interval should be chosen to allow enough time for the frame to get to the receiver, for the receiver to process it in the worst case, and for the acknowledgement frame to propagate back to the sender.
- Only when that time interval has elapsed is it safe to assume that either the transmitted frame or its acknowledgement has been lost, and to send a duplicate.

SLIDING WINDOW PROTOCOL.

a) Go Back N protocol and selective repeat protocol. .

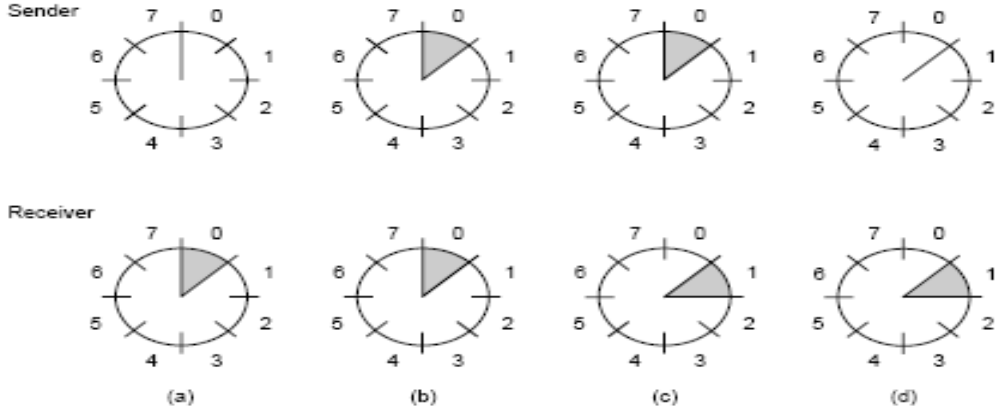
- In most practical situations, there is a need for transmitting data in both directions. One way of achieving full-duplex data transmission is to have two separate communication channels and use each one for simplex data traffic (in different directions).
- If this is done, we have two separate physical circuits, each with a "forward" channel (for data) and a "reverse" channel (for acknowledgements).
- In both cases the bandwidth of the reverse channel is almost entirely wasted. In effect, the user is paying for two circuits but using only the capacity of one.
- Data and control frames on the same circuit is an improvement over having two separate physical circuits, it is possible.
- When a data frame arrives, instead of immediately sending a separate control frame, the receiver restrains itself and waits until the network layer passes it the next packet.
- The acknowledgement is attached to the outgoing data frame. In effect, the acknowledgement gets a free ride on the next outgoing data frame.
- The technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame is known as piggybacking.

b) Sliding window protocol

- The next three protocols are bidirectional protocols that belong to a class called sliding window protocols.
- The three differ among themselves in terms of efficiency, complexity, and buffer requirements.
- The essence of all sliding window protocols is that at any instant of time, the sender maintains a set of sequence numbers corresponding to frames it is permitted to send.
- These frames are said to fall within the sending window.
- Similarly, the receiver also maintains a receiving window corresponding to the set of frames it is permitted to accept.
- The sender's window and the receiver's window need not have the same lower and upper limits or even have the same size.
- In some protocols they are fixed in size, but in others they can grow or shrink over the course of time as frames are sent and received.
- Here the window continuously maintains a list of unacknowledged frames.

c) A One-Bit Sliding Window Protocol

- A sliding window protocol with a maximum window size of 1. Such a protocol uses stop-and-wait since the sender transmits a frame and waits for its acknowledgement before sending the next one. If the frame is the one expected, it is passed to the network layer and the receiver's window is slid up.
- The acknowledgement field contains the number of the last frame received without error. If this number agrees with the sequence number of the frame the sender is trying to send, the sender knows it is done with the frame stored in buffer and can fetch the next packet from its network layer.
- If the sequence number disagrees, it must continue trying to send the same frame. Whenever a frame is received, a frame is also sent back. A peculiar situation



arises if both sides simultaneously send an initial packet. This synchronization difficulty is illustrated by Fig.

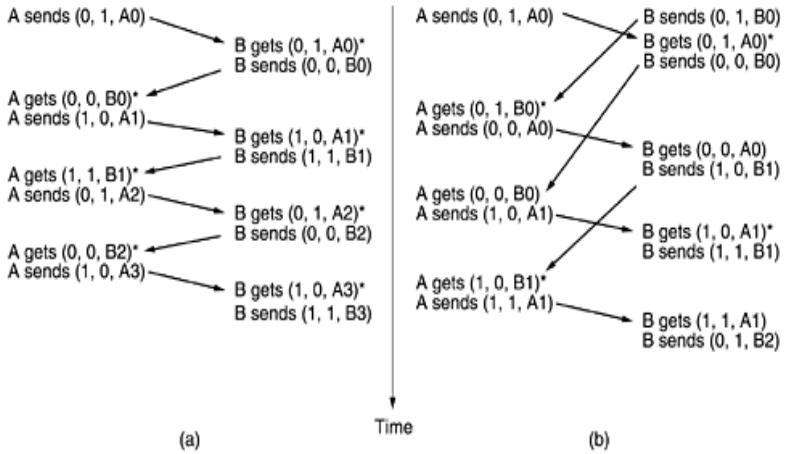


Figure 3-15. Two scenarios for protocol 4. (a) Normal case. (b) Abnormal case. The notation is (seq, ack, packet number). An asterisk indicates where a network layer accepts a packet.

- In part (a), the normal operation of the protocol is shown. In (b) the peculiarity is illustrated.
- If B waits for A's first frame before sending one of its own, the sequence is as shown in (a), and every frame is accepted. However, if A and B simultaneously initiate communication, their first frames cross, and the data link layers then get into situation (b).
- In (a) each frame arrival brings a new packet for the network layer; there are no duplicates.
- In (b) half of the frames contain duplicates, even though there are no transmission errors.
- Similar situations can occur as a result of premature timeouts, even when one side clearly starts first.
- In fact, if multiple premature timeouts occur, frames may be sent three or more times.

A Protocol Using Go Back N:

- The long round-trip time can have important implications for the efficiency of the bandwidth utilization. The problem described above can be viewed as a consequence of the rule requiring a sender to wait for an acknowledgement before sending another frame. If we relax that restriction, much better efficiency can be achieved.
- With an appropriate choice of w the sender will be able to continuously transmit frames for a time equal to the round-trip transit time without filling up the window. This technique is known as pipelining.
- Pipelining frames over an unreliable communication channel raises some serious issues. First, what happens if a frame in the middle of a long stream is damaged or lost?
- Large numbers of succeeding frames will arrive at the receiver before the sender even finds out that anything is wrong. When a damaged frame arrives at the receiver, it obviously should be discarded, but what should the receiver do with all the correct frames following it
- Two basic approaches are available for dealing with errors in the presence of pipelining. One way, called go back n, is for the receiver simply to discard all subsequent frames, sending no acknowledgements for the discarded frames.
- This strategy corresponds to a receive window of size 1. In other words, the data link layer refuses to accept any frame except the next one it must give to the network layer.
- If the sender's window fills up before the timer runs out, the pipeline will begin to empty. Eventually, the sender will time out and retransmit all unacknowledged frames in order, starting with the damaged or lost one.

A Protocol Using Selective Repeat:

- In this protocol, both sender and receiver maintain a window of acceptable sequence numbers. The sender's window size starts out at 0 and grows to some predefined maximum, MAX_SEQ.

- The receiver's window, in contrast, is always fixed in size and equal to MAX_SEQ. The receiver has a buffer reserved for each sequence number within its fixed window.

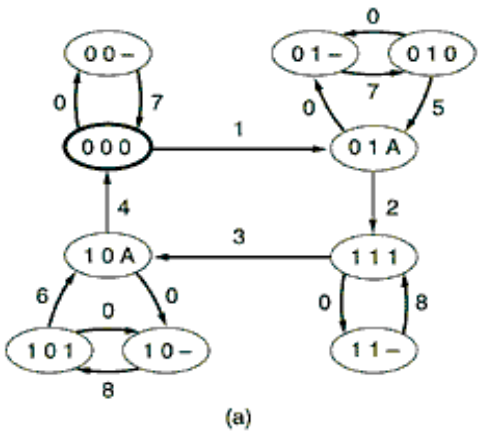
PROTOCOL VERIFICATION

Finite state machine:

- A key concept used in many protocol models is the finite state machine. In this each protocol machine is always in a specific state at every instant of time. Its state consists of all the values of its variables, including the program counter. Its used for analysis.
- From each state, there are zero or more possible transitions to other states. Transitions occur when some event happens. For a protocol machine, a transition might occur when a frame is sent, arrives, when a timer expires, when an interrupt occurs, etc.
- For the channel, typical events are insertion of a new frame onto the channel by a protocol machine, delivery of a frame, or loss of a frame due to noise.
- One particular state is designated as the initial state. This state corresponds to the description of the system when it starts running, or at some convenient starting place shortly thereafter.
- From the initial state, some, perhaps all, of the other states can be reached by a sequence of transitions.
- Using well-known techniques from graph theory, it is possible to determine which states are reachable and which are not. This technique is called reachability. This analysis can be helpful in determining whether a protocol is correct.

Formally, a finite state machine model of a protocol can be regarded as a quadruple (S, M, I, T), where:

1. S is the set of states the processes and channel can be in.
2. M is the set of frames that can be exchanged over the channel.
3. I is the set of initial states of the processes.
4. T is the set of transitions between states.



(a)

Transition	Who runs?	Frame accepted	Frame emitted	To network layer
0	–	(frame lost)		–
1	R	0	A	Yes
2	S	A	1	–
3	R	1	A	Yes
4	S	A	0	–
5	R	0	A	No
6	R	1	A	No
7	S	(timeout)	0	–
8	S	(timeout)	1	–

(b)

- At the beginning of time, all processes are in their initial states. Then events begin to happen, such as frames becoming available for transmission or timers going off.

- ❖ Each event may cause one of the processes or the channel to take an action and switch to a new state. By carefully enumerating each possible successor to each state, one can build the reachability graph and analyze the protocol.

Petri Net Models:

- ❖ A Petri net has four basic elements: places, transitions, arcs, and tokens. A place represents a state which (part of) the system may be in. Figure shows a Petri net with two places, A and B, both shown as circles.
- ❖ The system is currently in state A, indicated by the token (heavy dot) in place A. A transition is indicated by a horizontal or vertical bar. Each transition has zero or more input arcs coming from its input places, and zero or more output arcs, going to its output places.
- ❖ A transition is enabled if there is at least one input token in each of its input places. Any enabled transition may fire at will, removing one token from each input place and depositing a token in each output place. If the number of input arcs and output arcs differs, tokens will not be conserved.
- ❖ If two or more transitions are enabled, any one of them may fire. The choice of a transition to fire is indeterminate, which is why Petri nets are useful for modeling protocols. The Petri net of Fig. is deterministic and can be used to model any two-phase process

PPP—The Point-to-Point Protocol

- ❖ The Internet needs a point-to-point protocol for a variety of purposes, including router-to-router traffic and home user-to-ISP traffic.
- ❖ This protocol is PPP (Point-to-Point Protocol), which is defined in RFC 1661 and further elaborated on in several other RFCs (e.g., RFCs 1662 and 1663). PPP handles error detection, supports multiple protocols, allows IP addresses to be negotiated at connection time, permits authentication, and has many other features.

PPP provides three features:

1. A framing method that unambiguously delineates the end of one frame and the start of the next one. The frame format also handles error detection.

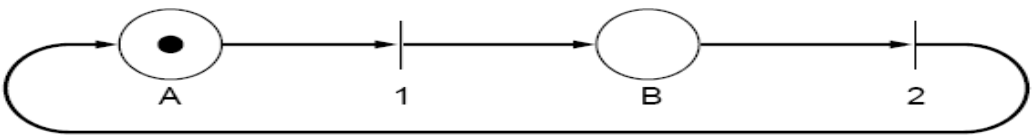
2. A link control protocol for bringing lines up, testing them, negotiating options, and bringing them down again gracefully when they are no longer needed. This protocol is called LCP (Link Control Protocol). It supports synchronous and asynchronous circuits and byte-oriented and bit-oriented encodings.

3. A way to negotiate network-layer options in a way that is independent of the network layer protocol to be used. The method chosen is to have a different NCP (Network Control Protocol) for each network layer supported.

THE CHANNEL ALLOCATION PROBLEM

This concept consist how to allocate a single broadcast channel among competing users.

Static Channel Allocation in LANs and MANs



- The traditional way of allocating a single channel, such as a telephone trunk, among multiple competing users is Frequency Division Multiplexing (FDM).
- If there are N users, the bandwidth is divided into N equal-sized portions (see Fig. 2-31), each user being assigned one portion. Since each user has a private frequency band, there is no interference between users.
- When there is only a small and constant number of users, each of which has a heavy (buffered) load of traffic (e.g., carriers' switching offices), FDM is a simple and efficient allocation mechanism.
- However, when the number of senders is large and continuously varying or the traffic is bursty, FDM presents some problems.
- If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted.
- If more than N users want to communicate, some of them will be denied permission for lack of bandwidth, even if some of the users who have been assigned a frequency band hardly ever transmit or receive anything.

Dynamic Channel Allocation in LANs and MANs

- Before we get into the first of the many channel allocation methods to be discussed in this chapter, it is worthwhile carefully formulating the allocation problem. Underlying all the work done in this area are five key assumptions, described below. Station Model.
- The model consists of N independent stations (e.g., computers, telephones, or personal communicators), each with a program or user that generates frames for transmission. Stations are sometimes called terminals.
- The probability of a frame being generated in an interval of length .t is ¥ë.t, where ë is a constant (the arrival rate of new frames). Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

A) Single Channel Assumption.

- A single channel is available for all communication. All stations can transmit on it and all can receive from it. As far as the hardware is concerned, all stations are equivalent, although protocol software may assign priorities to them.

B)Collision Assumption.

- If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled.
- This event is called a collision. All stations can detect collisions.
- A collided frame must be transmitted again later. There are no errors other than those generated by collisions.

C) Continuous Time.

Frame transmission can begin at any instant. There is no master clock dividing time into discrete intervals.

D). Slotted Time.

- Time is divided into discrete intervals (slots). Frame transmissions always begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

E) Carrier Sense.

- ❖ Stations can tell if the channel is in use before trying to use it. If the channel is sensed as busy, no station will attempt to use it until it goes idle.

F) No Carrier Sense.

- ❖ Stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.

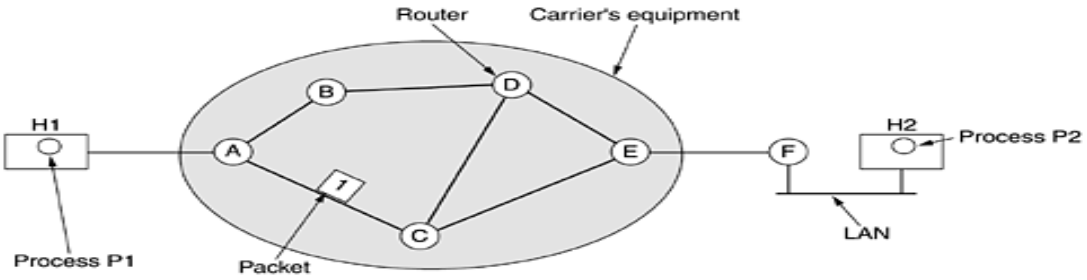
THE NETWORK LAYER

The network layer is concerned with getting packets from the source all the way to the destination

.NETWORK LAYER DESIGN ISSUES

1) Store-and-Forward Packet Switching

- ❖ The major components of the system are the carrier's equipment (routers connected by transmission lines), shown inside the shaded oval, and the customers' equipment, shown outside the oval.
- ❖ Host H1 is directly connected to one of the carrier's routers, A, by a leased line. In contrast, H2 is on a LAN with a router, F, owned and operated by the customer. This router also has a leased line to the carrier's equipment.
- ❖ We have shown F as being outside the oval because it does not belong to the carrier, but in terms of construction, software, and protocols, it is probably no different from the carrier's routers.This equipment is used as follows.
- ❖ A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the carrier. The packet is stored there until it has fully arrived so the checksum can be verified. Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching



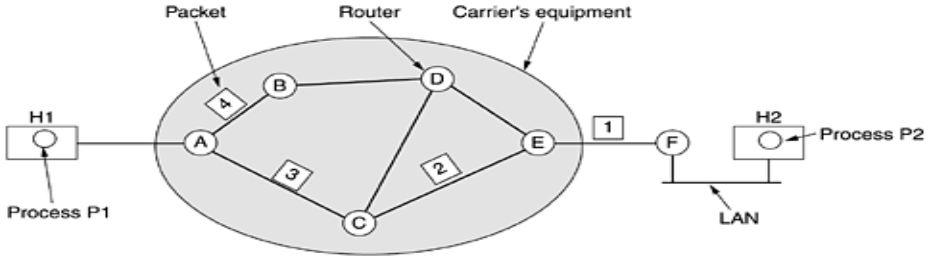
Services Provided to the Transport Layer

- ❖ The network layer provides services to the transport layer at the network layer/transport layer interface. An important question is what kind of services the network layer provides to the transport layer. The network layer services have been designed with the following goals in mind.

1. The services should be independent of the router technology.
2. The transport layer should be shielded from the number, type, and topology of the routers present.
3. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

Implementation of Connectionless Service

- If connectionless service is offered, packets are injected into the subnet individually and routed independently of each other. No advance setup is needed. In this context, the packets are frequently called **datagrams** (in analogy with telegrams) and the subnet is called a datagram subnet. If connection-oriented service is used, a path from the
- source router to the destination router must be established before any data packets can be sent. This connection is called a VC **(virtual circuit**), in analogy with the physical circuits set up by the telephone system, and the subnet is called a **virtual-circuit subnet**. In this section we will examine **datagram subnets;** in the next one we will examine virtual-circuit subnets.



A's table

Dest.	initially	later
A	–	–
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

C's table

Dest.	Line
A	A
B	A
C	–
D	D
E	E
F	E

E's table

Dest.	Line
A	C
B	D
C	C
D	D
E	–
F	F

- A has only two outgoing lines—to B and C—so every incoming packet must be sent to one of these routers, even if the ultimate destination is some other router. A's initial routing table is shown in the figure under the label "initially."
- As they arrived at A, packets 1, 2, and 3 were stored briefly (to verify their checksums). Then each was forwarded to C according to A's table. Packet 1 was then forwarded to E and then to F.
- When it got to F, it was encapsulated in a data link layer frame and sent to H2 over the LAN. Packets 2 and 3 follow the same route. However, something different happened to packet 4. When it got to A it was sent to router B, even though it is also destined for F. For some reason, A decided to send packet 4 via a different route than that of the first three. Perhaps it learned of a traffic jam somewhere along the ACE path and updated its routing table, as shown under the label "later." The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

Implementation of Connection-Oriented Service

- Host H1 has established connection 1 with host H2. It is remembered as the first entry in each of the routing tables.
- The first line of A's table says that if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C and given connection identifier 1. Similarly, the first entry at C routes the packet to E, also with connection identifier 1.

- Now let us consider what happens if H3 also wants to establish a connection to H2. It chooses connection identifier 1 (because it is initiating the connection and this is its only connection) and tells the subnet to establish the virtual circuit

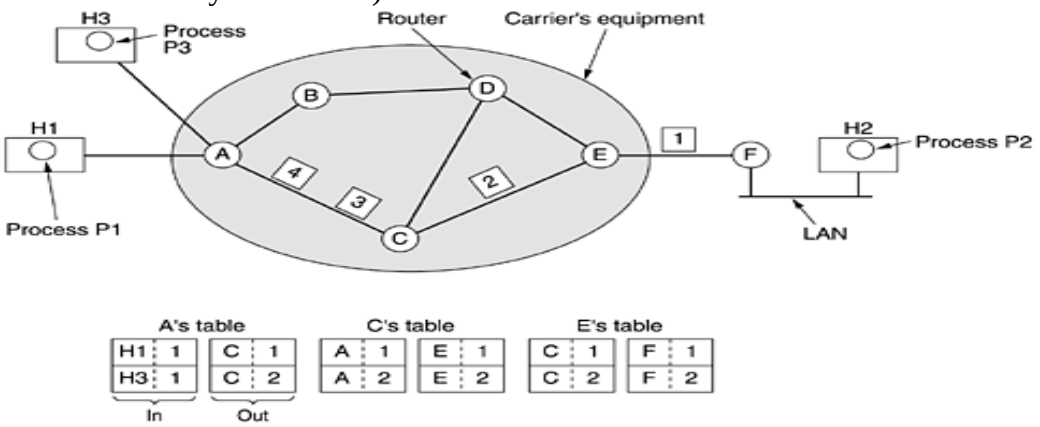
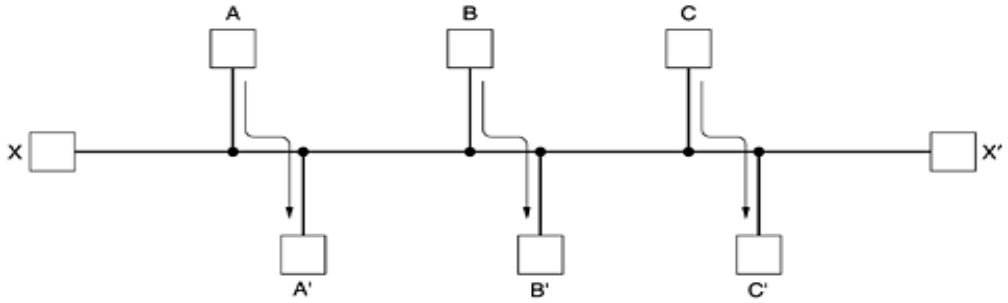


Fig : Connection-Oriented Service

ROUTING ALGORITHMS

- The main function of the network layer is routing packets from the source machine to the destination machine.
- The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on. If the subnet uses datagrams internally, this decision must be made anew for every arriving data packet since the best route may have changed since last time.
- If the subnet uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up. Thereafter, data packets just follow the previously-established route. The latter case is sometimes called **session routing**



Routing algorithms can be grouped into two major classes:1) Nonadaptive 2)Adaptive

1) **Nonadaptive algorithms** do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from *I* to *J* (for all *I* and *J*) is computed in advance, off-line, and downloaded to the routers when the network is booted. This procedure is sometimes called **static routing**.

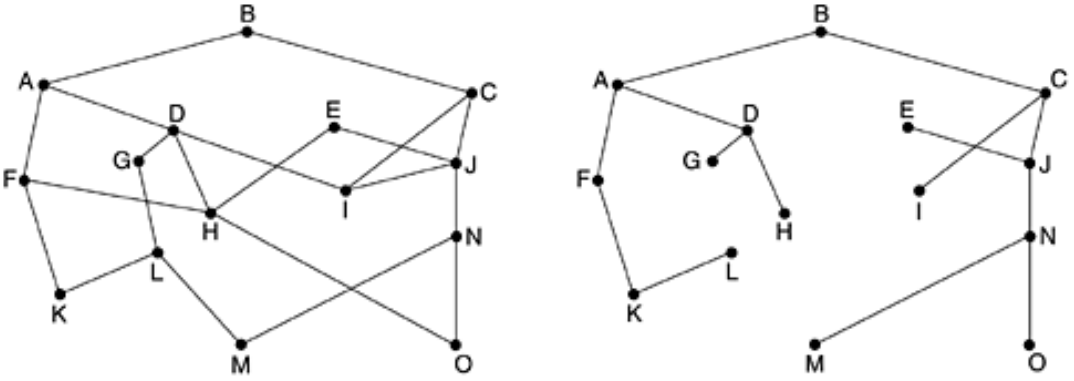
2)Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well. Adaptive algorithms differ in where they get their information (e.g., locally, from adjacent routers, or from all routers), when they change the routes

Forwarding

- To make a distinction between routing, which is making the decision which routes to use and forwarding which is what happens when a packet arrives

The Optimality Principle

- Before we get into specific algorithms, it may be helpful to note that one can make a general statement about optimal routes without regard to network topology or traffic. This statement is known as the optimality principle.A subnet. (b) A sink tree for router



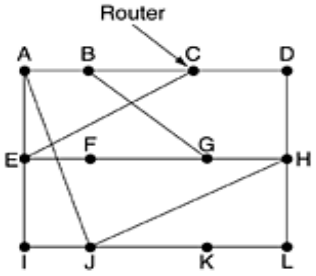
(a)

Shortest Path Routing

- The concept of a shortest path deserves some explanation. One way of measuring path length is the number of hops

Distance Vector Routing

- Distance vector routing algorithms operate by having each router maintain a table (i.e, a vector) giving the best known distance to each destination and which line to use to get there.
- These tables are updated by exchanging information with the neighbors. The distance vector routing algorithm is sometimes called by other names, most commonly the distributed Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm,



(a)

New estimated delay from J

To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J	

Vectors received from J's four neighbors

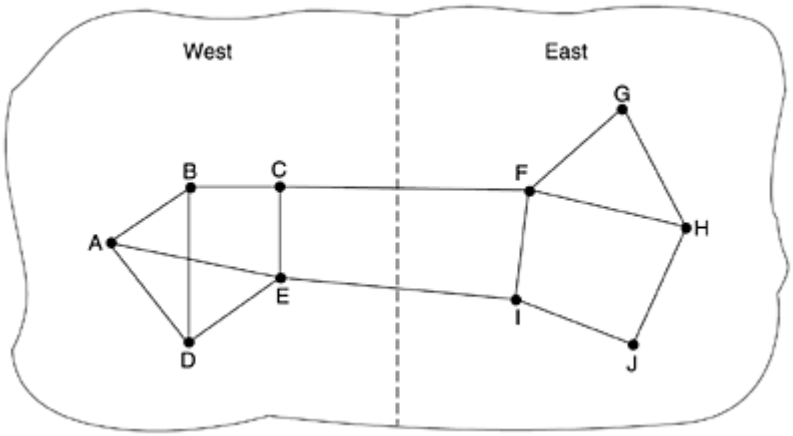
(b)

Link State Routing

The idea behind link state routing is simple and can be stated as five parts. Each router must do the following:

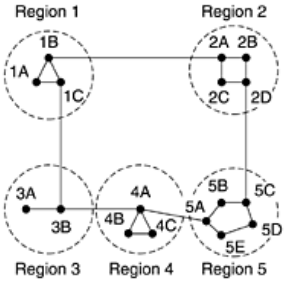
1. Discover its neighbors and learn their network addresses.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

A subnet in which the East and West parts are connected by two lines



Hierarchical Routing

- When hierarchical routing is used, the routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

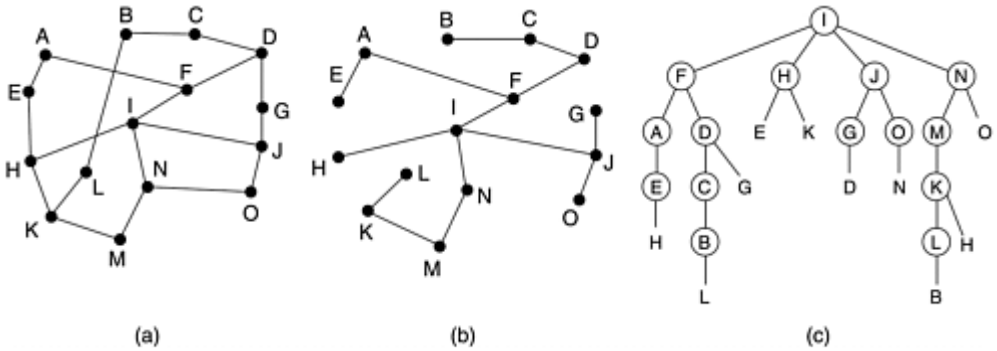
Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Broadcast Routing

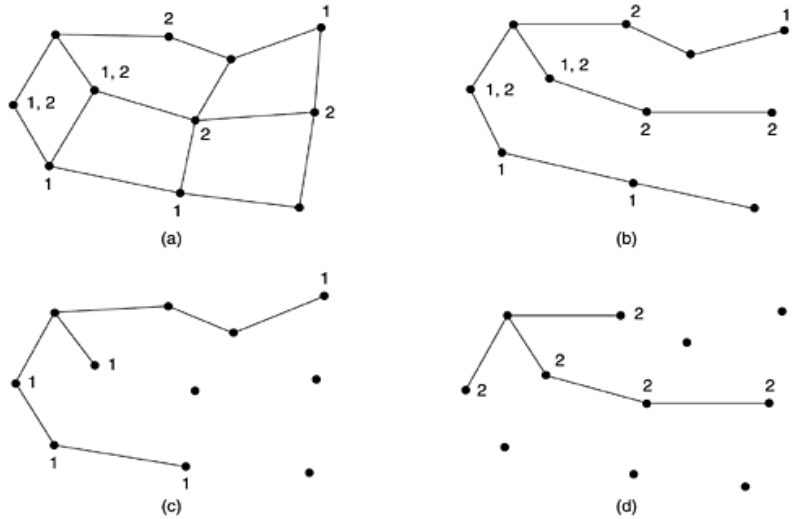
- Sending a packet to all destinations simultaneously is called broadcasting; various methods have been proposed for doing it.
- One broadcasting method that requires no special features from the subnet is for the source to simply send a distinct packet to each destination

- Each Packet contains either a list of destinations or a bit map indicating the desired destinations



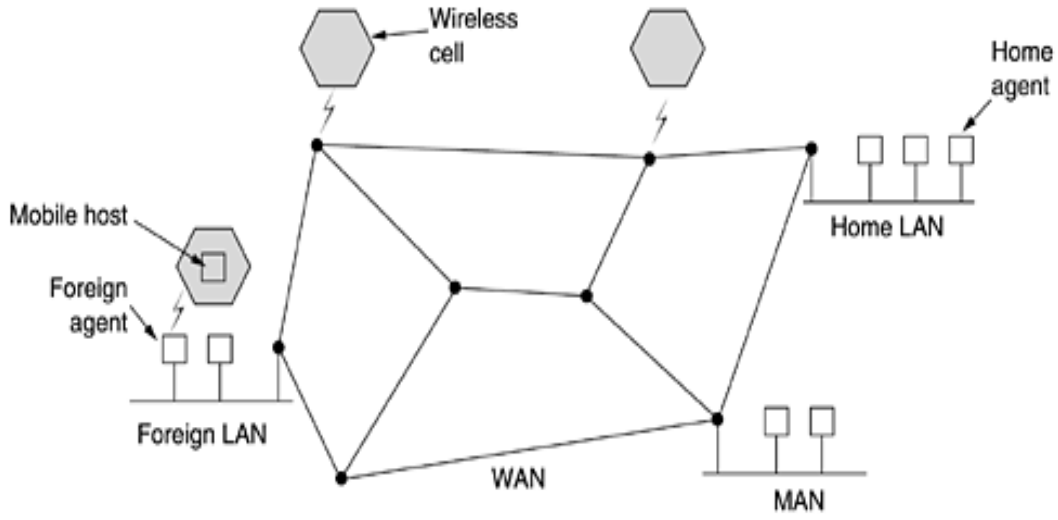
Multicast Routing

- Sending a message to such a group is called multicasting, and its routing algorithm is called multicast routing. In this section we will describe one way of doing multicast routing.



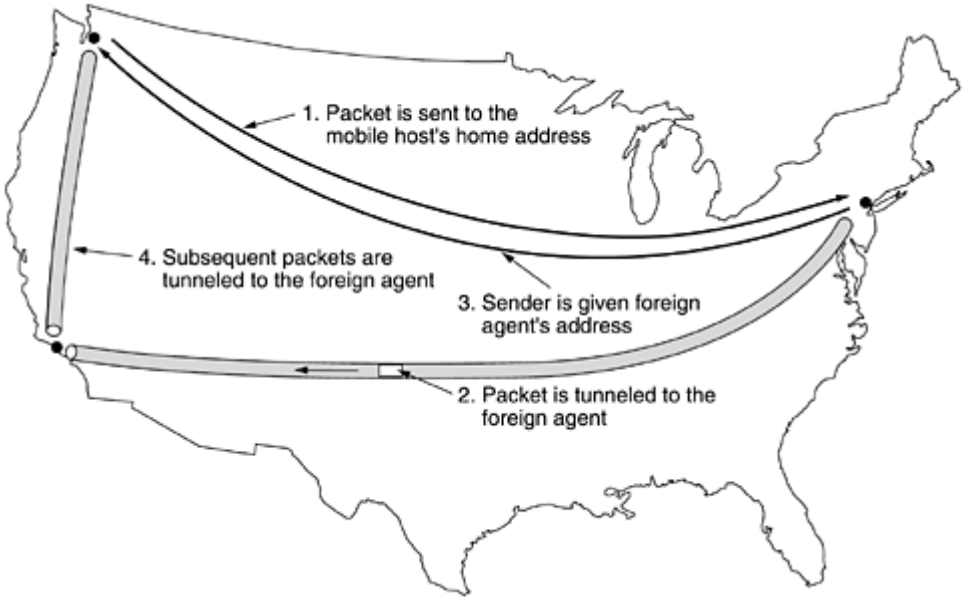
Routing for Mobile Hosts

- Millions of people have portable computers nowadays, and they generally want to read their e-mail and access their normal file systems wherever in the world they may be.
- These mobile hosts introduce a new complication: to route a packet to a mobile host, the network first has to find it. The subject of incorporating mobile hosts into a network is very young, but in this section we will sketch some of the issues and give a possible solution



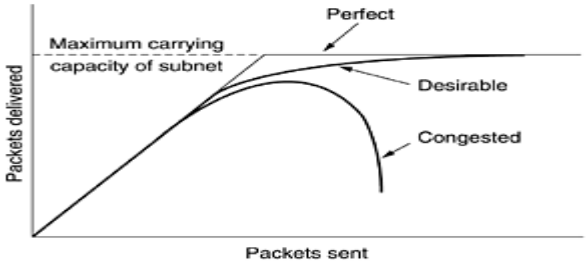
- the world is divided up (geographically) into small units. Let us call them areas, where an area is typically a LAN or wireless cell.
- Each area has one or more **foreign agents**, which are processes that keep track of all mobile hosts visiting the area. In addition, each area has a **home agent**, which keeps track of hosts whose home is in the area, but who are currently visiting another area.

Packet Routing For Mobile Hosts.



CONGESTION CONTROL ALGORITHMS

- When too many packets are present in (a part of) the subnet, performance degrades. This situation is called congestion.



- Congestion can be brought on by several factors. If all of a sudden, streams of packets begin arriving on three or four input lines and all need the same output line, a queue will build up. If there is insufficient memory to hold all of them, packets will be lost.

General Principles of Congestion Control

- Many problems in complex systems, such as computer networks, can be viewed from a control theory point of view. This approach leads to dividing all solutions into two groups: open loop and closed loop.
- Open loop solutions attempt to solve the problem by good design, in essence, to make sure it does not occur in the first place. This approach has three parts when applied to congestion control:
  1. Monitor the system to detect when and where congestion occurs.
  2. Pass this information to places where action can be taken.
  3. Adjust system operation to correct the problem.

  A variety of metrics can be used to monitor the subnet for congestion.

Congestion Prevention Policies

- Let us begin our study of methods to control congestion by looking at open loop systems. These systems are designed to minimize congestion in the first place, rather than letting it happen and reacting after the fact. They try to achieve their goal by using appropriate policies at various levels.

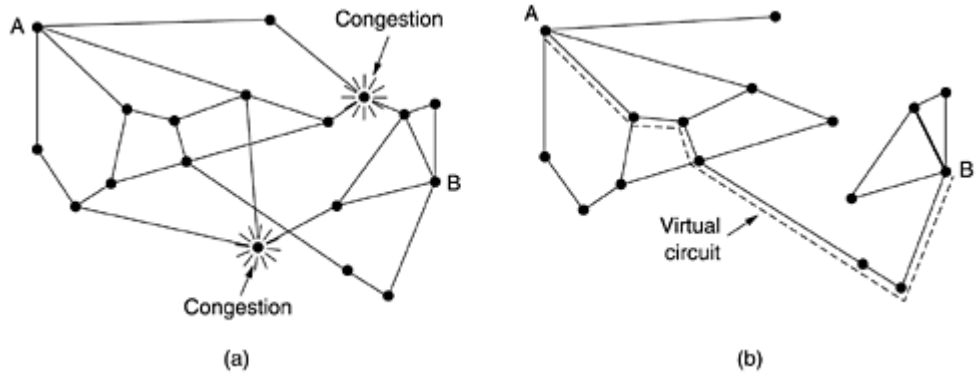
Policies that affect congestion.

- The congestion control methods described above are basically open loop: they try to prevent congestion from occurring in the first place, rather than dealing with it after the fact. In this section we will describe some approaches to dynamically controlling congestion in virtual-circuit subnets. In the next two, we will look at techniques that can be used in any subnet.
- One technique that is widely used to keep congestion that has already started from getting worse is **admission control**. The idea is simple: once congestion has been signaled, no more virtual circuits are set up until the problem has gone away

Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

(a) A congested subnet. (b) A redrawn subnet that eliminates the congestion. A virtual circuit from* A *to* B *is also shown.



❖ Suppose that a host attached to router A wants to set up a connection to a host attached to router B. Normally, this connection would pass through one of the congested routers. To avoid this situation, we can redraw the subnet as shown the congested routers and all of their lines. The dashed line shows a possible route for the virtual circuit that avoids the congested routers.

Congestion Control in Datagram Subnets

- To maintain a good estimate of u, a sample of the instantaneous line utilization, f (either 0 or 1), can be made periodically and u updated according to Where

$$u_{new} = au_{old} + (1 - a)f$$

The Warning Bit

- As long as the router was in the warning state, it continued to set the warning bit, which meant that the source continued to get acknowledgements with it set.

Choke Packets

- The previous congestion control algorithm is fairly subtle. It uses a roundabout means to tell the source to slow down., the router sends a choke packet back to the source host, giving it the destination found in the packet

QUALITY OF SERVICE

REQUIREMENTS

- A stream of packets from a source to a destination is called a flow.In a connection-oriented network, all the packets belonging to a flow follow the same route; in a connectionless network, they may follow different routes.
- The needs of each flow can be characterized by four primary parameters: reliability, delay, jitter, and bandwidth.
- Together these determine the **QoS** (**Quality of Service**) the flow requires. ATM networks classify flows in four broad categories with respect to their QoS demands as follows

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

1. Constant bit rate (e.g., telephony).
2. Real-time variable bit rate (e.g., compressed videoconferencing).
3. Non-real-time variable bit rate (e.g., watching a movie over the Internet).
4. Available bit rate (e.g., file transfer).

TECHNIQUES FOR ACHIEVING GOOD QUALITY OF SERVICE

1) Overprovisioning

An easy solution is to provide so much router capacity, buffer space, and bandwidth that the packets just fly through easily.

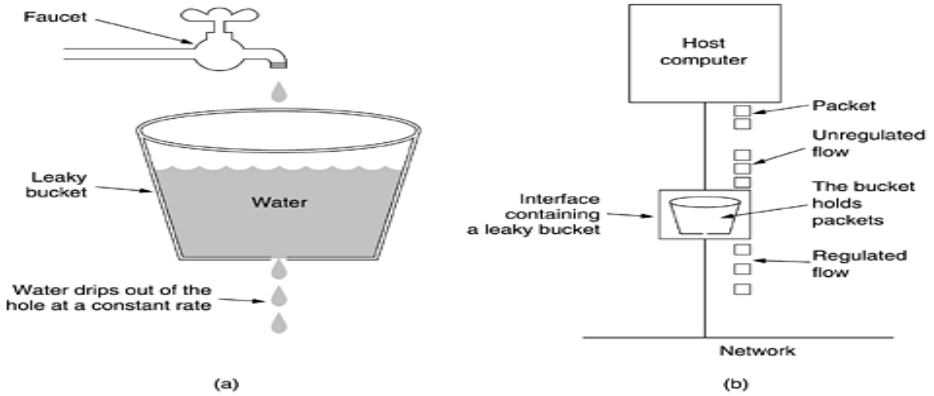
2)Buffering

- ❖ Flows can be buffered on the receiving side before being delivered. Buffering them does not affect the reliability or bandwidth, and increases the delay, but it smooths out the jitter. For audio and video on demand, jitter is the main problem,

3)Traffic Shaping

- Traffic shaping is about regulating the average rate (and burstiness) of data transmission. In contrast, the sliding window protocols we studied earlier limit the amount of data in transit at once, not the rate at which it is sent

The Leaky Bucket Algorithm

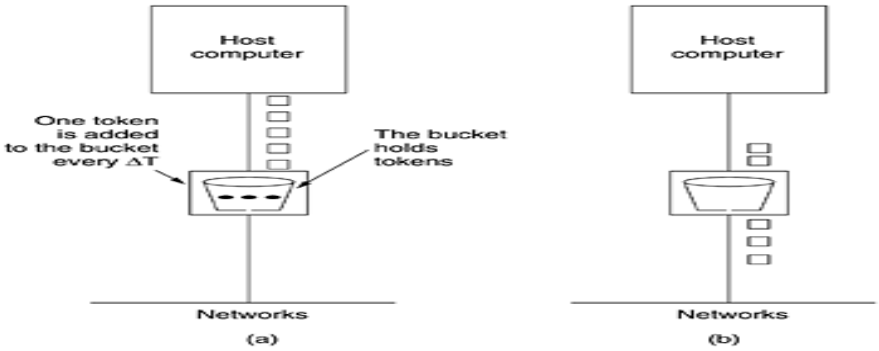


- ❖ It was first proposed by Turner (1986) and is called the **leaky bucket algorithm**. In fact, it is nothing other than a single-server queueing system with constant service time.
- ❖ The host is allowed to put one packet per clock tick onto the network. Again, this can be enforced by the interface card or by the operating system.
- ❖ This mechanism turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion.
- ❖ When the packets are all the same size (e.g., ATM cells), this

The Token Bucket Algorithm

- ❖ The leaky bucket algorithm enforces a rigid output pattern at the average rate, no matter how bursty the traffic is.
- ❖ For many applications, it is better to allow the output to speed up somewhat when large bursts arrive, so a more flexible algorithm is needed, preferably one that never loses data.

- ❖ One such algorithm is the token bucket algorithm. In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token every ΔT sec.
- ❖ The token bucket algorithm provides a different kind of traffic shaping than that of the leaky bucket algorithm.
- ❖ The leaky bucket algorithm does not allow idle hosts to save up permission to send large bursts later.



Resource Reservation

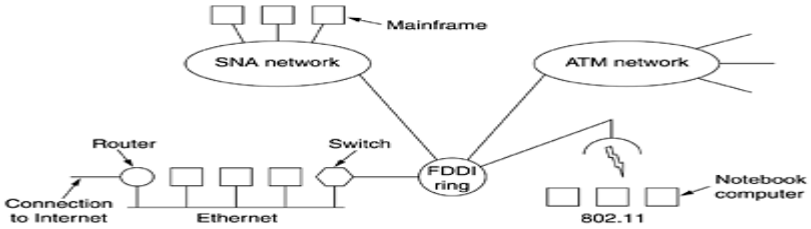
Three different kinds of resources can potentially be reserved:

1. Bandwidth.
2. Buffer space.
3. CPU cycles.

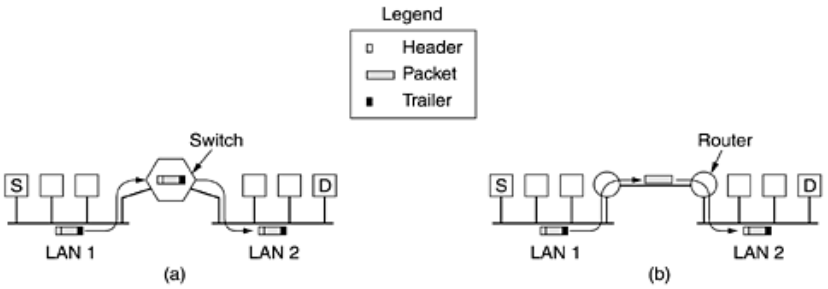
The first one, bandwidth, is the most obvious.

INTERNETWORKING

A collection of interconnected networks



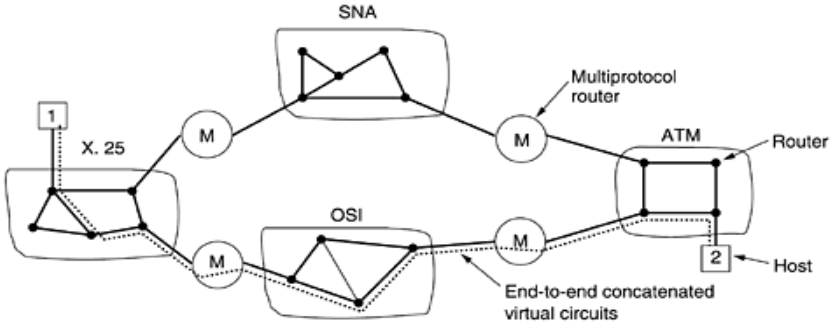
- ❖ The purpose of interconnecting all these networks is to allow users on any of them to communicate with users on all the other ones and also to allow users on any of them to access data on any of them. Accomplishing this goal means sending packets from one network to another.
- ❖ ***(a) Two Ethernets connected by a switch. (b) Two Ethernets connected by routers.***



Concatenated Virtual Circuits

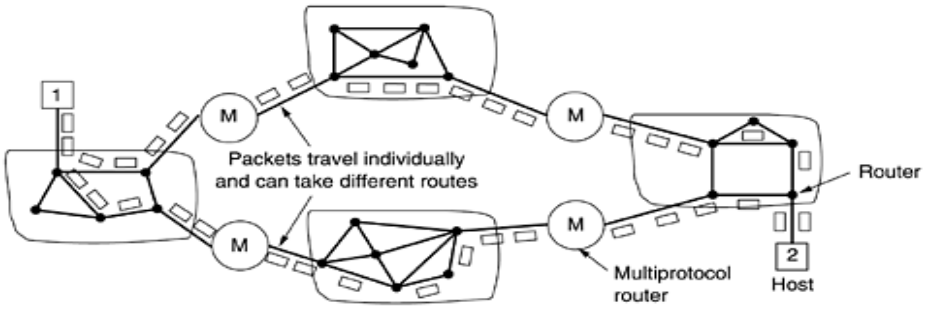
- Two styles of internetworking are possible: a connection-oriented concatenation of virtual-circuit subnets, and a datagram internet style. We will now examine these in turn, but first a word of caution.
- In the past, most (public) networks were connection oriented (and frame relay, SNA, 802.16, and ATM still are). Then with the rapid acceptance of the Internet, datagrams became fashionable

Internetworking using concatenated virtual circuits



Connectionless Internetworking

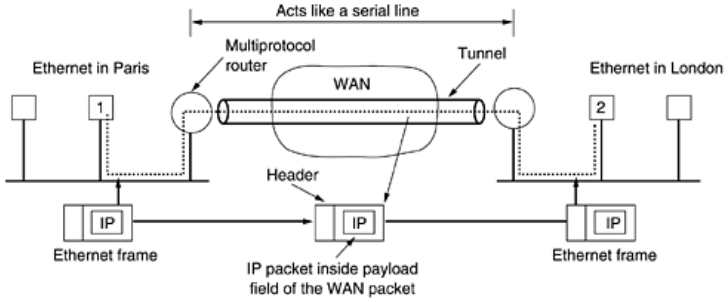
- The alternative internetwork model is the datagram model,. In this model, the only service the network layer offers to the transport layer is the ability to inject datagrams into the subnet and hope for the best.
- There is no notion of a virtual circuit at all in the network layer, let alone a concatenation of them. This model does not require all packets belonging to one connection to traverse the same sequence of gateways.



Tunneling

Tunneling a packet from Paris to London

- As an example, think of an international bank with a TCP/IP-based Ethernet in Paris, a TCP/IP-based Ethernet in London, and a non-IP wide area network (e.g., ATM) in between, as shown

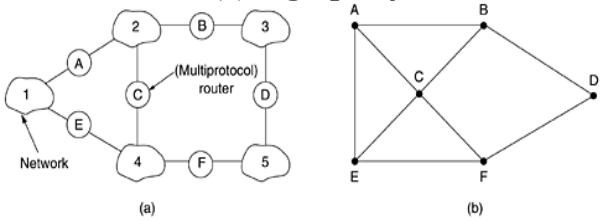


- The solution to this problem is a technique called **tunneling**. To send an IP packet to host 2, host 1 constructs the packet containing the IP address of host 2, inserts it into an Ethernet frame addressed to the Paris multiprotocol router, and puts it on the Ethernet.

Internetwork Routing

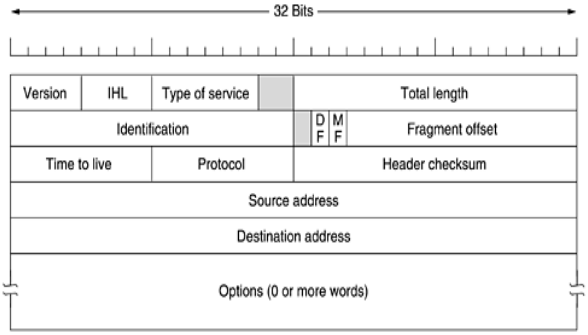
- Routing through an internetwork is similar to routing within a single subnet, but with some added complications.

(a) An internetwork. (b) A graph of the internetwork



The IP Protocol

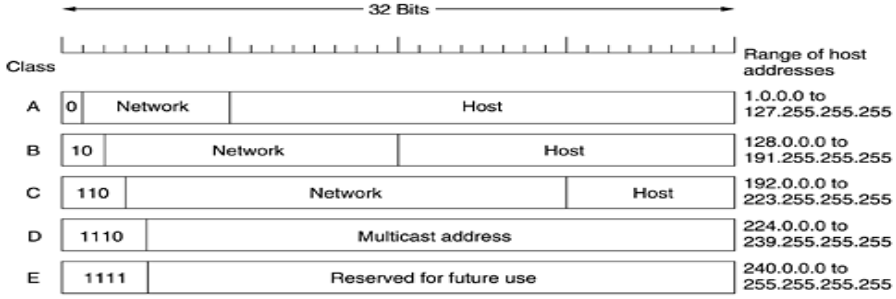
- An appropriate place to start our study of the network layer in the Internet is the format of the IP datagrams themselves. An IP datagram consists of a header part and a text part. The header has a 20-byte fixed part and a variable length optional part.



IP Addresses

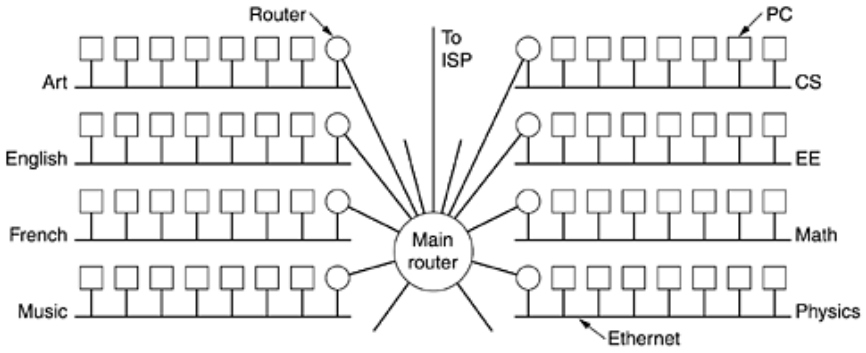
- Every host and router on the Internet has an IP address, which encodes its network number and host number.
- The combination is unique: in principle, no two machines on the Internet have the same IP address. All IP addresses are 32 bits long and are used in the Source

address and Destination address fields of IP packets. It is important to note that an IP address does not actually refer to a host.



Subnets

- As we have seen, all the hosts in a network must have the same network number. This property of IP addressing can cause problems as networks grow. ATM networks classify flows in four broad categories with respect to their QoS demands as follows

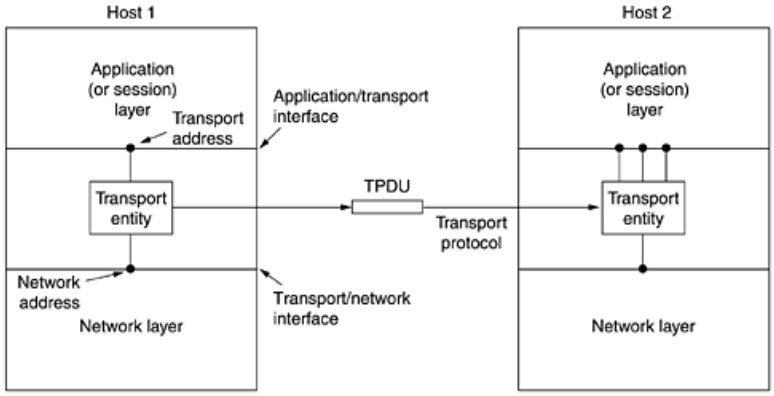


UNIT - III
THE TRANSPORT LAYER

The Transport Service

Services Provided to the Upper Layers

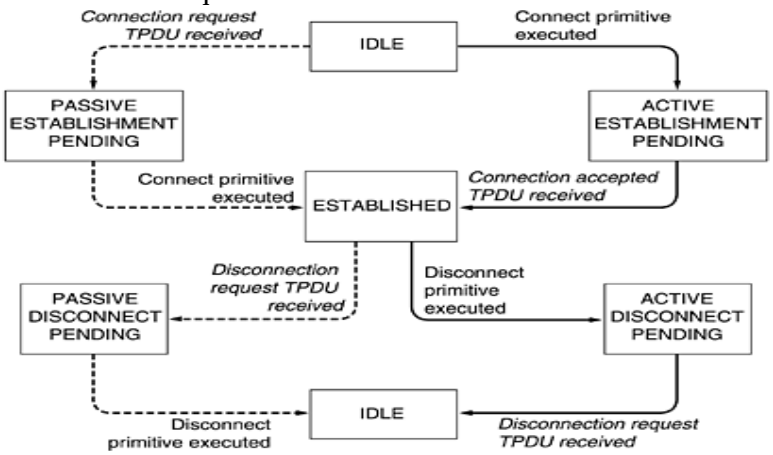
- The ultimate goal of the transport layer is to provide efficient, reliable, and cost-effective service to its users, normally processes in the application layer.
- To achieve this goal, the transport layer makes use of the services provided by the network layer. The hardware and/or software within the transport layer that does the work is called the **transport entity**.



Transport Service Primitives

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

state diagram for a simple connection management scheme. Transitions labeled in italics are caused by packet arrivals. The solid lines show the client's state sequence. The dashed lines show the server's state sequence.

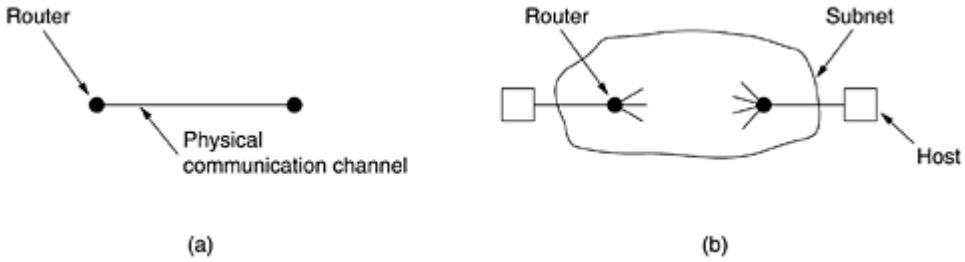


Berkeley Sockets

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

Elements of Transport Protocols

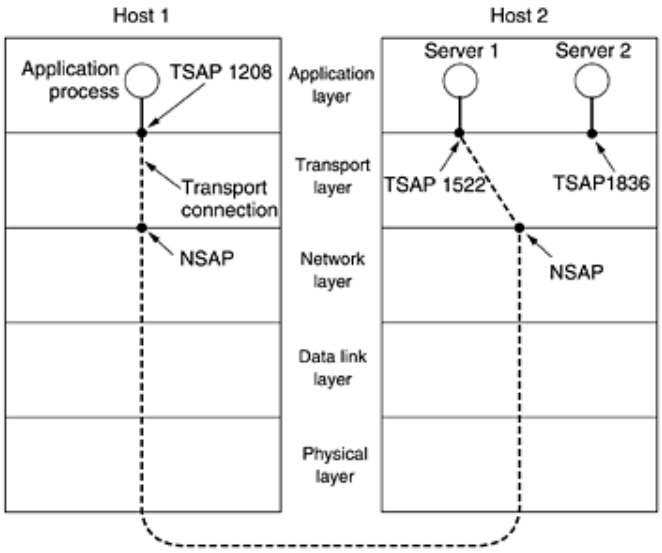
- The transport service is implemented by a transport protocol used between the two transport entities. In some ways, transport protocols resemble the data link protocols we studied in detail



(a) (b)

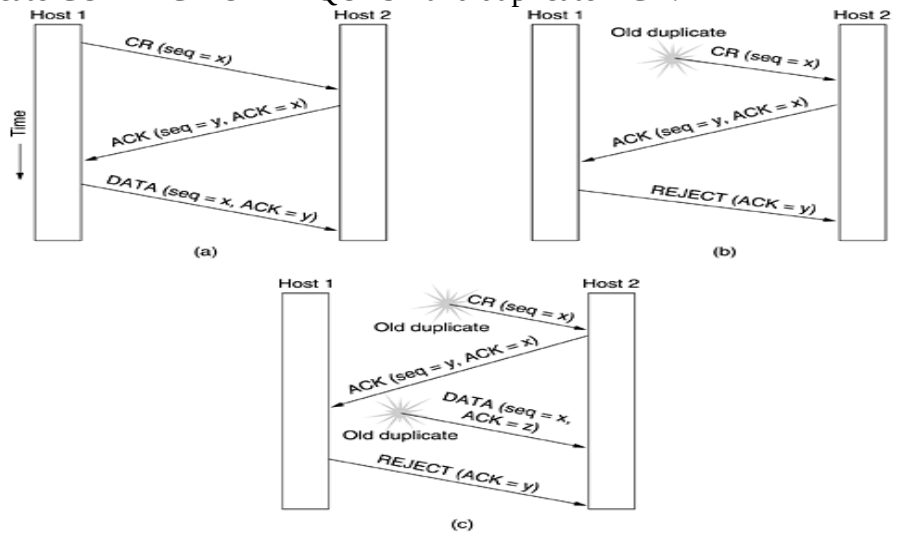
ADDRESSING

- When an application (e.g., a user) process wishes to set up a connection to a remote application process, it must specify which one to connect to. (Connectionless transport has the same problem:
- To whom should each message be sent?) The method normally used is to define transport addresses to which processes can listen for connection requests. In the Internet, these end points are called ports. In ATM networks, they are called AAL-SAPs. We will use the generic term TSAP, (Transport Service Access Point).
- The analogous end points in the network layer (i.e., network layer addresses) are then called NSAPs. IP addresses are examples of NSAPs.



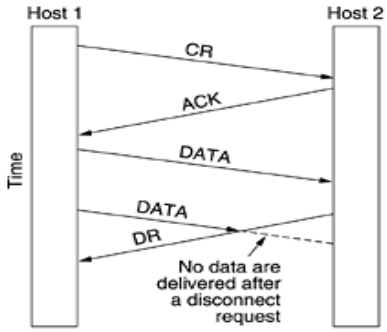
CONNECTION ESTABLISHMENT

- Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes **CONNECTION REQUEST.** (a) Normal operation. (b) Old duplicate **CONNECTION REQUEST** appearing out of nowhere. (c) Duplicate CONNECTION REQUEST and duplicate ACK.

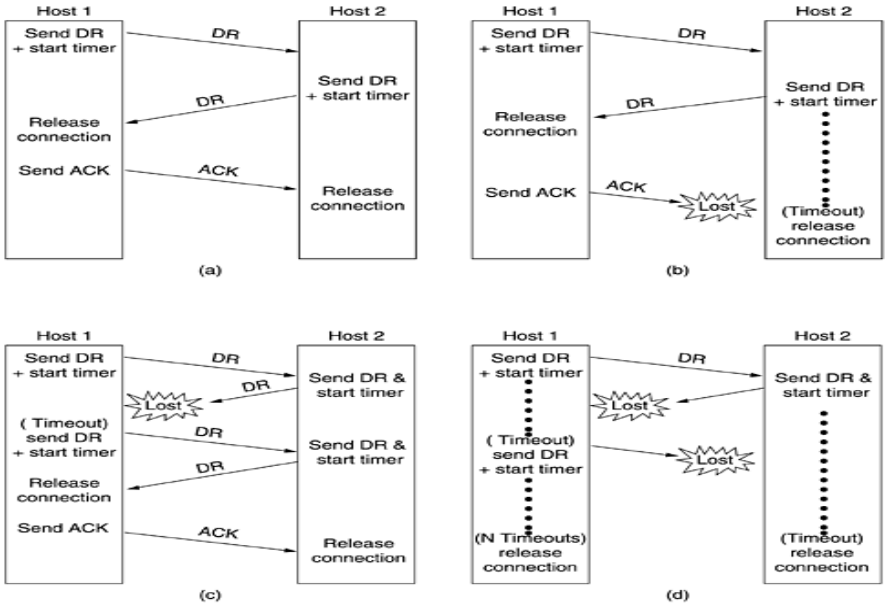


CONNECTION RELEASE

- Releasing a connection is easier than establishing one. Nevertheless, there are more pitfalls than one might expect. As we mentioned earlier, there are two styles of terminating a connection: asymmetric release and symmetric release.
- Asymmetric release is the way the telephone system works: when one party hangs up, the connection is broken. Symmetric release treats the connection as two separate unidirectional connections and requires each one to be released separately.



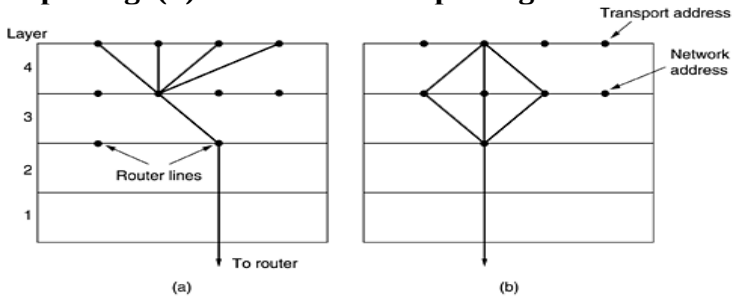
Four protocol scenarios for releasing a connection. (a) Normal case of three-way handshake. (b) Final ACK lost. (c) Response lost. (d) Response lost and subsequent DRs lost.



Multiplexing

- Multiplexing several conversations onto connections, virtual circuits, and physical links plays a role in several layers of the network architecture. In the transport layer the need for multiplexing can arise in a number of ways.
- For example, if only one network address is available on a host, all transport connections on that machine have to use it. When a TPDU comes in, some way is needed to tell which process to give it to. This situation, called upward multiplexing,

(a) Upward multiplexing. (b) Downward multiplexing.



A Simple Transport Protocol

Network packet	Meaning
CALL REQUEST	Sent to establish a connection
CALL ACCEPTED	Response to CALL REQUEST
CLEAR REQUEST	Sent to release a connection
CLEAR CONFIRMATION	Response to CLEAR REQUEST
DATA	Used to transport data
CREDIT	Control packet for managing the window

- The example protocol in graphical form. Transitions that leave the connection state unchanged have been omitted for simplicity.

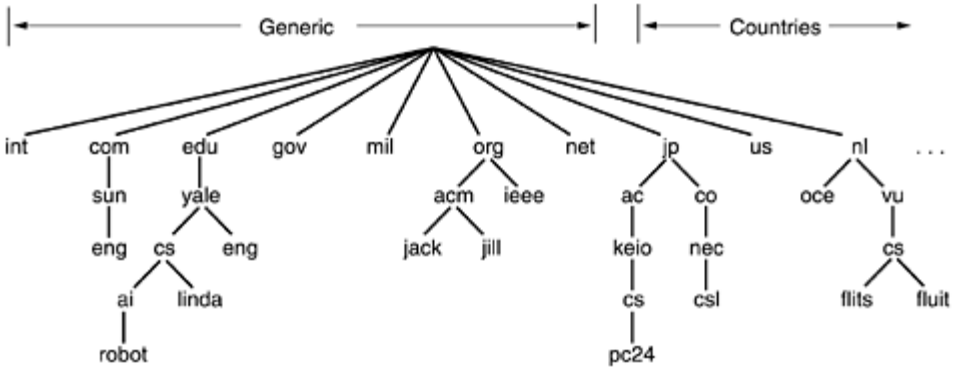
THE APPLICATION LAYER

DNS—The Domain Name System

- The essence of DNS is the invention of a hierarchical, domain-based naming scheme and a distributed database system for implementing this naming scheme.
- It is primarily used for mapping host names and e-mail destinations to IP addresses but can also be used for other purposes. DNS is defined in RFCs 1034 and 1035.
- Very briefly, the way DNS is used is as follows. To map a name onto an IP address, an application program calls a library procedure called the resolver

The DNS Name Space

Managing a large and constantly changing set of names is a nontrivial problem



A portion of the Internet domain name space.

- The top-level domains come in two flavors: generic and countries. The original generic domains were ***com*** *(commercial),* ***edu*** (educational institutions), ***gov*** (the U.S. Federal Government), ***int*** (certain international organizations), ***mil*** (the U.S. armed forces), ***net*** (network providers), and ***org*** (nonprofit organizations).

Resource Records

- Every domain, whether it is a single host or a top-level domain, can have a set of resource records associated with it.
- A resource record is a five-tuple. Although they are encoded in binary for efficiency, in most expositions, resource records are presented as ASCII text, one line per resource record. The format we will use is as follows:

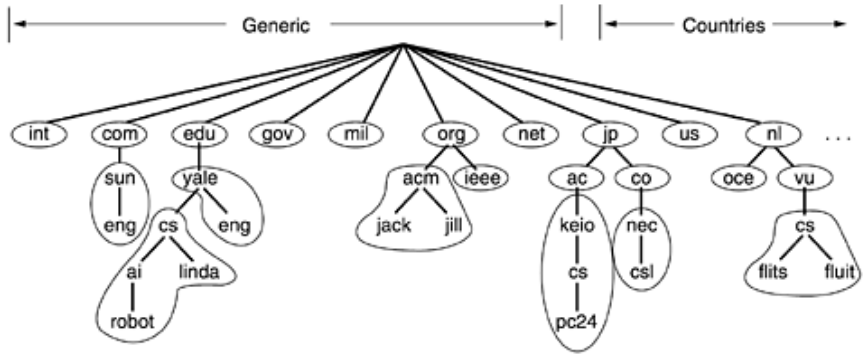
Domain_name Time_to_live Class Type Value

- The *Domain_name* tells the domain to which this record applies. Normally, many records exist for each domain and each copy of the database holds information about multiple domains.

The principal DNS resource record types for IPv4.

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

Name Servers



Electronic Mail

- Electronic mail, or e-mail, as it is known to its many fans, has been around for over two decades

Some smileys. They will not be on the final exam :-)

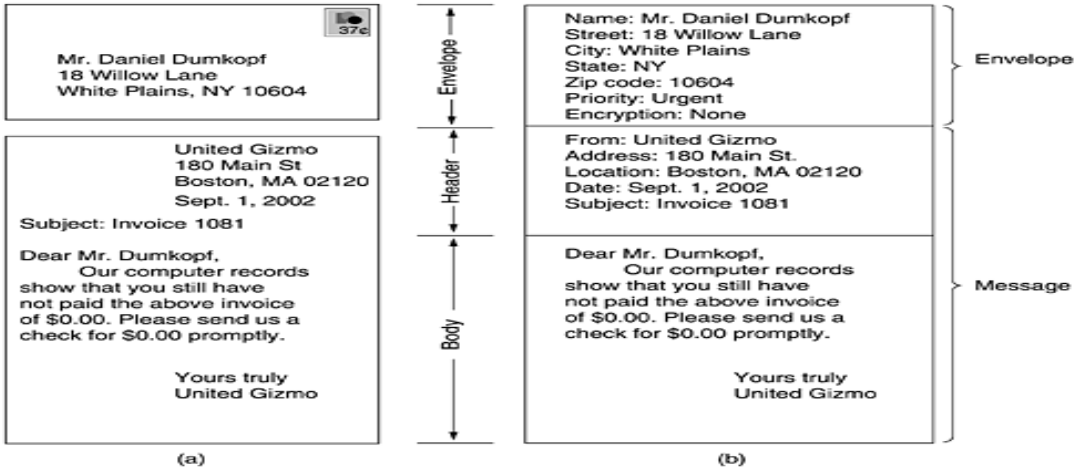
Smiley	Meaning	Smiley	Meaning	Smiley	Meaning
:-)	I'm happy	=|:-)	Abe Lincoln	:+)	Big nose
:-(	I'm sad/angry	=):-)	Uncle Sam	:-))	Double chin
:-|	I'm apathetic	*<:-)	Santa Claus	:-{)	Mustache
;-)	I'm winking	<:-(	Dunce	#:-)	Matted hair
:-(O)	I'm yelling	(-:	Australian	8-)	Wears glasses
:-(*)	I'm vomiting	:-)X	Man with bowtie	C:-)	Large brain

Architecture And Services

- In this section we will provide an overview of what e-mail systems can do and how they are organized.
- They normally consist of two subsystems: the **user agents**, which allow people to read and send e-mail, and the **message transfer agents**, which move the messages from the source to the destination.

E-Mail Systems Support Five Basic Functions

- **1)Composition** refers to the process of creating messages and answers. Although any text editor can be used for the body of the message, the system itself can provide assistance with addressing and the numerous header fields attached to each message
- **2)Transfer** refers to moving messages from the originator to the recipient
- **3)Reporting** has to do with telling the originator what happened to the message
- **4)Displaying** incoming messages is needed so people can read their e-mail. Sometimes conversion is required or a special viewer must be invoked,
- **5)Disposition** is the final step and concerns what the recipient does with the message after receiving it.
- Most systems allow users to create **mailboxes** to store incoming e-mail. Commands are needed to create and destroy mailboxes, inspect the contents of mailboxes, insert and delete messages from mailboxes, and so on.



MIME—The Multipurpose Internet Mail Extensions

- The basic idea of MIME is to continue to use the RFC 822 format, but to add structure to the message body and define encoding rules for non-ASCII messages. By not deviating from RFC 822, MIME messages can be sent using the existing mail programs and protocols

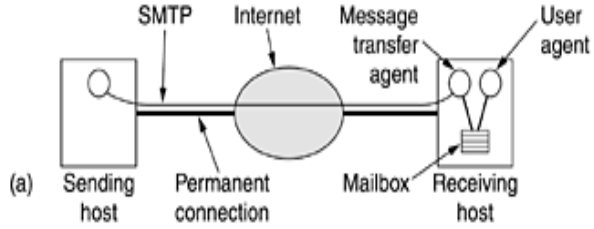
Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

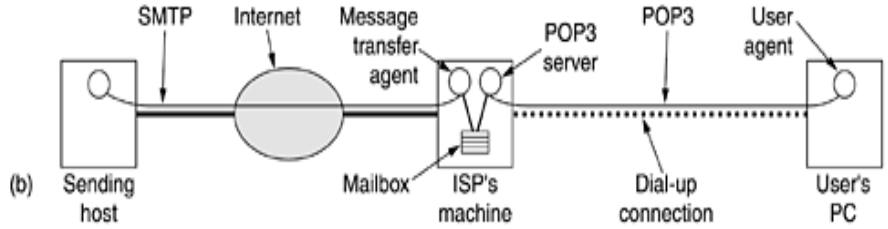
SMTP—The Simple Mail Transfer Protocol

- Within the Internet, e-mail is delivered by having the source machine establish a TCP connection to port 25 of the destination machine. Listening to this port is an e-mail daemon that speaks

SMTP (Simple Mail Transfer Protocol).

- SMTP is a simple ASCII protocol. After establishing the TCP connection to port 25, the sending machine, operating as the client, waits for the receiving machine, operating as the server, to talk first.





POP3

- POP3 begins when the user starts the mail reader. The mail reader calls up the ISP (unless there is already a connection) and establishes a TCP connection with the message transfer agent at port 110.
- Once the connection has been established, the POP3 protocol goes through three states in sequence:
    1. Authorization.
    2. Transactions.
    3. Update

IMAP

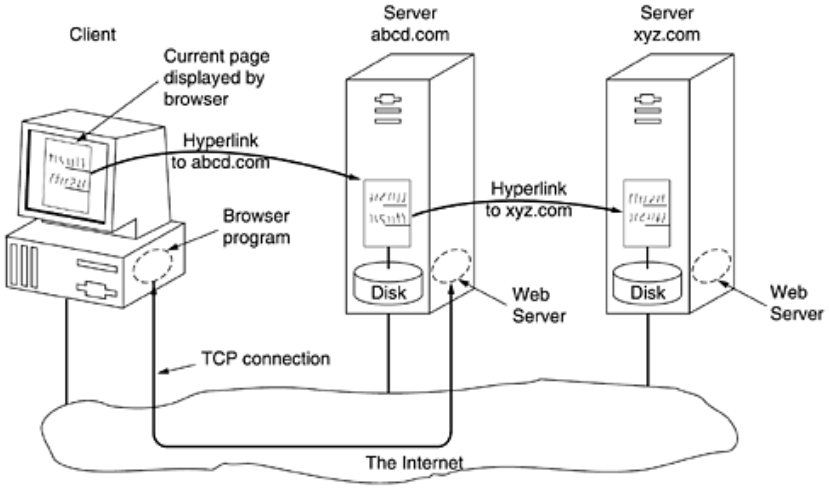
- This disadvantage gave rise to an alternative final delivery protocol, IMAP **(Internet Message Access Protocol),** which is defined in RFC 2060.

The World Wide Web

- In 1994, CERN and M.I.T. signed an agreement setting up the World Wide Web Consortium (sometimes abbreviated as **W3C**), an organization devoted to further

developing the Web, standardizing protocols, and encouraging interoperability between site

Architectural Overview

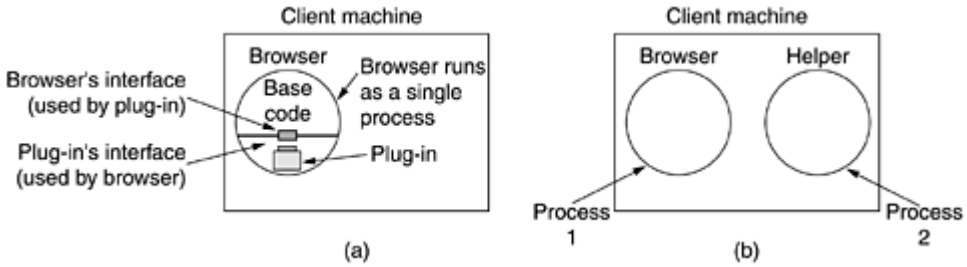


The Client Side

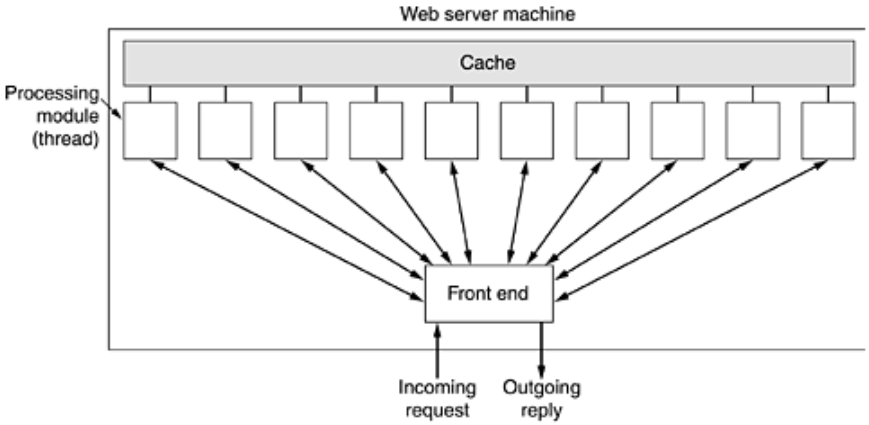
- Therefore, the embedded hyperlink needs a way to name any other page on the Web. Pages are named using **URLs** (**Uniform Resource Locators**). A typical URL is

http://www.abcd.com/products.html

.

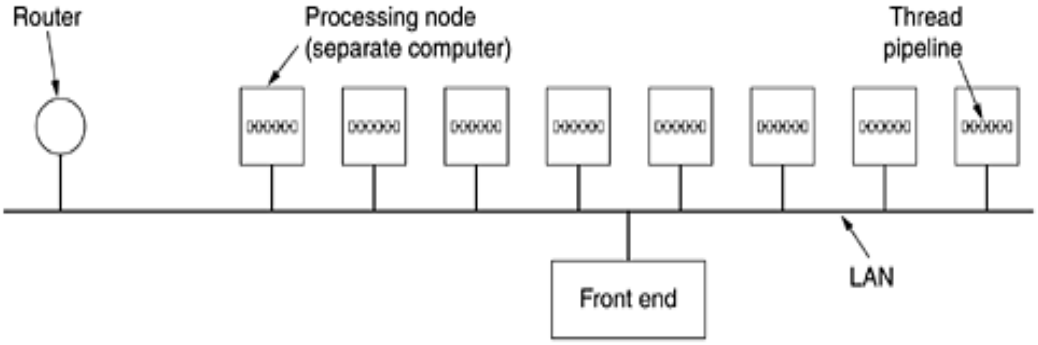


A multithreaded Web server with a front end and processing modules.

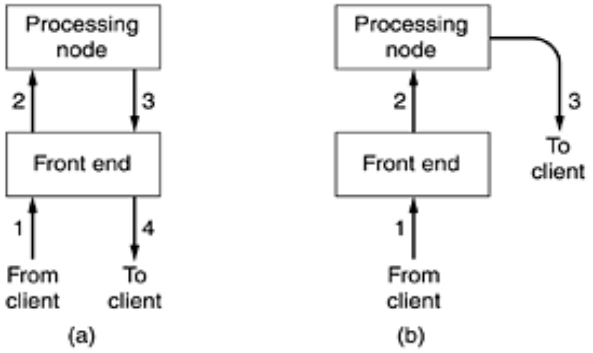


1. Resolve the name of the Web page requested.

2. Authenticate the client.
3. Perform access control on the client.
4. Perform access control on the Web page.
5. Check the cache.
6. Fetch the requested page from disk.
7. Determine the MIME type to include in the response.
8. Take care of miscellaneous odds and ends.
9. Return the reply to the client.
10. Make an entry in the server log.



(a) Normal request-reply message sequence. (b) Sequence when TCP handoff is used



URLs—Uniform Resource Locators

- The solution chosen identifies pages in a way that solves all three problems at once. Each page is assigned a URL (Uniform Resource Locator) that effectively serves as the page's worldwide name.
  - **http://www.cs.vu.nl/video/index-en.html**
- This URL consists of three parts: the protocol (http), the DNS name of the host (www.cs.vu.nl), and the file name (video/index-en.html), with certain punctuation separating the pieces. The file name is a path relative to the default Web directory at cs.vu.nl.

Some common URLs

Name	Used for	Example
http	Hypertext (HTML)	http://www.cs.vu.nl/~ast/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
news	Newsgroup	news:comp.os.minix
news	News article	news:AA0134223112@cs.utah.edu
gopher	Gopher	gopher://gopher.tc.umn.edu/11/Libraries
mailto	Sending e-mail	mailto:JohnUser@acm.org
telnet	Remote login	telnet://www.w3.org:80

HTML—The HyperText Markup Language

- Web pages are currently written in a language called **HTML** (**HyperText Markup Language**). HTML allows users to produce Web pages that include text, graphics, and pointers to other Web pages.

Tag	Description
<html> ... </html>	Declares the Web page to be written in HTML
<head> ... </head>	Delimits the page's head
<title> ... </title>	Defines the title (not displayed on the page)
<body> ... </body>	Delimits the page's body
<h *n*> ... </h*n*>	Delimits a level *n* heading
...	Set ... in boldface
...	Set ... in italics
...	Center ... on the page horizontally
...	Brackets an unordered (bulleted) list
...	Brackets a numbered list
...	Brackets an item in an ordered or numbered list
 	Forces a line break here
<p>	Starts a paragraph
<hr>	Inserts a horizontal rule
<img src="...">	Displays an image here
 ... 	Defines a hyperlink

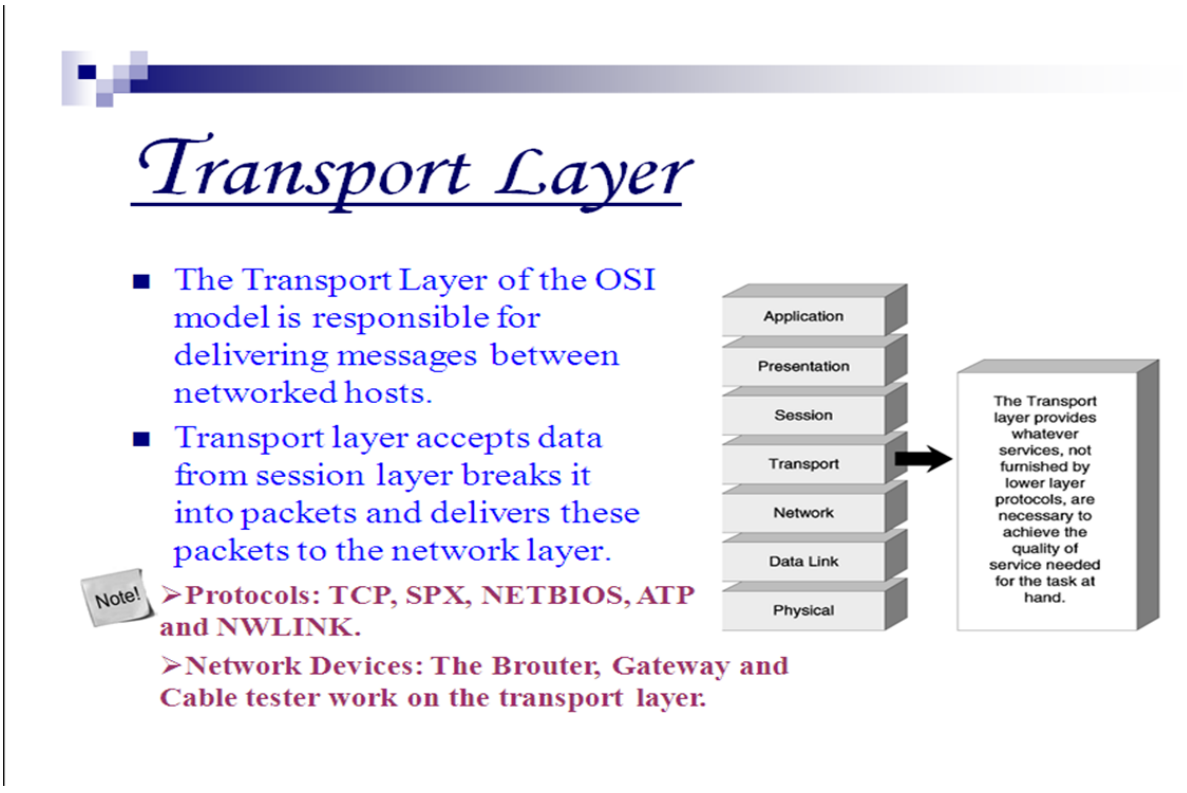
XHTML—The eXtended HyperText Markup Language

- HTML keeps evolving to meet new demands. Many people in the industry feel that in the future, the majority of Web-enabled devices will not be PCs, but wireless, handheld PDA-type devices.
- These devices have limited memory for large browsers full of heuristics that try to somehow deal with syntactically incorrect Web pages. Thus, the next step after HTML 4 is a language that is Very Picky. It is called **XHTML** (**eXtended HyperText Markup Language**)

UNIT-IV

TRANSPORT LAYER

In computer networking, the transport layer is a conceptual division of methods in the layered architecture of protocols in the network stack in the Internet protocol suite and the OSI model. The protocols of this layer provide host-to-host communication services for applications. It provides services such as connection-oriented communication, reliability, flow control, and multiplexing.

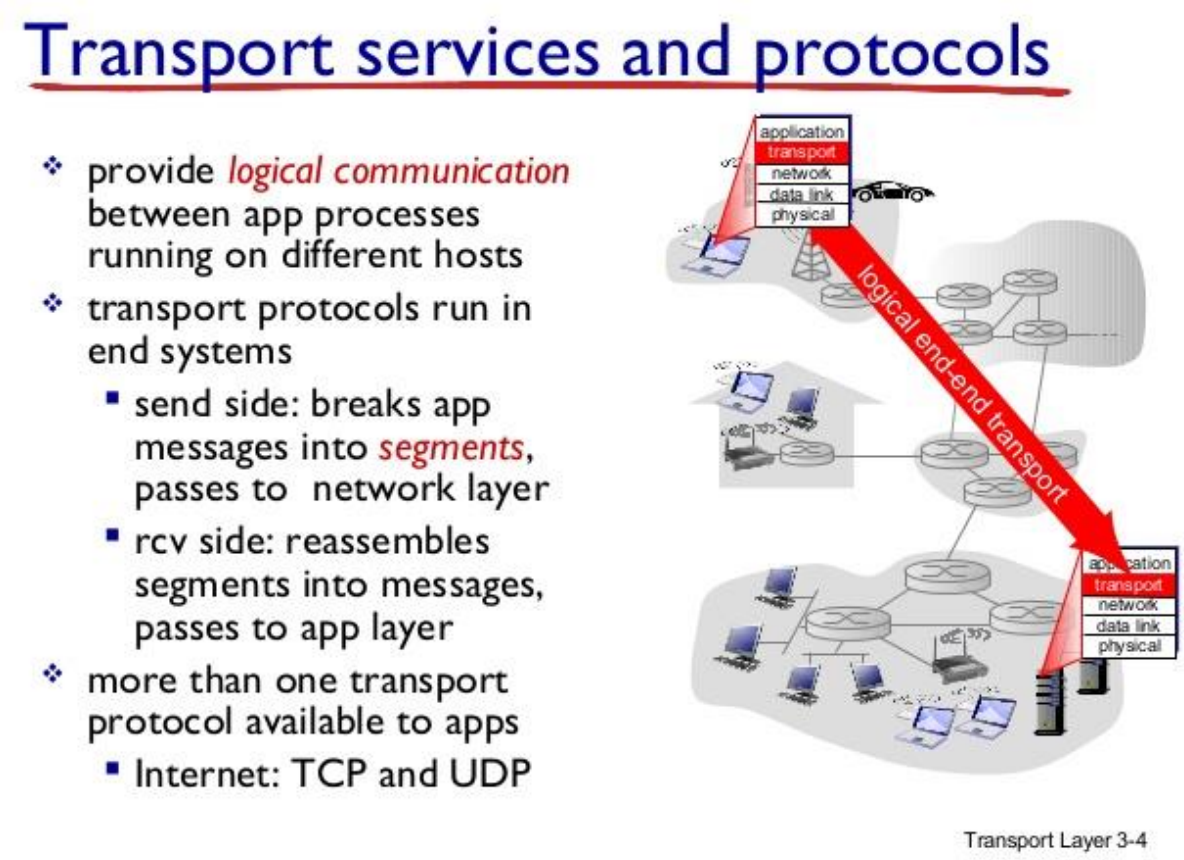


- The transport layer is a 4 th layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. ...
- The transport layer protocols are implemented in the end systems but not in the network routers.

TRANSPORT SERVICE

The services provided by the transport layer protocols can be divided into five categories:

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- Multiplexing



ELEMENT OF TRANSPORT PROTOCOL

1. ELEMENTS OF TRANSPORT PROTOCOL A PRESENTATION BY SHASHANK, ABHISHEK AND UDIT
2. TRANSPORT LAYER • To provide reliable, cost effective data transfer from source to destination • This layer deals with end to end transfer of data • Here transport entity ...
3. Elements of Transport Protocol • Addressing • Connection Establishment • Connection Release • Flow Control and Buffering • Multiplexing • Crash Recovery

Elements of Transport Protocols

The transport service is implemented by a **transport protocol used between t**he two transport entities.

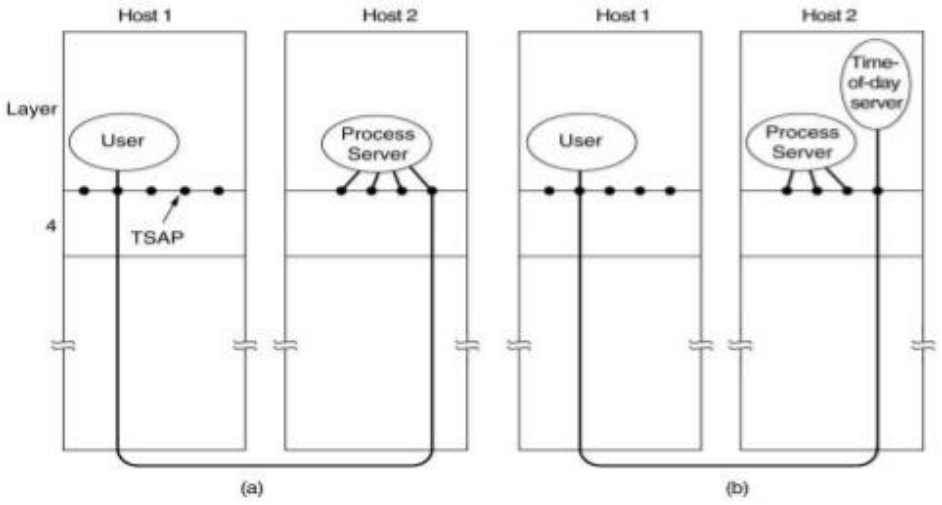
Though the transport protocols resemble the Data Link Protocols, significant differences are present due to the major dissimilarities between the environments in which the two protocols operate.

A physical channel exists in DLL, where as it is replaced by the entire subnet for Transport Layer

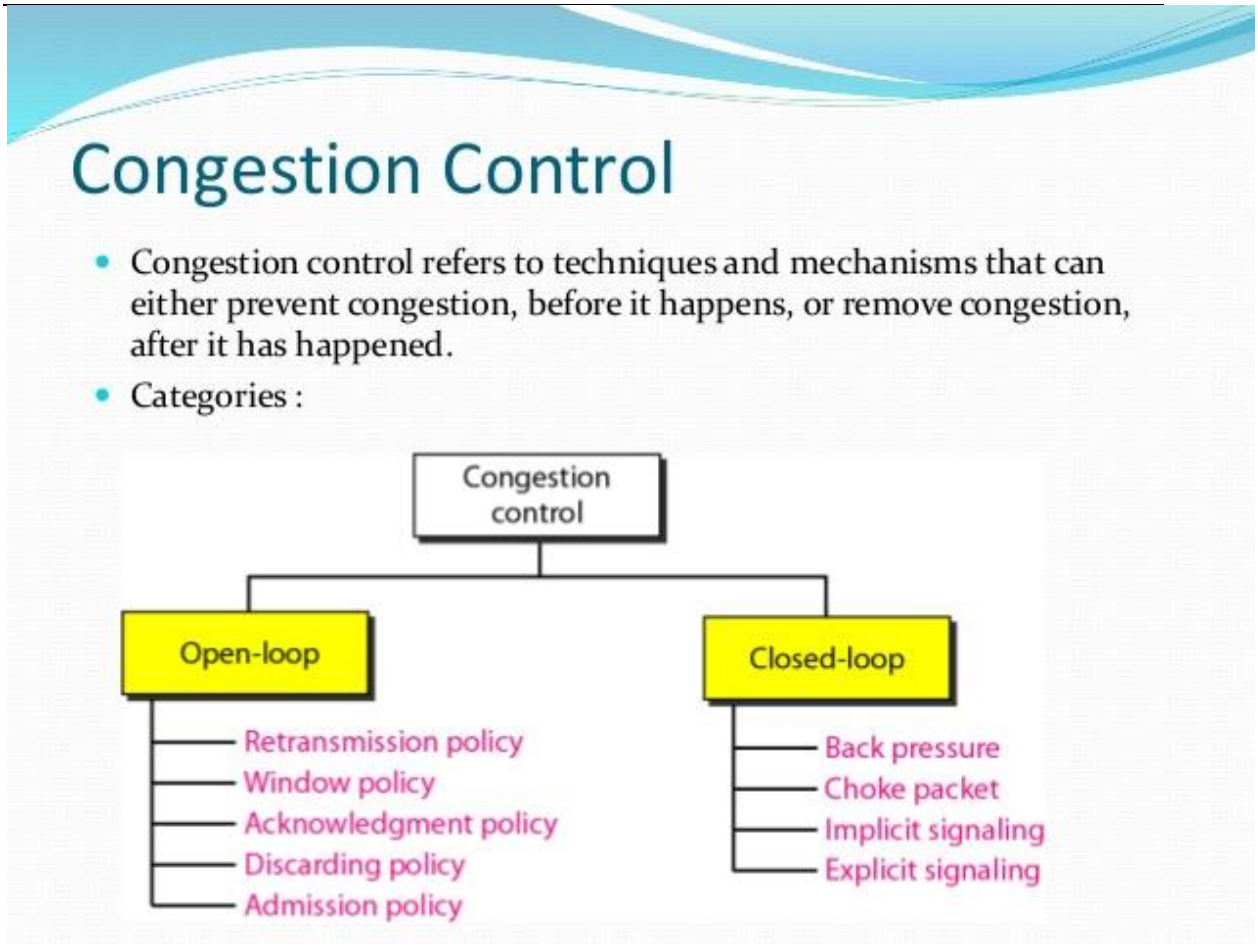
No explicit addressing of destinations is required in DLL, where it is required for Transport layer

A final difference between the data link and transport layers is one of amount rather than of kind. Buffering and flow control are needed in both layers, but the presence of a large and dynamically varying number of connections in the transport layer may require a different approach than we used in the data link layer

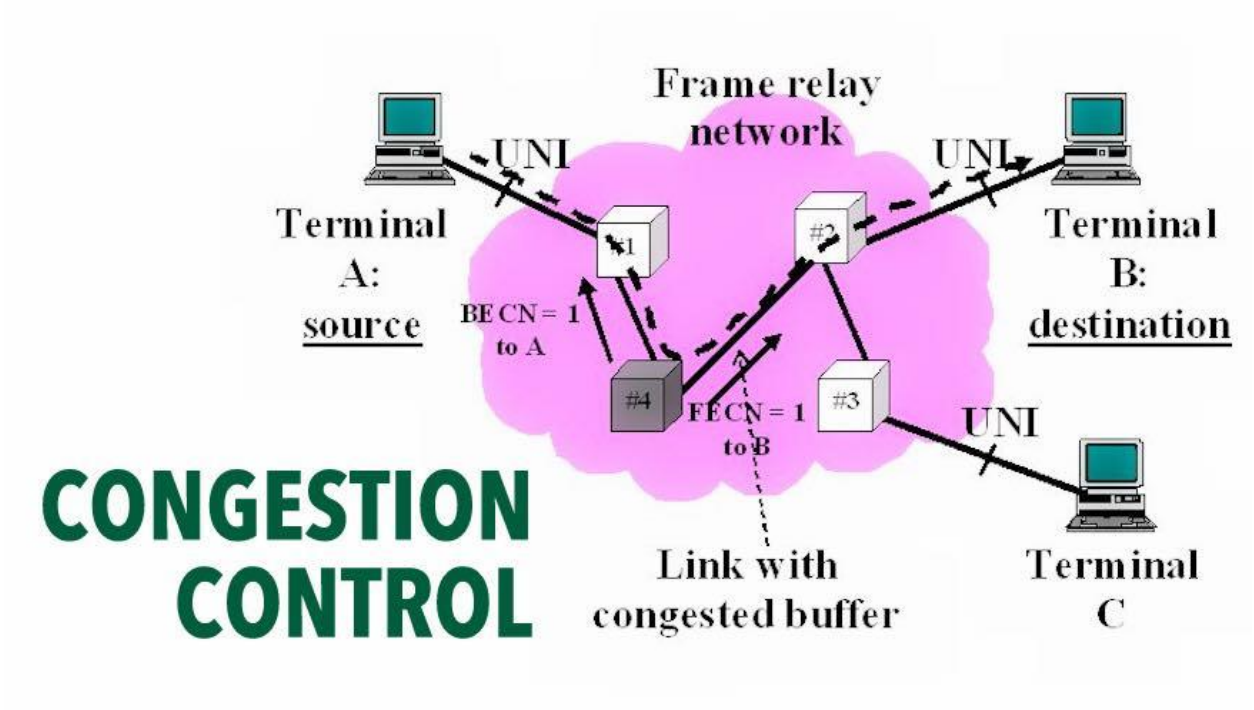
ELEMENTS OF TRANSPORT PROTOCOL



CONGESTION CONTROL



Networks use **congestion control** and **congestion avoidance** techniques to try to avoid collapse. These include: exponential backoff in protocols such as CSMA/CA in 802.11 and the similar CSMA/CD in the original Ethernet, window reduction in TCP, and fair queueing in devices such as routers and network switches. Other techniques that address congestion include priority schemes which transmit some packets with higher priority ahead of others and the explicit allocation of network resources to specific flows through the use of admission control.

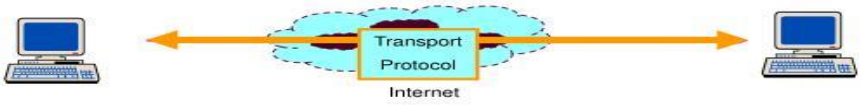


INTERNET TRANSPORT PROTOCOL

The two most widely deployed **transport protocols** on the **Internet** are the User Datagram **Protocol** (UDP) and the Transmission Control **Protocol** (TCP). A third important **transport protocol**, the Stream Control Transmission **Protocol** (SCTP) RFC 4960 appeared in the early 2000s. It is currently used by some particular applications such as signaling in Voice over IP networks.

Internet Transport Protocols

- Host computers run two transport protocols on top of IP to enable process-to-process communications.
  - User Datagram Protocol (UDP) enables best-effort transfer.
  - Transmission Control Protocol (TCP) enables reliable transfer.
- All Internet applications run on TCP or UDP. For example,
  - TCP: HTTP (web); SMTP (e-mail); FTP (file transfer)
  - UDP: DNS, RTP (voice & multimedia)



UNIVERSITY OF BIRMINGHAM

14

TYPE OF PROTOCOL

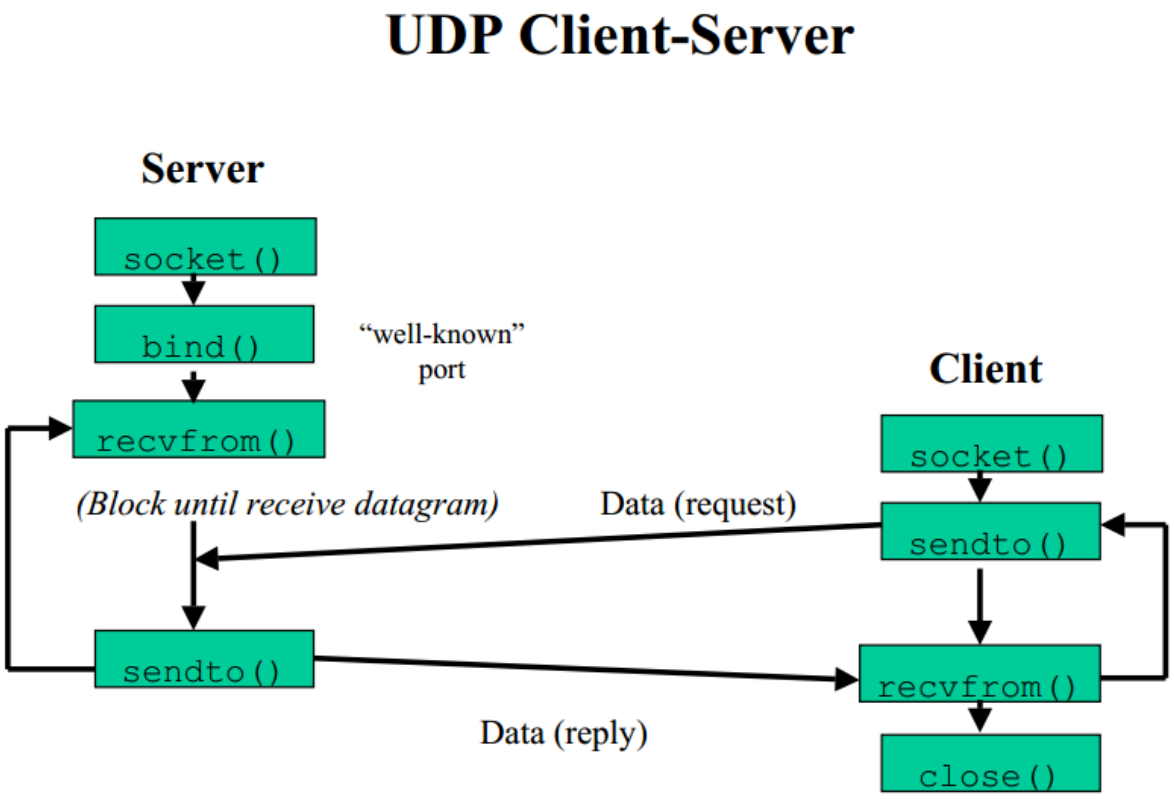
There are various types of protocols that support a major and compassionate role in communicating with different devices across the network. These are:

1. Transmission Control Protocol (TCP)
2. Internet Protocol (IP)
3. User Datagram Protocol (UDP)
4. Post office Protocol (POP)
5. Simple mail transport Protocol (SMTP)
6. File Transfer Protocol (FTP)
7. Hyper Text Transfer Protocol (HTTP)
8. Hyper Text Transfer Protocol Secure (HTTPS)
9. Telnet
10. Gopher

UDP

A UDP datagram consists of a datagram header and a data section. The UDP datagram header consists of 4 fields, each of which is 2 bytes (16 bits). The data section follows the header and is the payload data carried for the application. The use of the checksum and source port fields is optional in IPv4 (pink background in table). In IPv6 only the source port field is optional.

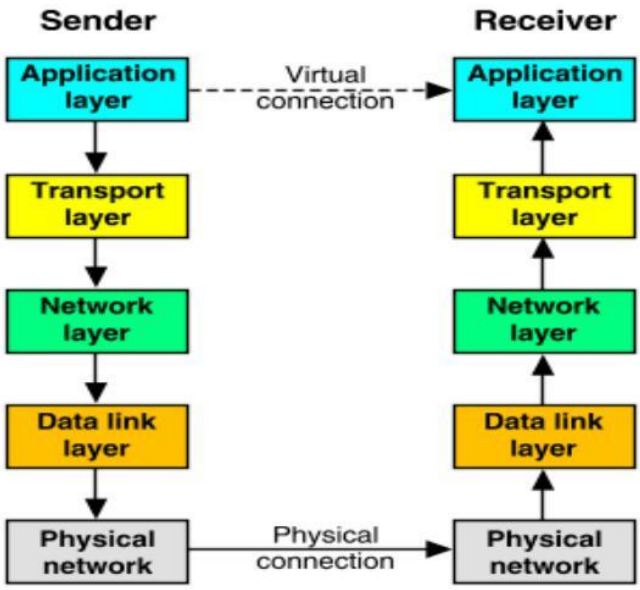
1. UDP is used when acknowledgement of data does not hold any significance.
2. UDP is good protocol for data flowing in one direction.
3. UDP is simple and suitable for query based communications.
4. UDP is not connection oriented.



TCP

The **Transmission Control Protocol** (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP.

TCP/IP Protocol Stack



by Caldera, Incorporated

Key Differences Between TCP and UDP

- TCP is Connection-oriented whereas, UDP is Connectionless protocol.
- TCP is highly reliable for transferring useful data as it takes the acknowledgement of information sent. Also, resends...
- TCP is slower as compared to UDP since TCP establishes the connection before transmitting data, and ensures the proper...
- Header size of UDP is 8 bytes, and that of TCP is more than double. TCP header size is 20 bytes since, and TCP header...
- Both TCP and UDP can check for errors, but only TCP can...

Difference between TCP & UDP

S.N	Parameter	TCP	UDP
1.	Acronym for	Transmission control protocol	User datagram protocol
2.	Connection	Connection oriented protocol	Connection less protocol
3.	Usage	TCP is suited for application that require higher reliability & transmission time is relatively less critical.	UDP is suitable for application that need fast, efficient transmission, such as games, UDP stateless nature is also useful for servers that

UNIT-V

APPLICATION LAYER

An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. The application layer abstraction is used in both of the standard models of computer networking: the Internet Protocol Suite (TCP/IP) and the OSI model. Although both models use the same term for their respective highest level layer, the detailed definitions and purposes are different.

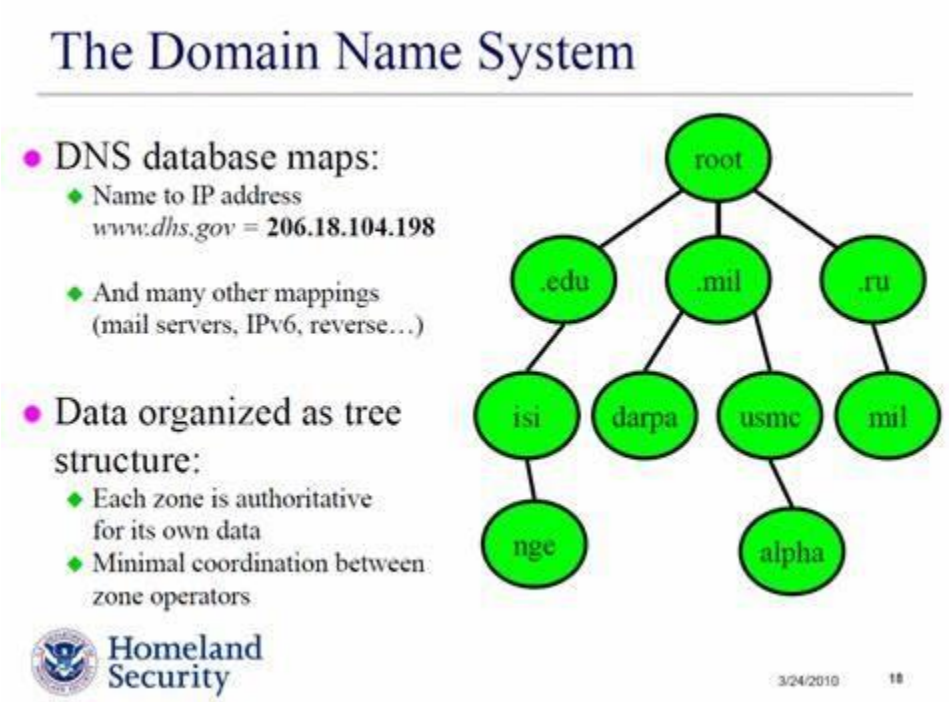
The Application layer includes the following functions:

- Identifying communication partners: The application layer identifies the availability of communication partners for an...
- Determining resource availability: The application layer determines whether sufficient network resources are available...

- Synchronizing communication: All the communications occur between the applications requires cooperation which is managed...

DOMAIN NAME SYSTEM

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System has been an essential component of the functionality of the internet since 1985.



ELECTRONIC MAIL

Email (electronic mail) **is the exchange of computer-stored messages by telecommunication.** Email **messages are usually encoded i Electronic mail (email or e-mail) is a method of exchanging messages ("mail") between people using electronic devices. Email entered limited use in the 1960s, but users could only send to users of the same computer, and some early email systems required the author and the recipient to both be online simultaneously, similar to instant messaging. Ray Tomlinsonis credited as the inventor of email; in 1971, he developed the first system able to send mail between users on different hosts across the ARPANET, … American Standard Code for Information Interchange text.However, you can also send nontext files -- such as graphic images and sound files -- as attachments sent in binary streams.**

Advantages of e-mail
Free delivery - Sending an e-mail is virtually free, outside the cost of Internet service. There is no …
Global delivery - E-mail can be sent to nearly anywhere around the world, to any country.
Instant delivery - An e-mail can be instantly sent and received by the recipient over the Internet.

THE WORLD WIDE WEB

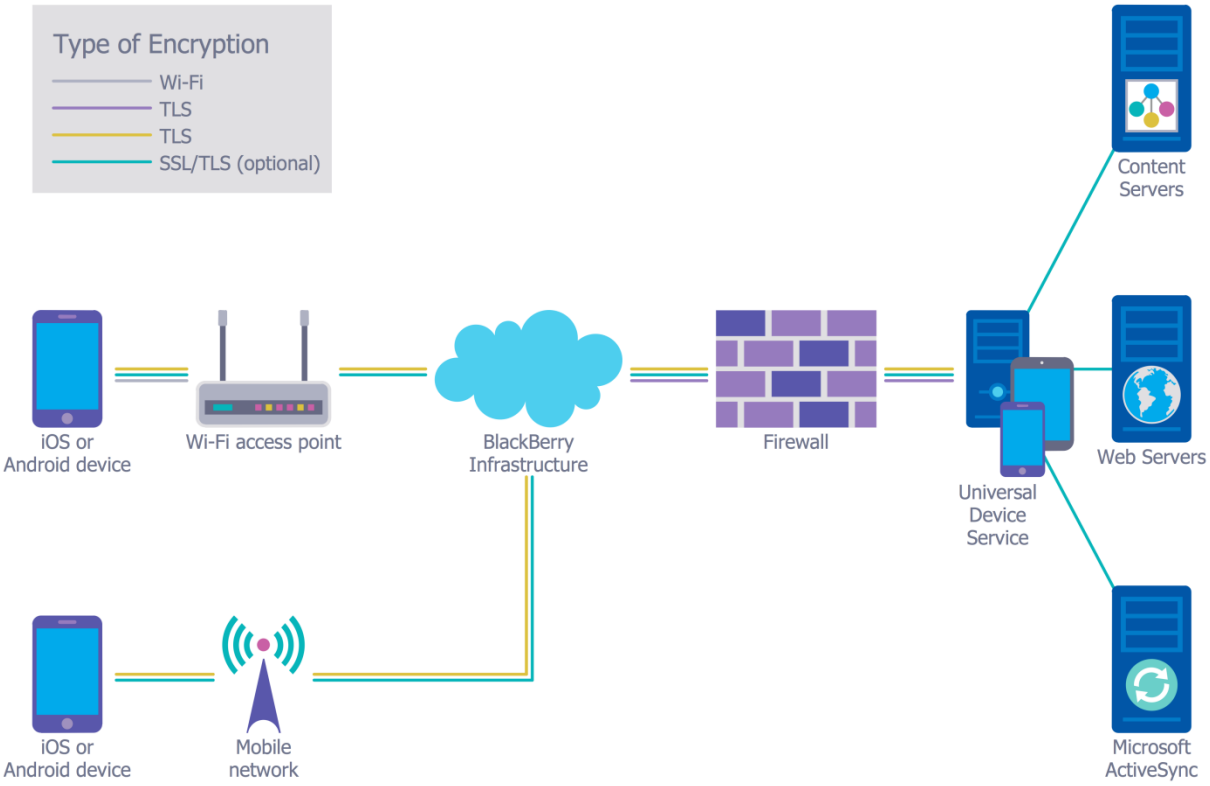
The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://example.com/), which may be interlinked by hypertext, and are accessible over the Internet. The resources of the Web are transferred via the Hypertext Transfer Protocol (HTTP), may be accessed by users by a software application called a web browser, and are published by a software application called a web server. The World Wide Web is not synonymous with the Internet, which pre-existed the Web in some form by over two decades and upon whose technologies the Web is built.

World Wide Web, which is also known as a Web , is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These

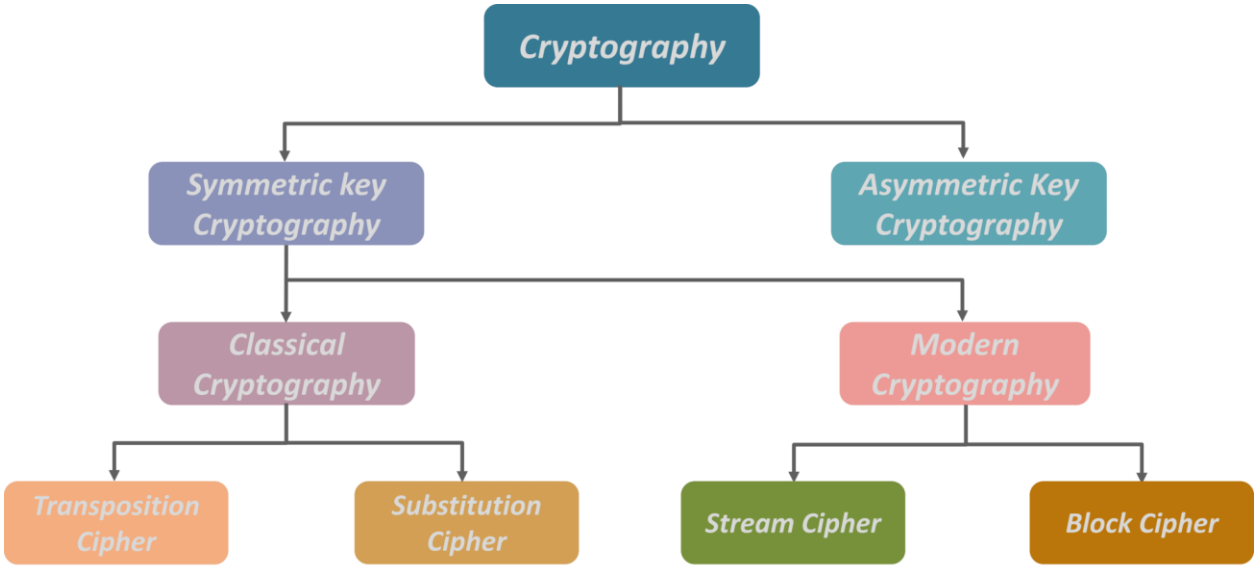
websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc.

NETWORK SECURITY

- Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs: conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: it secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.
- Types of Network Security Devices. Active Devices. These security devices block the surplus traffic.
- Firewalls. A firewall is a network security system that manages and regulates the network traffic based on some protocols.
- Antivirus. An antivirus is a tool that is used to detect and remove malicious software.
- Content Filtering. Content filtering devices screen unpleasant and offensive emails or webpages.
- Intrusion Detection Systems. Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.
-


Type of Encryption
Wi-Fi
TLS
TLS
SSL/TLS (optional)
Content Servers
iOS or Android device
Wi-Fi access point
BlackBerry Infrastructure
Firewall
Universal Device Service
Web Servers
iOS or Android device
Mobile network
Microsoft ActiveSync

CRYPTOGRAPHY



Examples of methods that use symmetric encryption include:

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)
- International Data Encryption Method (IDEA)
- Camelia
- Misty 1
- Skipjack
- Two Fish

SYMMETRIC

A geometric shape or object is symmetric if it can be divided into two or more identical pieces that are arranged in an organized fashion. This means that an object is symmetric if there is a transformation that moves individual pieces of the object, but doesn't change the overall shape. The type of symmetry is determined by the way the pieces are organized, or by the type of transformation:
• An object has reflectional symmetry (line or mirror symmetry) if there is a line (or in 3Da plane) going thr…

PUBLIC KEY ALGORITHMS

- Public Key Algorithms. Privacy is accomplished with public key algorithms in one of two fashions. The first method is to...
- The Secure Sockets Layer. The SSL protocol provides blanket security for network communications by utilizing the...

- Computer Security Introduction and Review. As we mentioned before, public-key cryptography is horribly inefficient. For...
- IoT Node Authentication. A problem with the use of public-key cryptography is confidence/proof that a particular public...

The public key algorithmsin use today are: Rivest-Shamir-Adleman (RSA) Elliptic Curve Digital Signature Algorithm (ECDSA) Digital Signature Algorithm (DSA) Diffie-Hellman key agreement protocol. RSA, developed by RSA Laboratories, is by far the most popularalgorithm and supports digital signatures and data encryption.