Computer Communication Networks

Introduction, Communication link, Multiplexing

Dr. Raja Vara Prasad

Assistant Professor

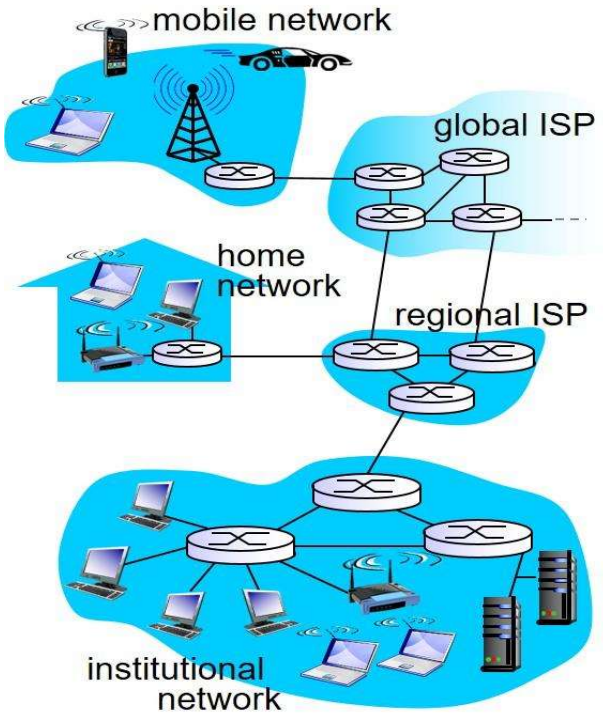
IIIT Sri City

Content

- Introduction
- Communication Link
  - Guided
  - Unguided
- Multiplexing
  - Frequency division multiplexing (FDM)
  - Time division multiplexing (TDM)

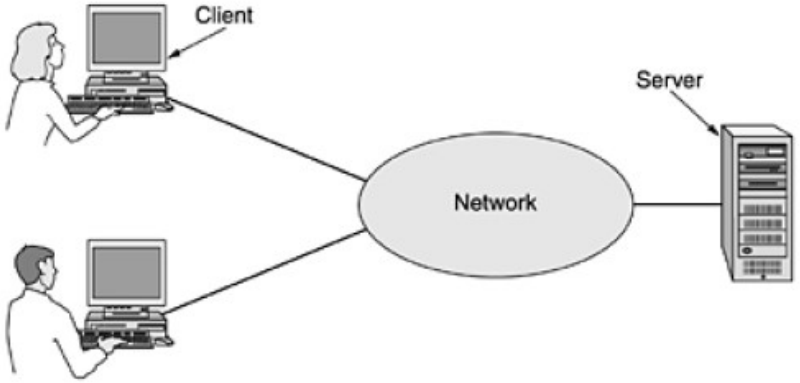
What is a Network?

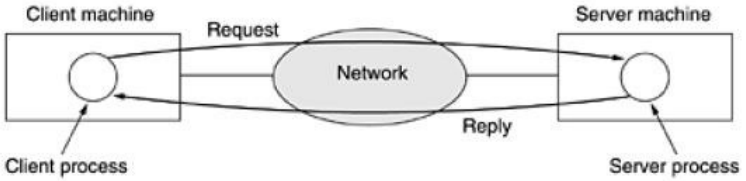
- A network is an interconnection of devices.
- The computers/laptops connected to the network are known as end systems or hosts.
- The digital data is fragmented into packets.



Uses of Computer network

- Business applications
  - Resource sharing
  - powerful medium of communication (email and online document preparation)
  - Video conferencing
  - Doing business electronically with other companies (ex: Isuzu).
  - Doing business with consumer (online market).





Uses of Computer network

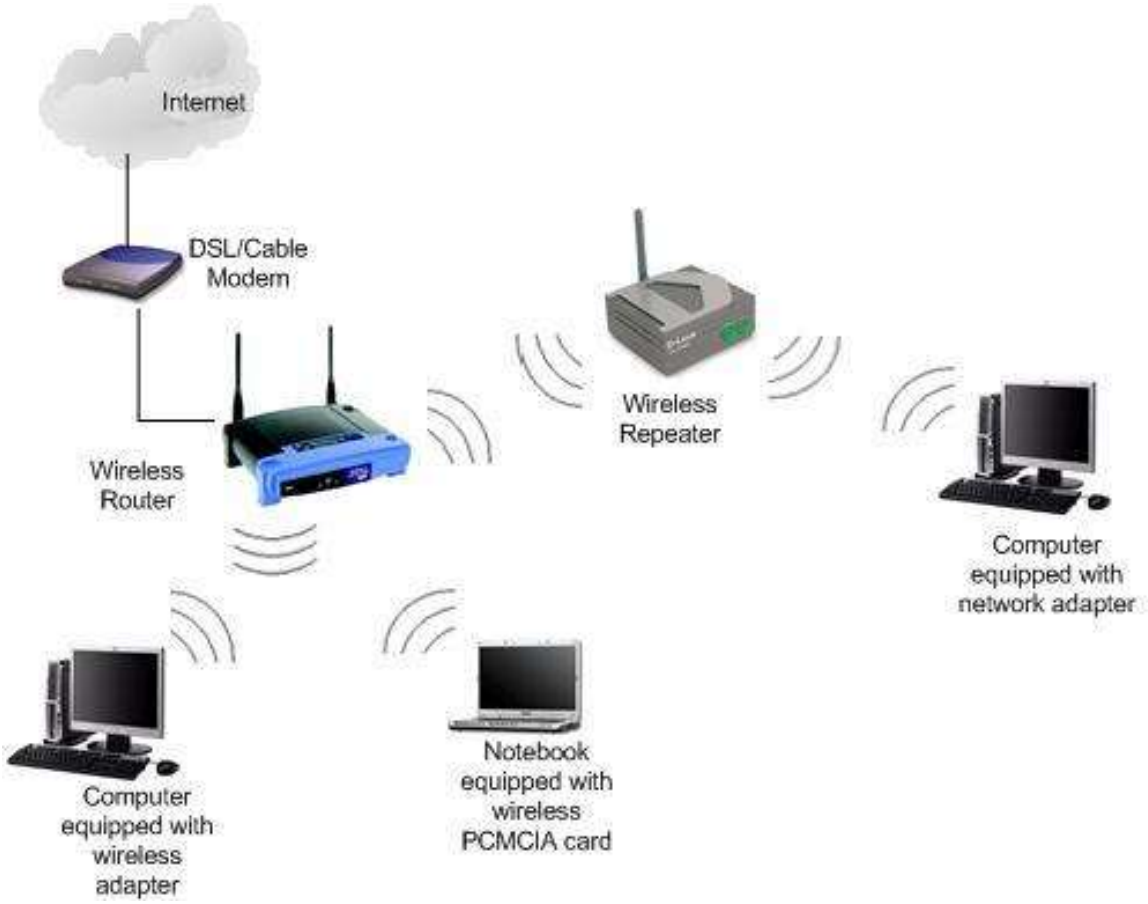
- Home applications
  - Why do people buy computer for home use?
    - Earlier days it is for word processing and gaming , now for “Internet access”
    - Internet provides access to remote information, person- to-person communication, entertainment, e-commerce.

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from 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

Network Essentials

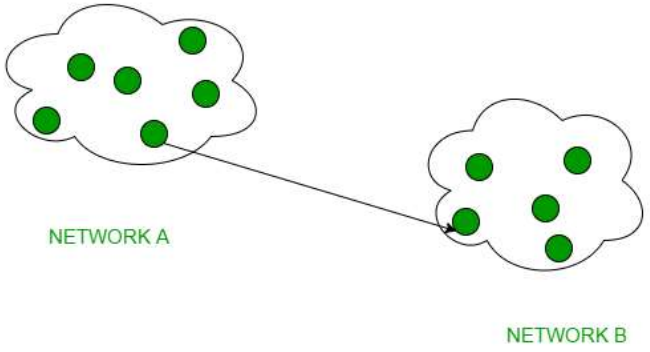
- **Modem**
- "Modulator and demodulator", is a hardware device that converts data into a format suitable for a transmission medium so that it can be transmitted from one computer to another.
- **Ethernet**
- System for connecting the number of computers to form a LAN.
- **Router**
- A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network.
- **Repeater**
- A **network** device used to regenerate or replicate a signal. **Repeaters** are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog **repeaters** frequently can only amplify the signal while digital **repeaters** can reconstruct a signal to near its original quality.

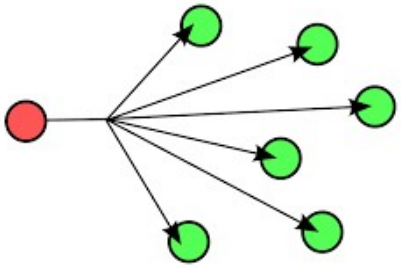
Wireless Network

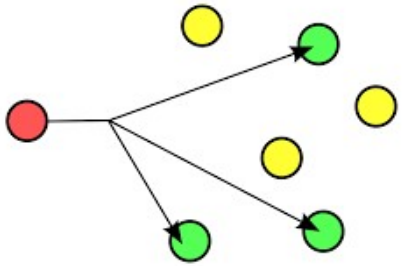


Classification of Networks

- Transmission technology:
  - Unicasting : transmission with exactly one sender and exactly one receiver
  - Broadcasting : information is intended to all hosts
  - Multicasting : information is intended for a subset of hosts in the network







Network Hardware: Classification

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

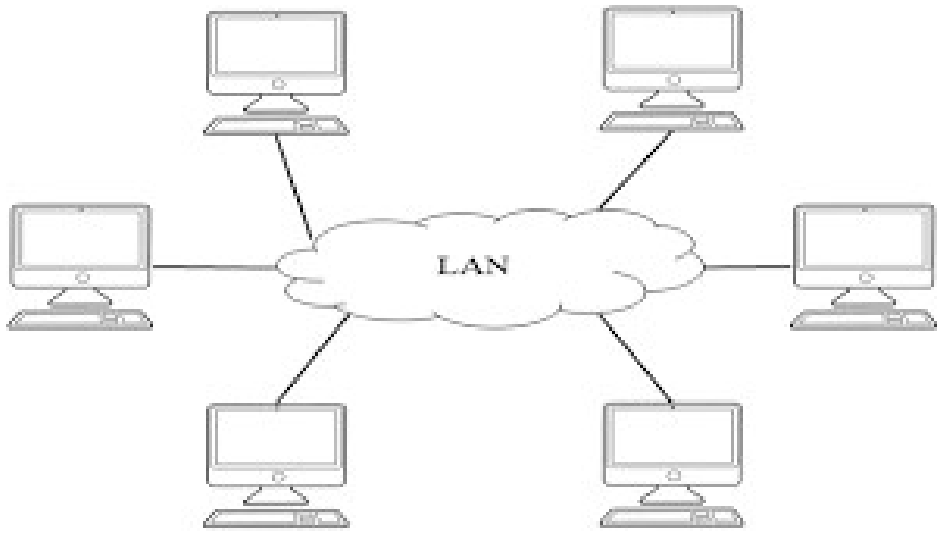
Classification of Networks:

- Personal area networks (PANs)
  - Organized around an individual person, with in a small office or residence.
  - With in the range of few meters
  - Notable example is Bluetooth
  - Watching movies on online streaming service to TV
  - With multiple uses with in a same residence then, referred as Home Area Network (HAN).

Connecting peripherals to computer via Bluetooth

Classification of Networks:

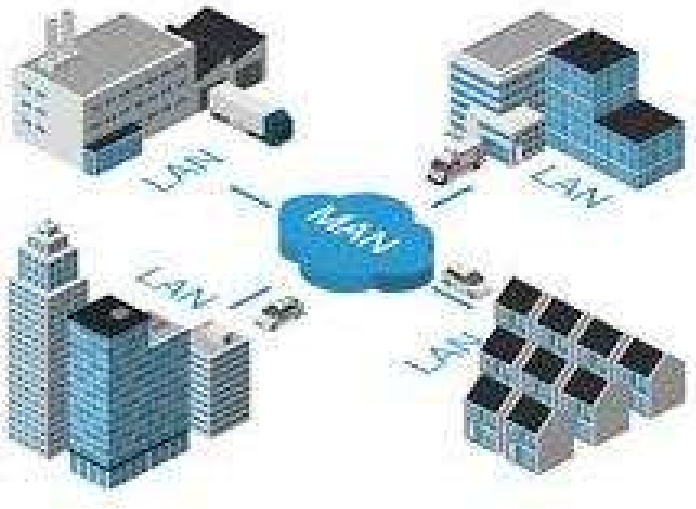
- Local area networks (LANs)
  - Typically an individual office building: suitable for sharing resources (data storage and printers).
  - Range: It can reach few hundred meters, can be increased further using wireless repeaters.
  - Wireless LAN: WLAN



Privately owned network: wireless/wired connections.

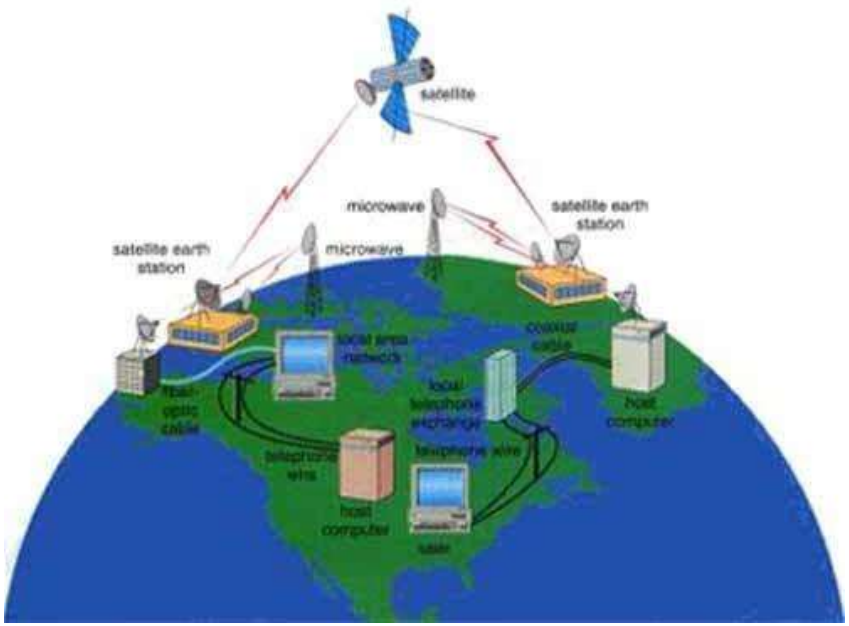
Classification of Networks:

- Metropolitan area networks (MANs)
  - Computer network across entire city, college campus or small region.
  - Referred as Campus Area Network (CAN).
  - Range: from several miles to tens of miles.
  - Connect several LANs together to form a bigger network.



Classification of Networks:

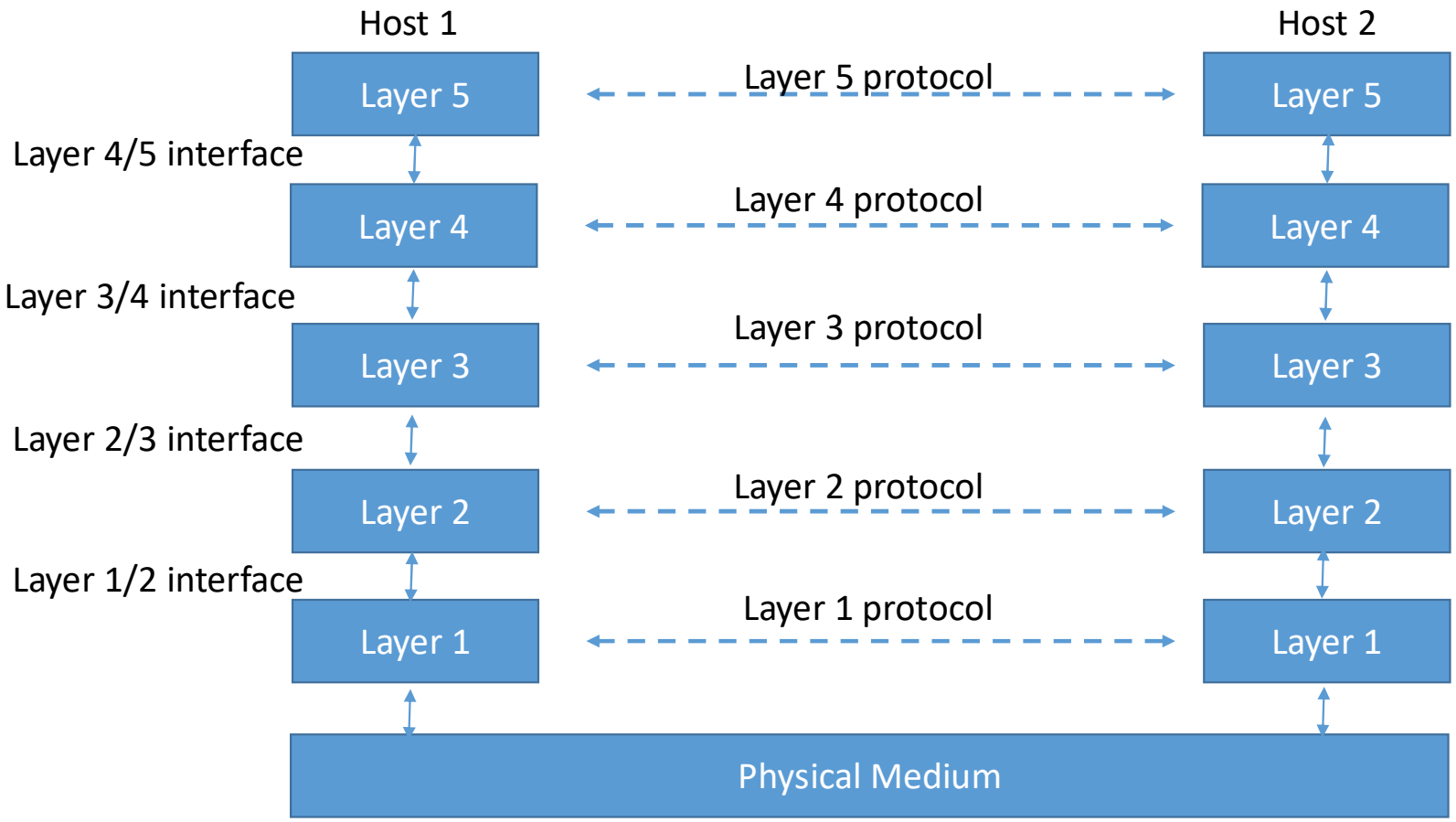
- Wide area networks (WANs)
  - Occupies a very large area, such as an entire country or the entire world
  - can contain multiple smaller networks, such as LANs or MANs
  - The most well-known WAN is the "**Internet**"



Network Software

- Protocol
  - Is an agreement between the communicating parties on how communication is to proceed.
  - Violation of protocol will make communication more difficult, if not completely impossible.

Layers, protocols, and interfaces

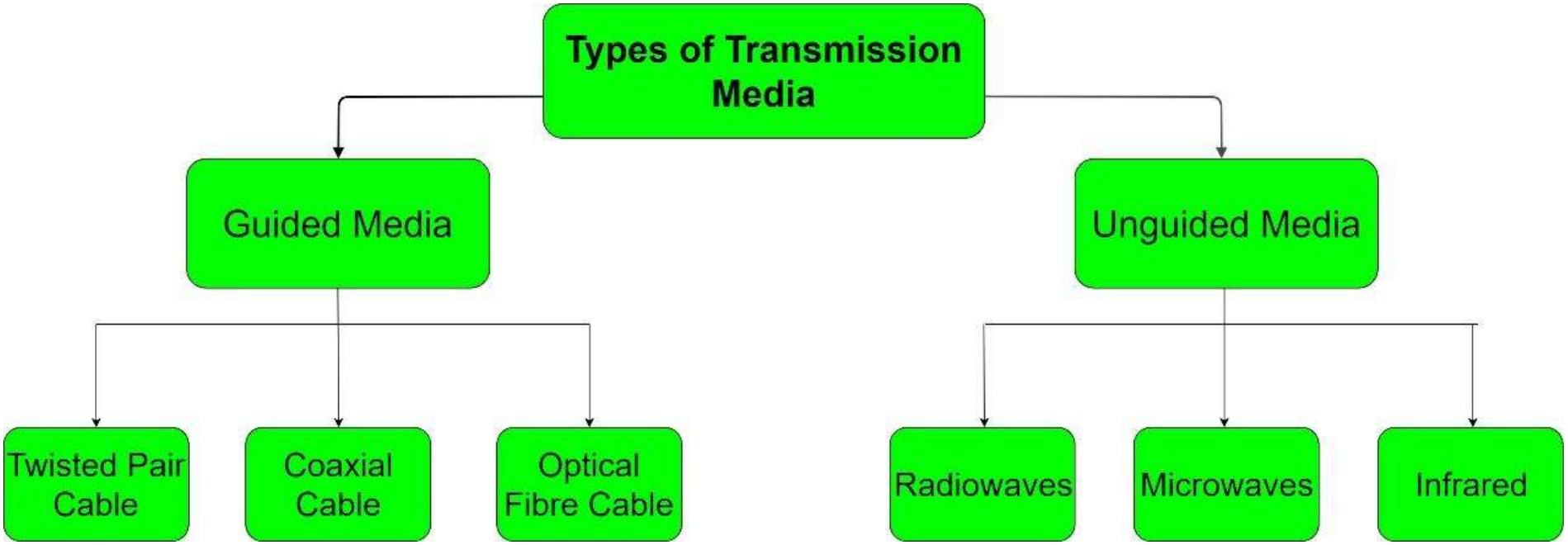


The Physical Layer

- Lowest of our protocol model
- Defines the electrical, timing and other interfaces by which bits are sent as signals over channels.
- The properties of different kinds of physical channels determine the performance.
- Kinds of transmission media: Guided and Unguided.

Communication Link?

Communication link : provides a way for information to move between physically separated components



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.
- It is often more cost effective, especially for applications in which high bandwidth or cost per bit transported is the key factor.

Floppy disc.

Hard Disc

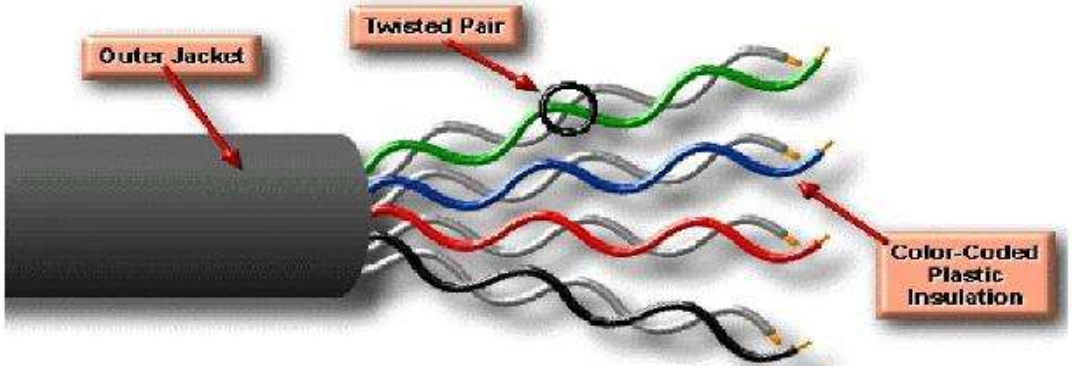
External hard Disc

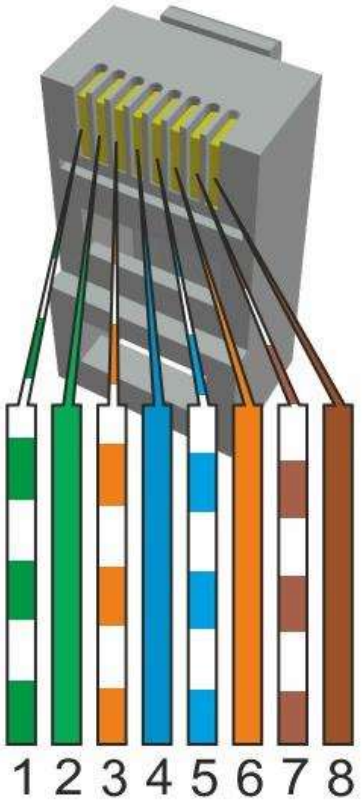
Twisted pair

- Used for telephone communications and most modern Ethernet networks.
- A pair of wires forms a circuit that can transmit data.
- The pairs are twisted to provide protection against *crosstalk*, the noise generated by adjacent pairs.
- When electrical current flows through a wire, it creates a small, circular magnetic field around the wire (Ampere's Law).
- When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Thus, the two magnetic fields cancel each other out.
- Twisting the wires can enhance this *cancellation effect.*
- *Two types: Unshielded, and shielded.*

UTP (unshielded)

- is a medium that is composed of pairs of wires (4 pairs for network medium)
- UTP cable often is installed using a Registered Jack 45 (RJ-45) connector





T-568A

Pin	Description	10base-T	100Base-T	1000Base-T
1	Transmit Data+ or BiDirectional	TX+	TX+	BI_DA+
2	Transmit Data- or BiDirectional	TX-	TX-	BI_DA-
3	Receive Data+ or BiDirectional	RX+	RX+	BI_DB+
4	Not connected or BiDirectional	n/c	n/c	BI_DC+
5	Not connected or BiDirectional	n/c	n/c	BI_DC-
6	Receive Data- or BiDirectional	RX-	RX-	BI_DB-
7	Not connected or BiDirectional	n/c	n/c	BI_DD+
8	Not connected or BiDirectional	n/c	n/c	BI_DD-

PinoutsGuide.com

UTP

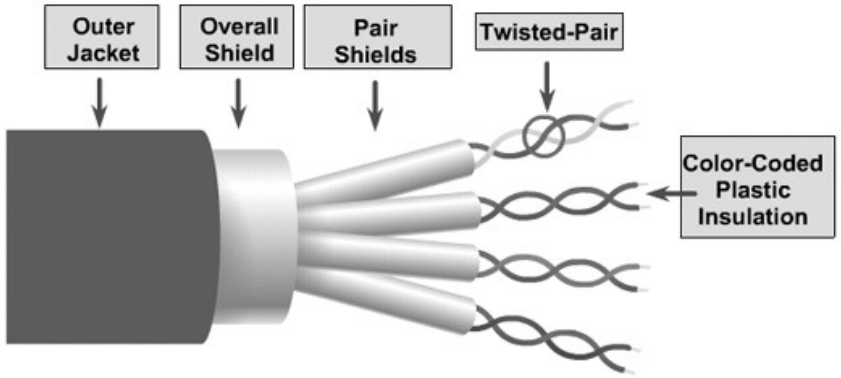
- Advantages: Smaller size (external diameter), easy to install and less expensive.
- Disadvantages: UTP cable is more prone to electrical noise and interference than other types of networking media, and the distance between signal boosts is shorter for UTP .
- The following summarizes the features of UTP cable:
  - Speed and throughput—10 to 1000 Mbps
  - Average cost per node—Least expensive
  - Media and connector size—Small
  - Maximum cable length—100 m (short)

UTP cabling

- **Category 1 (1 pair)**—Used for telephone communications. Not suitable for transmitting data.
- **Category 2 (2 pairs)**—Capable of transmitting data at speeds up to 4 megabits per second (Mbps).
- **Category 3 (4 pairs)**—Used in 10BASE-T networks, Can transmit data at speeds up to 10 Mbps.
- **Category 4 (4 pairs)**—Used in Token Ring networks, Can transmit data at speeds up to 16 Mbps.
- **Category 5 (4 pairs)**—Can transmit data at speeds up to 100 Mbps.
- **Category 5e (4 pairs)** —Used in networks running at speeds up to 1000 Mbps (1 gigabit per second [Gbps]).
- **Category 6 (4 pairs)**—Typically, Category 6 cable consists of four pairs of 24 American Wire Gauge (AWG) copper wires. Category 6 cable is currently the fastest standard for UTP.

STP (Shielded Twisted Pair)

- Combines the techniques of shielding, cancellation, and wire twisting.
- Each pair of wires is wrapped in a metallic foil. The four pairs of wires then are wrapped in an overall metallic braid or foil.
- Reduces electrical noise both within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI)



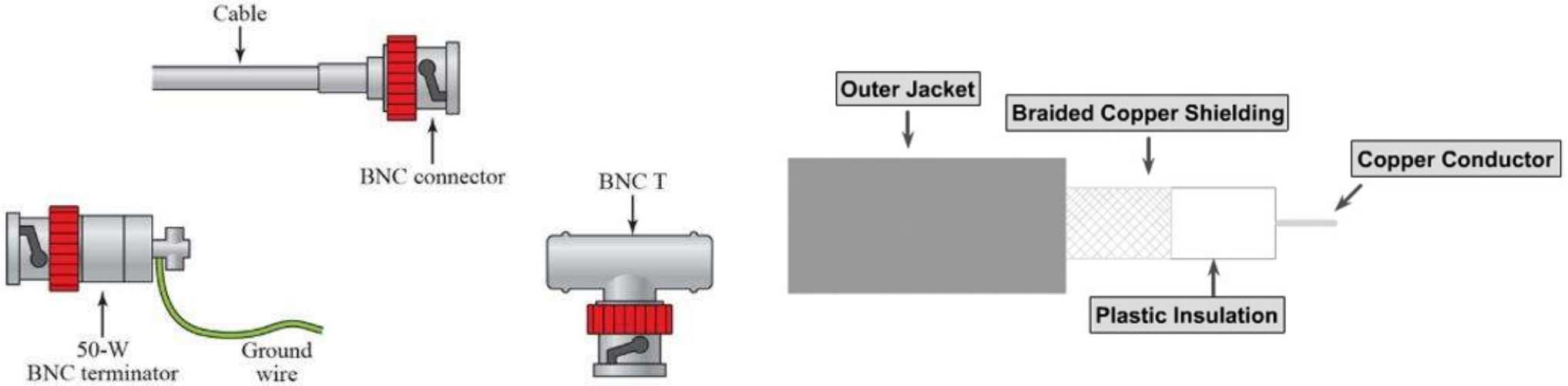
- Speed and throughput: 10-100 Mbps
- Cost per node: Moderately expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m (short)

STP comparison with UTP

- Although STP prevents interference better than UTP, it is more expensive and difficult to install.
- the metallic shielding must be grounded at both ends. If it is improperly grounded, the shield acts like an antenna and picks up unwanted signals.
- Because of its cost and difficulty with termination, STP is rarely used in Ethernet networks.
- The speed of both types of cable is usually satisfactory for local-area distances.

Coaxial Cable

- Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield.
- The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.
- The most common type of connector used the Bayonet Neill-Concelman (BNC) connector



Categories of Coax.

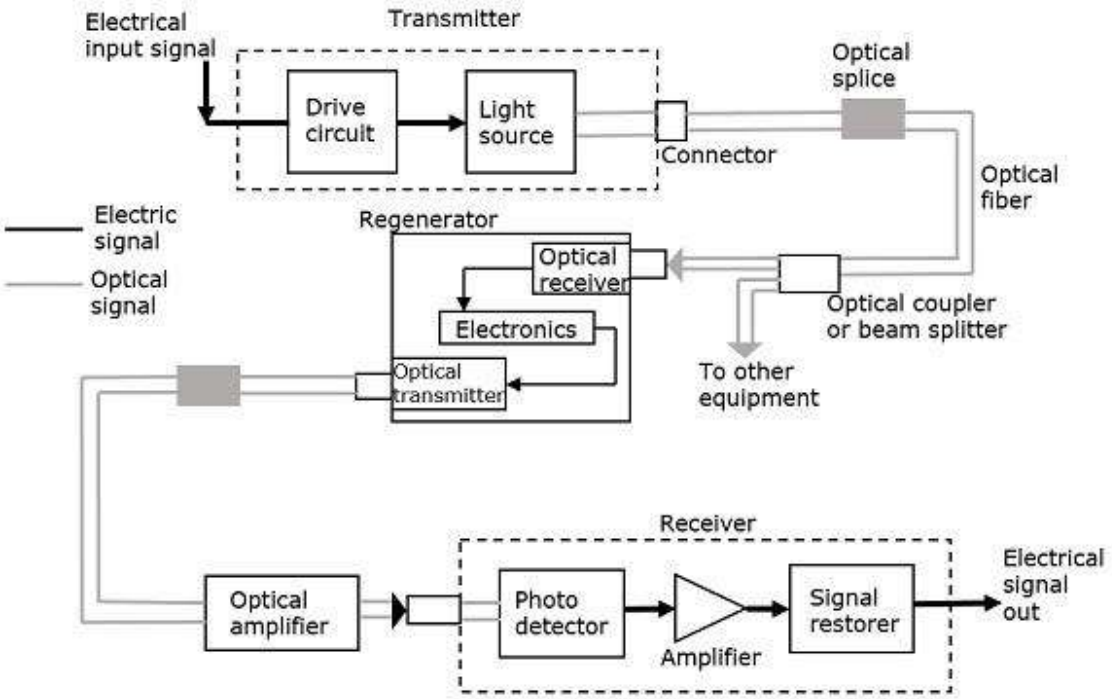
- Base band
- For digital transmission, a 50 ohm (Ω) coaxial cable is used. It defines a process of transmitting a single signal at a time with a very high speed. It is generally used for LAN's.
- Broadband
- Analog transmission on standard cable television 75 ohm (Ω) cabling is used by this. It defines a process of transmitting multiple signals simultaneously with very high speed. It covers a large area as compared to Baseband Coaxial Cable.

Advantages and Disadvantages

- It can be used for both analog and digital transmission.
- It offers higher bandwidth as compared to twisted pair cable and can span longer distances.
- Because of better shielding in coaxial cable, loss of signal or attenuation is less.
- Better shielding also offers good noise immunity.
- It is relatively inexpensive as compared to optical fibers.
- It has lower error rates as compared to twisted pair.
- It is not as easy to tap as twisted pair because copper wire is contained in plastic jacket.
- It is usually more expensive than twisted pair.

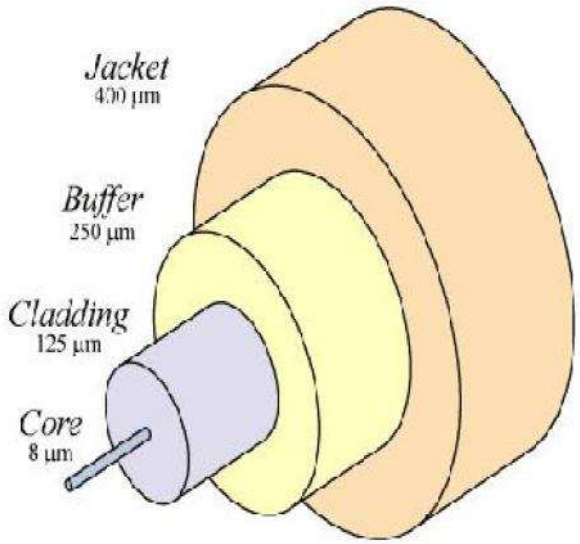
Fiber optics

- An optical transmission system has three key components:
- the light source,
- the transmission medium, and
- the detector



Fiber Optics: Construction

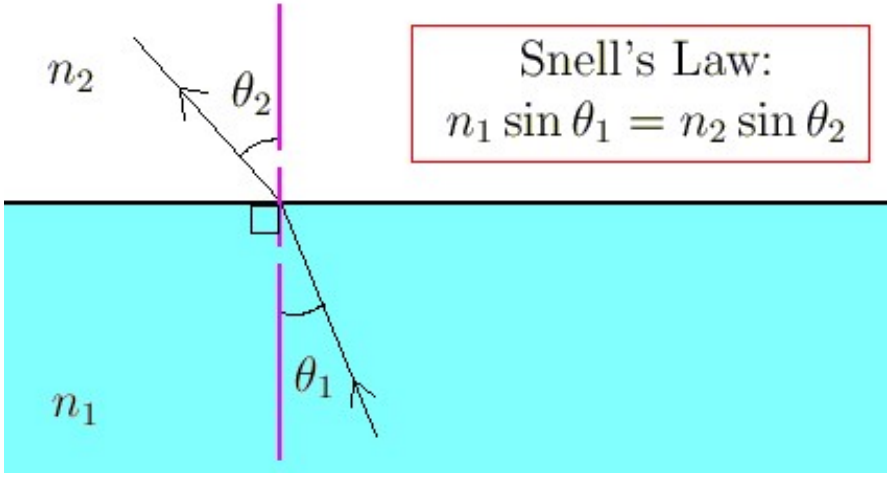
- Core: The core of a fiber cable is a cylinder of plastic that runs all along the fiber cable's length. The diameter of the core depends on the application used.
- Cladding: Cladding is an outer optical material that protects the core. The main function of the cladding is that it reflects the light back into the core.
- Buffer: The main function of the buffer is to protect the fiber from damage and thousands of optical fibers arranged in hundreds of optical cables.
- Jacket: These bundles are protected by the cable's outer covering that is called jacket.

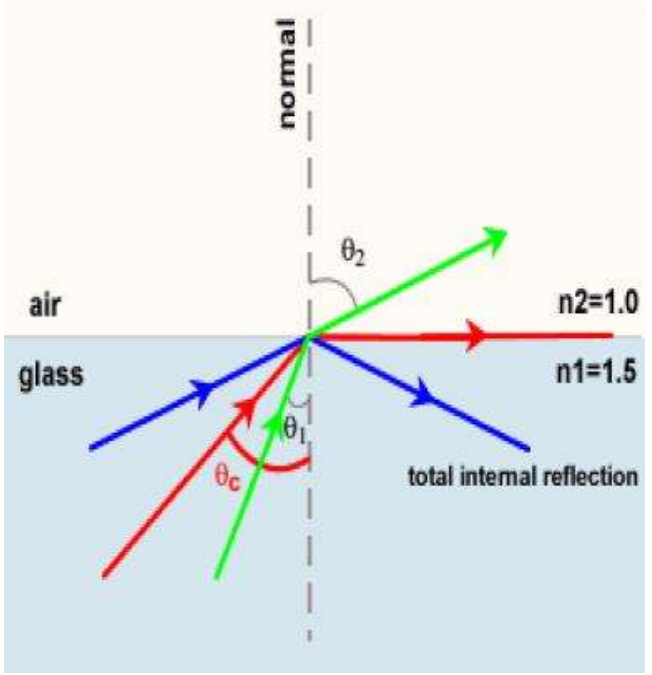


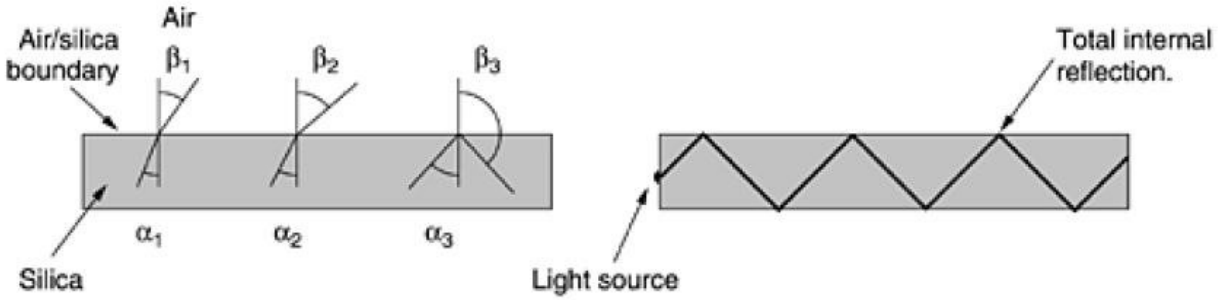
Fiber Optics: Working Principle

- A hair-thin Fiber consist of two concentric layers of high-purity silica glass the core and the cladding, which are enclosed by a protective sheath.
- Core and cladding have different refractive indices, with the core having a refractive index, n1, which is slightly higher than that of the cladding, n2.
- When light enters the fiber made of material with higher refractive index than the cladding surrounding it, it stays inside the material due to total internal reflection and is thus transmitted forward.
- **Index of refraction:** Index of refraction is a measurement of speed of light in material.

Snell's Law: Law of Refraction, Critical Angle, total internal Reflection

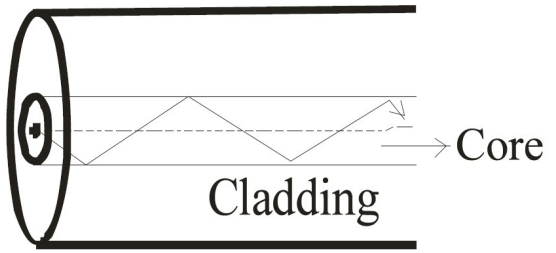


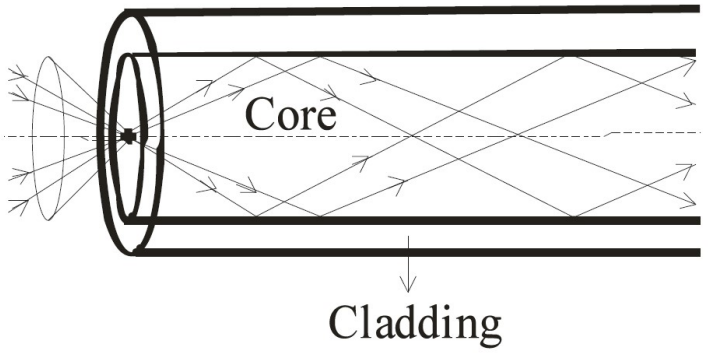




Fiber Optics: Modes

- Mode is the one which describes the nature of propagation of electromagnetic waves (light) in a wave guide (Fiber).
- Single mode fiber: In a fiber, if only one mode is transmitted through it, then it is said to be a single mode fiber.
- If more than one mode is transmitted through optical fiber, then it is said to be a multimode fiber.
- The larger core radii of multimode fibers make it easier to launch optical power into the fiber and facilitate the end to end connection of similar powers.





Types of Fibers

- **Step-index fiber** – The refractive index of the core is uniform throughout and undergoes an abrupt change (or step) at the cladding boundary.
- **Graded-index fiber** – The core refractive index is made to vary as a function of the radial distance from the center of the fiber.
- Further divided into:
- **Single-mode fiber** – These are excited with laser.
- **Multi-mode fiber** – These are excited with LED.

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

Fiber Optics: Advantages and Disadvantages

- **Advantages:**
- The transmission bandwidth of the fiber optic cables is higher than the metal cables.
- The amount of data transmission is higher in fiber optic cables.
- The power loss is very low and hence helpful in long-distance transmissions.
- Fiber optic cables provide high security and cannot be tapped.
- Fiber optic cables are the most secure way for data transmission.
- Fiber optic cables are immune to electromagnetic interference.
- These are not affected by electrical noise.
- **Disadvantages:**
- Though fiber optic cables last longer, the installation cost is high.
- The number of repeaters are to be increased with distance.
- They are fragile if not enclosed in a plastic sheath. Hence, more protection is needed than copper ones

Media Type	Maximum Segment Length	Speed	Cost	Advantages	Disadvantages
UTP	100 m	10 Mbps to 1000 Mbps	Least expensive	Easy to install; widely available and widely used	Susceptible to interference; can cover only a limited distance
STP	100 m	10 Mbps to 100 Mbps	More expensive than UTP	Reduced crosstalk; more resistant to EMI than Thinnet or UTP	Difficult to work with; can cover only a limited distance
Coaxial	500 m (Thicknet) 185 m (Thinnet)	10 Mbps to 100 Mbps	Relatively inexpensive, but more costly than UTP	Less susceptible to EMI interference than other types of copper media	Difficult to work with (Thicknet); limited bandwidth; limited application (Thinnet); damage to cable can bring down entire network
Fiber-Optic	10 km and farther (single-mode) 2 km and farther (multimode)	100 Mbps to 100 Gbps (single mode) 100 Mbps to 9.92 Gbps (multimode)	Expensive	Cannot be tapped, so security is better; can be used over great distances; is not susceptible to EMI; has a higher data rate than coaxial and twisted-pair cable	Difficult to terminate

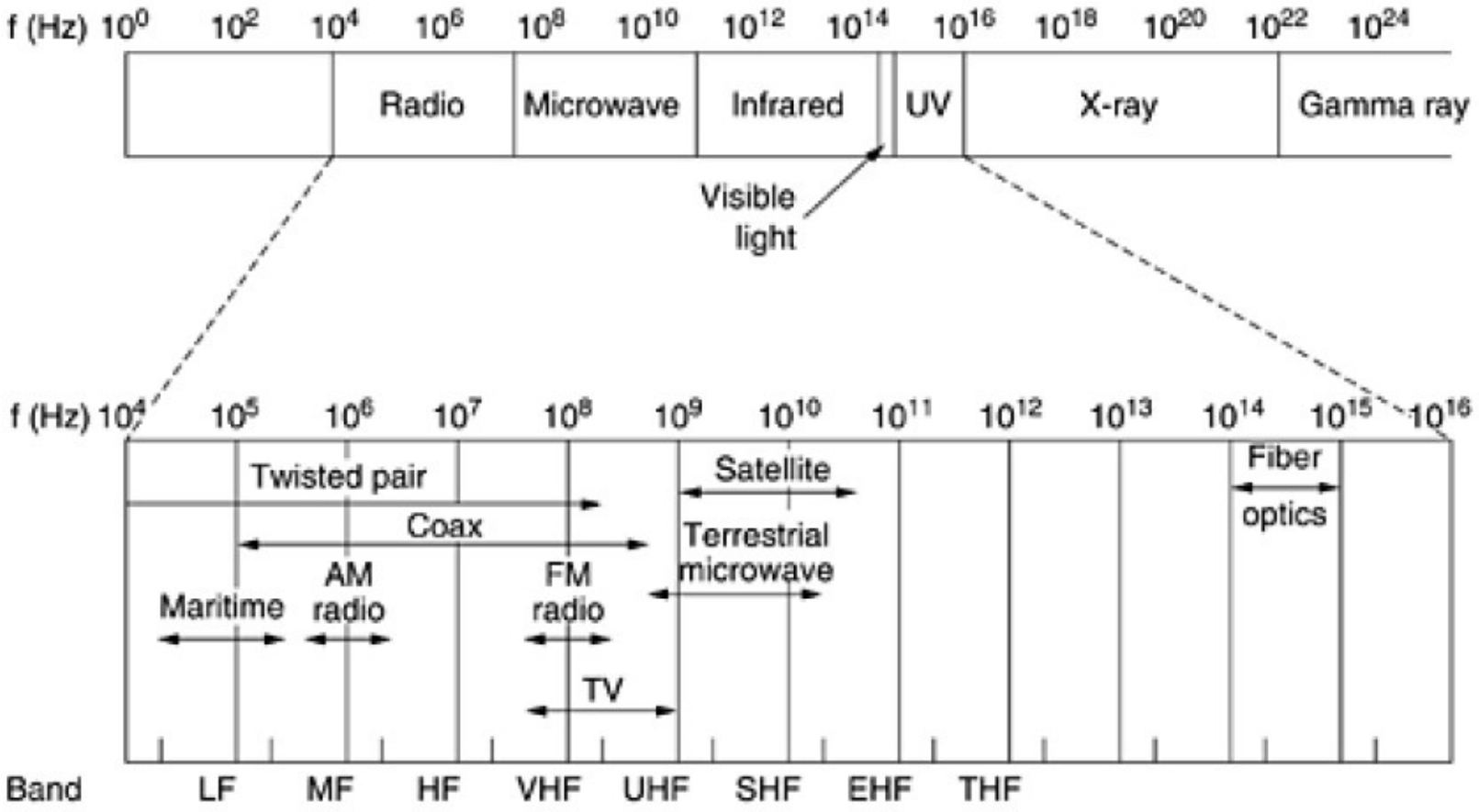
Unguided Media: Wireless Transmission

- Electromagnetic Spectrum
- Radio transmission
- Microwave Transmission
- Infrared Transmission
- Light Transmission

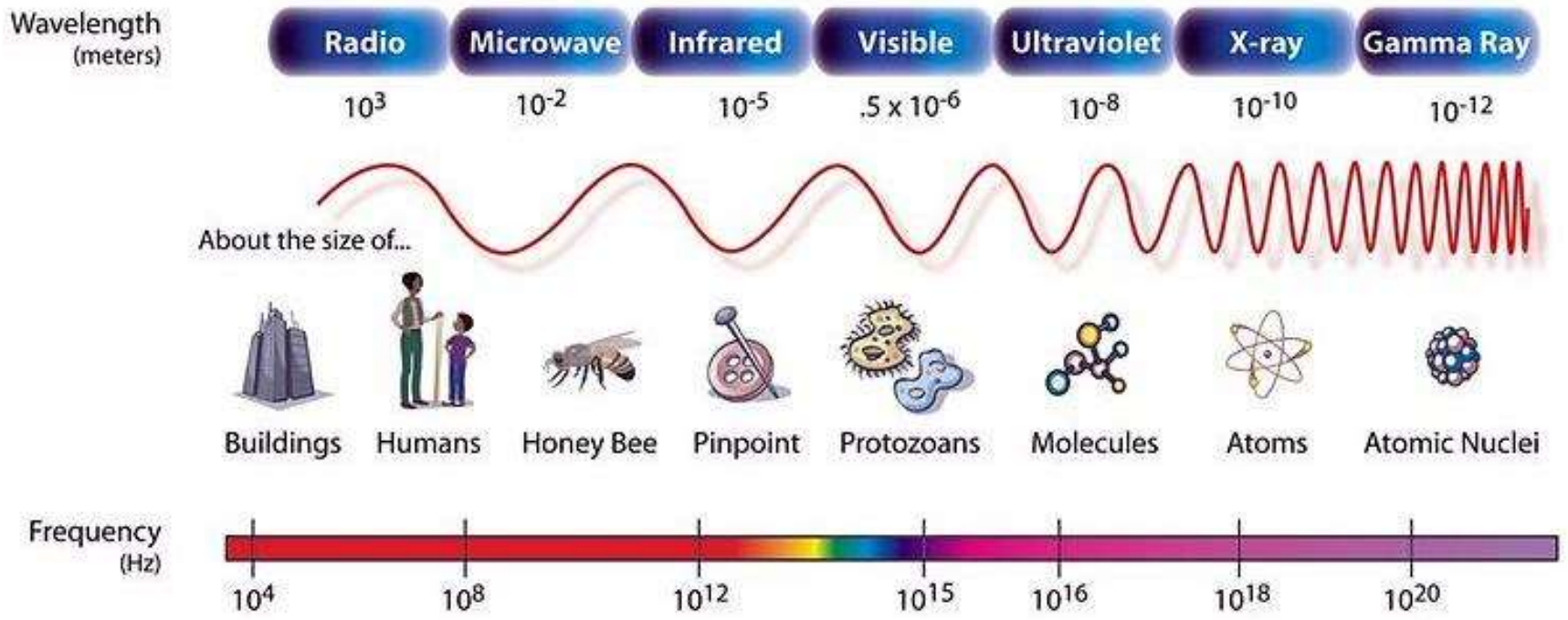
Electromagnetic Spectrum

- Electromagnetic waves, can propagate through space, were predicted by J C Maxwell in 1865 and observed by Heinrich Hertz in 1887.
- When an antenna of the appropriate size is attached to an electrical circuit, the electromagnetic waves can be broadcast efficiently and received by a receiver some distance away.
- In vacuum, all electromagnetic waves travel at the same speed, no matter what their frequency.
- In copper or fiber the speed slows to about 2/3 of this value and becomes slightly frequency dependent.

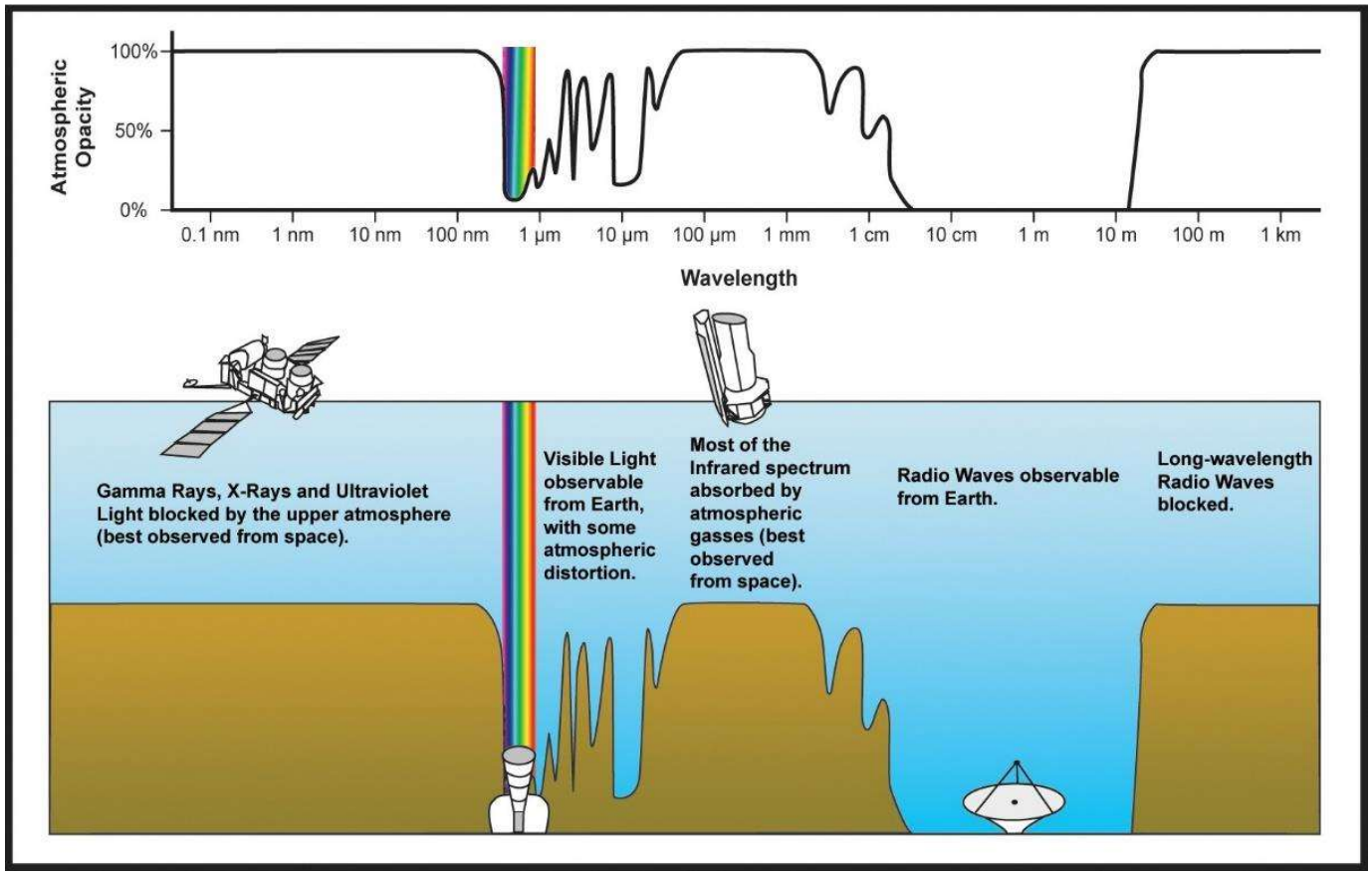
Electromagnetic spectrum and its uses for communication



Electromagnetic spectrum and its uses for communication



Electromagnetic spectrum and its uses for communication



Electromagnetic spectrum and its uses for communication

- 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.
- Ultraviolet light, X-rays, and gamma rays would be even better, due to their higher frequencies.
- but they are hard to produce and modulate, do not propagate well through buildings, and are dangerous to living things.

Radio Transmission (10 kHz – 300 MHz)

- easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.
- Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.
- Due to radio's ability to travel long distances, interference between users is a problem. For this reason, all governments tightly license the use of radio transmitters.
- There is a wide range of subcategories contained within radio including AM and FM radio

Radio Transmission

- **AM radio waves**: commercial radio signals (540 and 1600 kHz), information is carried by amplitude variation, while the frequency remains constant.
- **FM radio waves**: commercial radio signals (88 and 108 MHz), information is carried by frequency modulation, while the signal amplitude remains constant.
- TV broadcast: (174 – 216 MHz).

Microwave Transmission (300 MHz – 300 GHz)

- Microwaves are “small” compared to waves used in typical radio broadcasting.
- The microwave portion of the electromagnetic spectrum can be subdivided into:
  - **Extremely High Frequency (30 to 300 GHz):** wavelength range of 10 to 1 mm, so it is sometimes called the millimeter band.
  - **Super High Frequency (3 to 30 GHz):** ten to one centimeters, used for wireless LANs, cell phones, satellite communication, microwave radio relay links, and numerous short range terrestrial data links
  - **Ultra-High Frequency (300 MHz to 3 GHz):** 10 centimeters to 1 meter, used for television broadcasting, cordless phones, walkie-talkies, satellite communication, and numerous other applications

Infrared and Millimeter Wave

- Unguided infrared and millimeter waves are widely used for short-range communication (The remote controls used on televisions, VCRs, and stereos all use infrared communication).
- They are relatively directional, cheap, and easy to build but have a major drawback: they do not pass through solid objects.
- In general, as we go from long-wave radio toward visible light, the waves behave more and more like light and less and less like radio.
- On the other hand, infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings.
- Infrared communication has a limited use on the desktop, for example, connecting notebook computers and printers, it is not a major player in the communication.

Light Wave Transmission

- A more modern application is to connect the LANs in two buildings lasers mounted on their rooftops.
- Coherent optical signaling using lasers is inherently unidirectional, so each building needs its own laser and its own photodetector. This scheme offers very high bandwidth and very low cost.
- It is also relatively easy to install and, unlike microwave, does not require an FCC license.

Multiplexing

- **Definition**: Multiplexing is a technique which combines multiple signals into one signal, suitable for transmission over a communication channel such as coaxial cable or optical fiber.

- **By doing multiplexing**, large amount bandwidth can be saved, cost can be reduced, circuit complexity can be reduced and multiple signals can be sent simultaneously over a single communication channel.

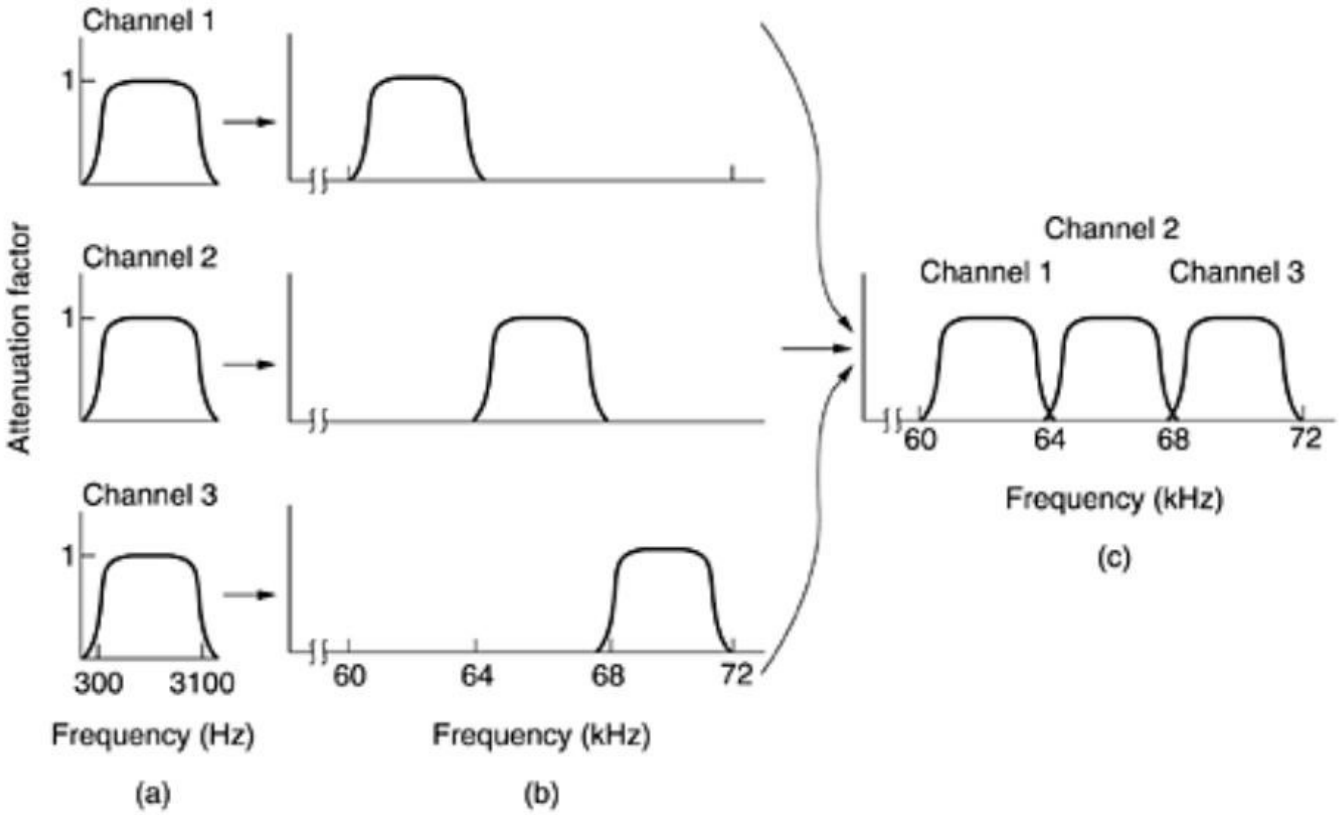
- **Analog**: Frequency Division Multiplexing and Wavelength Division Multiplexing

- **Digital**: Time Division Multiplexing

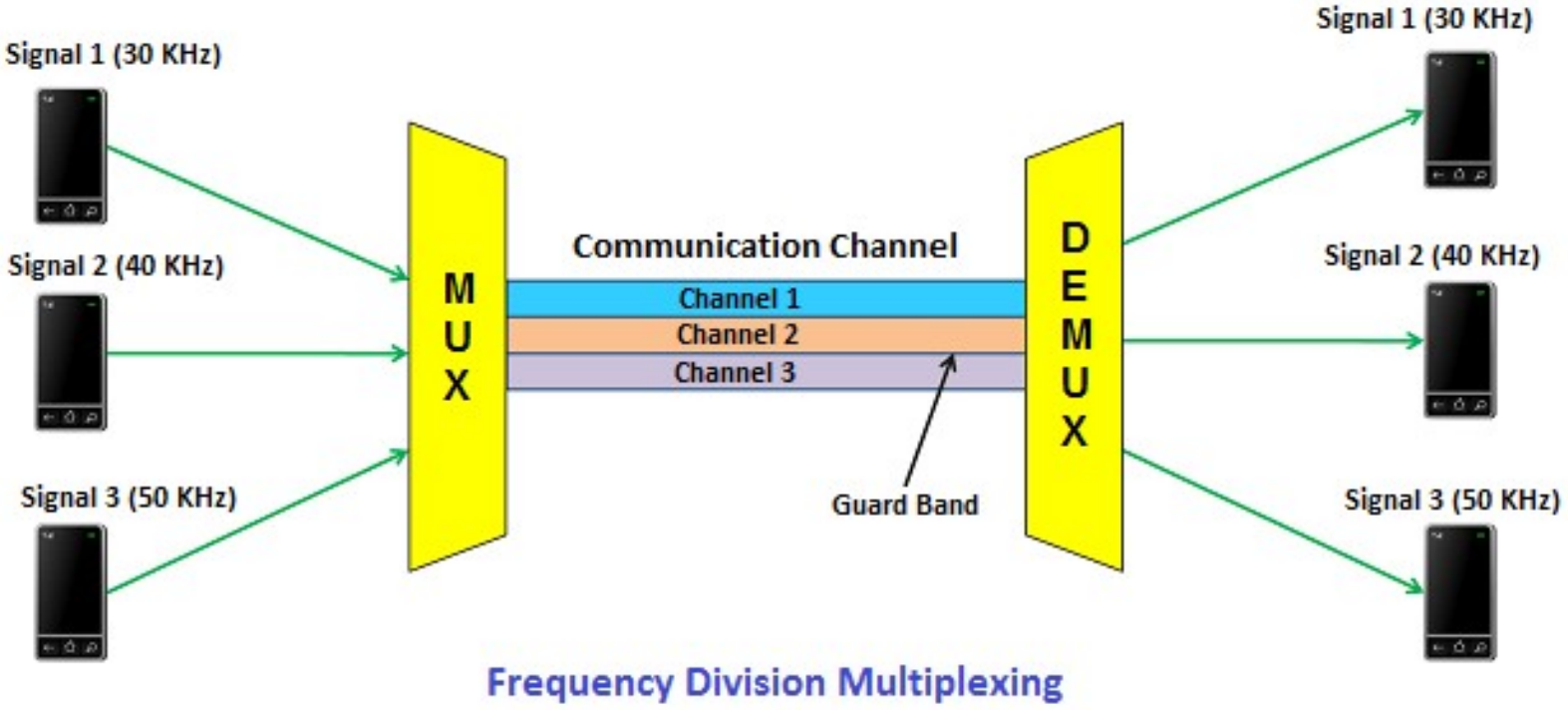
Frequency Division Multiplexing (FDM)

- popular multiplexing technique in TV and radio.
- combines multiple signals into one signal → transmitted over the communication channel.
- bandwidth of the communication channel should be greater than the combined bandwidth of individual signals.
- divides the bandwidth of a channel into several logical sub-channels and each logical sub-channel is separated by an unused bandwidth called Guard Band to prevent overlapping of signals.
- A guard band is a narrow frequency range that separates two signal frequencies.

FDM Operation



FDM Operation



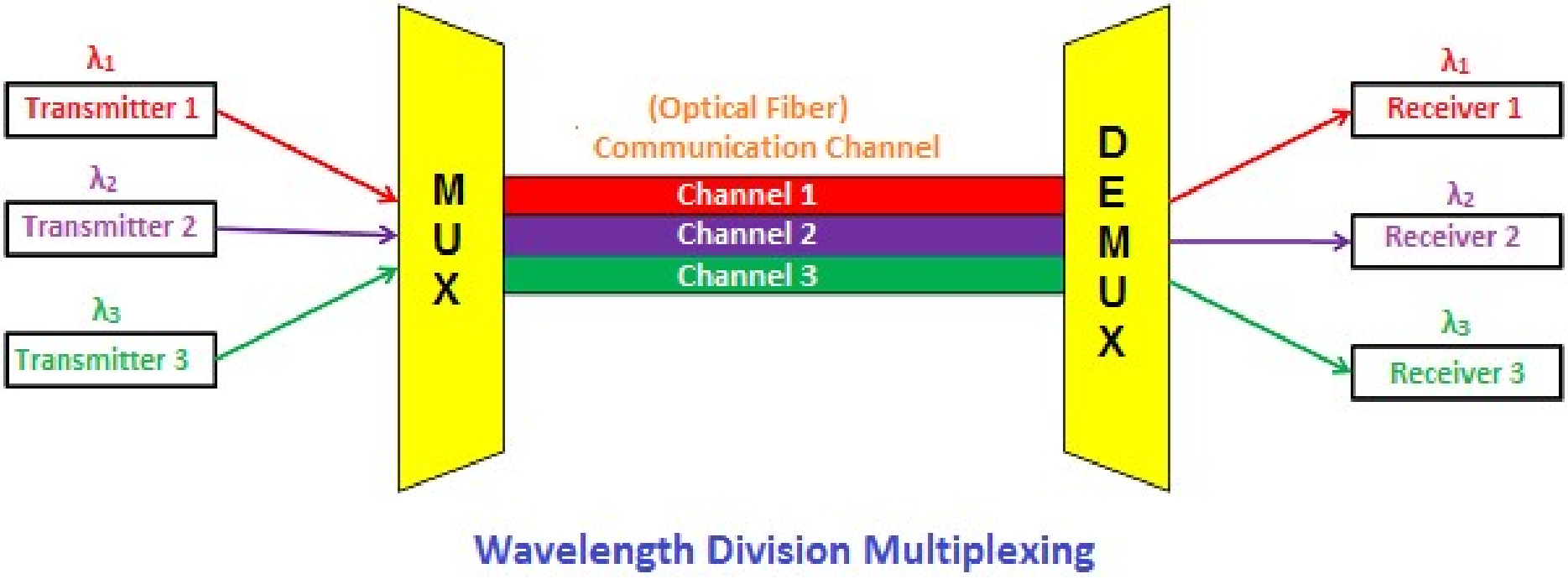
FDM

- **Advantages of Frequency Division Multiplexing (FDM)**
  - It transmits multiple signals simultaneously.
  - In frequency division multiplexing, the demodulation process is easy.
  - It does not need Synchronization between transmitter and receiver.
- **Disadvantages of Frequency Division Multiplexing (FDM)**
  - It needs a large bandwidth communication channel.
- **Applications of Frequency Division Multiplexing (FDM)**
  - Frequency division multiplexing is used for FM and AM radio broadcasting.
  - It is used in first generation cellular telephone.
  - It is used in television broadcasting.

Wavelength Division Multiplexing (WDM)

- Wavelength division multiplexing is a technology that increases the bandwidth of a communication channel (optical fiber) by simultaneously allowing multiple optical signals through it.
- the working principle of wavelength division multiplexing is similar to frequency division multiplexing. The only difference is in wavelength division multiplexing optical signals are used instead of electrical signals.
- The main advantage of WDM system is that only need to upgrade the multiplexer and demultiplexer at each end; no need to buy more fibers which are more expensive.

WDM



Wavelength Division Multiplexing

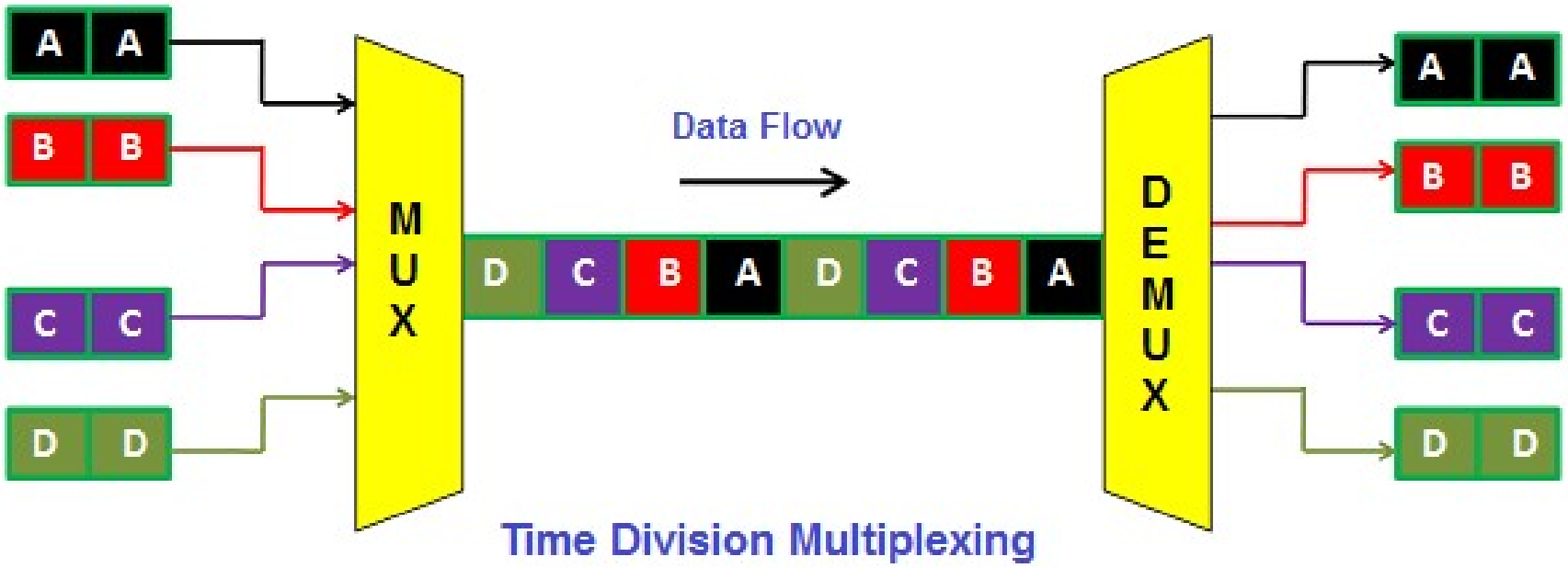
WDM

- WDM techniques are of two types:
  - Dense Wavelength Division Multiplexing (longer distances)
  - Coarse Wavelength Division Multiplexing (Shorter distances)
- **Advantages of Wavelength Division Multiplexing (WDM)**
  - WDM allows transmission of data in two directions simultaneously
  - Low cost
  - Greater transmission capacity
  - High security
  - Long distance communication with low signal loss

Time Division Multiplexing (digital)

- multiple signals are combined and transmitted one after another on the same communication channel.
- in time division multiplexing, all signals operate with the same frequency are transmitted at different times.

TDM

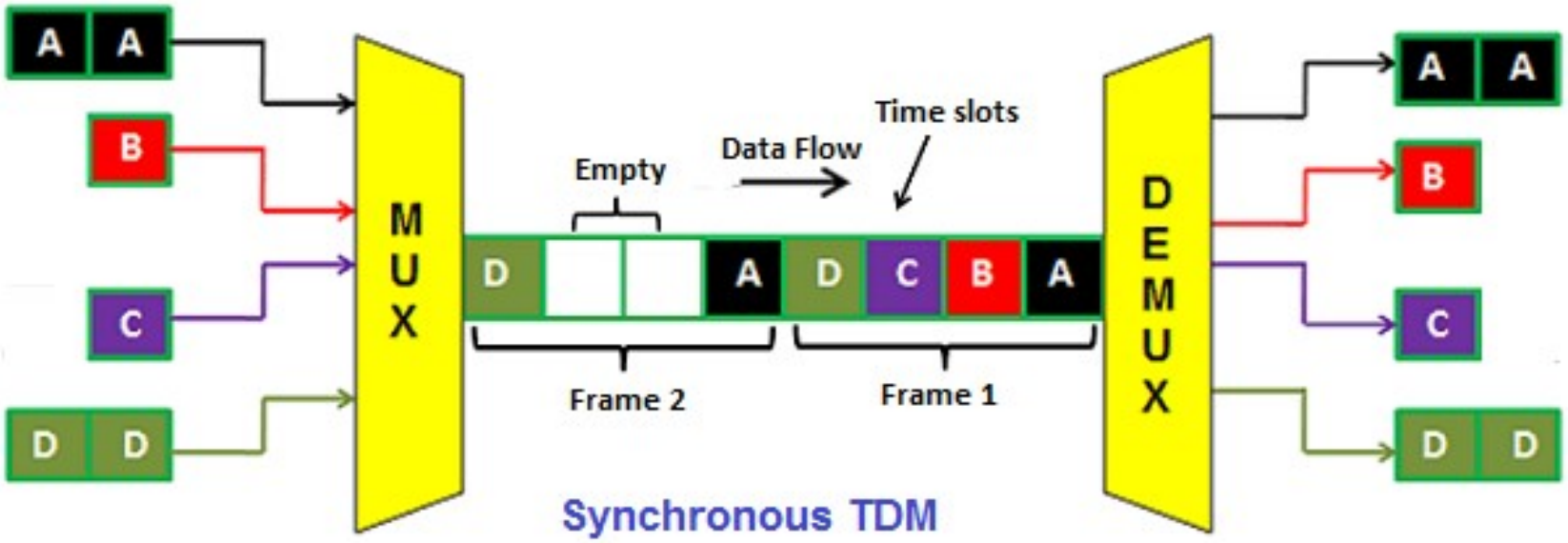

A A
B B
C C
D D
MUX
Data Flow
D C B A D C B A
DEMUX
A A
B B
C C
D D
Time Division Multiplexing

TDM

- Time Division Multiplexing is mainly classified into two types:
  - Synchronous TDM (fixed time slots)
  - Asynchronous TDM (no fixed time slots they are flexible).
- **Advantages of Time Division Multiplexing (TDM)**
  - Full bandwidth is utilized by a user at a particular time.
  - The time division multiplexing technique is more flexible than frequency division multiplexing.
  - In time division multiplexing, the problem of crosstalk is very less.
- **Disadvantages of Time Division Multiplexing (TDM)**
  - In time division multiplexing, synchronization is required.

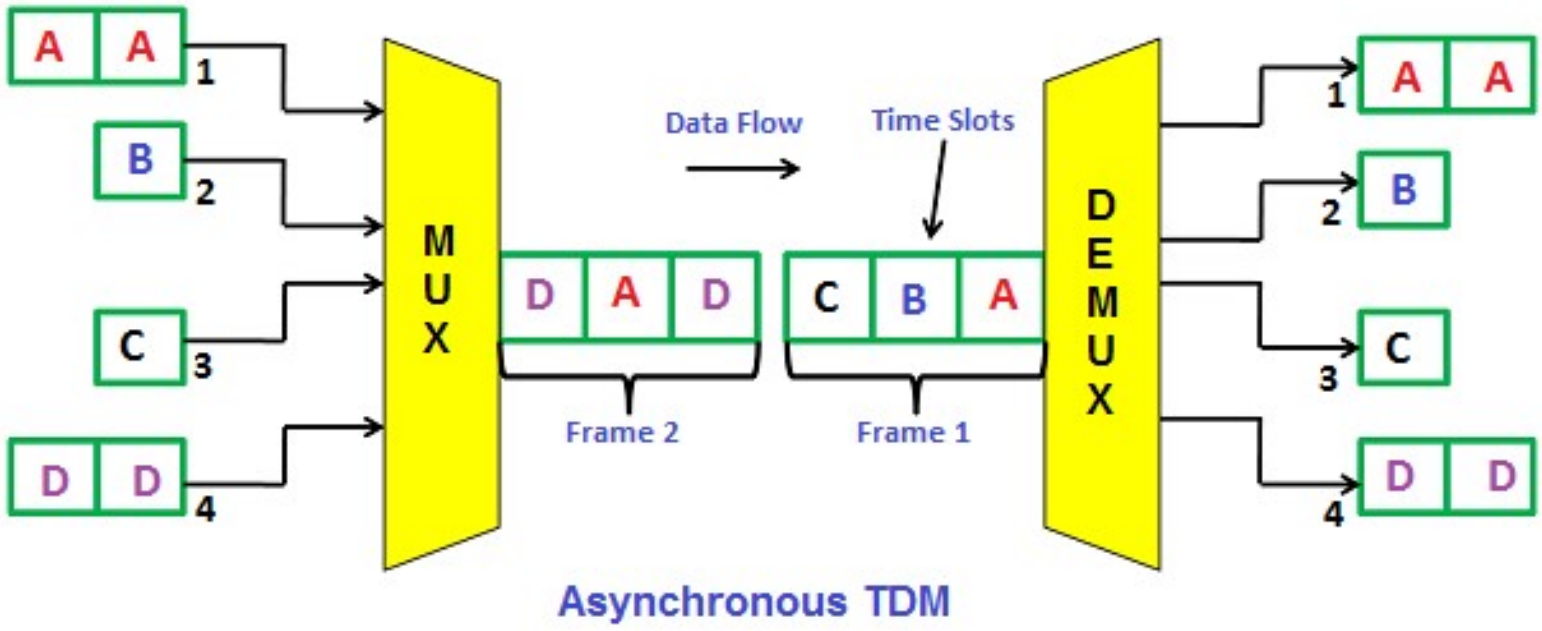
Synchronous TDM

synchronous TDM, the number of time slots is equal to the number of transmitters.



Asynchronous TDM

in Asynchronous TDM, the number of time slots is not equal to the number of devices (transmitters). The time slots in asynchronous TDM are always less than the number of devices (transmitter)



Computer Communication Networks

Introduction, Communication link, Multiplexing

Dr. Raja Vara Prasad

Assistant Professor

IIIT Sri City

CDMA—Code Division Multiple Access

Figure 2-45. (a) Binary chip sequences for four stations. (b) Bipolar chip sequences. (c) Six examples of transmissions. (d) Recovery of station C's signal.

A: 0 0 0 1 1 0 1 1	A: (–1 –1 –1 +1 +1 –1 +1 +1)
B: 0 0 1 0 1 1 1 0	B: (–1 –1 +1 –1 +1 +1 +1 –1)
C: 0 1 0 1 1 1 0 0	C: (–1 +1 –1 +1 +1 +1 –1 –1)
D: 0 1 0 0 0 0 1 0	D: (–1 +1 –1 –1 –1 –1 +1 –1)
(a)	(b)

Six examples:

– – 1 –	$\mathbf{C}$	$S_1 = (-1 +1 -1 +1 +1 +1 -1 -1)$
– 1 1 –	$\mathbf{B} + \overline{\mathbf{C}}$	$S_2 = (-2 \ 0 \ 0 \ 0 +2 +2 \ 0 -2)$
1 0 – –	$\mathbf{A} + \overline{\mathbf{B}}$	$S_3 = (\ 0 \ 0 -2 +2 \ 0 -2 \ 0 +2)$
1 0 1 –	$\mathbf{A} + \overline{\mathbf{B}} + \mathbf{C}$	$S_4 = (-1 +1 -3 +3 +1 -1 -1 +1)$
1 1 1 1	$\mathbf{A} + \mathbf{B} + \mathbf{C} + \mathbf{D}$	$S_5 = (-4 \ 0 -2 \ 0 +2 \ 0 +2 -2)$
1 1 0 1	$\mathbf{A} + \mathbf{B} + \overline{\mathbf{C}} + \mathbf{D}$	$S_6 = (-2 -2 \ 0 -2 \ 0 -2 +4 \ 0)$

(c)

$S_1 \bullet C = (1 +1 +1 +1 +1 +1 +1 +1)/8 = 1$
$S_2 \bullet C = (2 +0 +0 +0 +2 +2 +0 +2)/8 = 1$
$S_3 \bullet C = (0 +0 +2 +2 +0 -2 +0 -2)/8 = 0$
$S_4 \bullet C = (1 +1 +3 +3 +1 -1 +1 -1)/8 = 1$
$S_5 \bullet C = (4 +0 +2 +0 +2 +0 -2 +2)/8 = 1$
$S_6 \bullet C = (2 -2 +0 -2 +0 -2 -4 +0)/8 = -1$

(d)

two stations, A and C, both transmit a 1 bit at the same time that B transmits a 0 bit.

If the received chip sequence is S and the receiver is trying to listen to a station whose chip sequence is

$$\mathbf{S} \bullet \mathbf{C} = (\mathbf{A} + \overline{\mathbf{B}} + \mathbf{C}) \bullet \mathbf{C} = \mathbf{A} \bullet \mathbf{C} + \overline{\mathbf{B}} \bullet \mathbf{C} + \mathbf{C} \bullet \mathbf{C} = 0 + 0 + 1 = 1$$

CDMA—Code Division Multiple Access

two stations, A and C, both transmit a 1 bit at the same time that B transmits a 0 bit.

If the received chip sequence is S and the receiver is trying to listen to a station whose chip sequence is C

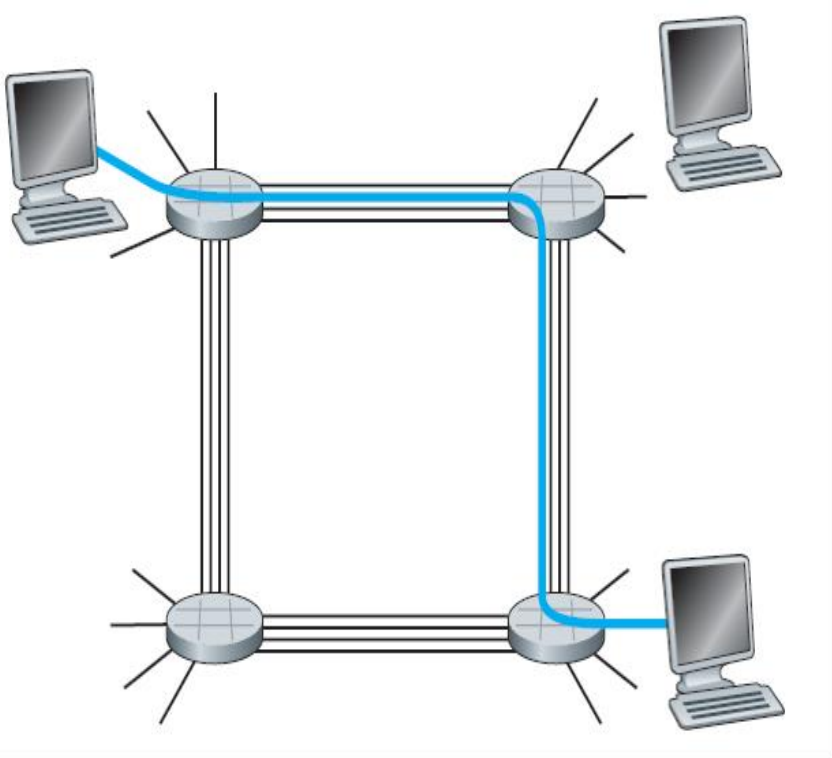
$$S \bullet C = (A + \overline{B} + C) \bullet C = A \bullet C + \overline{B} \bullet C + C \bullet C = 0 + 0 + 1 = 1$$

How are the end systems connected

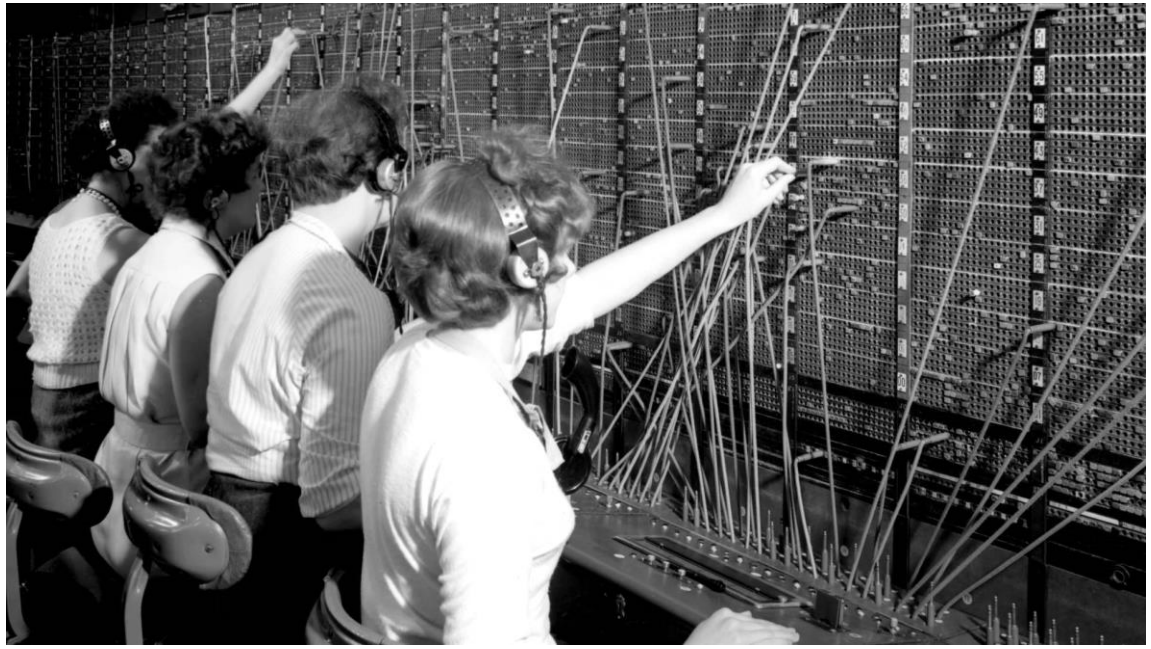
- Circuit switching
  - A dedicated path from source to destination
  - Resources on the path are reserved for the source-destination pair
- Packet switching
  - No dedicated path from source to destination
  - A switch/router forwards packets to another router / destination on the path.

Circuit switching

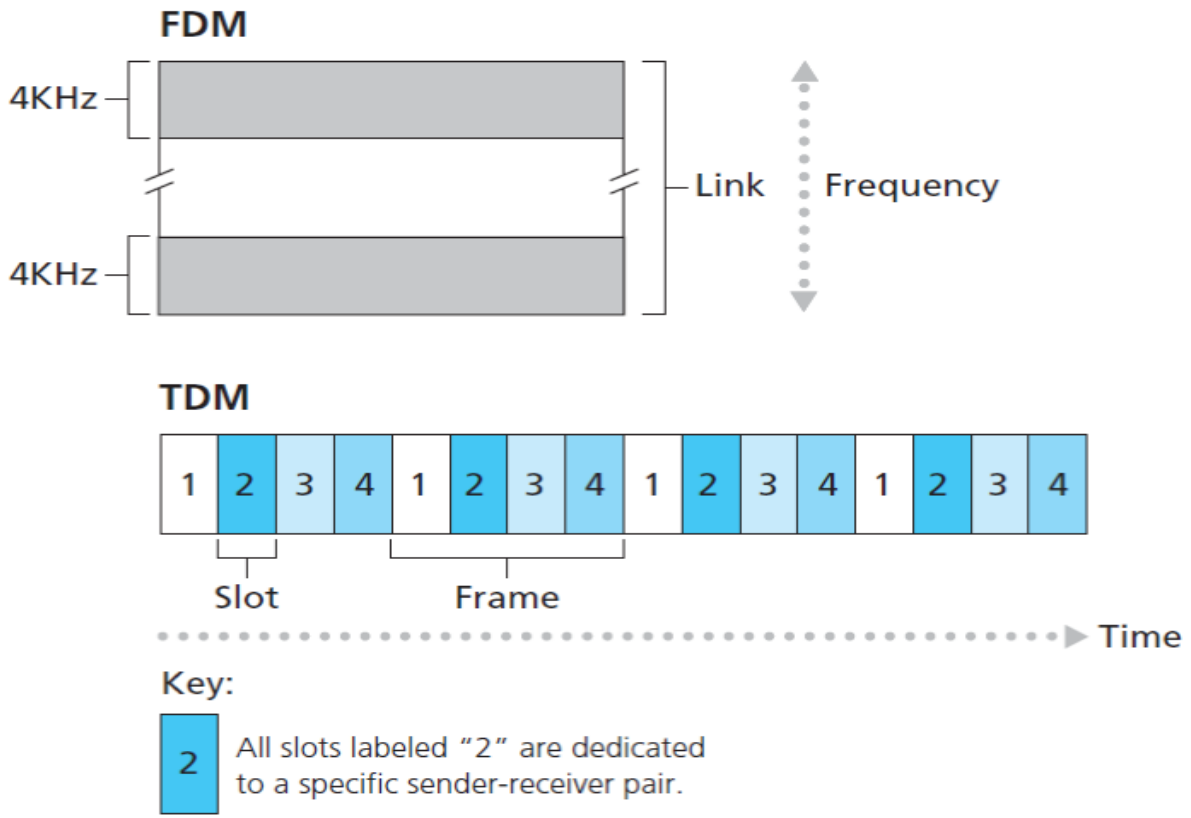
- The network establishes a connection from source to its destination. This connection is called circuit.
- Resources such as bandwidth, buffers on the circuit are blocked for the duration of communication.
- Telephone network is a circuit switching network.
- Links are finite, so very few users can be supported simultaneously.



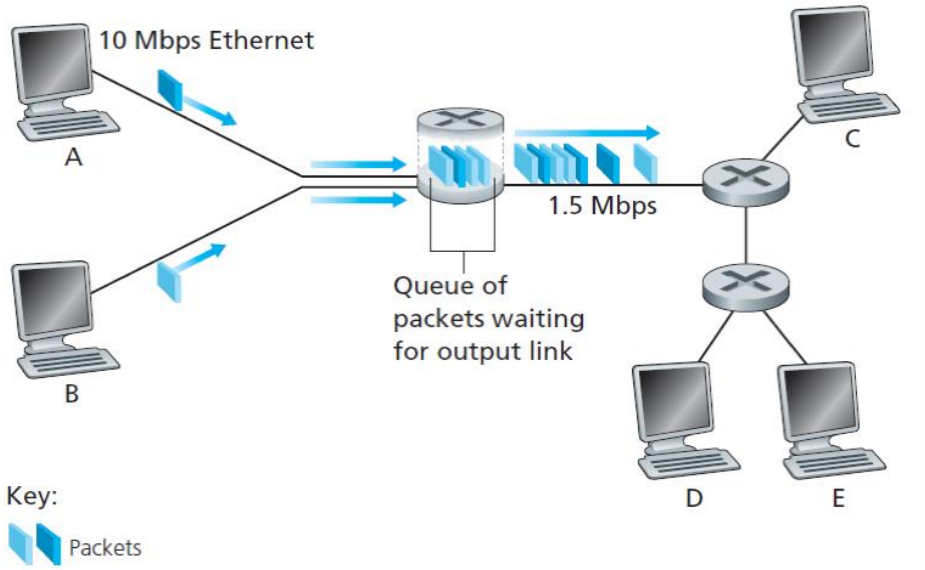
Circuit switching

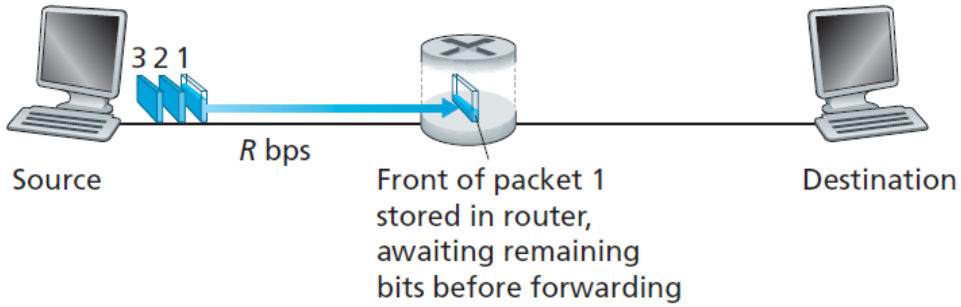


Multiplexing in circuit switching



Packet switching





Statistical multiplexing

- Suppose users share a 1Mbps link.
- A user can be active or inactive. User will generate 100Kbps when active and we assume that a user is active for 10% of the time.
- Circuit switching : 100Kbps must be reserved for each user all the time, can support 10 users simultaneously!
- Circuit switching with TDM:
  - Say, one-second frame is divided into 10 frames each of 100ms.
  - Only 10 simultaneous connections are supported!!!

Statistical multiplexing

- Packet switching: Let there be 35 users in the system. What is the probability that 11 or more users are active simultaneously?
  - Approximately 0.0004
- As the probability of more than 10 users being active simultaneously is small, Packet switching can support 35 users!
- Packet switching allocate links on demand
- On demand allocation of resources is referred to as Statistical multiplexing.

Circuit switching vs Packet switching

Circuit switching

- Waste of bandwidth in silent periods
- Expensive
- Supports less number of connections
- Suitable for real-time services (video conferencing, etc)

Packet switching

- Effective use of bandwidth
- Cheaper than circuit switched network
- Supports more simultaneous connections
- Queuing delays
- Packet loss
- Not suitable for delay constrained applications

Layered Network Architecture

Why Layered Architecture?

- Organizing a network is a big and complicated task.
- Divide and conquer
- Example: Organization of an institute
  - academic section
  - finance section
  - administration section
  - procurement section

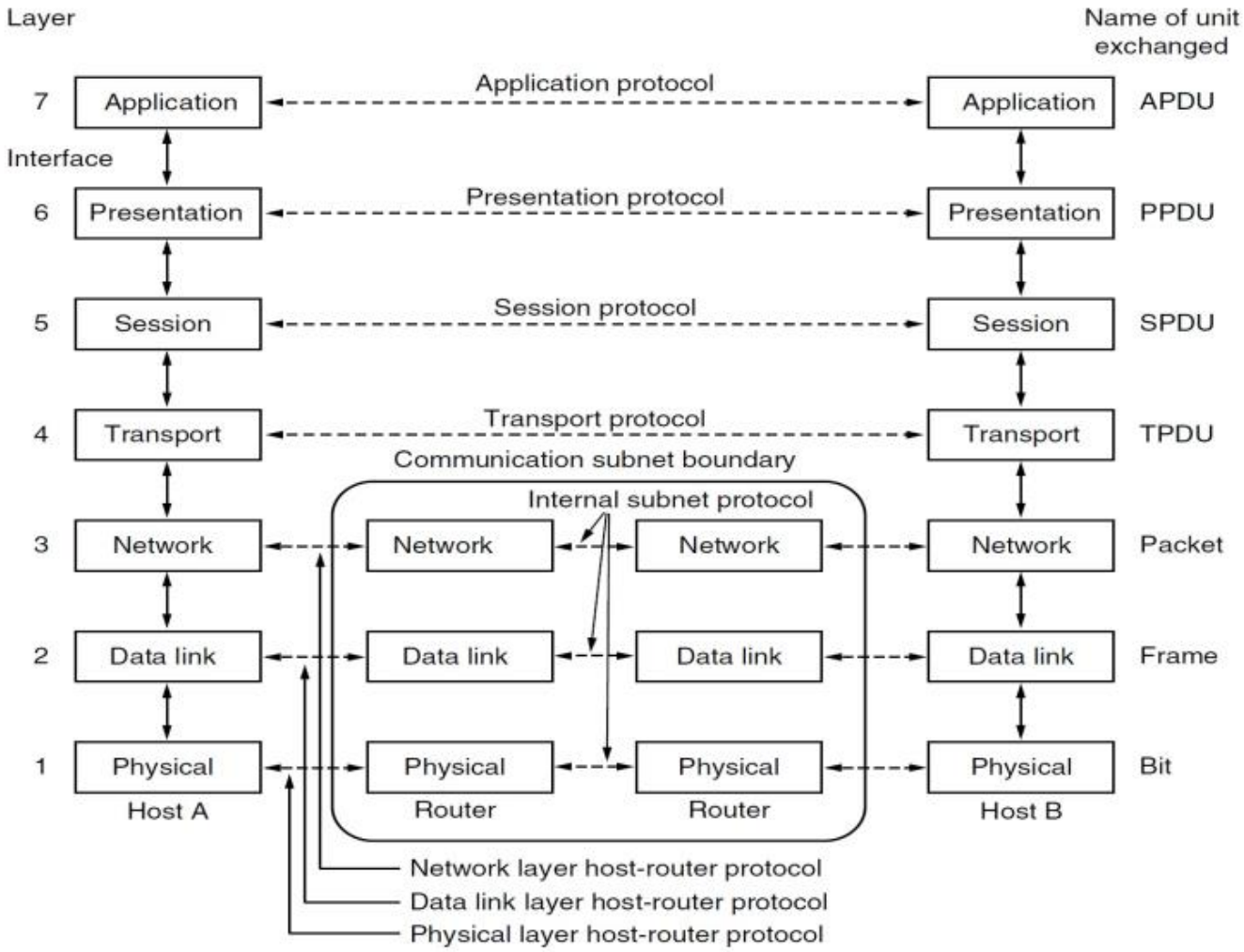
Advantages of Layered Architecture

- Divide the design issues into small pieces.
- A layer provides a service (set of actions) to the immediate higher layer.
- New technologies can be adopted in a layer without affecting other layers.
- Each layer can be analysed and tested independently.

Open System Interconnection (OSI) Reference Model

- Developed by International Organization for Standardization (ISO)
- 7-layer model:
  - Application layer
  - Presentation layer
  - Session layer
  - Transport layer
  - Network layer
  - Data-link layer
  - Physical layer

Layers


Layer
Name of unit exchanged
7
Application
Application protocol
Application
APDU
Interface
6
Presentation
Presentation protocol
Presentation
PPDU
5
Session
Session protocol
Session
SPDU
4
Transport
Transport protocol
Transport
TPDU
Communication subnet boundary
Internal subnet protocol
3
Network
Network
Network
Network
Packet
2
Data link
Data link
Data link
Data link
Frame
1
Physical
Physical
Physical
Physical
Bit
Host A
Router
Router
Host B
Network layer host-router protocol
Data link layer host-router protocol
Physical layer host-router protocol

Application Layer

- Consists of user programs, network applications that does work at hand
- Examples:
  - File transfer, Remote login, Mail, Web access
- Protocols: FTP, Telnet, Simple Mail Transfer Protocol(SMTP), HTTP.

Presentation Layer

- Concerned with syntax and semantics of information transmitted
- Translation
- Encoding data: Data compression/conversion, encryption and decryption

Session Layer

- Allows to establish a session between peers
- Dialogue control: Session can allow bidirectional traffic or only unidirectional traffic.
- Token management: In some protocols, it is required that both sides do not attempt same operation at same time. Session layer provides tokens to perform such actions
- Synchronization: Pausing and resuming a download.

Transport Layer

- Connection-oriented services to applications
  - flow control
  - guaranteed delivery of messages to destination
- Ensures data delivery is
  - error-free
  - in sequence
  - no loss, duplication and corruption of packets

Network Layer

- Interface between host and network
- Routing
- Congestion and deadlock
- Internetworking

Data-Link Layer and Physical Layer

- Data-link layer
  - Takes packet from network layer and moves it to the next router
  - error-free delivery: computes error detection information
- Physical layer
  - Controls transmission into the network cable.
  - Defines electrical signals.

Internet Protocol Stack

- Application layer
- Transport layer
- Network layer
- Data-link layer
- Physical layer

Encapsulation

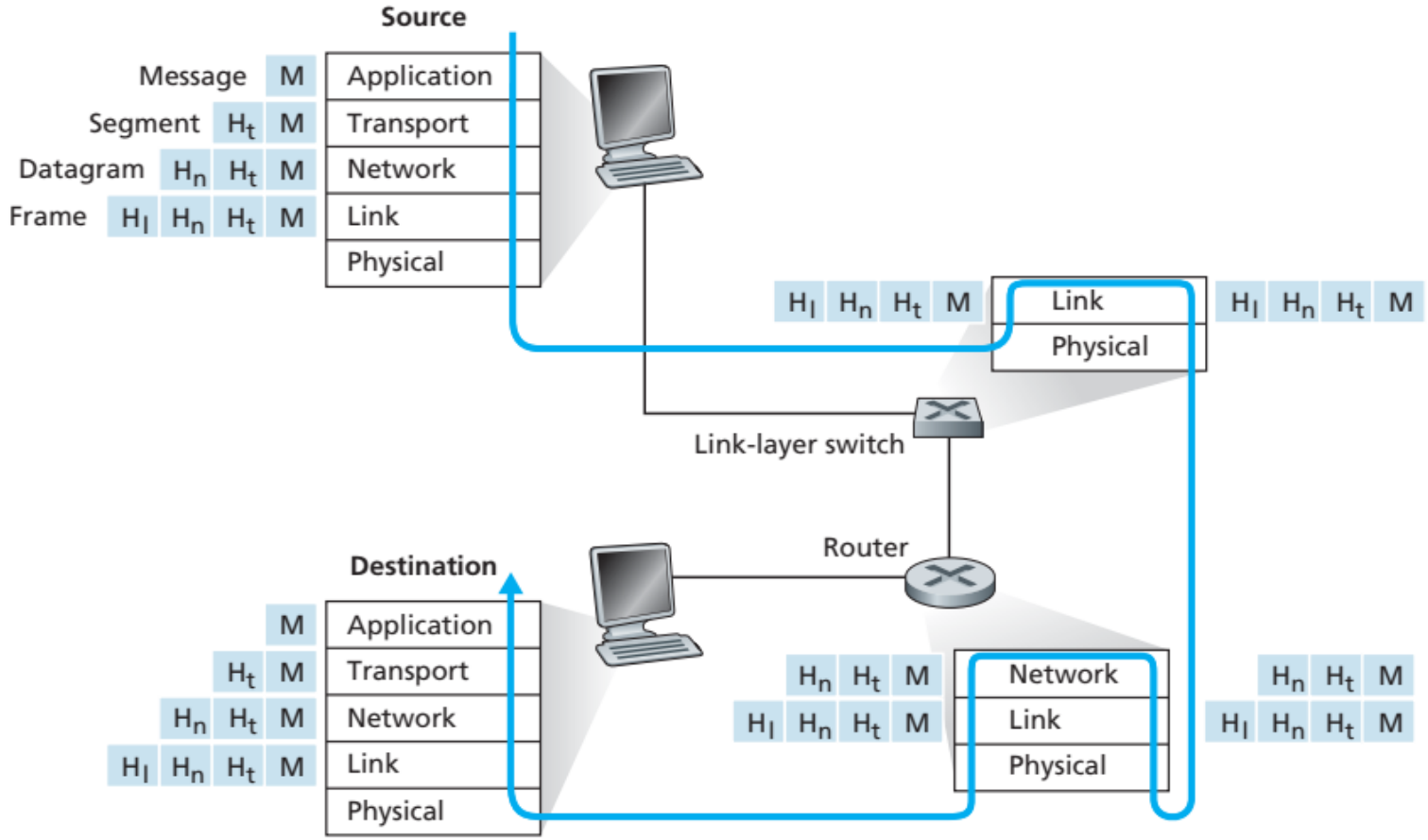


Figure 1.24 ♦ Hosts, routers, and link-layer switches; each contains a different set of layers, reflecting their differences in functionality

Computer Communication Networks

Introduction, Communication link, Multiplexing

Dr. Raja Vara Prasad

Assistant Professor

IIIT Sri City

Delays in Packet Switched Networks

- Packets travel from source to destination via intermediate routers/switches.
  - Processing delay
  - Queueing delay
  - Transmission delay
  - Propagation delay
- Nodal delay = Processing delay + Queuing delay + Transmission delay + Propagation delay

Processing Delay

- Time required to examine the packets header
  - Determines where to direct the packet
  - Check for errors
- Order of microseconds

Queuing Delay

- If a router is busy in processing and transmitting a packet, a freshly arrived packet has to wait in queue (buffer) for its turn.
- No queuing delay if the router is idle.
- Queuing delay varies with time and location. In general, it is a random variable.
- Order of microseconds to milliseconds.

Transmission Delay

- Time required to push the packet into the link
- If the length of the packet is L bits and transmission rate of the link is R bps, then

$$\text{Transmission delay} = \frac{L}{R}$$

- Order of microseconds to milliseconds

Propagation Delay

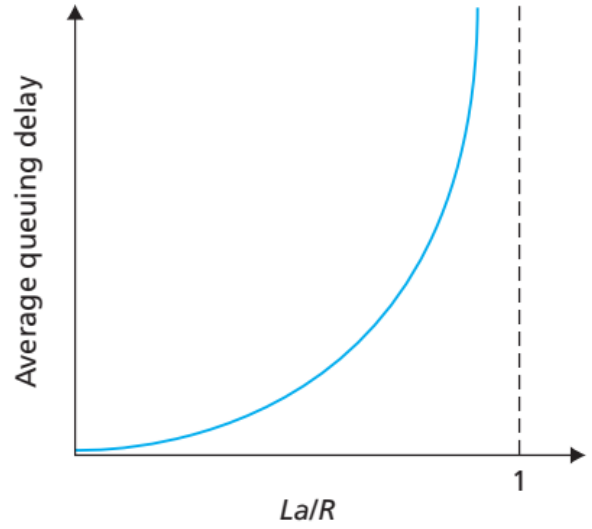
- Time required to propagate from one end of the link to the other end
- The propagation speed depends on the physical link between the routers
- In general, propagation speed s, is in the order of $2 \times 10^8 - 3 \times 10^8 m/s$.
- Propagation speed depends on the distance bewteen the routers, d
- Propagation delay $= \frac{d}{s}$

Traffic Intensity

- Queuing delays are random in nature
- Arrivals to a queue are also random in nature
- Traffic intensity is an indication of queuing delay
- Let a be the average number of packets arriving at a queue
- Each packet is of length L bits adn transmission rate is R bps
- Traffic intensity $= \frac{La}{R}$

Traffic Intensity

- If traffic intensity > 1, the *queuelength* increases to ∞
- It is desirable to have traffic intensity < 1.
- If traffic intensity close to 1, there will be a significant queuing delay



Dependence of average queuing delay on traffic intensity

Throughput

- Suppose Host A is sending data to Host B across a computer network
- Instantaneous throughput is the rate at which Host B is receiving data
- Suppose it takes T seconds to transfer F bits from Host A to Host B, then average throughput $= \frac{F}{T}$ bps.

Throughput

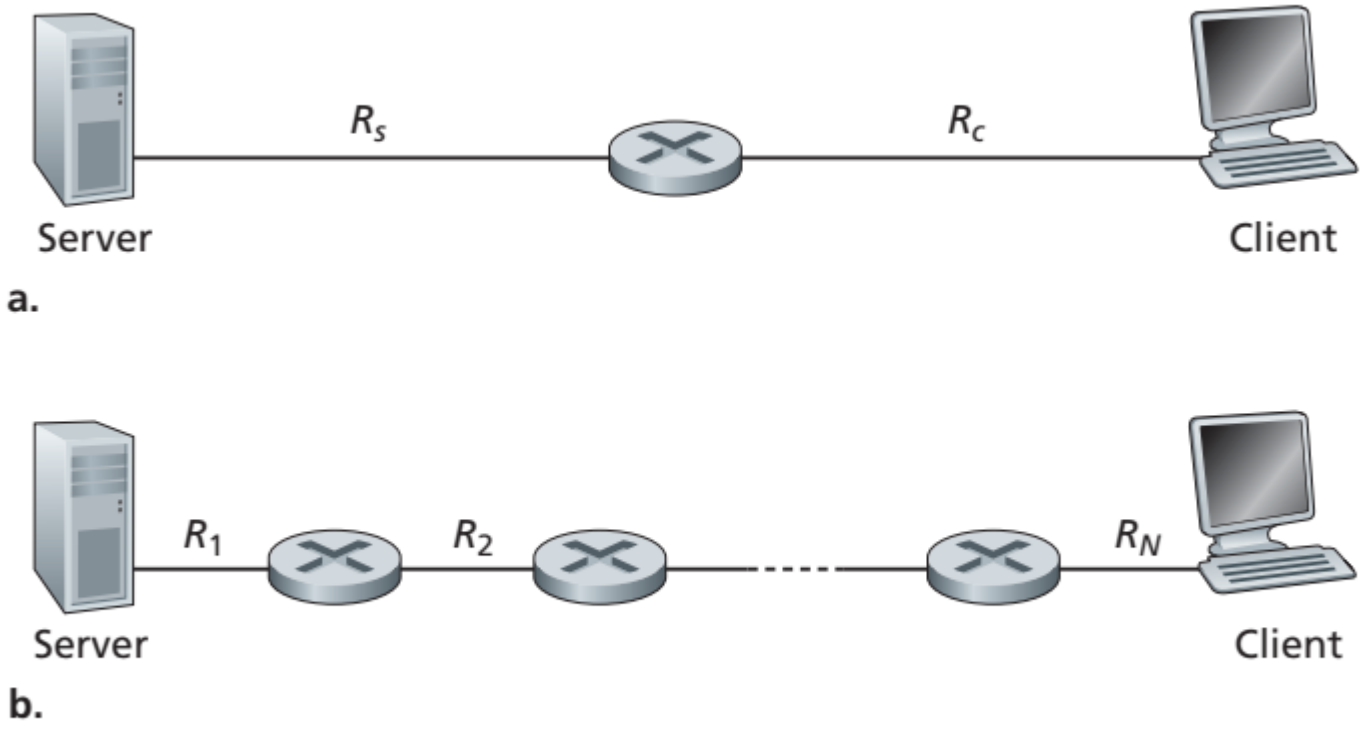


Figure 1.19 ♦ Throughput for a file transfer from server to client

Throughput - Challenges

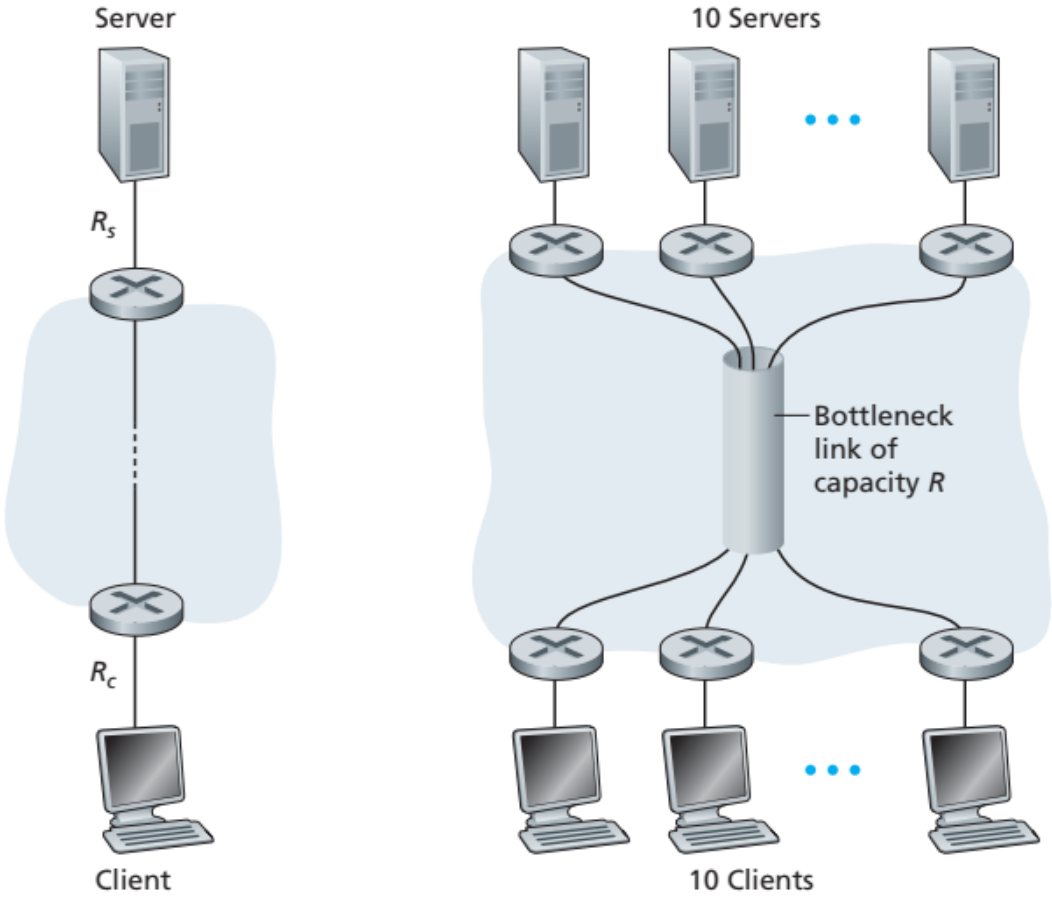


Figure 1.20 ♦ End-to-end throughput: (a) Client downloads a file from server; (b) 10 clients downloading with 10 servers

Case-a:

R, is large—say a hundred times larger than both *Rs* and *Rc*—then the throughput for each download will once again be min{*Rs*, *Rc*}.

Case-b:

Suppose R_s = 2 Mbps, R_c = 1 Mbps, R = 5 Mbps,

- common link divides its transmission rate equally among the 10 downloads.
- Then the bottleneck for each download is no longer in the access network
- instead the shared link in the core, which only provides each download with 500 kbps of throughput.

the end-to-end throughput for each download is now reduced to 500 kbps

Tutorial – Problems

1.Suppose users share a 2 Mbps link. Also suppose each user transmits continuously at 1 Mbps when transmitting, but each user transmits only 20 percent of the time.

a. When circuit switching is used, how many users can be supported?

b. For the remainder of this problem, suppose packet switching is used. Why will there be essentially no queuing delay before the link if two or fewer users transmit at the same time? Why will there be a queuing delay if three users transmit at the same time?

c. Find the probability that a given user is transmitting.

d. Suppose now there are three users. Find the probability that at any given time, all three users are transmitting simultaneously. Find the fraction of time during which the queue grows.

Problem 3

Suppose N packets arrive simultaneously to a link at which no packets are currently being transmitted or queued. Each packet is of length L bits and the link has a transmission rate of R bits/sec. What is the average queueing delay for the N packets ?

Problems

- Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has three links of rates $R_1 = 500$kbps, $R_2 = 2$Mbps, $R_3 = 1$Mbps.
  - Assuming no other traffic, what is the throughput for the file transfer
  - Suppose the file size is 4 million bytes, how long will it take to transfer the file from A to B?
- How long does it take for a packet of length 1000 bytes to propagate over a link of propagation speed 2.5×10^8 m/s. Length of the link is 2,500 Km and transmission rate is 2Mbps.

P6. This elementary problem begins to explore propagation delay and transmission delay, two central concepts in data networking. Consider two hosts, A and B, connected by a single link of rate R bps. Suppose that the two hosts are separated by m meters, and suppose the propagation speed along the link is s meters/sec. Host A is to send a packet of size L bits to Host B.

a. Express the propagation delay, d_{prop}, in terms of m and s.

b. Determine the transmission time of the packet, d_{trans}, in terms of L and R.

c. Ignoring processing and queuing delays, obtain an expression for the end-to-end delay.

d. Suppose Host A begins to transmit the packet at time $t = 0$. At time $t = d_{trans}$, where is the last bit of the packet?

e. Suppose d_{prop} is greater than d_{trans}. At time $t = d_{trans}$, where is the first bit of the packet?

f. Suppose d_{prop} is less than d_{trans}. At time $t = d_{trans}$, where is the first bit of the packet?

g. Suppose $s = 2.5 \cdot 10^8$, $L = 120$ bits, and $R = 56$ kbps. Find the distance m so that d_{prop} equals d_{trans}.

P12. A packet switch receives a packet and determines the outbound link to which the packet should be forwarded. When the packet arrives, one other packet is halfway done being transmitted on this outbound link and four other packets are waiting to be transmitted. Packets are transmitted in order of arrival. Suppose all packets are 1,500 bytes and the link rate is 2 Mbps. What is the queuing delay for the packet? More generally, what is the queuing delay when all packets have length L, the transmission rate is R, x bits of the currently-being-transmitted packet have been transmitted, and n packets are already in the queue?

Traceroute

- program that can run in any Internet host
- When the user specifies a destination hostname, the program in the source host sends multiple, special packets toward that destination
- packets work their way toward the destination, they pass through a series of routers
- router receives one of these special packets, it sends back to the source a short message that contains the name and address of the router
- source will send *N* special packets into the network, with each packet addressed to the ultimate destination
- source records the time that elapses between when it sends a packet and when it receives the corresponding return message
- the source can reconstruct the route taken by packets flowing from source to destination, and the source can determine the round-trip delays to all the intervening routers

```
1 cs-gw (128.119.240.254) 1.009 ms 0.899 ms 0.993 ms
2 128.119.3.154 (128.119.3.154) 0.931 ms 0.441 ms 0.651 ms
3 border4-rt-gi-1-3.gw.umass.edu (128.119.2.194) 1.032 ms 0.484 ms 0.451 ms
4 acr1-ge-2-1-0.Boston.cw.net (208.172.51.129) 10.006 ms 8.150 ms 8.460 ms
5 agr4-loopback.NewYork.cw.net (206.24.194.104) 12.272 ms 14.344 ms 13.267 ms
6 acr2-loopback.NewYork.cw.net (206.24.194.62) 13.225 ms 12.292 ms 12.148 ms
7 pos10-2.core2.NewYork1.Level3.net (209.244.160.133) 12.218 ms 11.823 ms 11.793 ms
8 gige9-1-52.hsipaccess1.NewYork1.Level3.net (64.159.17.39) 13.081 ms 11.556 ms 13.297 ms
9 p0-0.polyu.bbnplanet.net (4.25.109.122) 12.716 ms 13.052 ms 12.786 ms
10 cis.poly.edu (128.238.32.126) 14.080 ms 13.035 ms 12.802 ms
```

Networks Under Attack

- “attempt to wreak havoc in our daily lives by damaging our Internet-connected computers, violating our privacy, and rendering inoperable the Internet services on which we depend”

malicious stuff—collectively known as **malware**—that can enter and infect devices

- deleting our files.
- installing spyware that collects our private information, such as social security numbers, passwords, and keystrokes
- sends this over the Internet back to attacker

compromised host may also be enrolled in a network of thousands of similarly compromised devices, collectively known as a **botnet**

✓ **self-replicating**

✓ **Viruses** are malware that require some form of user interaction to infect the user’s device

✓ **Worms** are malware that can enter a device without any explicit user interaction

Networks Under Attack

Denial-of-service (DoS) attacks:

- renders a network, host, or other piece of infrastructure unusable by legitimate users
- *Vulnerability attack:* sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. The service can stop or, worse, the host can crash.
- *Bandwidth flooding:* sends a deluge of packets to the targeted host, so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server.
- *Connection flooding.* The attacker establishes a large number of half-open or fully open TCP connections at the target host. The host stops accepting legitimate connections due to the bogus connections.

- **Distributed DoS (DDoS)** attack: leveraging botnets with thousands of comprised hosts; much harder to detect and defend against than a DoS attack from a single host.

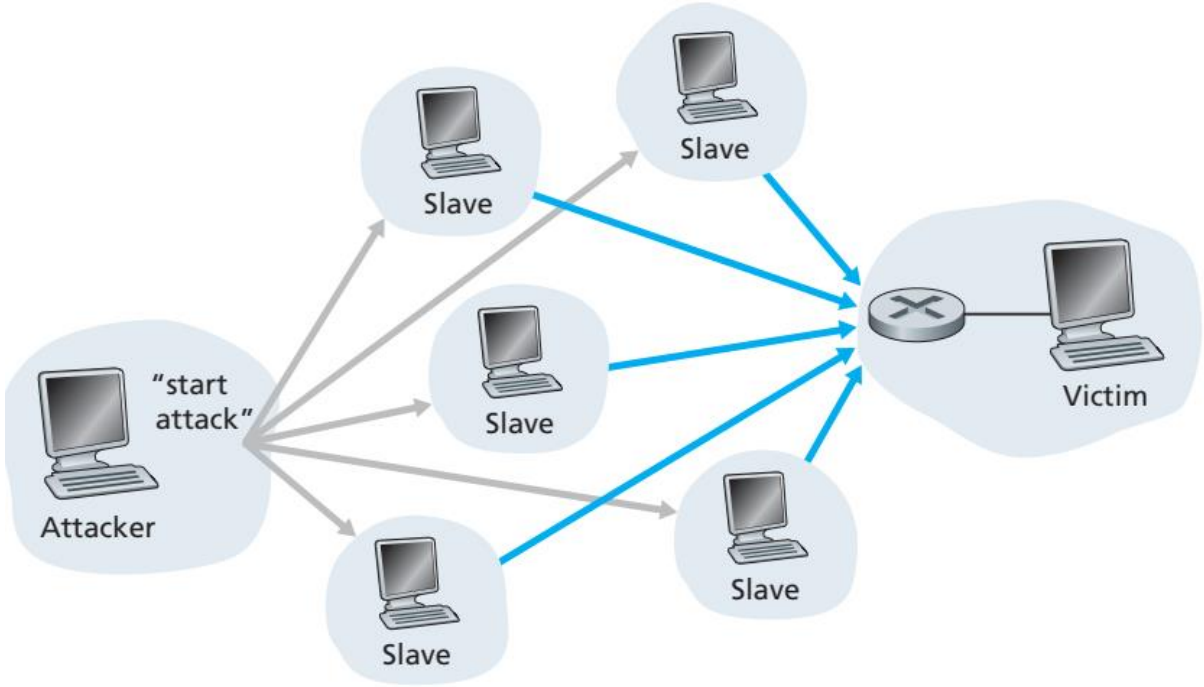
Networks Under Attack

Distributed DoS (DDoS) attack: leveraging botnets with thousands of comprised hosts

- much harder to detect and defend against than a DoS attack from a single host.

Packet Sniffers:

- placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted



- packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages.
- Sniffed packets can then be analyzed offline for sensitive information
- Wireshark: a packet sniffer
- packet sniffers are passive—do not inject packets into the channel—difficult to detect
- defenses against packet sniffing involve cryptography

Computer Communication Networks

Application Layer

Dr. Raja Vara Prasad

Assistant Professor

IIIT Sri City

Application Layer

Network Applications

Network application development -- writing programs that run on

different end systems and communicate with each other over the network

Example:

Web application → two distinct programs that communicate with each other:

- the browser program running in the user's host (desktop, laptop, tablet, smartphone, and so on);
- the Web server program running in the Web server host.
- in P2P file-sharing system there is a program in each host that participates in the file-sharing community

Network Applications

- do not need to write software that runs on network core devices, such as routers or link-layer switches
- Network core devices do not function at the application layer
- function at lower layers— specifically at the network layer and below

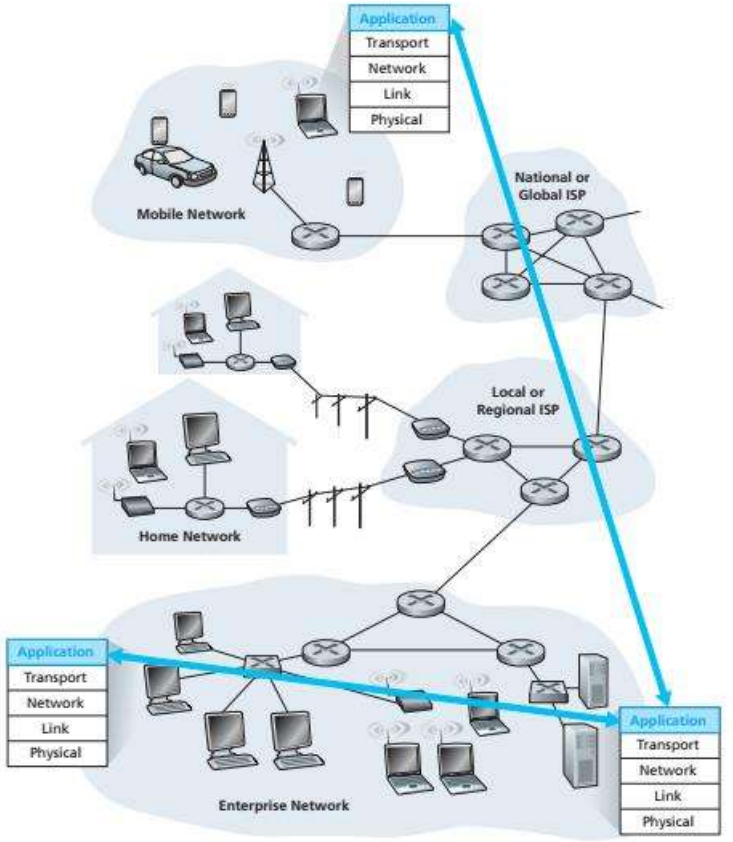


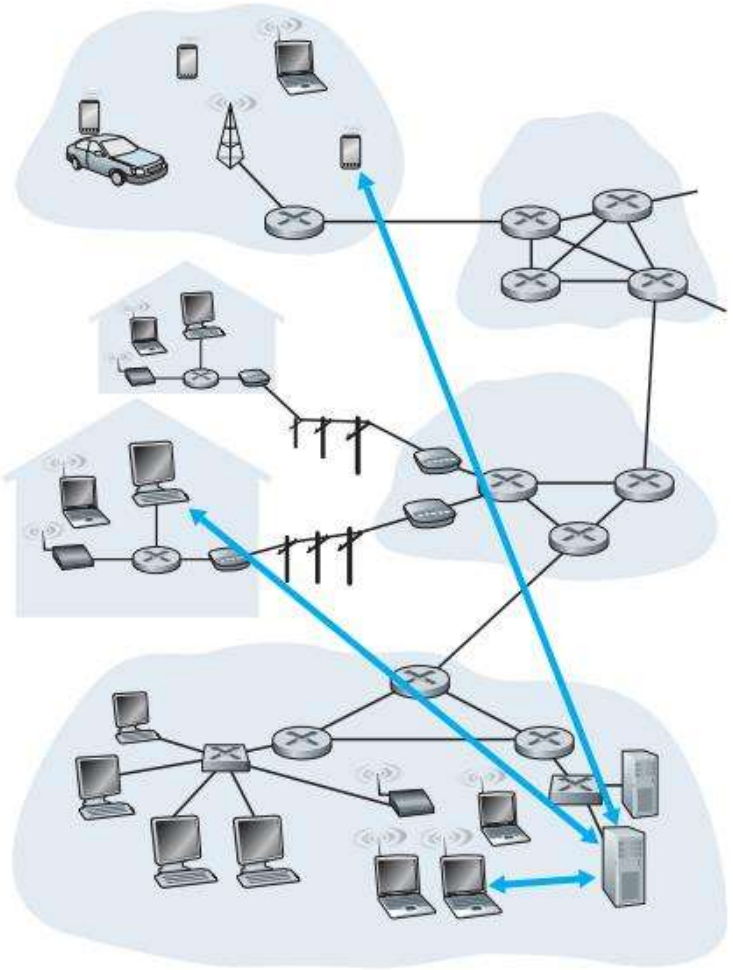
Figure 2.1 • Communication for a network application takes place between end systems at the application layer

Network Applications

- Applications use the services of network (Transport layer)
- For an application developer, architecture and services of network are fixed
- Architectures of applications:
  - Client-Server architecture
  - Peer-to-Peer (P2P) architecture
- Application developer decides on the architecture and services of transport layer to be used.

Client-Server Architecture

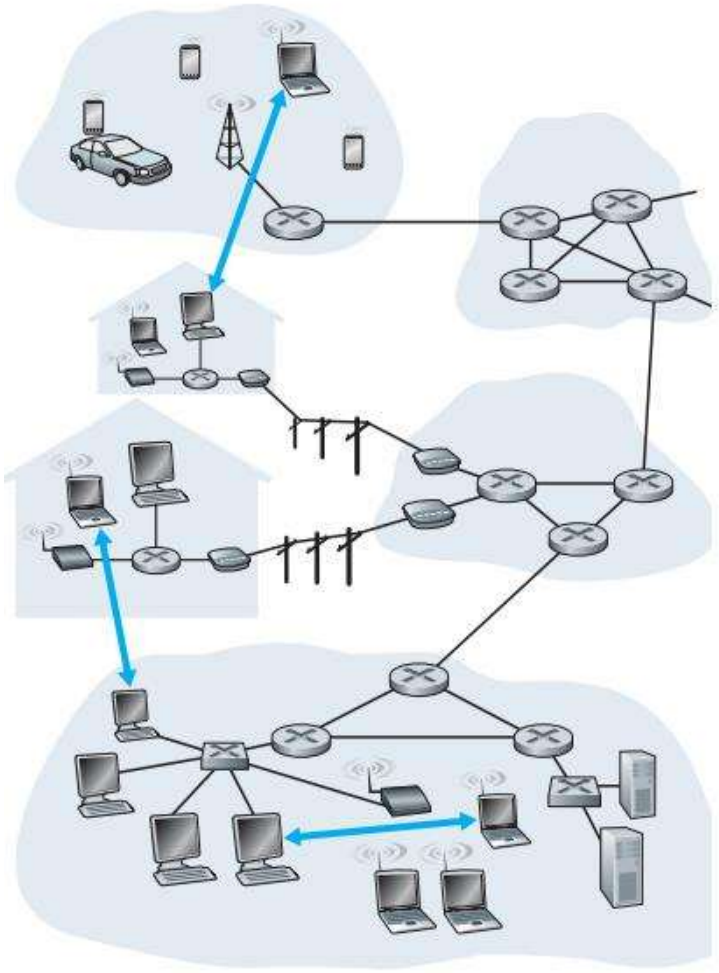
- Server: An end system that serves the requests from various hosts.
- A server is always ON.
- Client: An end system that requests a server for content.
- A client can be either ON-OFF or always ON.
- Example applications using this architecture: web, e-mail, file transfer, etc.



a. Client-server architecture

Peer-to-Peer Architecture

- End systems communicate by a direct connection.
- The end systems are called peers.
- Example applications: skype, internet telephony, torrents, etc
- Advantages:
  - File distribution
  - Self-scalable: can handle growth in traffic
  - Cost effective: no server infrastructure and server bandwidth.
- Challenges in P2P Architecture:
  - ISP friendly: asymmetric data traffic.
  - Security
  - Incentives: Peers should share bandwidth.



b. Peer-to-peer architecture

Processes Communicating

- A process is a program that is running within an end system.
- A client process is a process running on a client and a server process is process running on a server.
- It is the client process and server processes that are actually communicating.
- A process sends and receives messages to and from transport layer through a software interface known as socket.
- A socket is also known as Application Programming Interface (API).

Interface Between the Process: API

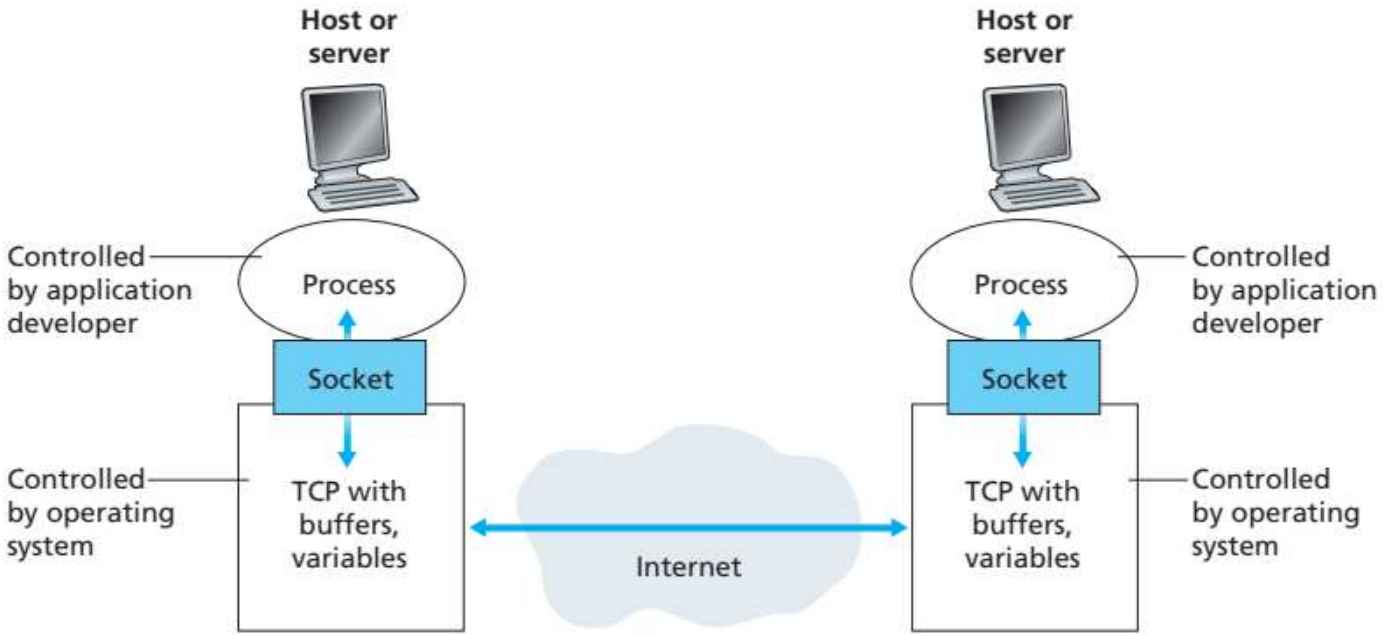


Figure 2.3 ♦ Application processes, sockets, and underlying transport protocol

Services of Transport Layer

- Reliable data transfer: Guaranteed data delivery service.
- Throughput
- Timing: for example, it is guaranteed that a packet will be delivered no more than 100 msec later.
- security: end-point authentication, encryption and decryption.

Requirements of Applications

Application	Data Loss	Throughput	Time-Sensitive
File transfer/download	No loss	Elastic	No
E-mail	No loss	Elastic	No
Web documents	No loss	Elastic (few kbps)	No
Internet telephony/ Video conferencing	Loss-tolerant	Audio: few kbps–1Mbps Video: 10 kbps–5 Mbps	Yes: 100s of msec
Streaming stored audio/video	Loss-tolerant	Same as above	Yes: few seconds
Interactive games	Loss-tolerant	Few kbps–10 kbps	Yes: 100s of msec
Instant messaging	No loss	Elastic	Yes and no

Figure 2.4 ♦ Requirements of selected network applications

Transport protocols

- Transmission Control Protocol (TCP)
  - Connection oriented service: handshaking, full-duplex connection
  - Reliable data transfer service: packets get delivered without error and in proper order.
  - Congestion control
- User Datagram Protocol (UDP)
  - Connectionless
  - Unreliable data transfer service.
  - No congestion control

- can often provide satisfactory service to time-sensitive applications,
- cannot provide any timing or throughput guarantees

Applications

Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP [RFC 5321]	TCP
Remote terminal access	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
File transfer	FTP [RFC 959]	TCP
Streaming multimedia	HTTP (e.g., YouTube)	TCP
Internet telephony	SIP [RFC 3261], RTP [RFC 3550], or proprietary (e.g., Skype)	UDP or TCP

Addressing Processes

- There are many processes running on a host, how to identify the destination process?
- We identify host by IP address.
- We identify processes by port numbers!
- For example, web server is identified by port number 80, mail server is identified by port number 25.

Application Layer - Introduction

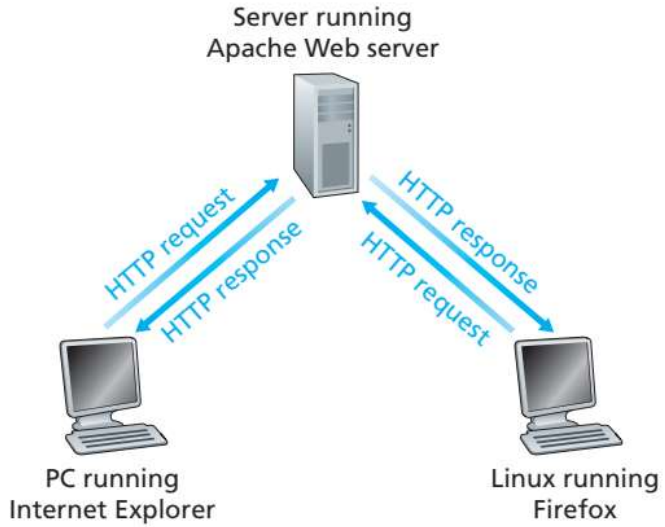
Application-layer protocol defines:

- The types of messages exchanged, for example, request messages and response messages
- The syntax of the various message types, such as the fields in the message and how the fields are delineated
- The semantics of the fields - meaning of the information in the fields
- Rules for determining when and how a process sends messages and responds to messages

Application-layer protocol is only one piece of a network application

Web and HTTP

- A web page is a document and consists of objects
- An object is nothing but a file such as HyperText Markup Language (HTML) file, an image file, applet or video clip.
- If a web page contains a basic html file and ten images, we say the web page contains 11 objects.
- HyperText Transfer Protocol (HTTP) is the web's application layer protocol
- HTTP uses client-server architecture with TCP.
- The client program and server program talk to each other by exchanging HTTP messages.



HTTP request-response behavior

Uniform Resource Locater

- An object should be addressable by a URL.
- Each URL consists of hostname and objects path name
- For example, http://www.iiits.ac.in/wp-content/uploads/2017/05/Untitled-design-15.png is url for an image.
- www.iiits.ac.in is host name
- wp-content/uploads/2017/05/Untitled-design-15.png is path name.
- Client side of HTTP is implemented in Web browser and server side is implemented in Web server.
- Examples: Apache and Microsoft Internet Information server.

- ✓ base HTML file plus objects
- ✓ base HTML file references the other objects in the page with the objects' URLs.

HTTP

- HTTP client initiates a connection with HTTP server (handshaking).
- Once the connection is established, client and server exchange messages through socket interface.
- Client sends an HTTP request and receives HTTP messages through its socket
- Server receives HTTP requests and sends HTTP responses through its socket interface.
- Client/server need not worry about packets (does not have any control) after sending through their socket.
- Server sends requested files without storing state information of client. Thus HTTP is a stateless protocol.

HTTP Connection

- Let us say, a web page has one html file and 10 images.
- How does client retrieve the web page?
- Nonpersistent and Persistent
- Nonpersistent: one TCP connection for each file
- Persistent: one TCP connection for all files

Nonpersistent Connection

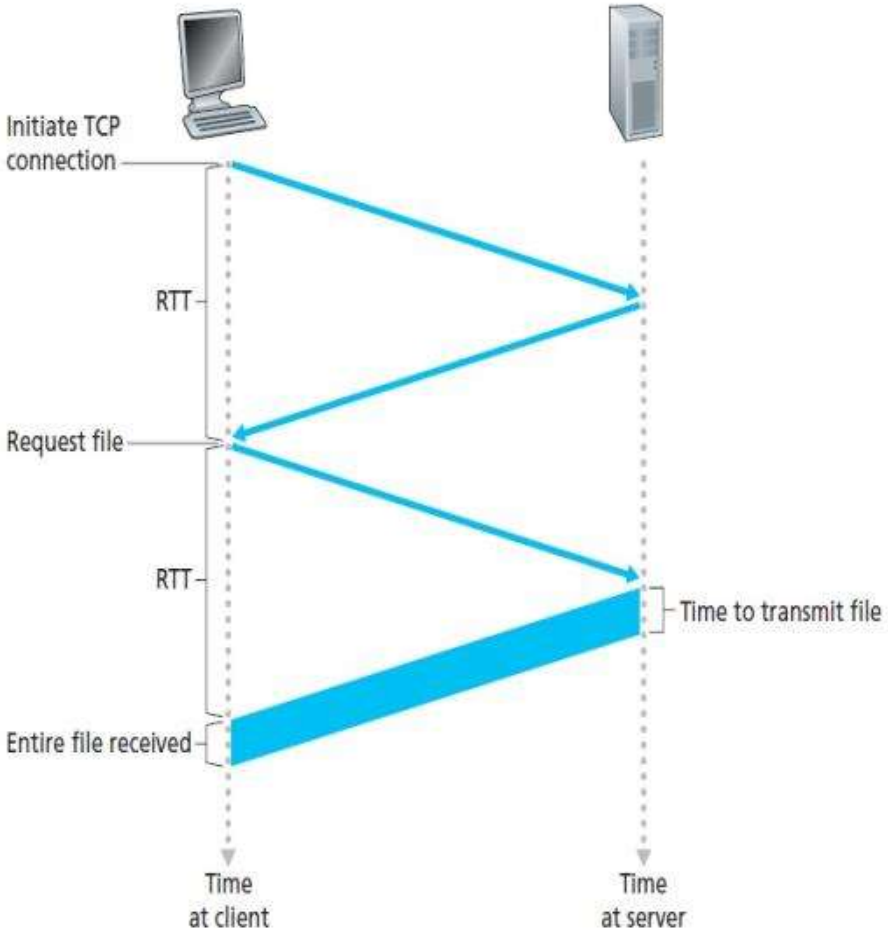
- For each file:
  - HTTP client initiates a TCP connection to the server on port number 80
  - Client sends its HTTP request and it includes the path name to the file
  - HTTP server receives the request and retrieves the file and sends the HTTP response to the client
  - HTTP server tells TCP to close the connection.
- TCP connections can be serial or parallel depending on browser's configuration

Example: Non-Persistent

- steps of transferring a Web page from server to client for the case of non-persistent connections.
- page consists of a base HTML file and 10 JPEG images → 11 objects reside on the same server.
- URL for the base HTML file is: http://www.someSchool.edu/someDepartment/home.index

1. The HTTP client process initiates a TCP connection to the server `www.someSchool.edu` on port number 80, which is the default port number for HTTP. Associated with the TCP connection, there will be a socket at the client and a socket at the server.
2. The HTTP client sends an HTTP request message to the server via its socket. The request message includes the path name `/someDepartment/home.index`. (We will discuss HTTP messages in some detail below.)
3. The HTTP server process receives the request message via its socket, retrieves the object `/someDepartment/home.index` from its storage (RAM or disk), encapsulates the object in an HTTP response message, and sends the response message to the client via its socket.
4. The HTTP server process tells TCP to close the TCP connection. (But TCP doesn't actually terminate the connection until it knows for sure that the client has received the response message intact.)
5. The HTTP client receives the response message. The TCP connection terminates. The message indicates that the encapsulated object is an HTML file. The client extracts the file from the response message, examines the HTML file, and finds references to the 10 JPEG objects.
6. The first four steps are then repeated for each of the referenced JPEG objects.

Round-Trip Time



Persistent Connection

- Server leaves the connection after sending the HTTP response
- Pipelining: A browser can request for files without waiting for the reception of pending requests.
- TCP closes after some idle period
- Default mode HTTP: Persistent connection with pipelining.

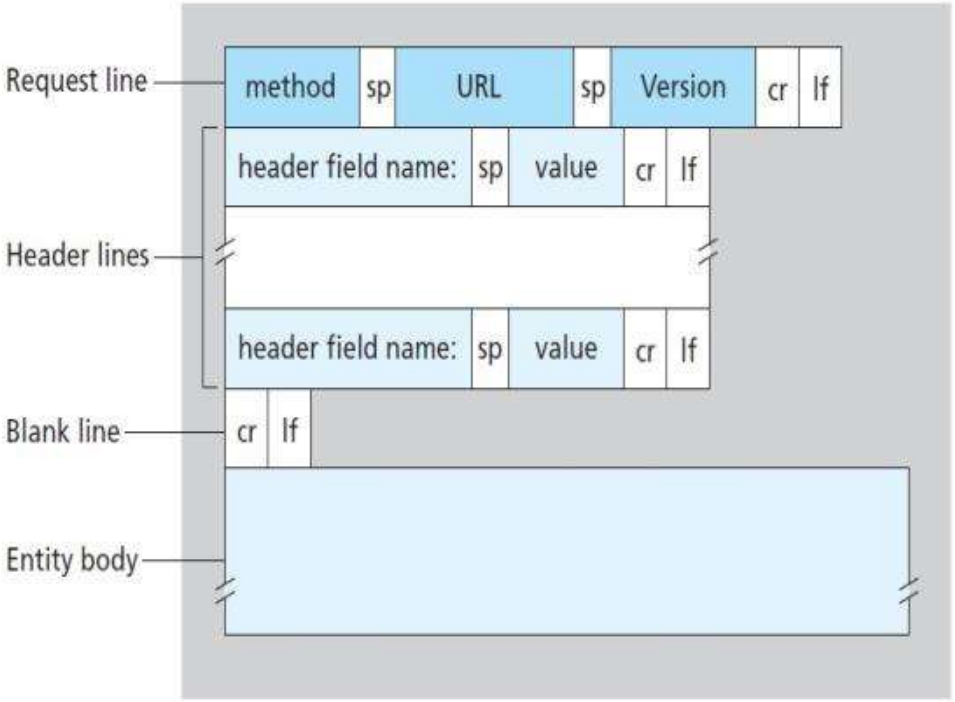
HTTP Request Format

- HTTP request message:

```
GET /somedir/page.html HTTP/1.1
Host: www.iitm.ac.in
Connection: close
User-agent: Mozilla/4.0
Accept-language: En
```

- Methods: GET, PUT, POST, HEAD, DELETE

HTTP Request



Computer Communication Networks

Application Layer

Dr. Raja Vara Prasad

Assistant Professor

IIIT Sri City

Application Layer

Application Layer - Introduction

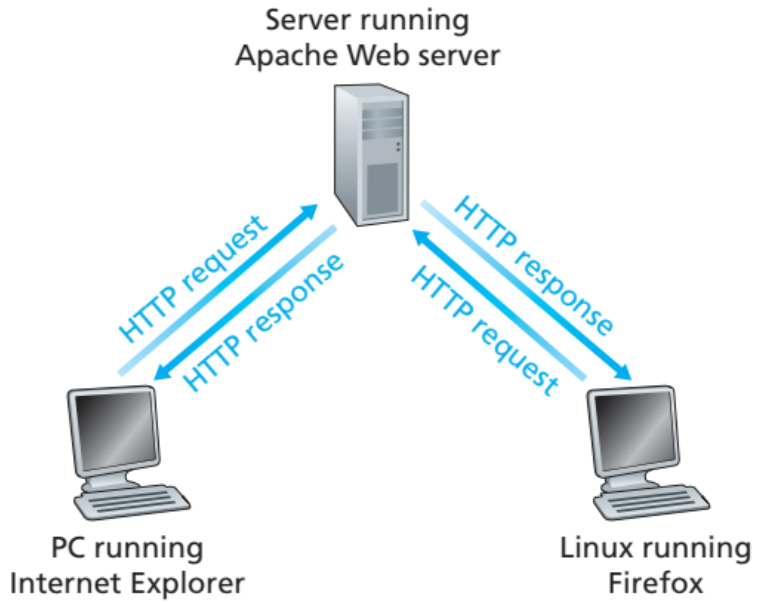
Application-layer protocol defines:

- The types of messages exchanged, for example, request messages and response messages
- The syntax of the various message types, such as the fields in the message and how the fields are delineated
- The semantics of the fields - meaning of the information in the fields
- Rules for determining when and how a process sends messages and responds to messages

Application-layer protocol is only one piece of a network application

Web and HTTP

- A web page is a document and consists of objects
- An object is nothing but a file such as HyperText Markup Language (HTML) file, an image file, applet or video clip.
- If a web page contains a basic html file and ten images, we say the web page contains 11 objects.
- HyperText Transfer Protocol (HTTP) is the web's application layer protocol
- HTTP uses client-server architecture with TCP.
- The client program and server program talk to each other by exchanging HTTP messages.



HTTP request-response behavior

Uniform Resource Locater

- An object should be addressable by a URL.
- Each URL consists of hostname and objects path name
- For example, http://www.iiits.ac.in/wp-content/uploads/2017/05/Untitled-design-15.png is url for an image.
- www.iiits.ac.in is host name
- wp-content/uploads/2017/05/Untitled-design-15.png is path name.
- Client side of HTTP is implemented in Web browser and server side is implemented in Web server.
- Examples: Apache and Microsoft Internet Information server.

- ✓ base HTML file plus objects
- ✓ base HTML file references the other objects in the page with the objects' URLs.

HTTP

- HTTP client initiates a connection with HTTP server (handshaking).
- Once the connection is established, client and server exchange messages through socket interface.
- Client sends an HTTP request and receives HTTP messages through its socket
- Server receives HTTP requests and sends HTTP responses through its socket interface.
- Client/server need not worry about packets (does not have any control) after sending through their socket.
- Server sends requested files without storing state information of client. Thus HTTP is a stateless protocol.

HTTP Connection

- Let us say, a web page has one html file and 10 images.
- How does client retrieve the web page?
- Nonpersistent and Persistent
- Nonpersistent: one TCP connection for each file
- Persistent: one TCP connection for all files

Nonpersistent Connection

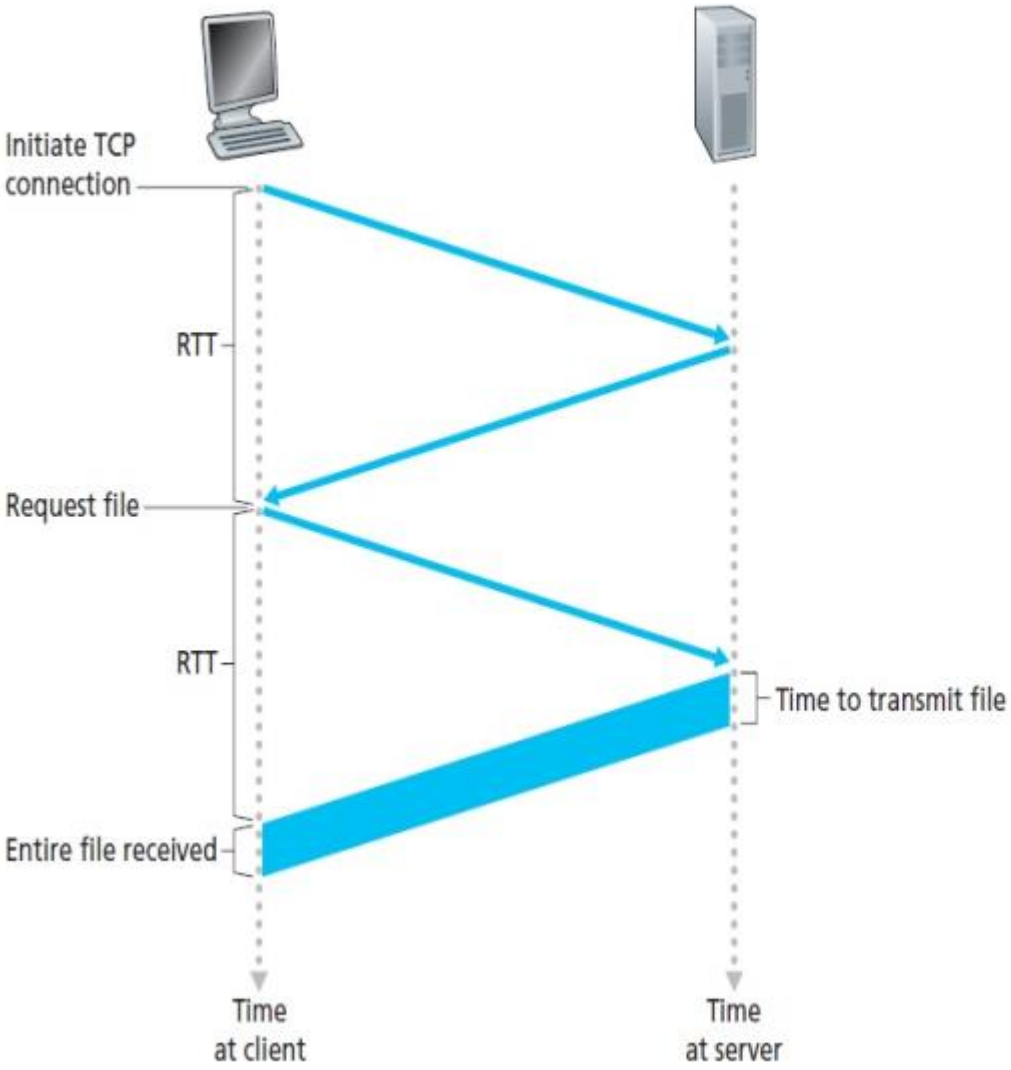
- For each file:
  - HTTP client initiates a TCP connection to the server on port number 80
  - Client sends its HTTP request and it includes the path name to the file
  - HTTP server receives the request and retrieves the file and sends the HTTP response to the client
  - HTTP server tells TCP to close the connection.
- TCP connections can be serial or parallel depending on browser's configuration

Example: Non-Persistent

- steps of transferring a Web page from server to client for the case of non-persistent connections.
- page consists of a base HTML file and 10 JPEG images → 11 objects reside on the same server.
- URL for the base HTML file is: http://www.someSchool.edu/someDepartment/home.index

1. The HTTP client process initiates a TCP connection to the server `www.someSchool.edu` on port number 80, which is the default port number for HTTP. Associated with the TCP connection, there will be a socket at the client and a socket at the server.
2. The HTTP client sends an HTTP request message to the server via its socket. The request message includes the path name `/someDepartment/home.index`. (We will discuss HTTP messages in some detail below.)
3. The HTTP server process receives the request message via its socket, retrieves the object `/someDepartment/home.index` from its storage (RAM or disk), encapsulates the object in an HTTP response message, and sends the response message to the client via its socket.
4. The HTTP server process tells TCP to close the TCP connection. (But TCP doesn't actually terminate the connection until it knows for sure that the client has received the response message intact.)
5. The HTTP client receives the response message. The TCP connection terminates. The message indicates that the encapsulated object is an HTML file. The client extracts the file from the response message, examines the HTML file, and finds references to the 10 JPEG objects.
6. The first four steps are then repeated for each of the referenced JPEG objects.

Round-Trip Time



Persistent Connection

- Server leaves the connection after sending the HTTP response
- Pipelining: A browser can request for files without waiting for the reception of pending requests.
- TCP closes after some idle period
- Default mode HTTP: Persistent connection with pipelining.

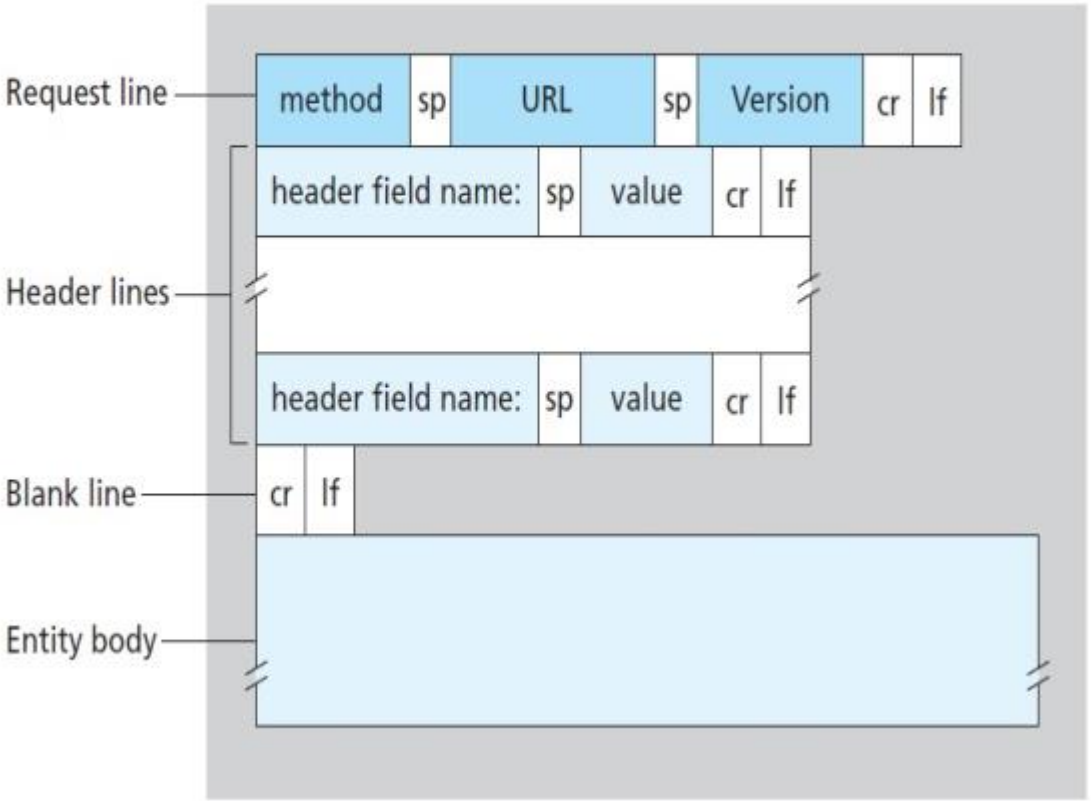
HTTP Request Format

- HTTP request message:

```
GET /somedir/page.html HTTP/1.1
Host: www.iitm.ac.in
Connection: close
User-agent: Mozilla/4.0
Accept-language: En
```

- Methods: GET, PUT, POST, HEAD, DELETE

HTTP Request

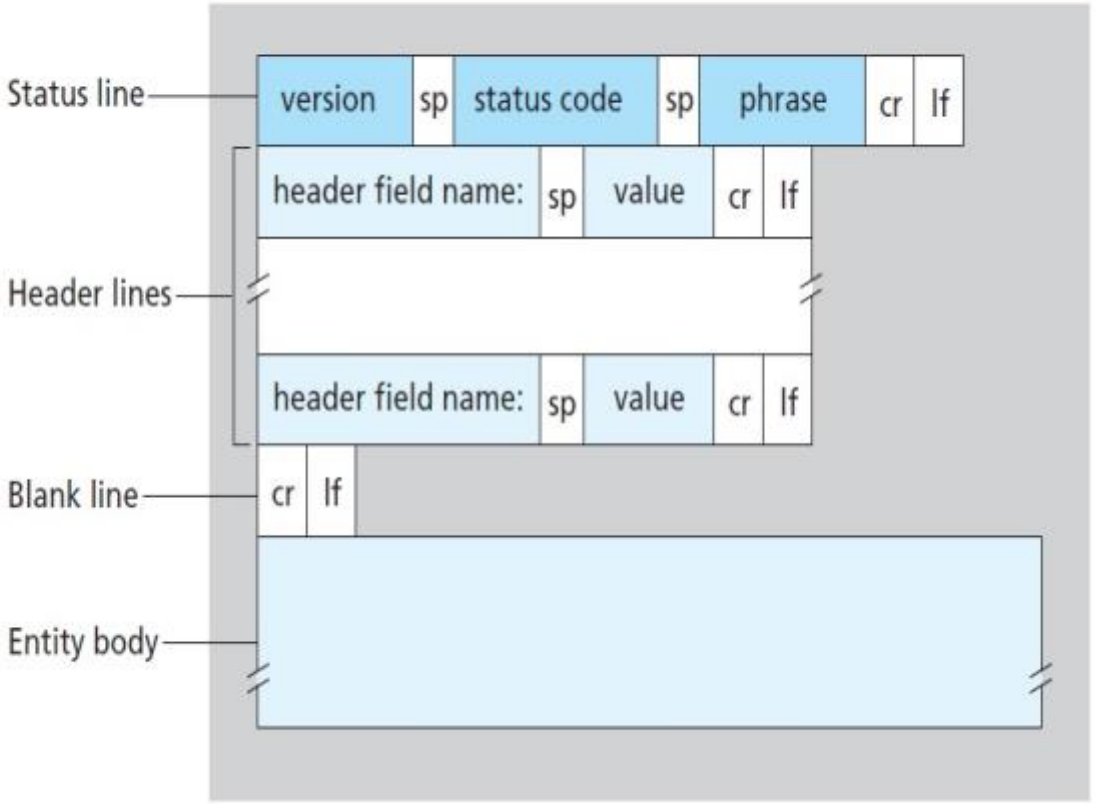


HTTP Response

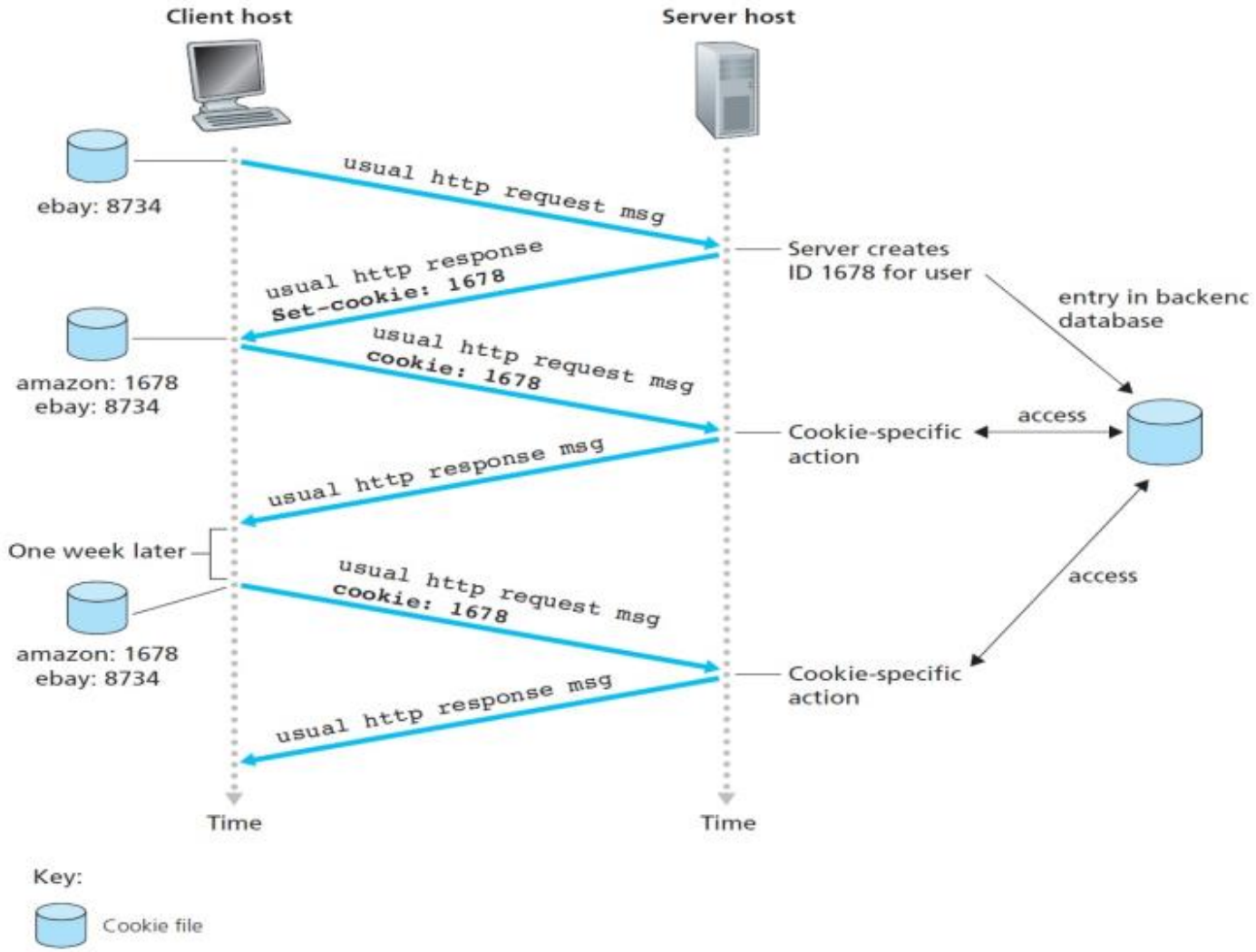
- HTTP response message:

  HTTP/1.1 200 OK
  Connection: close
  Date: Sat, 07 Jul 2007 12:00:15 GMT
  Server: Apache/1.3.0 (Unix)
  Last-Modified: Sun, 6 May 2007 09:23:24 GMT
  Content-length: 6821
  Content-Type: text/html
  (data data ... data)
- 200 OK
- 301 Moved Permanently
- 404 Not Found

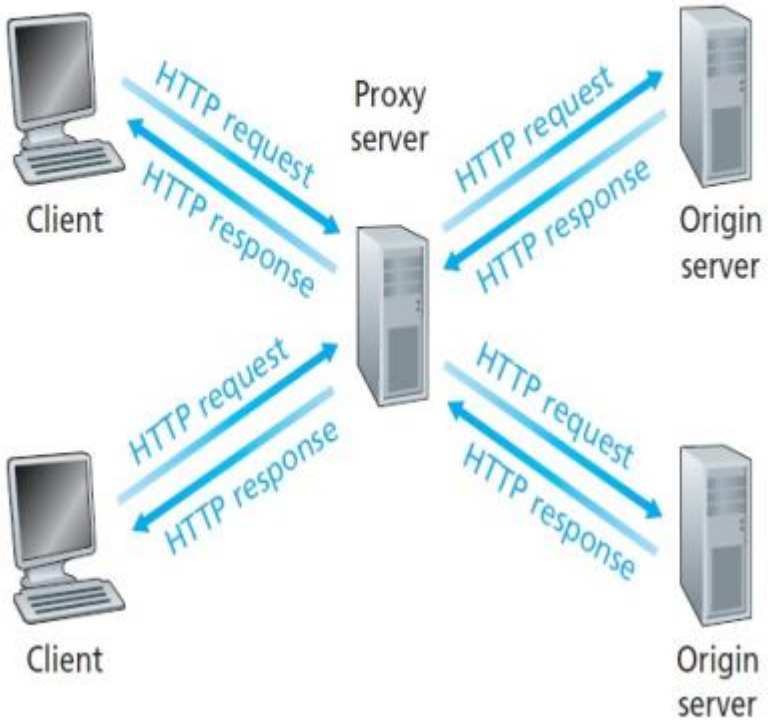
HTTP Response



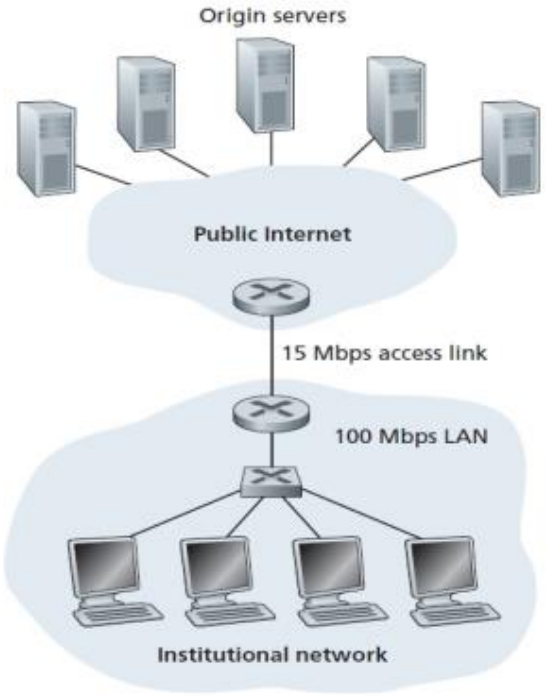
Cookies


Client host
Server host
ebay: 8734
usual http request msg
usual http response
Set-cookie: 1678
Server creates
ID 1678 for user
entry in backend
database
amazon: 1678
ebay: 8734
usual http request msg
cookie: 1678
Cookie-specific
action
access
usual http response msg
One week later
amazon: 1678
ebay: 8734
usual http request msg
cookie: 1678
access
Cookie-specific
action
usual http response msg
Time
Time
Key:
Cookie file

Web Caching


Proxy
server
HTTP request
HTTP response
HTTP request
HTTP response
Client
Origin
server
HTTP request
HTTP response
HTTP request
HTTP response
Client
Origin
server

Problem



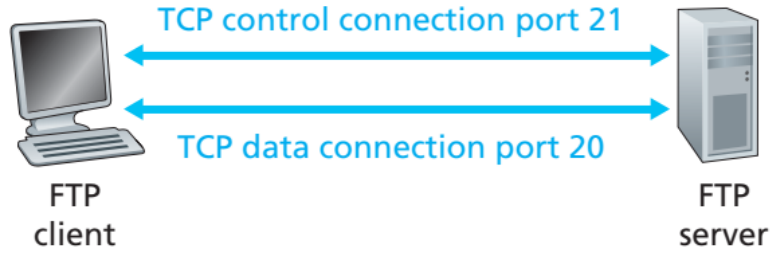
- Average object size is 1Mbits
- Average request rate 15 objects per sec.
- Average response time from internet is 2 sec.

Toatal Resposne Time

- Traffic intensity on the LAN
- 0.15
- Traffic intensity on the access link
- 1
- Suppose the access link is upgraded to 100Mbps, find traffic intensity on the access link
- Find the average resposne time
- Expensive solution

File Transfer Protocol

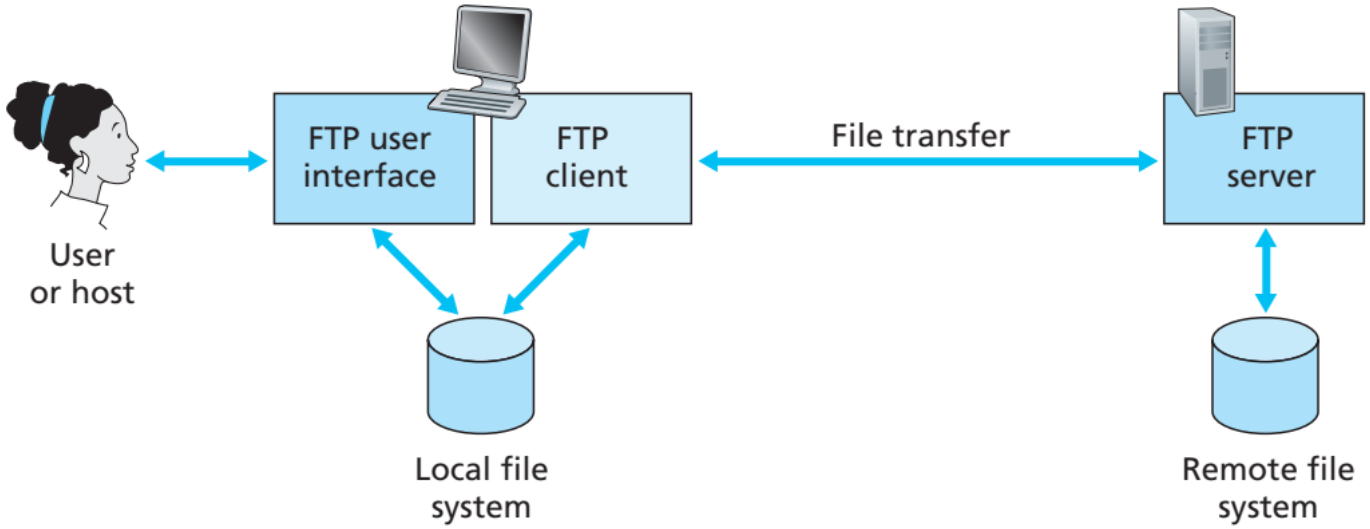
- Similar to HTTP: client-server architecture, transmission control protocol
- Two parallel TCP connections to transfer a file: TCP control connection and TCP data connection
- Control information:
  - User identification
  - Change remote directory
  - Commands to put and get files
- FTP is said to control information out-of-band where as HTTP is said to control information in-band.



Control and data connections

FTP

- Commands:
  - USER username
  - PASS password
  - LIST
  - RETR filename
  - STOR filename
- Replies:
  - 331 username OK, password required
  - 125 data connection already open; transfer starting
  - 425 can not open data connection
  - 452 error writing file



Electronic Mail

- Asynchronous communication medium
- Major components of e-mail system:
  - User agent: allows users to read, forward, save and compose messages
  - Mail server
  - SMTP
- Examples of user agents: Microsoft Outlook, Mozilla Thunderbird, Apple Mail

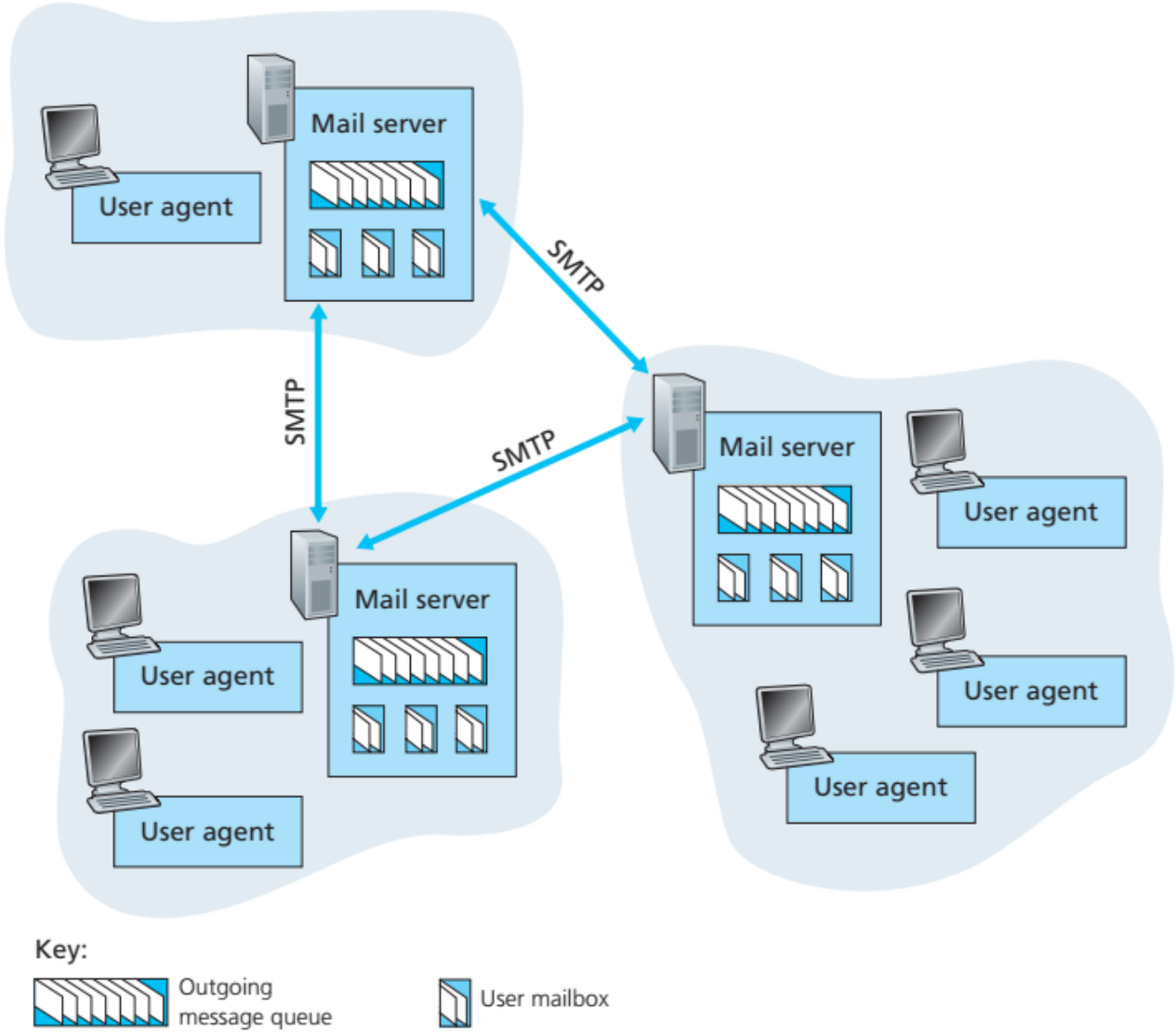


Figure 2.16 ♦ A high-level view of the Internet e-mail system

SMTP

- User agent sends message to user's mail server.
- SMTP transfers message from user's mail server to recipient's mail server.
- Client side of SMTP is running on sender's mail server and server side of SMTP is running on recipient's mail server.
- Recipient's mail server delivers the message in recipient's mail box.

SMTP Sequence of Operations

- Alice composes message using her user agent. Provides Bob's mail address and instructs to send the message.
- User agent sends the message to her mail server and message waits in the queue of the server.
- SMTP client sees the message in the mail server and it opens a TCP connection to an SMTP server running on Bob's mail server.
- SMTP transfers the message from client to server.
- SMTP server receives the message. Bob's mail server places the message in Bob's mail box.
- Bob invokes his user agent to read the message.

SMTP Sequence of Operations

- If recipient's mail server is down, SMTP client reattempts to send the message (say for every 30 minutes)
- If the delivery is not successful after some duration, it will be notified to the sender and message will be dropped.

SMTP:

- restricts the body of all mail messages to simple 7-bit ASCII
- Valid when transmission capacity was scarce and no one was e-mailing large attachments or large image, audio, or video files.
- message does not get placed in some intermediate mail server

Client-Server Conversation

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250 Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr ... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

Message Formats

- Header lines similar to those in HTTP messages
- Header must have From:, To:
- Optional header lines include Subject:

Comparison with HTTP

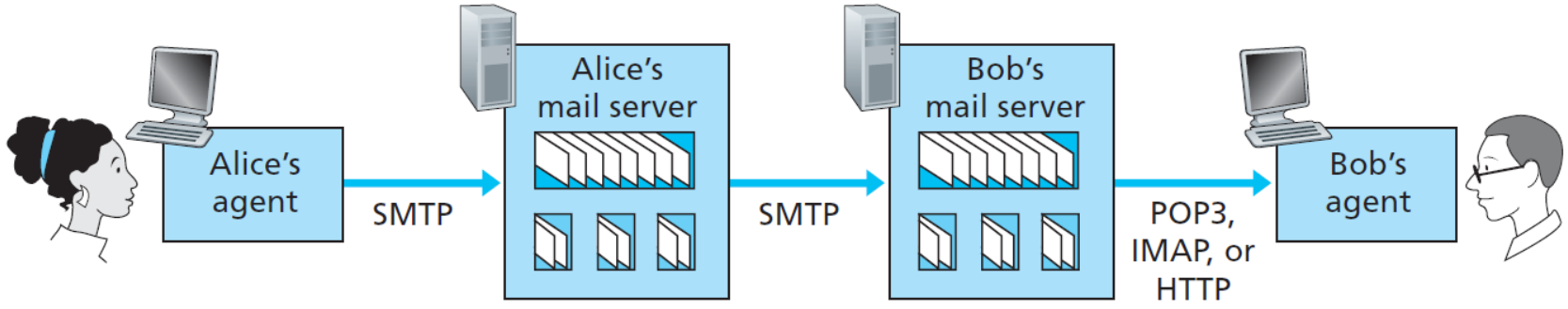
- HTTP is a pull protocol
- SMTP is push protocol
- SMTP requires each message to be 7-bit ASCII format. HTTP does not have this restriction
- HTTP encapsulates each object in its own HTTP response message. Internet mail places all of its objects into one message.

Mail Access Protocols

- In early days of internet, Bob reads mail by logging onto mail server and executing a mail reader on that host
- Client-server architecture
- Reads e-mail by running a client on the user's end system
- Mail access protocol transfers message from Bob's mail server to his local PC.
- Popular mail access protocols: Post Office Protocol - version 3 (POP3), Internet Mail Access Protocol (IMAP) and HTTP

POP3

- Begins when a user agent opens a TCP connection with mail server on port 110.
- POP3 progresses in three phases:
  - Authorization
  - Transaction
  - Update
- Authorization: user <username> and pass <password>
- Transaction: user agent sends commands and server responds with +OK and -ERR



POP3 Transaction

- Two modes:
  - download and delete
  - download and keep
- Download and delete:

```
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: (blah blah ...
S: ..................
S: ..........blah)
S: .
C: dele 1
C: retr 2
S: (blah blah ...
S: ..................
S: ..........blah)
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

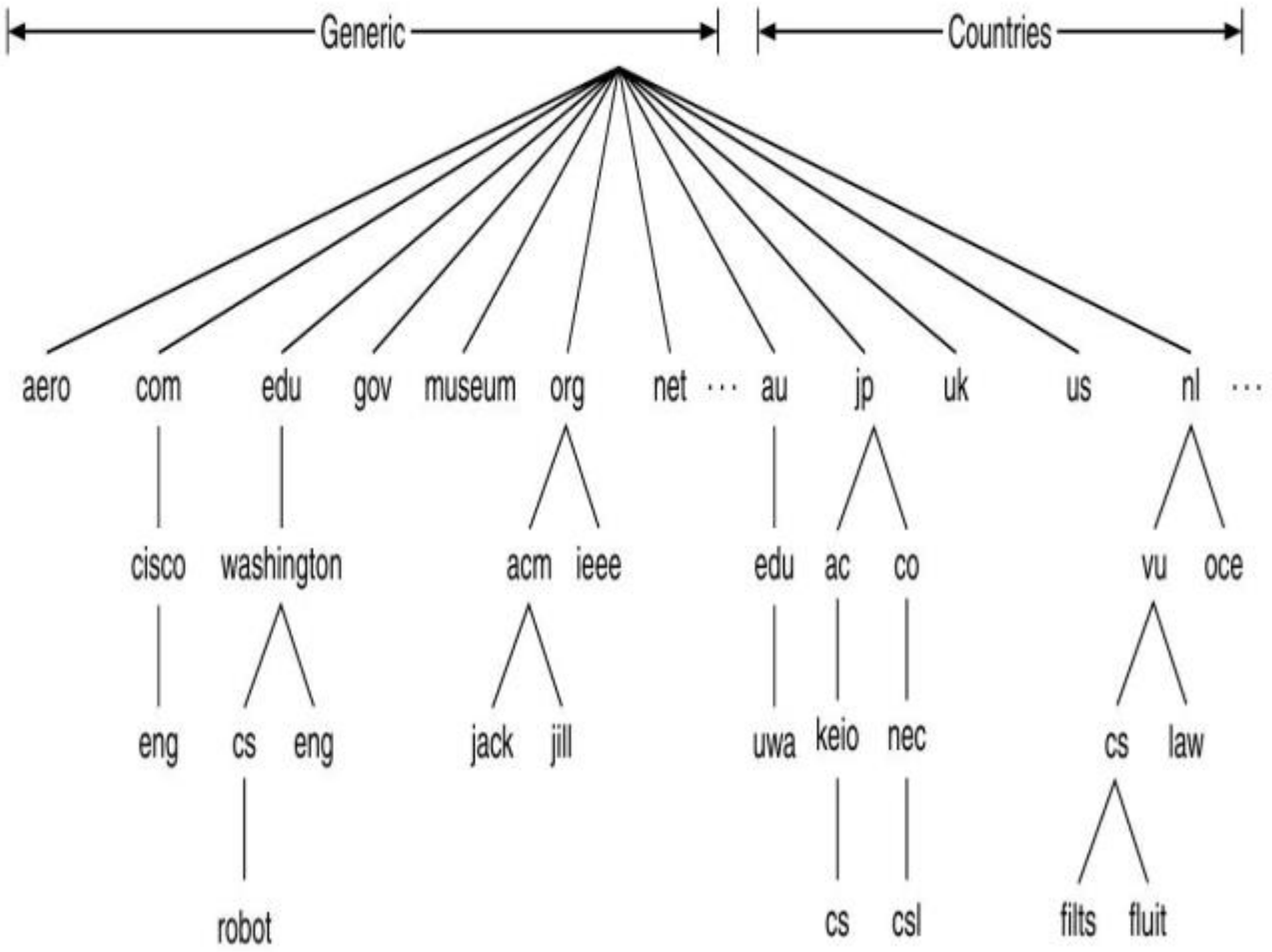
IMAP and HTTP

- IMAP associates each message with a folder
- Provides commands to allow users to create folder and move messages across folders
- Provides commands to search for a message
- Maintains user state information across IMAP sessions
- Components of messages can be retrieved
- HTTP:
  - e-mail access through web browser
  - web browser communicates to the mail server via HTTP

What is a Domain Name

- Consider www.iiits.in
- Domain: in
- What is the domain name of www.iitm.ac.in
- Domain: in, subdomain: ac
- **250** top-level domains; examples: com, org, edu.

Domain Name Space



Examples of Domains

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No

Who Manages Domains

- ICANN: Internet Corporation for Assigned Names and Numbers
- Registrars of ICANN check for uniqueness
- Domain names can be **absolute** or **relative**
- Absolute domain names end with **.**
- Relative domain names have to be interpreted based on the context

Domain Name Server: The Directory

- We identify hosts by hostnames. For example, www.amazon.in
- For a network, there is a very little information about the host. Network needs IP address for processing
- Domain name servers (DNS) provides the necessary mapping from hostname to IP address
- DNS is an application layer protocol used by other applications
- Client-Server architecture; uses UDP at its transport layer

DNS Example:

1. The same user machine runs the client side of the DNS application.
2. The browser extracts the hostname, `www.someschool.edu`, from the URL and passes the hostname to the client side of the DNS application.
3. The DNS client sends a query containing the hostname to a DNS server.
4. The DNS client eventually receives a reply, which includes the IP address for the hostname.
5. Once the browser receives the IP address from DNS, it can initiate a TCP connection to the HTTP server process located at port 80 at that IP address.

DNS adds an additional delay—sometimes substantial—to the Internet applications that use it

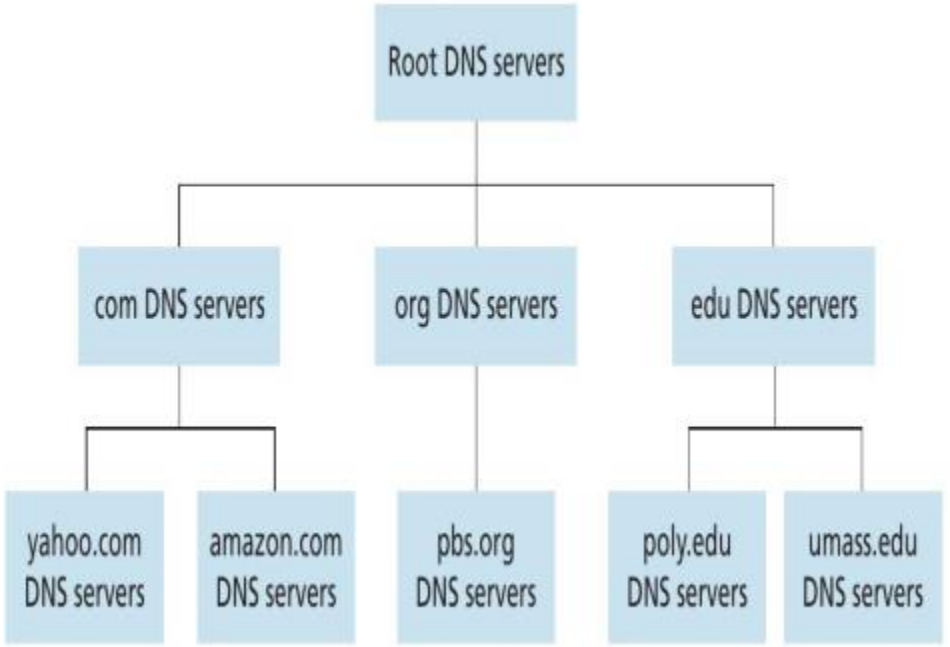
Aliases

- We typically memorize alias hostnames but the actual hostnames are very complicated
- The canonical hostnames are not mnemonic. Canonical: *according to the rules*
- Example: *www.timesofindia.com* is the alias but the actual host name or canonical name is *timesofindia.indiatims.com*
- Different canonical names might have the same alias
- Many hosts can be installed within a domain or subdomain. Example: *www.ee.iitm.ac.in*, *www.cse.iitm.ac.in*, *smail.iitm.ac.in*

Services of DNS

- The Internet's directory service
- Host aliasing
- Mail Server aliasing
- Load distribution, example: *IRCTC*

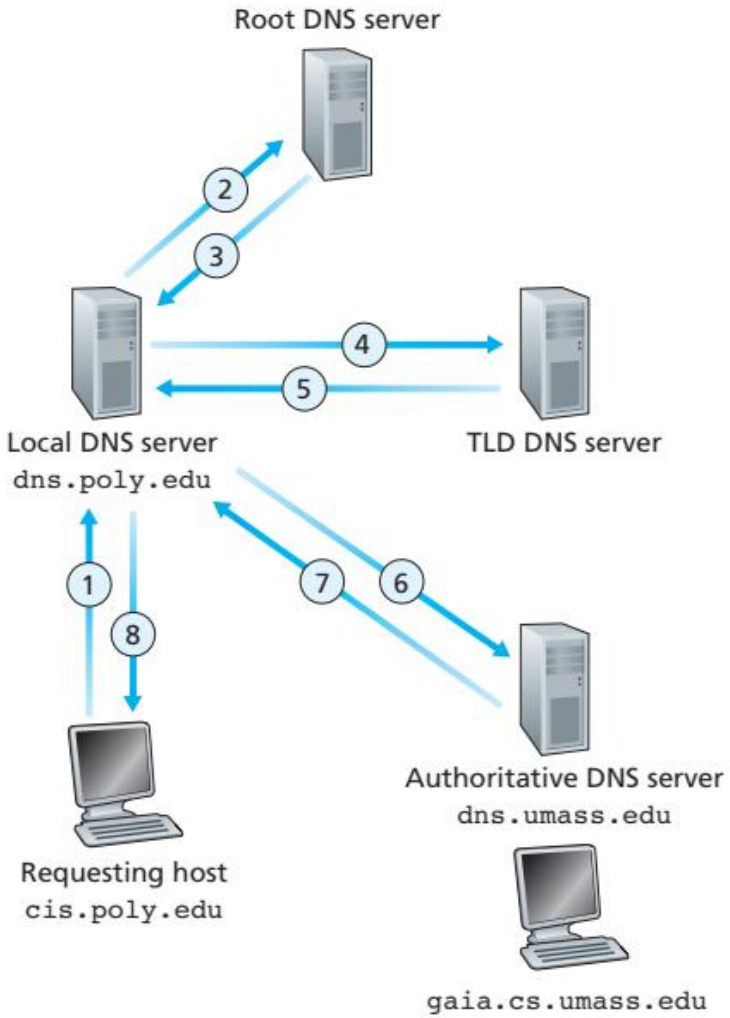
Hierarchy of DNS

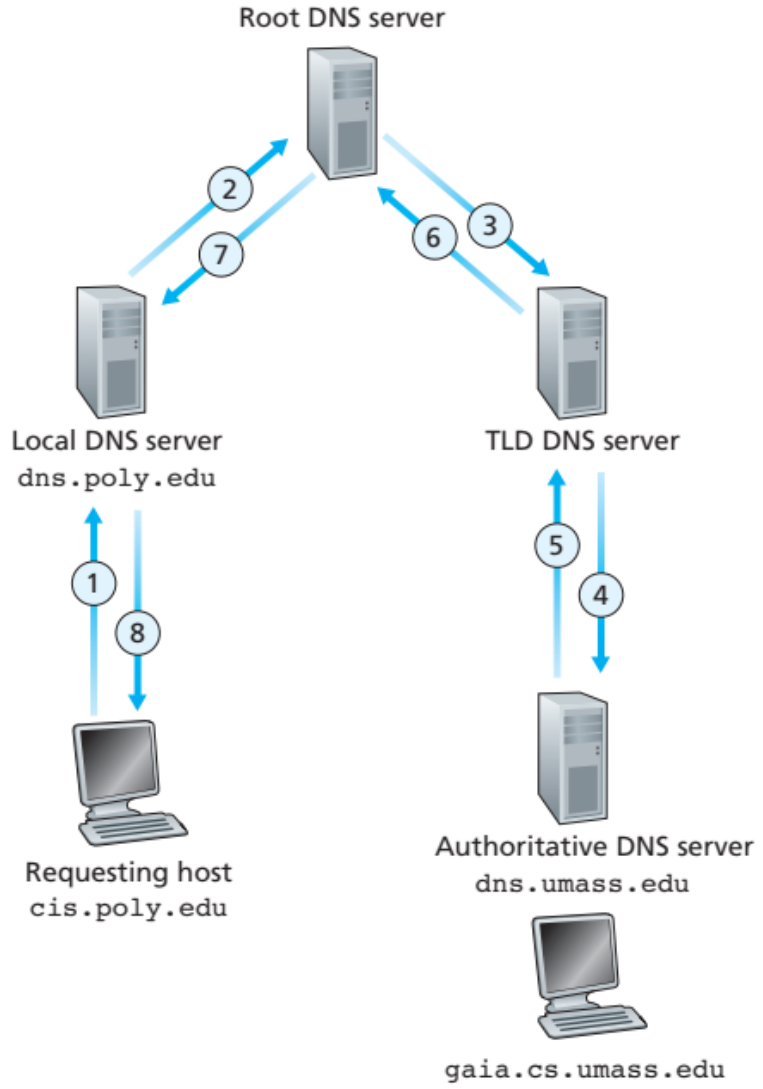


Problems of Single DNS:

- A single point of failure
- Traffic volume
- Distant centralized database
- Maintenance

How does DNS Work: Recursive and Iterative Query





Local DNS

- An ISP can provide local DNS
- Host will query the local DNS and that takes it forward to the root DNS
- Cache DNS replies

DNS Resource Records:

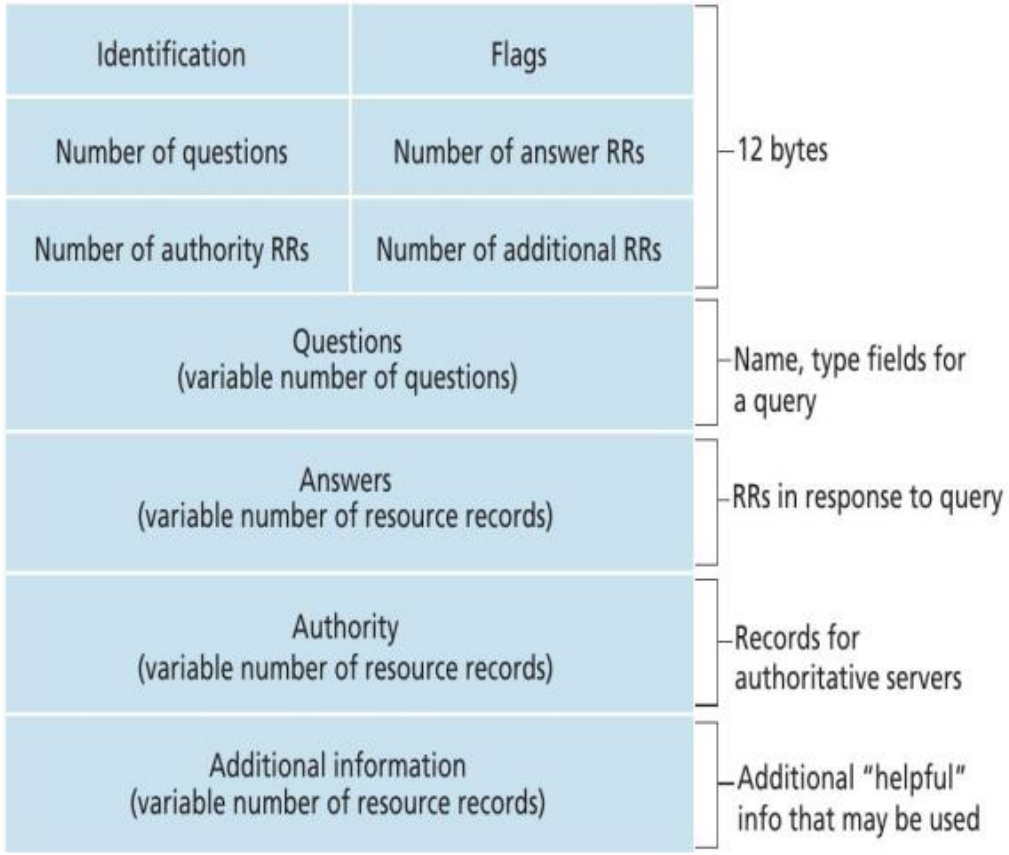
- DNS distributed database store resource records
- Resource Record is four tuple: (Name, Value, Type, TTL)
- TTL: Time-to-Live
- The interpretation of Name and Value files change based on Type

Types in RR

- Type = A: *Name* is a hostname and *Value* is the IP address of the host
- Type = NS: *Name* is a domain and *Value* is the hostname of the authoritative DNS server
- Type = CNAME: *Name* is an alias and *Value* is the canonical hostname of the alias.
- Type = MX: *Name* is an alias hostname and *Value* is the canonical hostname of a mail server of the alias.

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

DNS Message Fromat



Flags:

- 1-bit flag to indicate its a query/reply
- 1-bit recursion flag is set if the DNS supports recursion

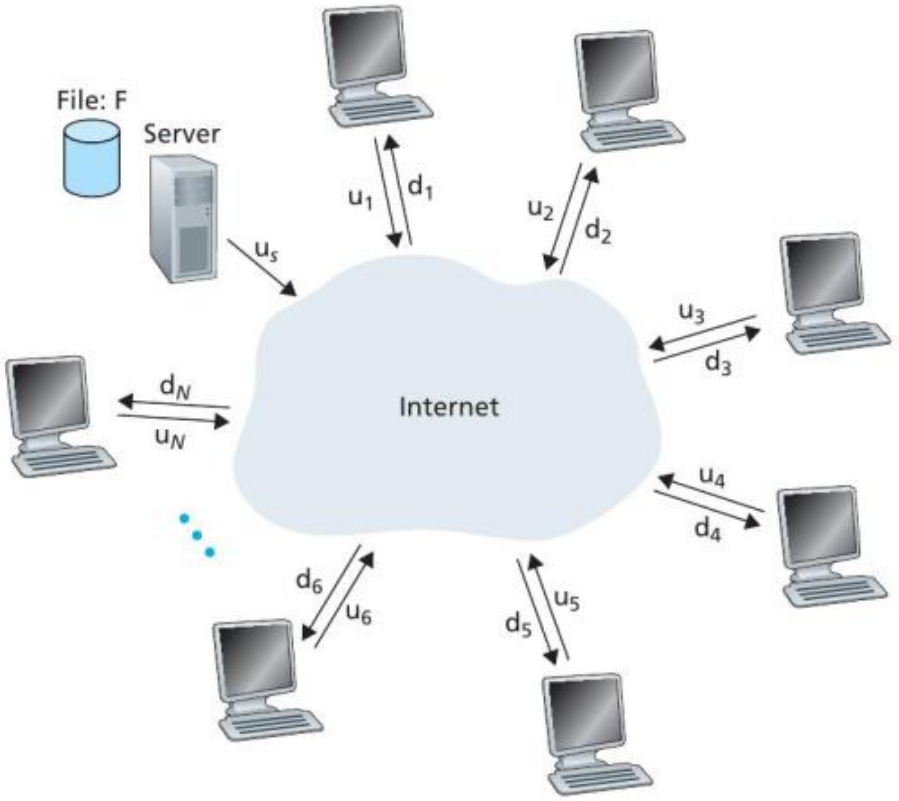
Applications of Peer-to-Peer Architecture

- File distribution: application that transfers a file from a single source to multiple peers.
- Database distributed over a large community of peers.
- Internet telephony : Skype.

File Distribution:

- Each peer can redistribute any portion of the file to any other peer
- Popular file distribution protocol : BitTorrent,developed by Bram Cohen
- Scalability

Scalability



- N peers
- Distribution time: the time required to distribute a file to all peers.

Assumptions

- Internet has abundant bandwidth and all bottlenecks are in the network access
- All the server and client bandwidth is available for file distribution

Distribution Time for Client-Server Architecture

- Let D_{cs} denote the distribution time for client-server architecture for a file size of F bits
- The server has to transmit a total of NF bits at an upload rate of $u_s bps$.
- Minimum time required for distribution is $\frac{NF}{u_s}$ seconds
- Let $d_{min} = \min\{d_1, \ldots, d_N\}$
- Minimum distribution time is $\frac{F}{d_{min}}$ seconds
- Thus,

$$D_{cs} \geq \max\left\{\frac{NF}{u_s}, \frac{F}{d_{min}}\right\}$$

- Show that

$$D_{cs} = \max\left\{\frac{NF}{u_s}, \frac{F}{d_{min}}\right\}$$

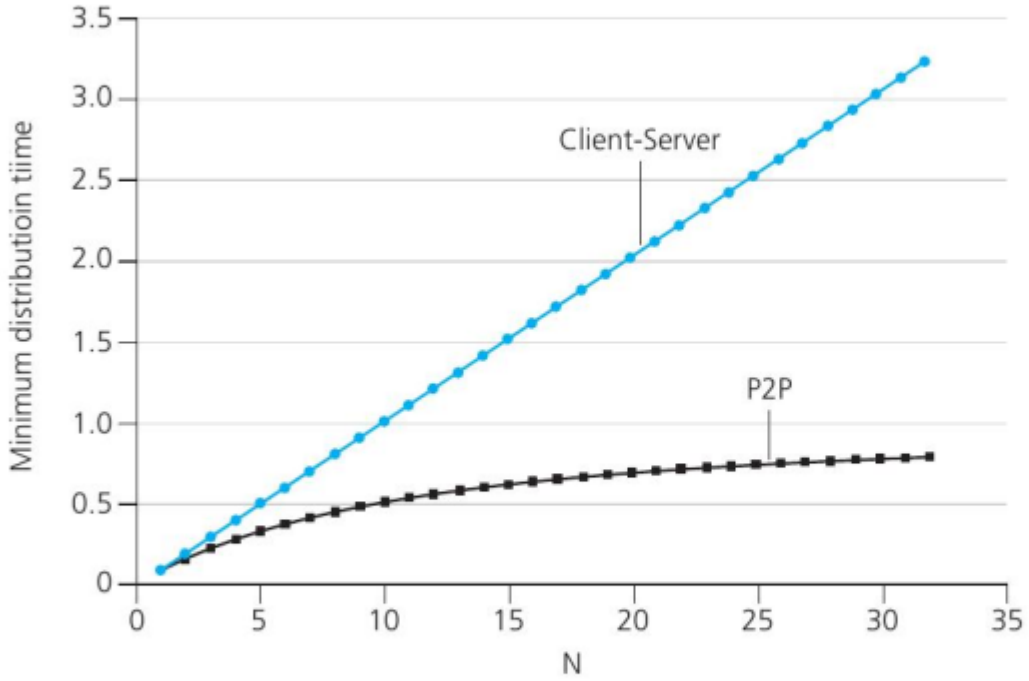
Distribution Time for P2P Architecture

- The server has to send each bit of the file at least once: Minimum distribution time is at least $\frac{F}{u_s}$ seconds
- The peer with lowest download rate can not obtain F bits in less than $\frac{F}{d_{min}}$ seconds
- The total upload rate $u_{total} = u_s + u_1 + \cdots + u_N$. The system must deliver F bits to each of the N peers: Minimum distribution time is $\frac{NF}{u_{total}}$
- Thus, minimum distribution time D_{P2P} is at least

$$\max\{\frac{F}{u_s}, \frac{F}{d_{min}}, \frac{NF}{u_{total}}\}$$

- Assumption: each peer can redistribute a bit as soon as it receives the bit.
- There is a scheme that actually achieves this lower bound.

Distribution Time for P2P Architecture



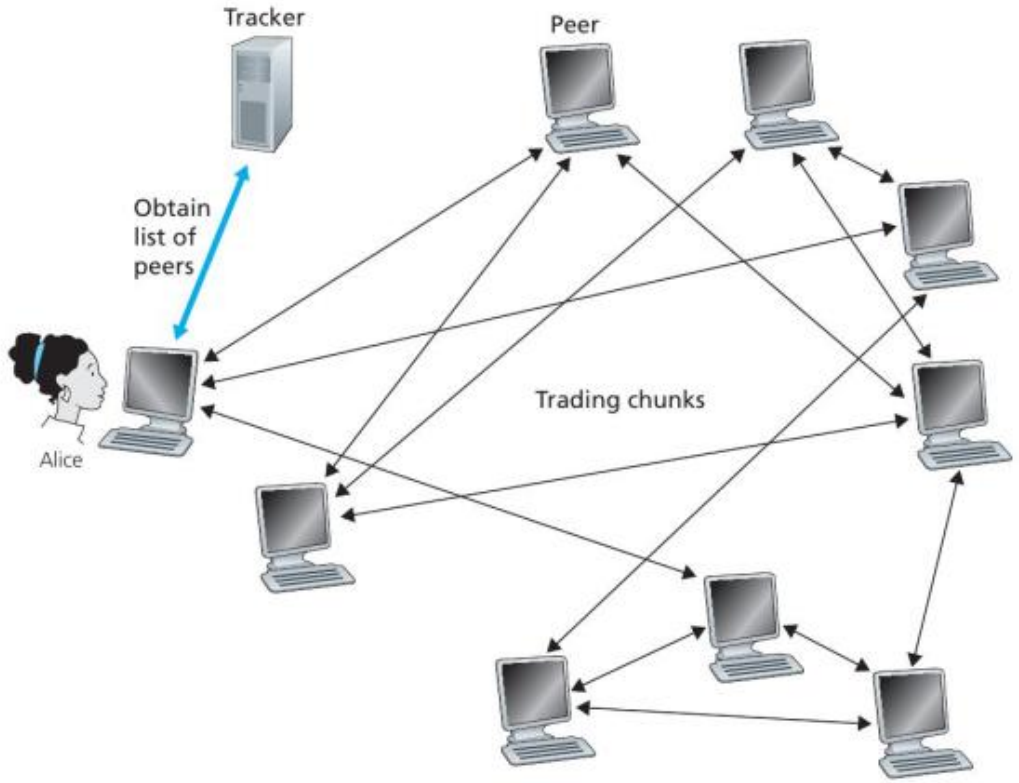
- All peers upload at a rate of u bps.
- $\frac{F}{u} = 1$ hour, $u_s = 10u$ and $d_{min} \geq u_s$.

Bit Torrent

- Collection of peers participating in the distribution of a file is called a torrent
- Peers in a torrent download equal-size chunks of the file (typically 256 KBytes)
- A peer accumulates more and more chunks over time
- Once a peer has acquired complete file, it may leave the torrent or continue to participate in the torrent
- Peers may leave torrents with subsets of chunks

Bit Torrent

- Each torrent has a node called tracker.
- When a peer joins the torrent, it registers with the tracker
- Each peer in the torrent periodically updates the tracker about its presence.



Bit Torrent

- Alice receives a subset of participating peers in the torrent
- She establishes TCP connection with some of the peers and we call them as neighboring peers of Alice
- Neighboring peers may vary over time
- Each peer will have some subset of chunks from the file, with different peers having different subsets
- Alice maintains a list of chunks that her neighbors have.

Bit Torrent

- Alice will issue requests for chunks she currently does not have
- Which chunks should be requested first?

- Rarest first: finds the chunks that are rarest among her neighbors

  - Alice will issue requests for chunks she currently does not have
  - To which of her neighbors should she send requested chunks?
  - Tit-for-tat

Tit-for-tat

- Alice gives priority to the neighbors that are currently supplying her data at the highest rate
- Typically four neighbors are chosen. These peers are said to be unchoked
- Every 30 seconds, she also picks one additional neighbor at random and sends it chunks. Let it be Bob.
- Bob is said to be optimistically unchoked.
- In due course of time, Alice, may become one of the top uploaders in which case Bob could start sending data to Alice.

Distributed Hash Tables (DHT)

- Huge database to be stored among number of peers in a distributed way
- Database is consists of (key, value) pairs. For Example, (PAN No., Aadhar No.), (Content Name, IP), etc.
- Peers query the database by supplying the key and database replies the matching pairs to the querying peer
- How to store database among the peers

DHT

- Assign an identifier to each peer.
- An identifier is an integer in $[0, 2^n - 1]$ for some fixed n
- (key, value) pairs are also identified by integers using hash functions
- Hash function is available to all peers.

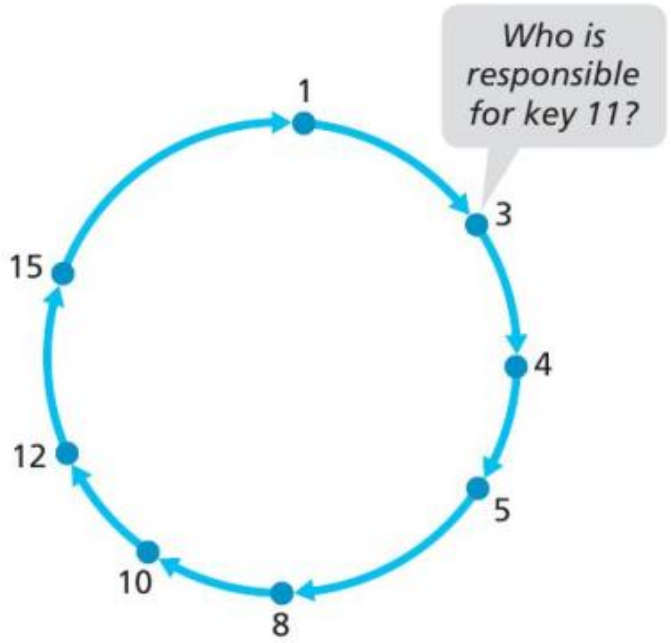
The index for a specific string will be equal to sum of ASCII values of characters multiplied by their respective order in the string after which it is modulo with 2069 (prime number).

String	Hash function	Index
abcdef	(97*1* + *98*2 + 99*3* + *100*4 + 101*5* + *102*6)%2069	38
bcdefa	(98*1* + *99*2 + 100*3* + *101*4 + 102*5* + *97*6)%2069	23
cdefab	(99*1* + *100*2 + 101*3* + *102*4 + 97*5* + *98*6)%2069	14
defabc	(100*1* + *101*2 + 102*3* + *97*4 + 98*5* + *99*6)%2069	11

Storing in DHT

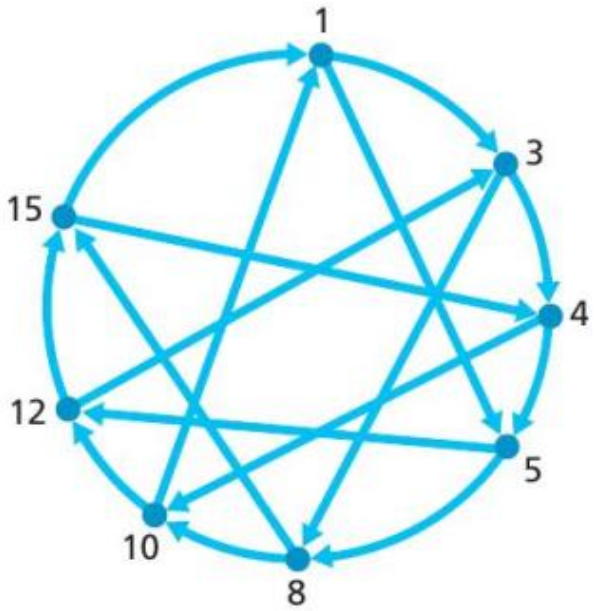
- Define a rule for assigning keys to peers
- Closest to the key:
- For example, $n = 4$, with eight peers: 1,3,4,5,8,10,12 and 15. Store (11, 0123-4567-8910) in one of the eight peers
- By closest convention, peer 12 is the immediate successor for key 11. Store in peer 12.
- If the key is larger than all the peer identifiers, we use modulo-2^n convention.

Circular DHT



- Each peer is aware of only its immediate predecessor and successor
- N messages at most

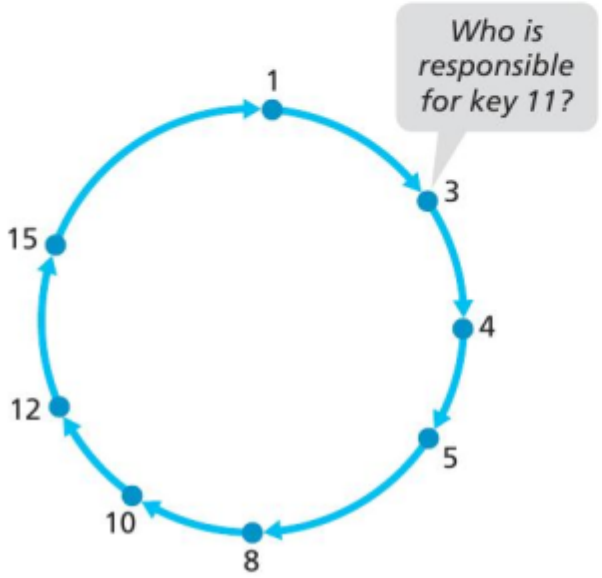
Shortcut



- Number of shortcuts are relatively small in number
- How many shortcut neighbors and which peers should be these shortcut neighbors? Research problem: $O(\log(N))$

Peer Churn

- Peers can come and go without warning
- Peers keep track to two immediate predecessor and successors.
- When a peer abruptly leaves, its predecessor and successor learn that a peer has left and updates the list of its predecessor and successor.



Computer Communication Networks

Transport Layer

Dr. Raja Vara Prasad

Assistant Professor

IIIT Sri City

Transport Layer

Transport Layer

how two entities can communicate reliably over a medium that may lose and corrupt data ?

controlling the transmission rate of transport-layer entities in order to avoid

Or

recover from, congestion within the network.

Transport Layer Services

- **logical communication**
- Transport-layer **segments**
- Transport-layer protocol provides logical communication between *processes* running on different hosts
- a network-layer protocol provides logical communication between *hosts*
- services that a transport protocol can provide are often constrained by the service model of the underlying network-layer protocol
- a transport protocol can offer reliable data transfer service to an application even when the underlying network protocol is unreliable
- can use encryption

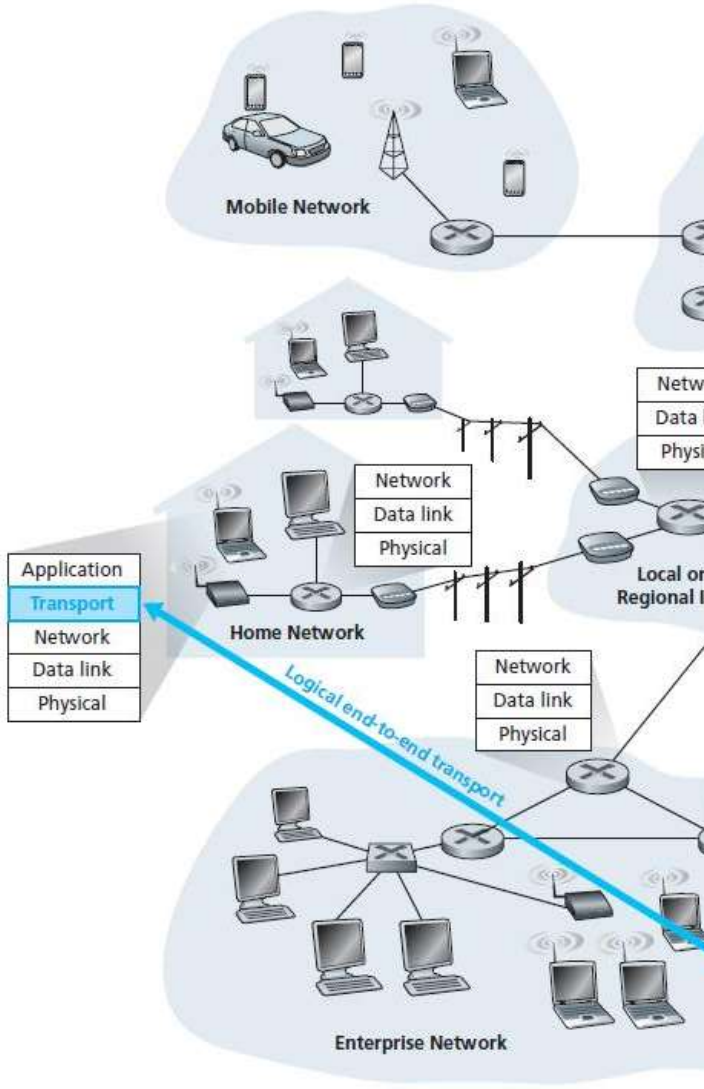


Figure 3.1 ♦ The transport layer provides logical rather than physi communication between application processes

Transport Layer in the Internet

- Internet Protocol. IP provides logical communication between hosts.
- IP service model is a **best-effort delivery service**
- "best effort" to deliver segments between communicating hosts → *makes no guarantees.*
- not guarantee segment delivery
- it does not guarantee orderly delivery of segments
- does not guarantee the integrity of the data in the segments

UDP Services:

process-to-process data delivery and error checking

TCP:

- reliable data transfer
- correct and in order → using flow control, sequence numbers, acknowledgments, and timers
- **congestion control**

Multiplexing and Demultiplexing

- host-to-host delivery service provided by the network layer
- process-to-process delivery service for applications running on the hosts – Transport Layer

- a process can have one or more **sockets**
- transport layer in the receiving host does not deliver data directly to a process → to an intermediary
- more than one socket in the receiving host → each socket → unique identifier
- Each transport-layer segment has a set of fields

Demultiplexing:

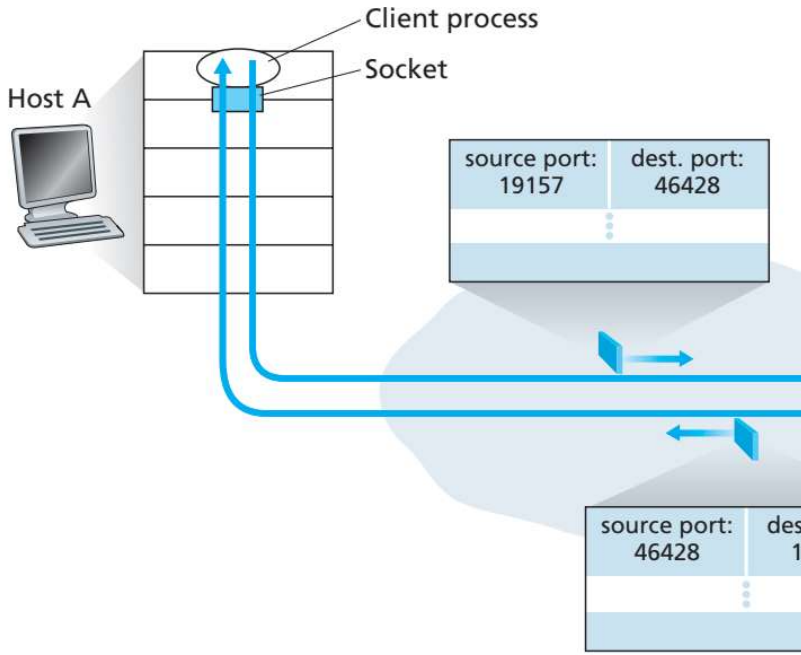
- receiving end → the transport layer examines these fields to identify the receiving socket
- directs the segment to that socket
- **Multiplexing**
  gathering data chunks at the source host from different sockets
- encapsulating each data chunk with header information to create segments
- passing the segments to the network layer is called

Connectionless Multiplexing and Demultiplexing

UDP socket:

- transport layer assigns a port number in the range 1024 to 65535 that is currently not being used by any other UDP port in the host

  Ex: A process in Host A, with UDP port 19157 → to send a chunk of application data to a process with UDP port 46428 in Host B.
- UDP socket: identified by a two-tuple → a destination IP address and a destination port number



if two UDP segments have different source IP addresses and/or source port numbers, but have the same *destination* IP address and *destination* port number ?

Connection Oriented Multiplexing and Demultiplexing

TCP socket:

- TCP socket is identified by a four-tuple
  source IP , source port number, destination IP, destination port number
- host uses all four values to direct the segment to the appropriate socket

  server host may support many simultaneous TCP connection sockets, with
  each socket attached to a process, and with each socket identified by its own four tuple.

Web Servers and TCP:

---all segments will have destination port 80.

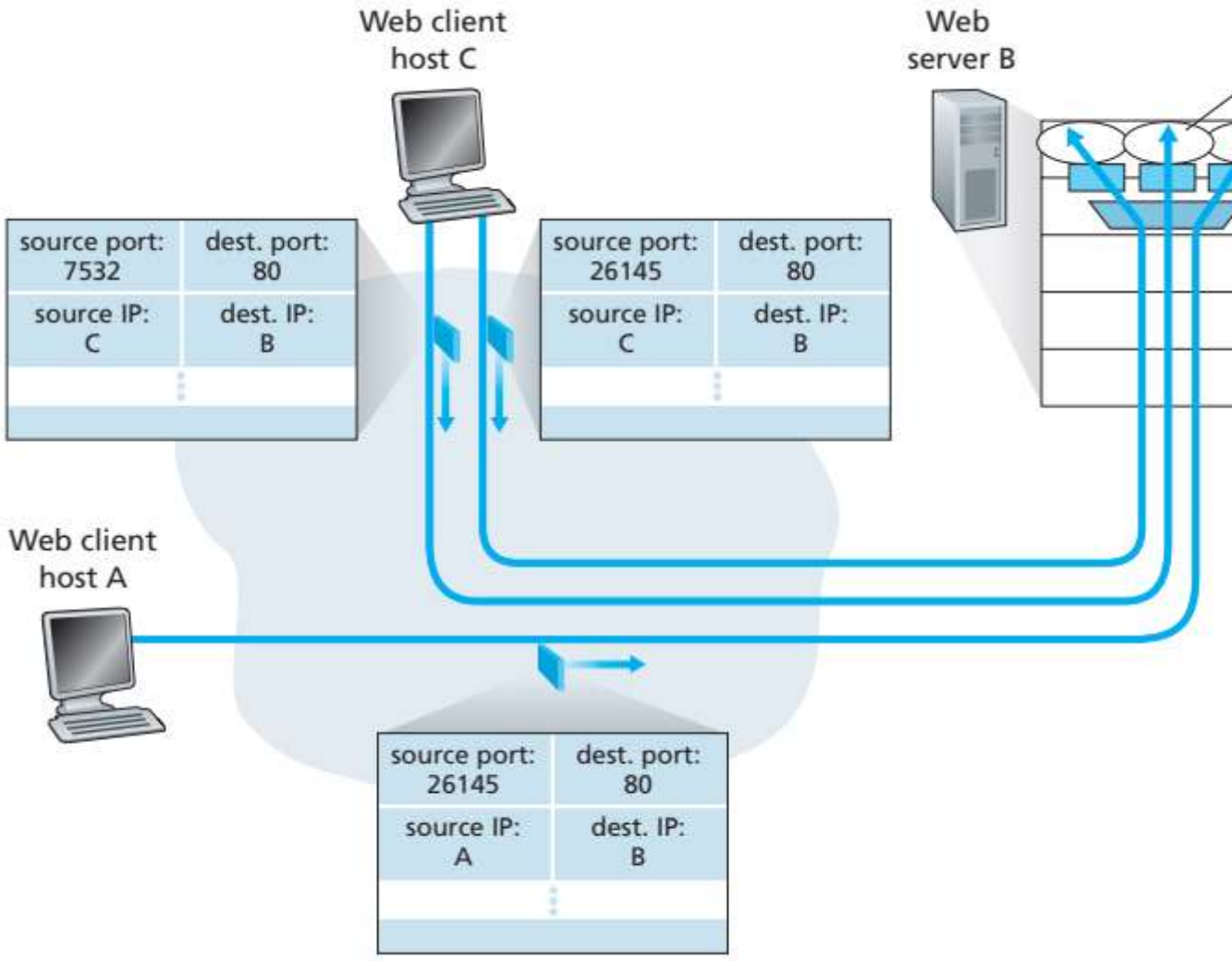
---Web servers often use only one process, and create a new thread with a new connection socket for ea
client connection .

---client and server using persistent HTTP → same server socket

---non-persistent HTTP → a new TCP connection is created and closed for every request/respon

---frequent creating and closing of sockets --- severely impact the performance of a busy Web se

Connection Oriented Multiplexing and Demultiplexing



Connectionless - UDP

- UDP → no handshaking between sending and receiving transport-layer →UDP is said to be *connectionless*
  Example: DNS → a query → DNS query message and passes the message to UDP

- many applications are better suited for UDP for the following reasons:
- ***Finer application-level control over what data is sent, and when***
  →TCP will also continue to resend a segment until the receipt of the segment has been acknowledge destination, regardless of how long reliable delivery takes → real-time applications
- ***No connection establishment***
- ***No connection state*** **: Connection state** includes receive and send buffers, congestion-control paran and sequence and acknowledgment number parameters
  "can typically support many more active clients when the application runs over UDP rather than TC
- ***Small packet header overhead*** : TCP segment has 20 bytes of header : UDP: 8 bytes

Connectionless - UDP

- UDP is used for RIP routing table updates
- carry network management data

Multimedia applications, such as Internet phone, real-time video conferencing, and streaming of stored audio and video.

- Internet phone and video conferencing, react very poorly to TCP's congestion control
- When packet loss rates are low and some organizations blocking UDP traffic for security reasons TCP becomes an increasingly attractive protocol for streaming media transport.
- lack of congestion control in UDP can result in high loss rates between a UDP sender and receiver, and the crowding out of TCP sessions

Application	Application-Layer Protocol	U Pr
Electronic mail	SMTP	TC
Remote terminal access	Telnet	TC
Web	HTTP	TC
File transfer	FTP	TC
Remote file server	NFS	Ty
Streaming multimedia	typically proprietary	UI
Internet telephony	typically proprietary	UI
Network management	SNMP	Ty
Routing protocol	RIP	Ty
Name translation	DNS	Ty