COMPUTER NETWORKS(21CS52)

- Continuous Internal Evaluation: Three Unit Tests each of 20 Marks (duration 01 hour)
- 1. First test at the end of 5th week of the semester
- 2. Second test at the end of the 10th week of the semester
- 3. Third test at the end of the 15th week of the semester
- Two assignments each of 10 Marks
- 4. First assignment at the end of 4th week of the semester
- 5. Second assignment at the end of 9th week of the semester

- Practical Sessions need to be assessed by appropriate rubrics and viva-voce method. This will contribute to 20 marks.
- Rubrics for each Experiment taken average for all Lab components – 15 Marks.
- Viva-Voce– 5 Marks (more emphasized on demonstration topics) The sum of three tests, two assignments, and practical sessions will be out of 100 marks and will be scaled down to 50 marks

- Suggested Learning Resources:

Textbooks:

1. Computer-Networks- Andrew S. Tanenbaum and David J. Wetherall, Pearson Education, 5thEdition.

2. Computer Networking A Top-Down Approach -James F. Kurose and Keith W. Ross Pearson Education 7th Edition.

Scope

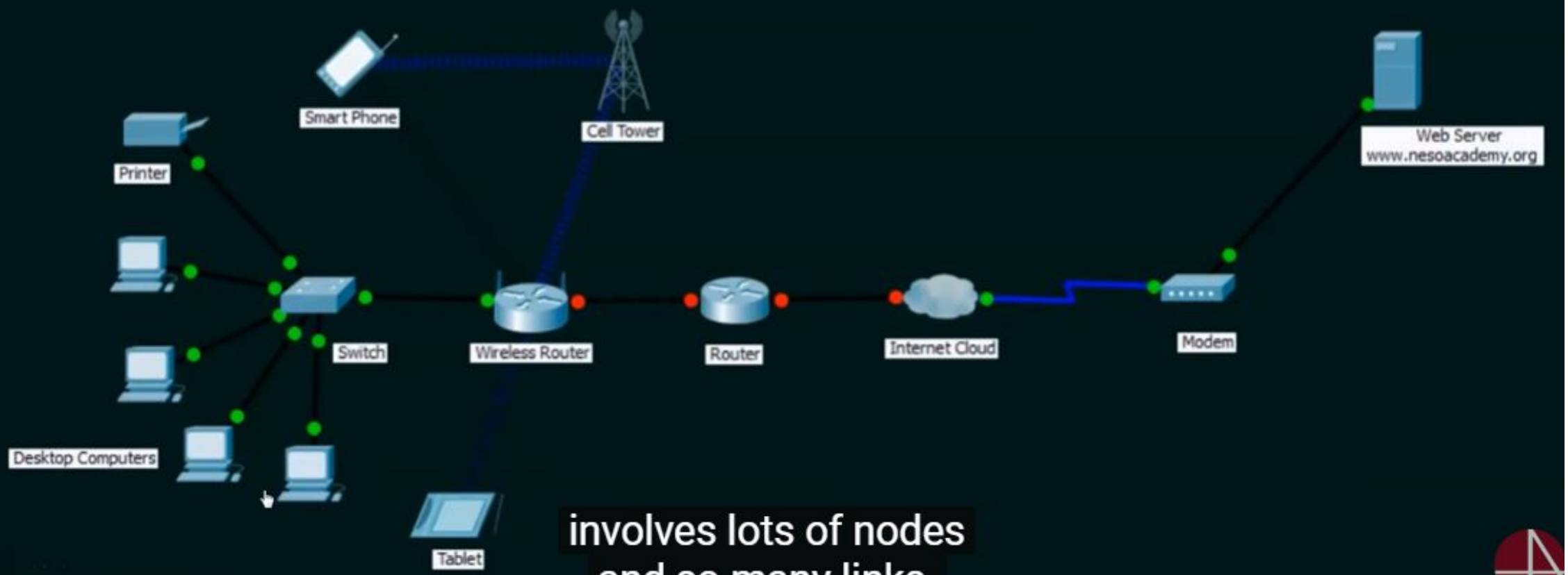
- Networking is Everywhere
- Networking supports the way we learn
- Networking supports the way we communicate
- Networking supports the way we work
- Networking supports the way we Play
- Computer network is a set of **nodes** connected by **communication links**
- Node is Computer, printer or any other device which is capable of sending and receiving data from other nodes in the network.

- Example

Computers, Printers, Server, Security camera, Switches, bridges, routers etc

- A Communication link can be a wired link or wireless link.
- Link can be a wire or medium of Air in wireless.
- A computer network is mainly used for resource sharing
- There are end devices and intermediary nodes in the network

An example computer network



involves lots of nodes
and so many links.

NETWORK HARDWARE

- Broadly speaking, there are two types of transmission technology that are in widespread use: broadcast links and point-to-point links.
- Point-to-point links connect individual pairs of machines.
- Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called unicasting.
- Broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient.
- Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

- A wireless network is a common example of a broadcast link, with communication shared over a coverage region that depends on the wireless channel and the transmitting machine.
- An alternative criterion for classifying networks is by scale. Distance is important as a classification metric because different technologies are used at different scales.
- Classification of interconnected processors by scale

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

Networks that are meant for one person(PAN)

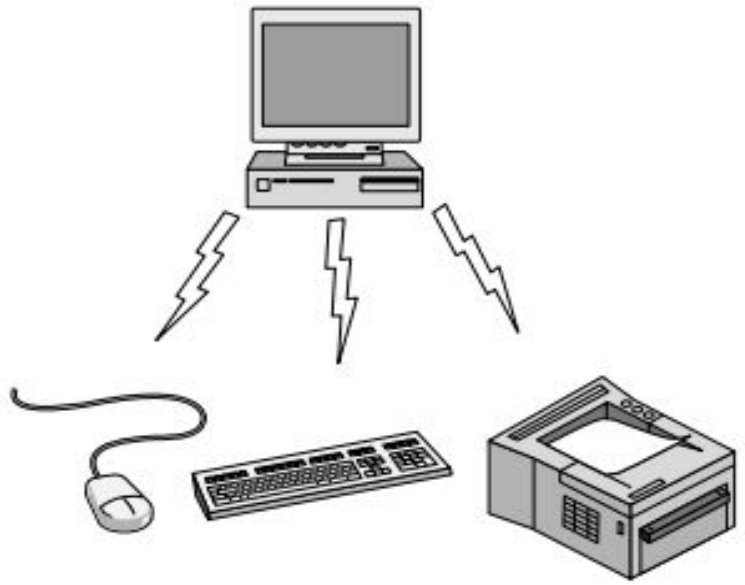
Beyond these come longer-range networks.

Finally, the connection of two or more networks is called an internetwork.

Personal Area Networks

- PANs (Personal Area Networks) let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals.
- In the simplest form, Bluetooth networks use the master-slave paradigm of Fig.

The system unit (the PC) is normally the master, talking to the mouse, keyboard, etc., as slaves. Other examples are RFID

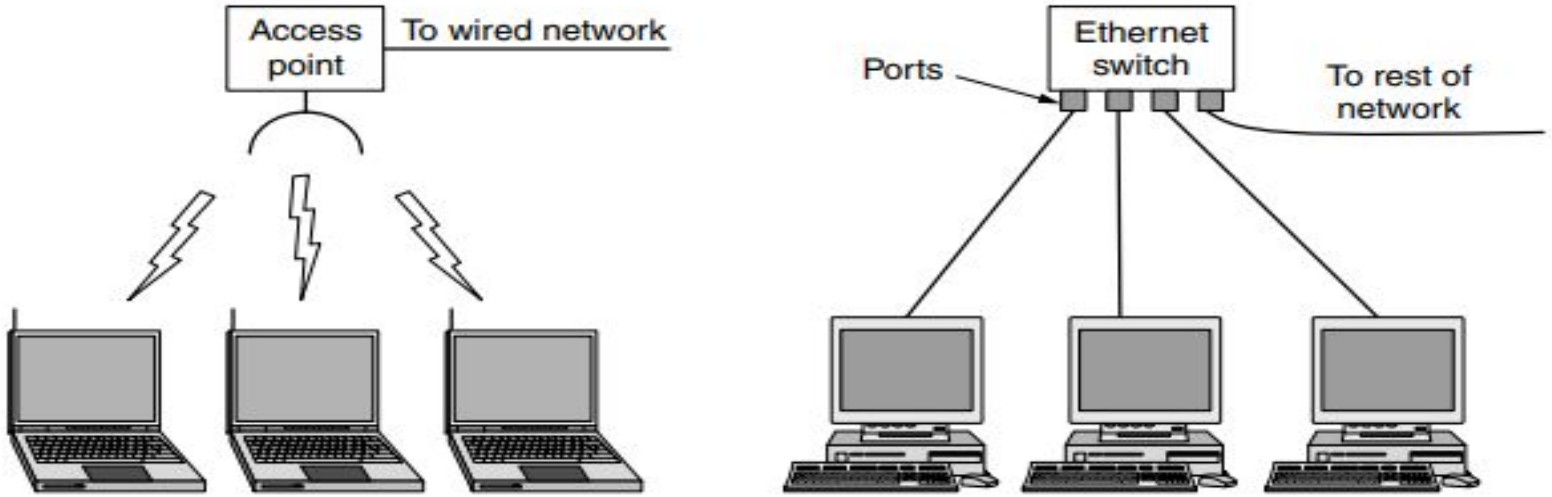


Bluetooth PAN configuration

Local Area Networks

- A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory.
- LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.
- When LANs are used by companies, they are called enterprise network
- In wireless LAN, every computer has a radio modem and an antenna that it uses to communicate with other computers.
- This device, called an AP (Access Point), wireless router, or base station, relays packets between the wireless computers and also between them and the Internet.

- There is a standard for wireless LANs called IEEE 802.11, popularly known as WiFi, which has become very widespread with data speed of 11 to hundreds of Mbps.
- The topology of many wired LANs is built from point-to-point links. IEEE 802.3, popularly called Ethernet, is, by far, the most common type of wired LAN.

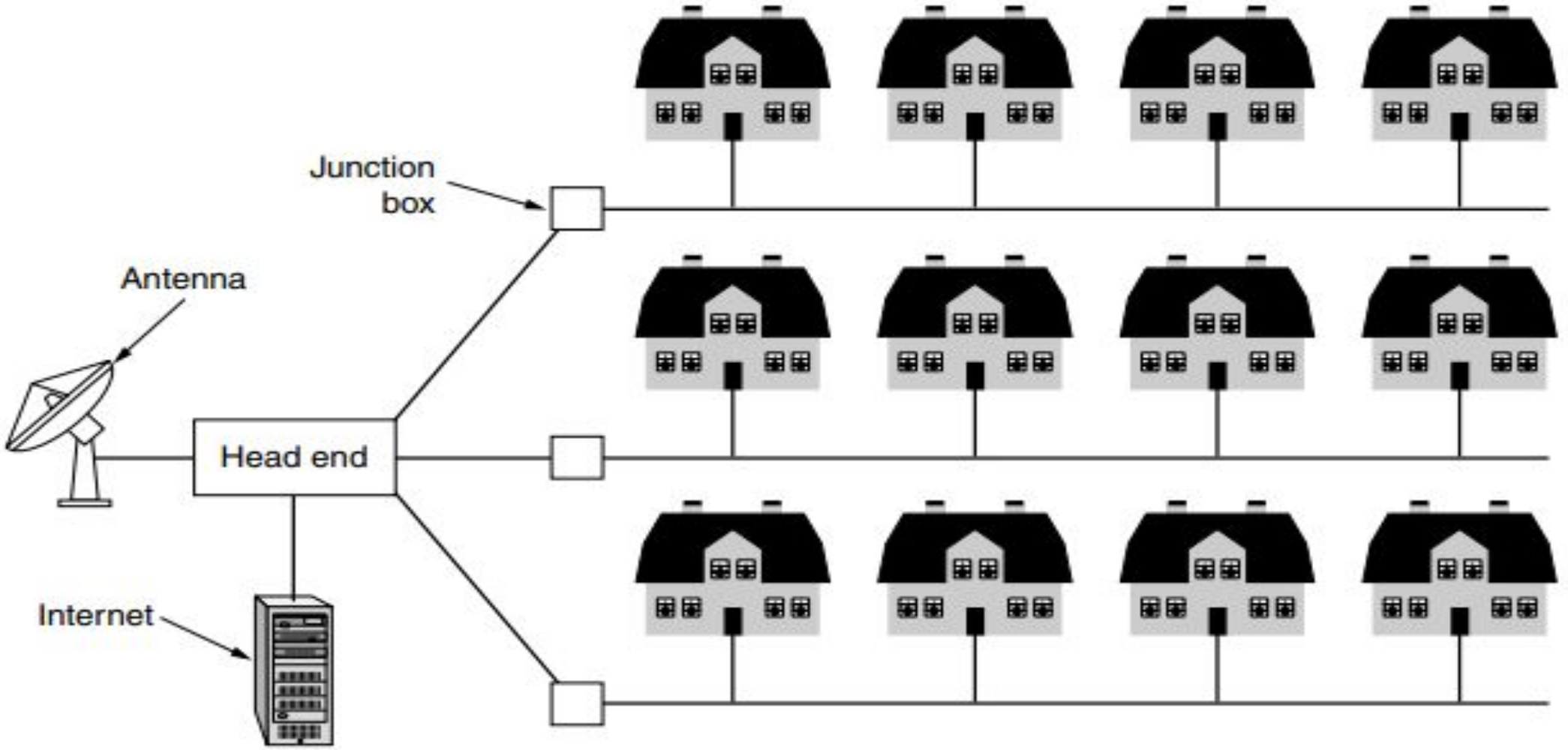


Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

Metropolitan Area Networks

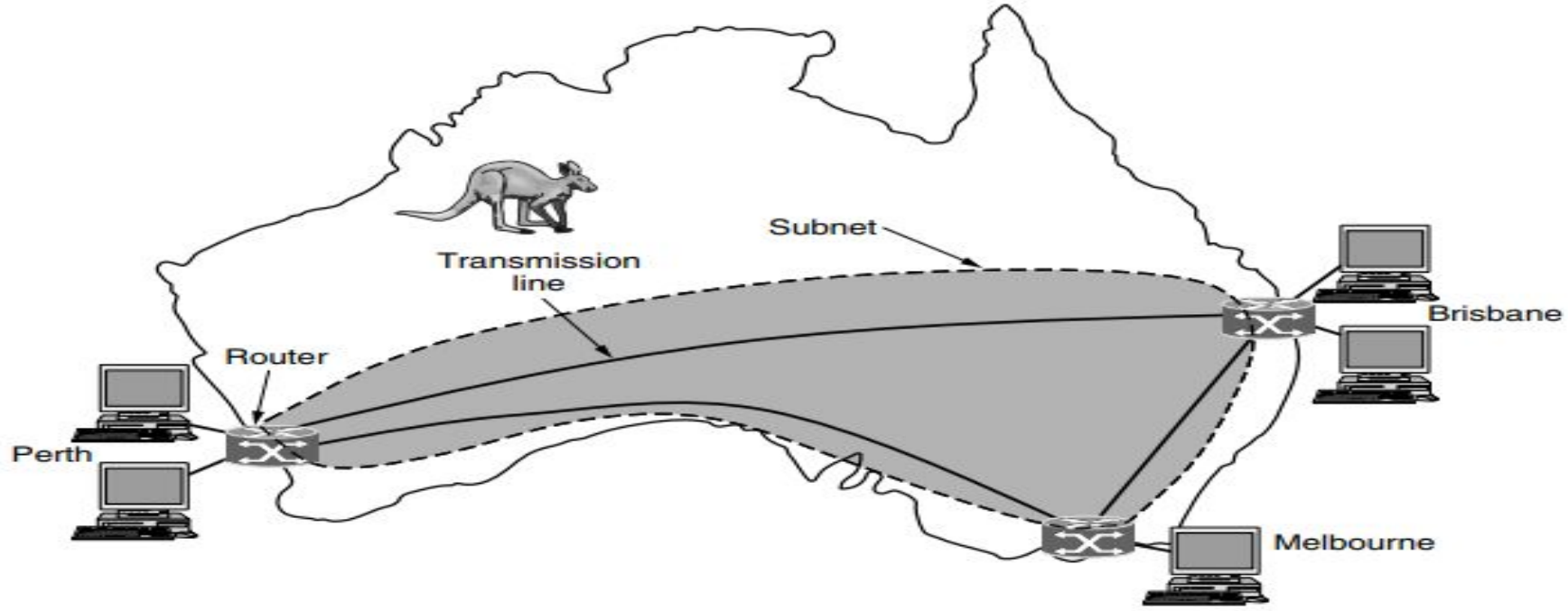
- A MAN (Metropolitan Area Network) covers a city (ex: Cable television networks in city)
- In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers' houses.
- In the figure we see both television signals and Internet being fed into the centralized cable headend for subsequent distribution to people's homes.
- Cable television is not the only MAN, though. Recent developments in highspeed wireless Internet access have resulted in another MAN, which has been standardized as IEEE 802.16 and is popularly known as WiMAX.

A metropolitan area network based on cable TV



Wide Area Networks

- A WAN (Wide Area Network) spans a large geographical area, often a country or continent.
- The WAN in Fig is a network that connects offices in Perth, Melbourne, and Brisbane. Each of these offices contains computers(hosts) intended for running user (i.e., application) programs.



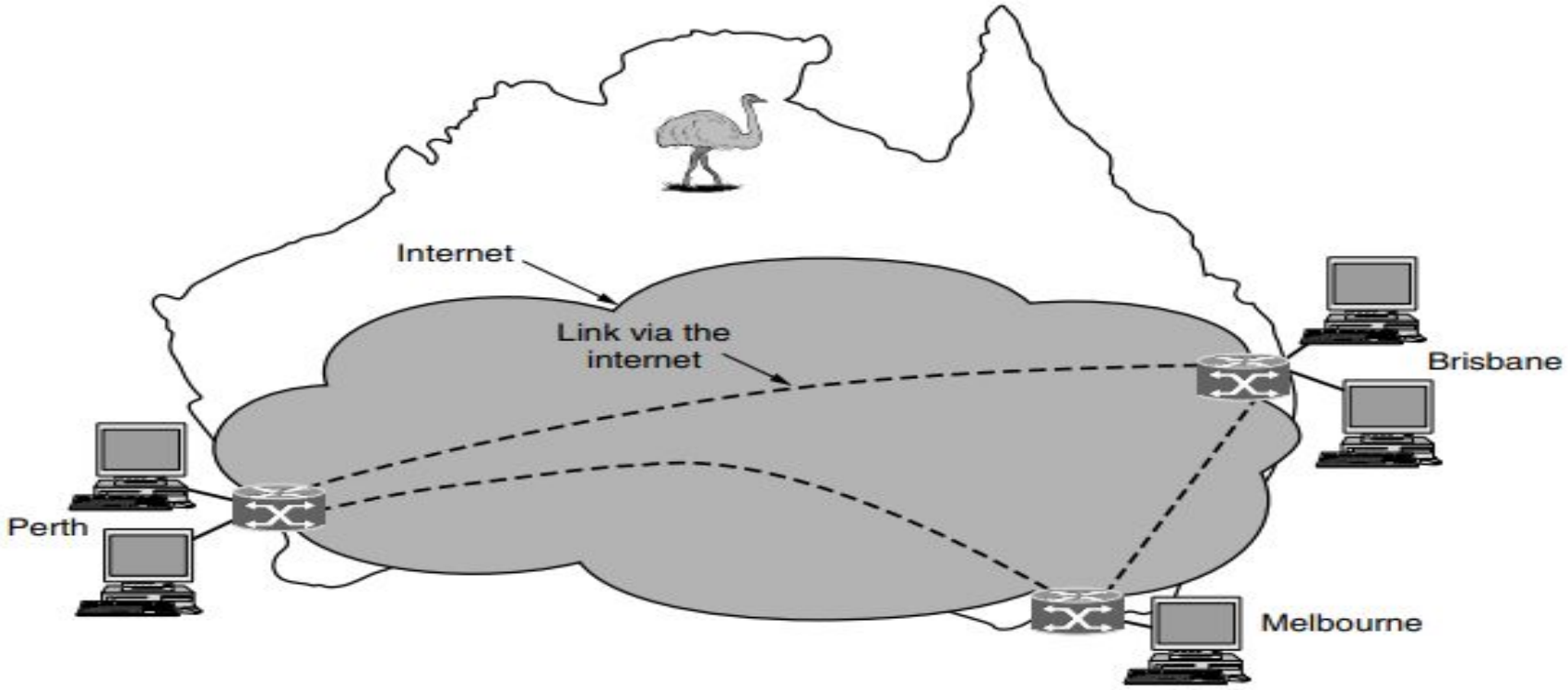
- The rest of the network that connects these hosts is then called the communication subnet
- The job of the subnet is to carry messages from host to host.
- In most WANs, the subnet consists of two distinct components.
- Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links.
- Switching elements, or just switches, are specialized computers that connect two or more transmission lines.

Deference's in LAN and WAN

- Usually in a WAN, the hosts and subnet are owned and operated by different people.
- A second difference is that the routers will usually connect different kinds of networking technology. (ethernet switch in LAN and SONET(synchronous optical networking) in WAN)

VPN (Virtual Private Network).

- Compared to the dedicated arrangement, a VPN has the usual advantage of virtualization, which is that it provides flexible reuse of a resource (Internet connectivity).



Internetworks

- A collection of interconnected networks is called an internetwork or internet.
- The Internet uses ISP(Internet service provider) networks to connect enterprise networks, home networks, and many other networks.
- Subnets, networks, and internetworks are often confused
- The term ‘‘subnet’’ makes the most sense in the context of a wide area network, where it refers to the collection of routers and communication lines owned by the network operator.
- A network is formed by the combination of a subnet and its hosts.
- An internetwork might also be described as a network, as in the case of the WAN

NETWORK SOFTWARE

- Network software is now highly structured.

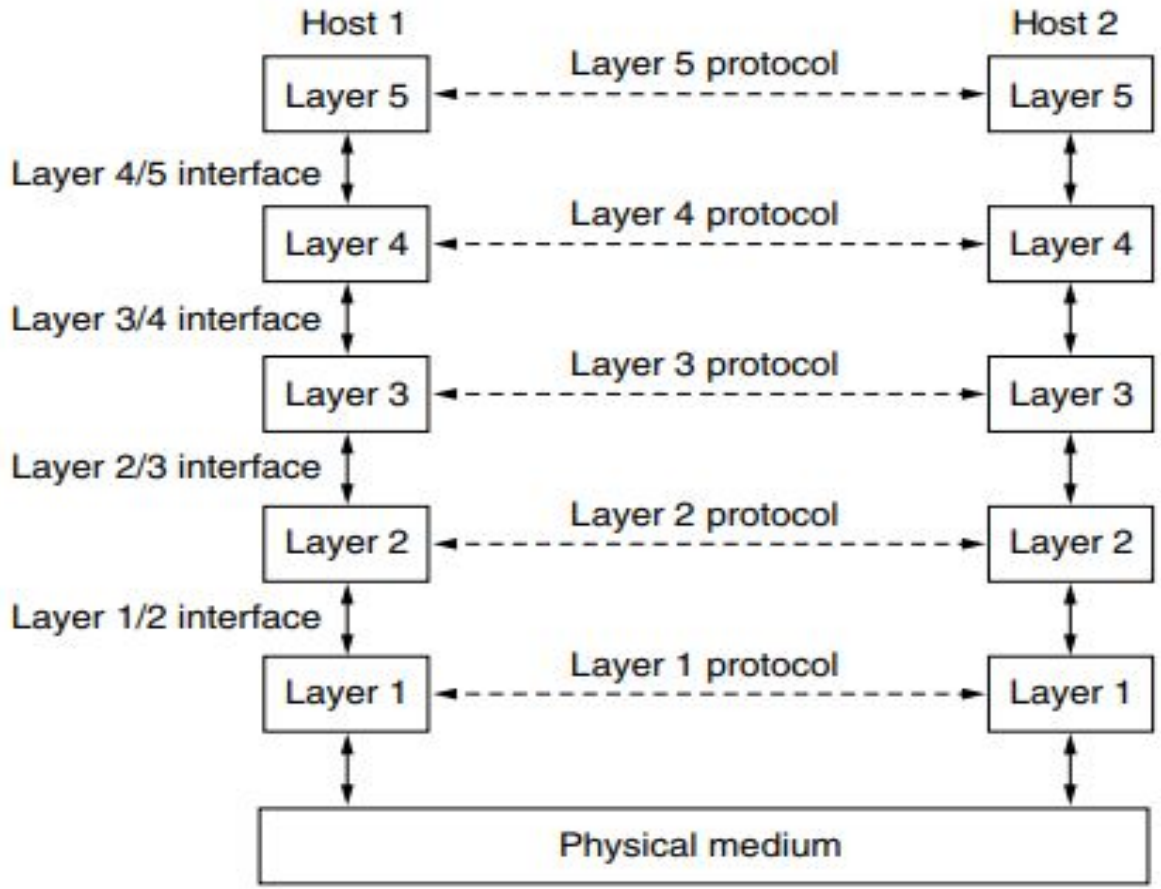
Protocol Hierarchies

- Most networks are organized as a stack of layers or levels, each one built upon the one below it.
- The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.
- Each layer is a kind of virtual machine, offering certain services to the layer above it.
- Basically, a **protocol** is an agreement between the communicating parties on how communication is to proceed.
- A five-layer network is illustrated in Fig
- The entities comprising the corresponding layers on different machines are called peers.

- The peers may be software processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol to talk to each other.
- Below layer 1 is the physical medium through which actual communication occurs.

Virtual communication is shown by dotted lines and physical communication by solid lines.

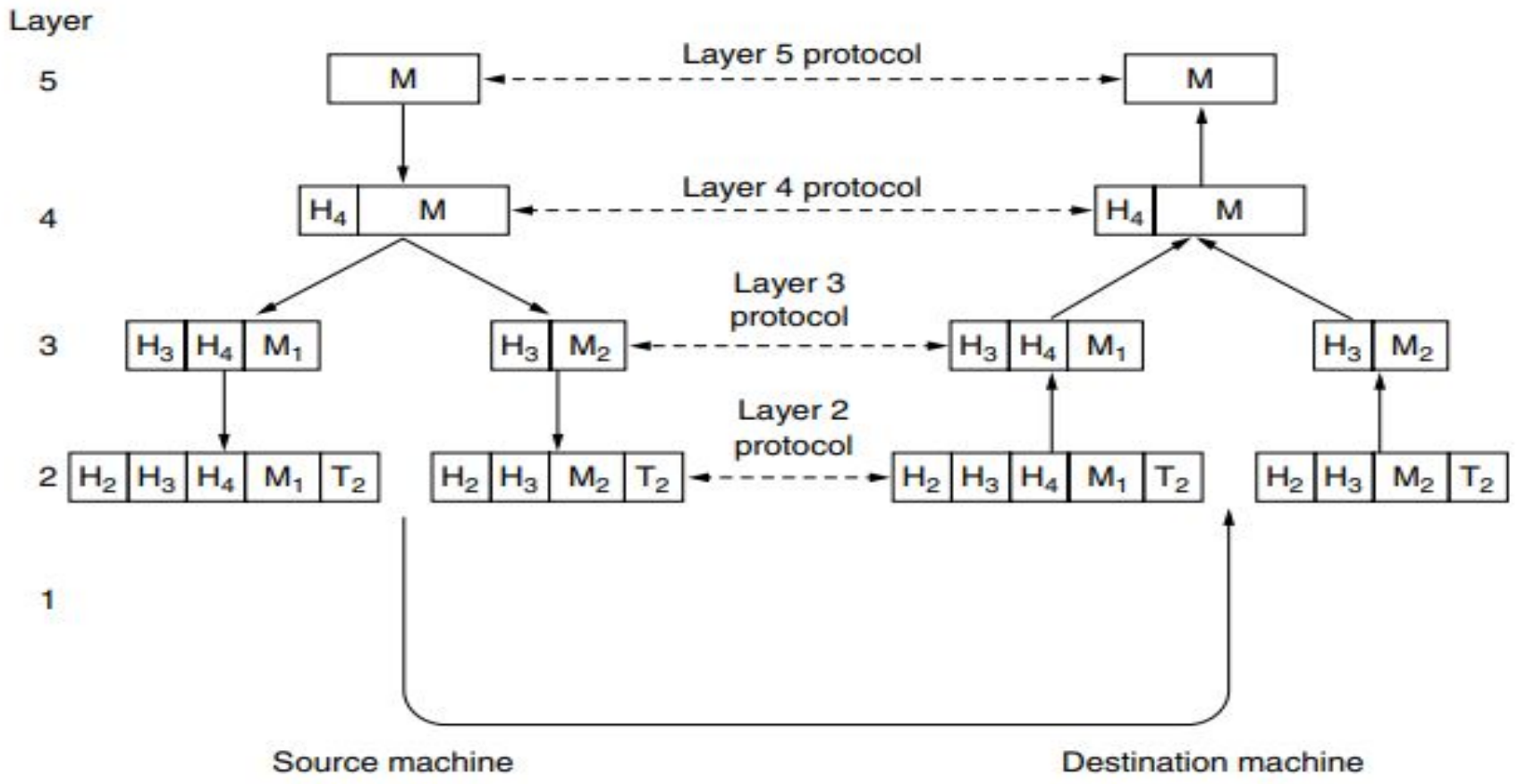
- Between each pair of adjacent layers is an interface



- When network designers decide how many layers to include in a network and what each one should do, one of the most important considerations is defining clean interfaces between the layers.
- A set of layers and protocols is called a network architecture.
- The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.
- A list of the protocols used by a certain system, one protocol per layer, is called a protocol stack.

How to provide communication to the top layer of the five-layer network

- A message, M, is produced by an application process running in layer 5 and given to layer 4 for transmission.



- Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3.
- The header includes control information, such as addresses, to allow layer 4 on the destination machine to deliver the message.
- No limit is placed on the size of messages transmitted in the layer 4 protocol but there is nearly always a limit imposed by the layer 3 protocol.
- Consequently, layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 header to each packet.
- Layer 2 adds to each piece not only a header but also a trailer, and gives the resulting unit to layer 1 for physical transmission.
- At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses.

Design Issues for the Layers

- Reliability is the design issue of making a network that operates correctly even though it is made up of a collection of components that are themselves unreliable
- One mechanism for finding errors in received information uses codes for error detection.
- More powerful codes allow for error correction, where the correct message is recovered from the possibly incorrect bits that were originally received.
- Another reliability issue is finding a working path through a network
- The network automatically making decision is called routing.

- A second design issue concerns the evolution of the network
- . Over time, networks grow larger and new designs emerge that need to be connected to the existing network.
- key structuring mechanism used to support change is Protocol layering.
- Designs that continue to work well when the network gets large are said to be scalable.
- A third design issue is resource allocation
- Statistical multiplexing, meaning sharing based on the statistics of demand.
- An allocation problem that occurs at every level is how to keep a fast sender from swamping a slow receiver with data.
- Feedback from the receiver to the sender is often used. This subject is called flow control.
- This overloading of the network is called congestion.

- Quality of service is the name given to mechanisms that reconcile real-time delivery and high throughput competing demands.
- The last major design issue is to secure the network by defending it against different kinds of threats.
- Mechanisms that provide confidentiality defend against this threat, and they are used in multiple layers.
- Mechanisms for authentication prevent someone from impersonating someone else.
- As an example they might be used to tell fake banking Web sites from the real one

Connection-Oriented Versus Connectionless Service

- Layers can offer two different types of service to the layers above them
- Connection-oriented service is modeled after the telephone system.
- To use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- A circuit is another name for a connection with associated resources, such as a fixed bandwidth.
- Connectionless service is modeled after the postal system.
- Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages.

- There are Six different types of service
- Usually, a reliable service is implemented by having the receiver acknowledge the receipt of each message so the sender is sure that it arrived.

Unreliable (meaning not acknowledged) connectionless service is often called datagram Service

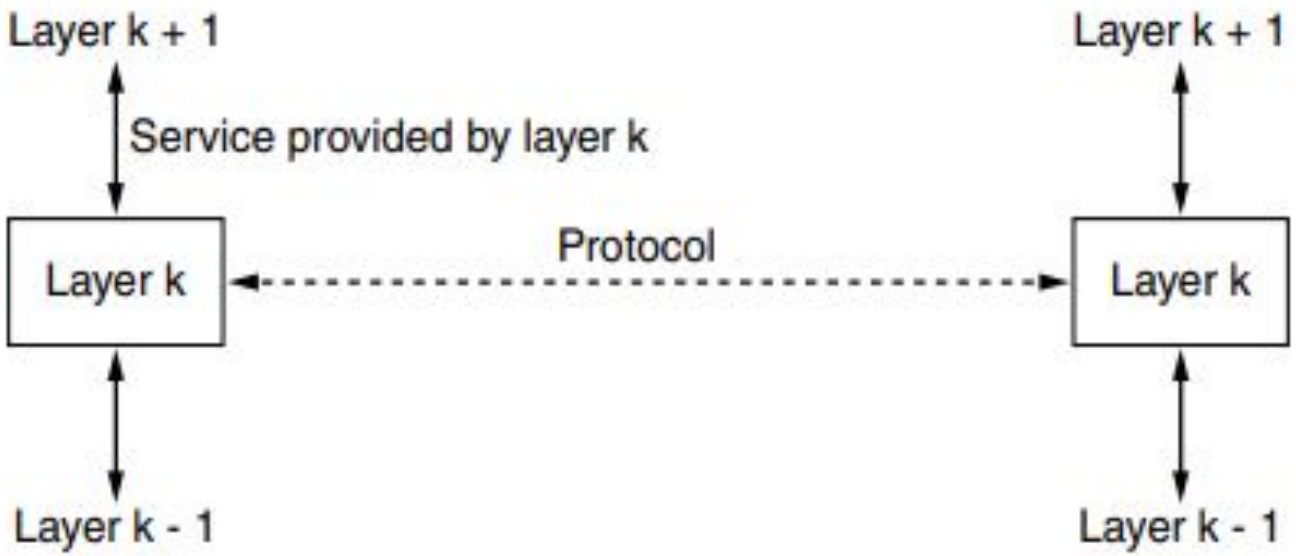
	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

The acknowledged datagram service is like, sending a registered letter and requesting a return receipt. When the receipt comes back, the sender is absolutely sure that the letter was delivered to the intended party and not lost along the way. Text messaging on mobile phones is an example.

The Relationship of Services to Protocols

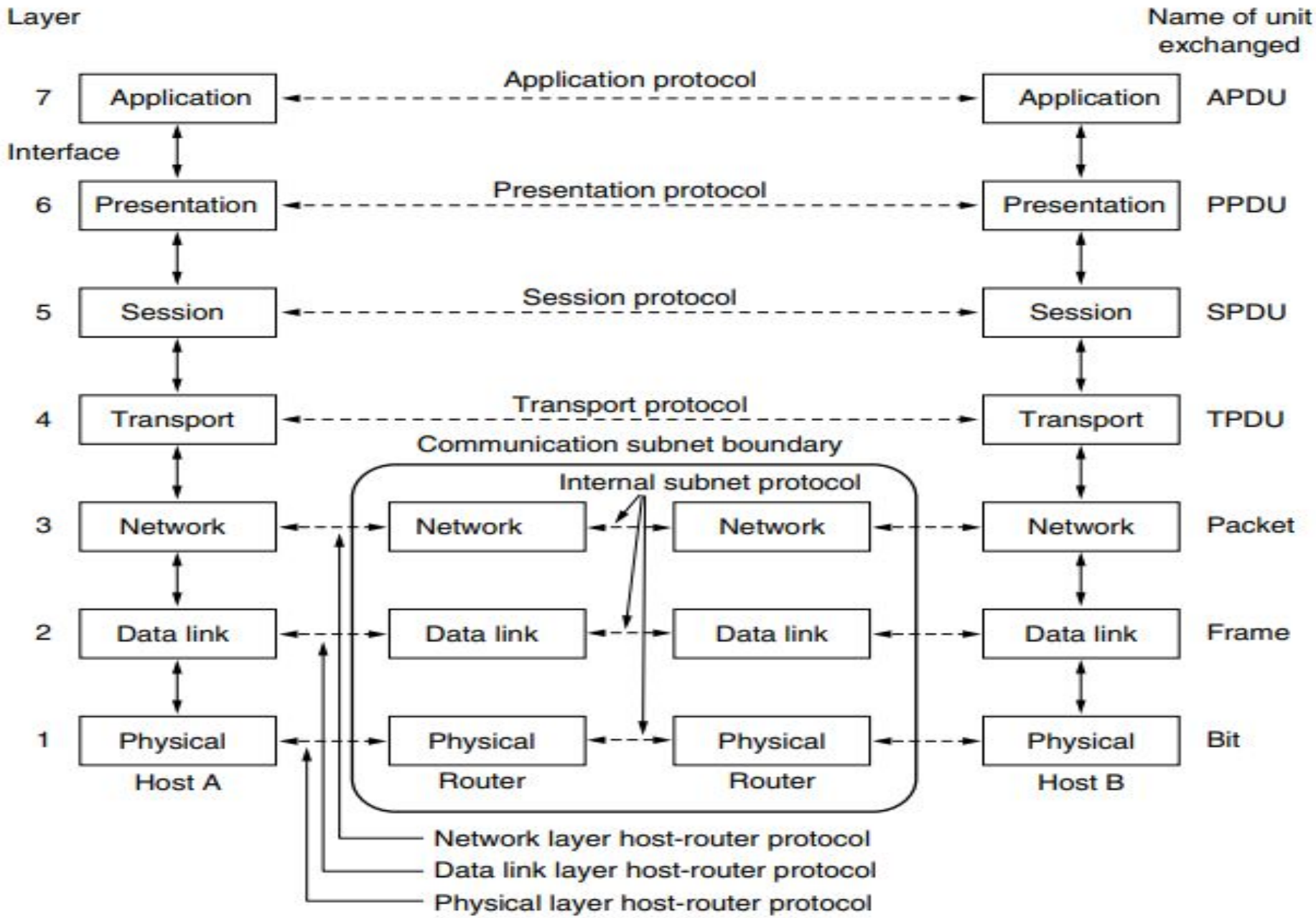
- A service is a set of primitives (operations) that a layer provides to the layer above it.
- The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented.
- A service relates to an interface between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

The relationship between a service and a protocol.



The OSI Reference Model

- The OSI model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers.
- The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.


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

The Physical Layer

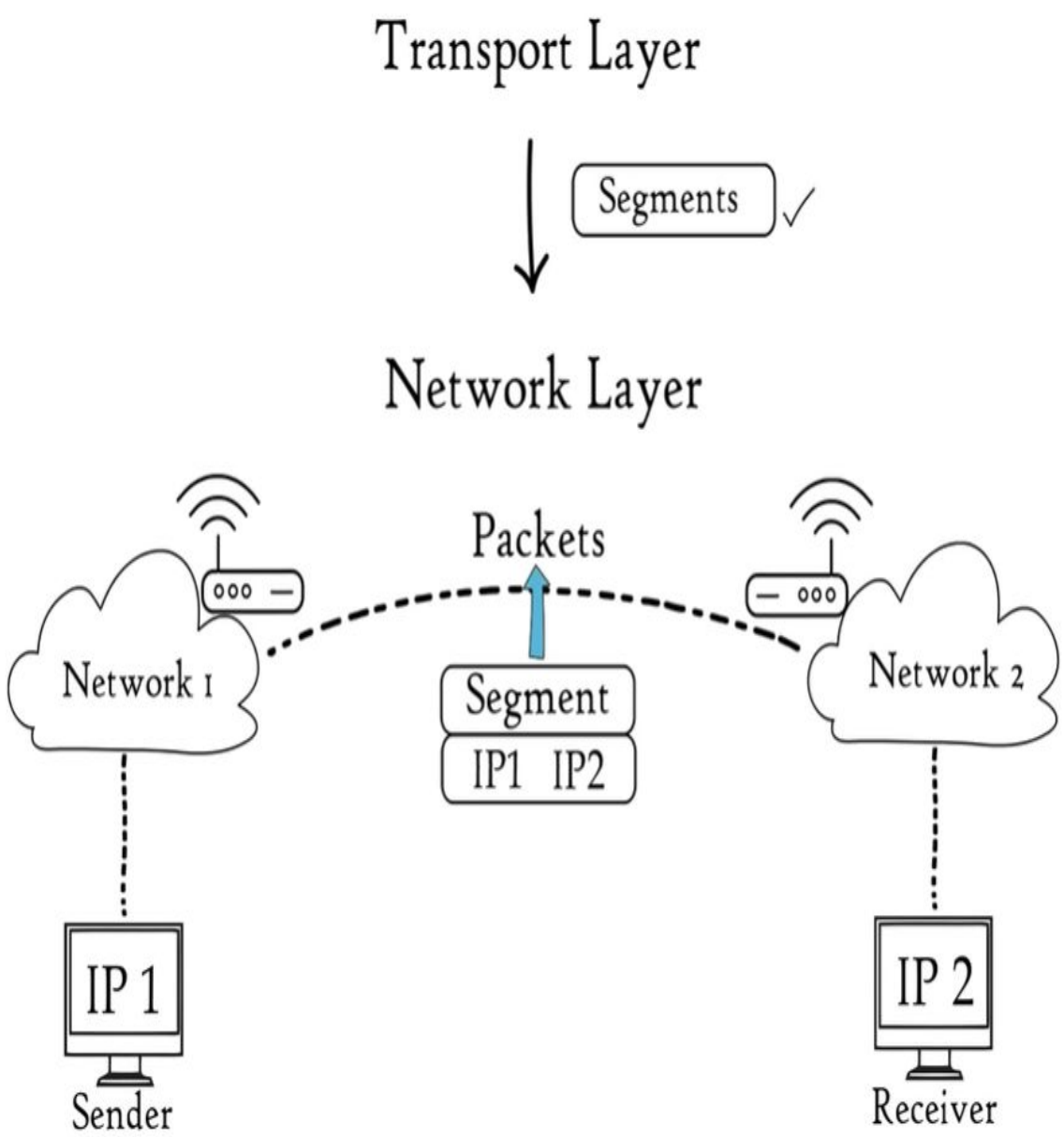
- The physical layer is concerned with transmitting raw bits over a communication channel.
- The design issues have to do with making sure that when one side sends a 1 bit it is received by the other side as a 1 bit, not as a 0 bit.
- What electrical signals should be used to represent a 1 and a 0, how many nanoseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established, how it is torn down when both sides are finished, how many pins the network connector has, and what each pin is used for.
- These design issues largely deal with mechanical, electrical, and timing interfaces, as well as the physical transmission medium, which lies below the physical layer.

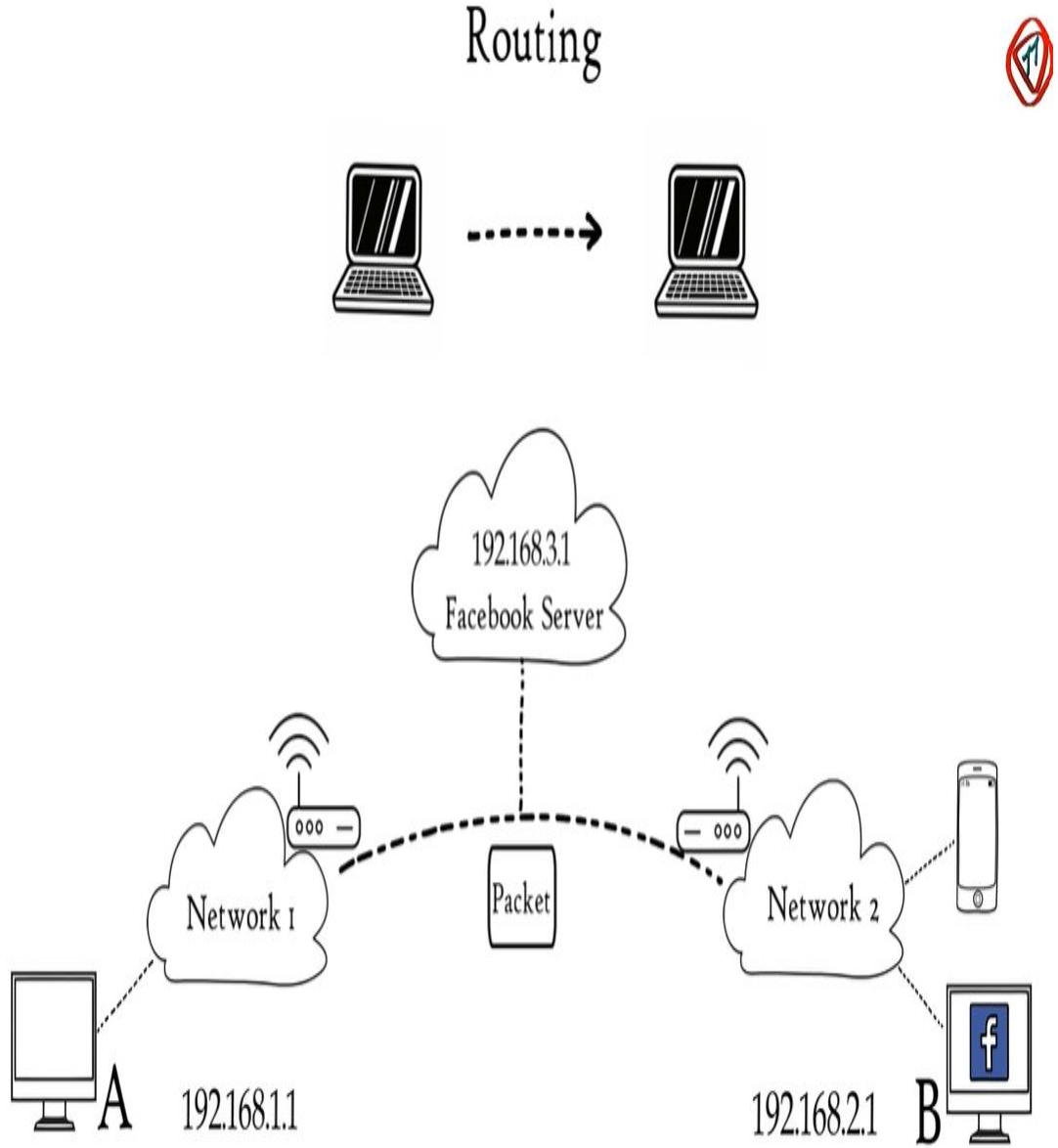
The Data Link Layer

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

The Network Layer

- The network layer controls the operation of the subnet.
- A key design issue is determining how packets are routed from source to destination.
- Routes can be based on static tables that are ‘‘wired into’’ the network and rarely changed, or more often they can be updated automatically to avoid failed components.
- Handling congestion is also a responsibility of the network layer, in conjunction with higher layers that adapt the load they place on the network.
- Network layer to overcome all network addressing problems(Source and destination with different addressing) to allow heterogeneous networks to be interconnected.


Transport Layer
Segments
Network Layer
Packets
Network 1
Segment
IP1 IP2
Network 2
IP 1
IP 2
Sender
Receiver


Routing
192.168.3.1
Facebook Server
Network 1
Packet
Network 2
A
192.168.1.1
192.168.2.1
B

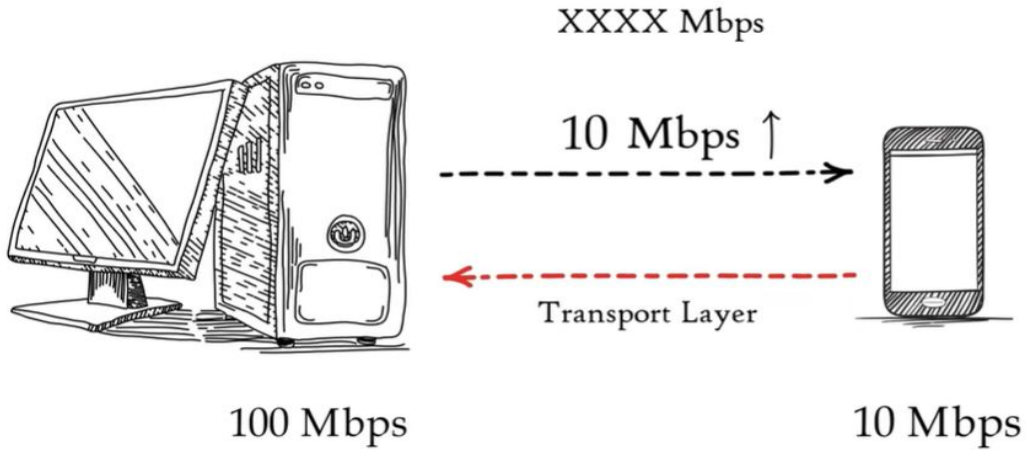
The Transport Layer

- The basic function of the transport layer is to accept data from above it, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.
- The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network.
- The transport layer is a true end-to-end layer. ; it carries data all the way from the source to the destination.
- In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages.

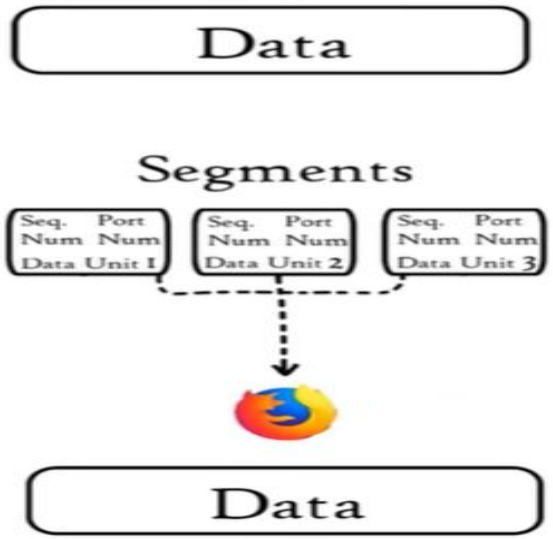
Transport Layer

Segmentation
Flow Control
Error Control

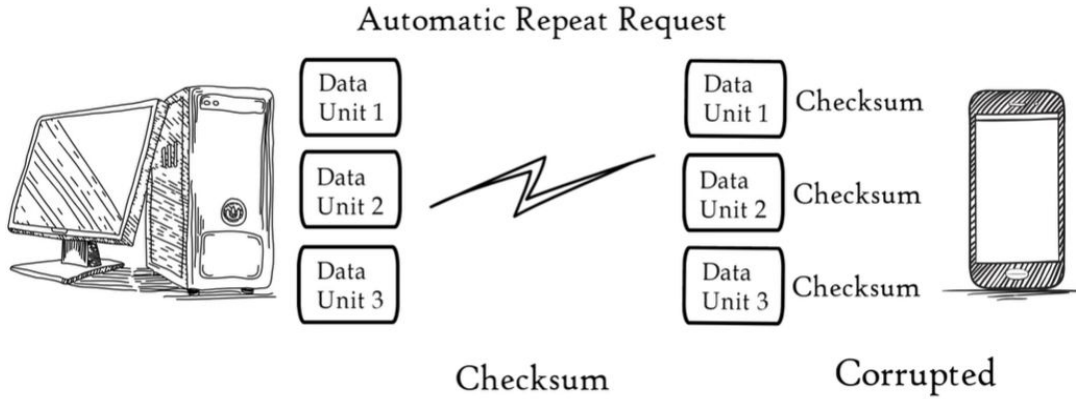
Flow Control:



Segmentation:

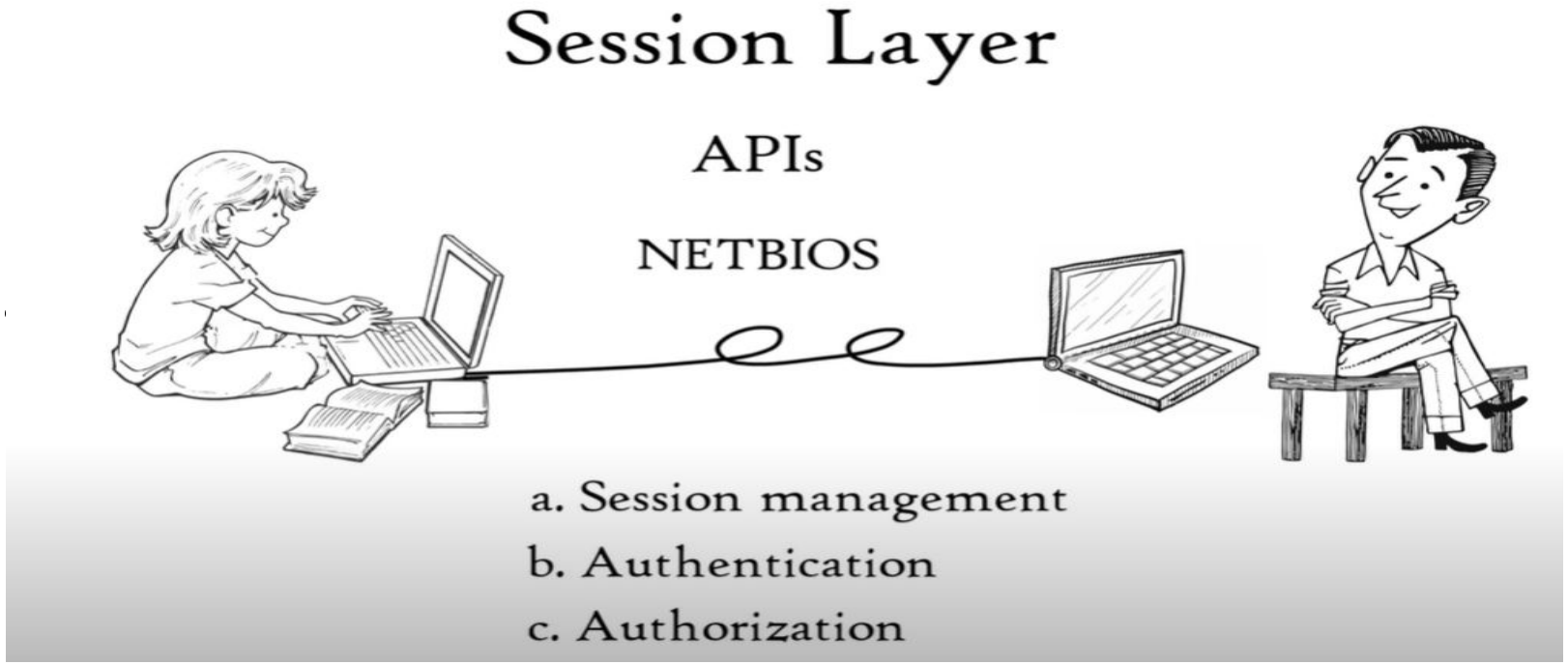


Error Control:



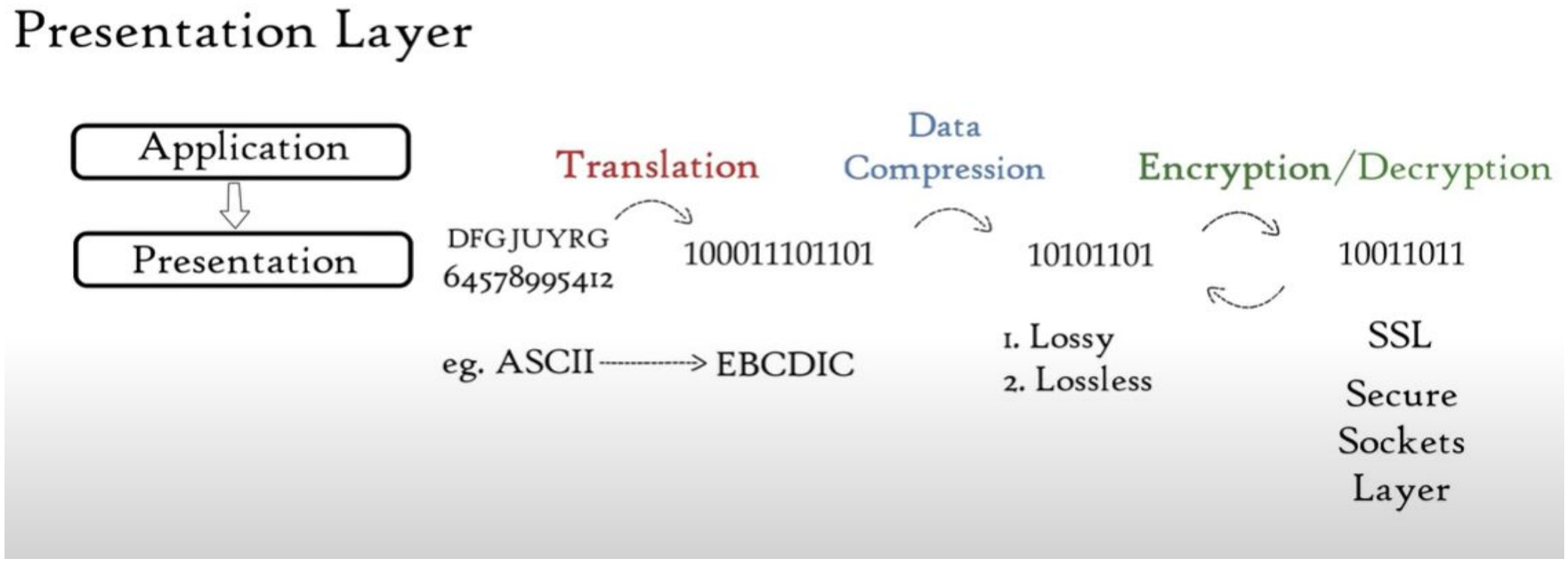
The Session Layer

- The session layer allows users on different machines to establish sessions between them.
- Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation simultaneously), and synchronization (checkpointing long transmissions to allow them to pickup from where they left off in the event of a crash and subsequent recovery).



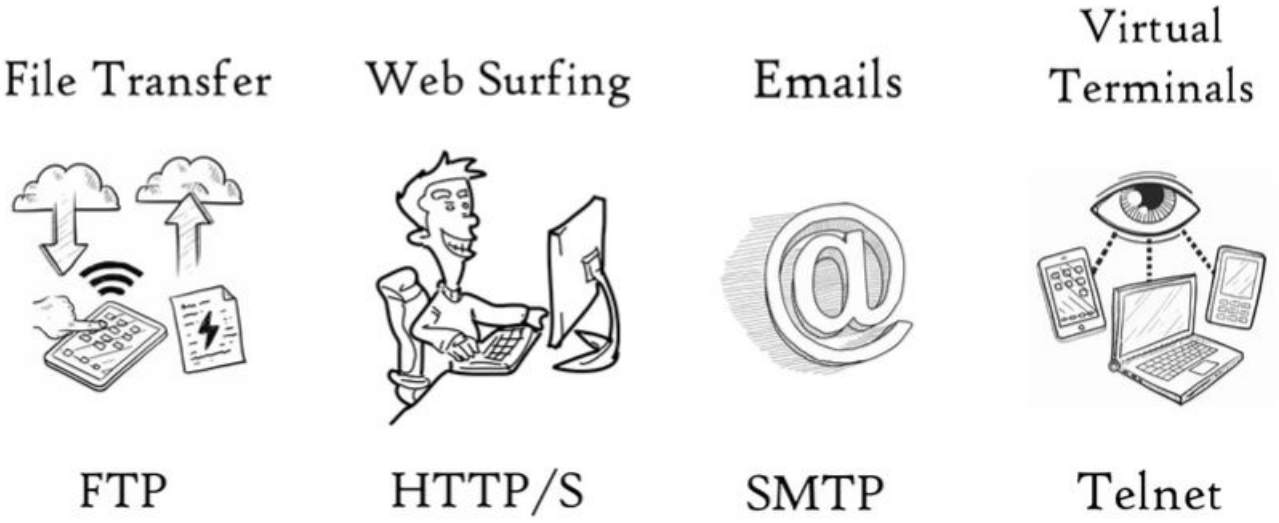
The Presentation Layer

- The presentation layer is concerned with the syntax and semantics of the information transmitted.
- In order to make it possible for computers with different internal data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used ‘‘on the wire”



The Application Layer

- The application layer contains a variety of application protocols that are commonly needed by users.
- One widely used application protocol is HTTP (HyperText Transfer Protocol), which is the basis for the World Wide Web.
- When a browser wants a Web page, it sends the name of the page it wants to the server hosting the page using HTTP. The server then sends the page back.



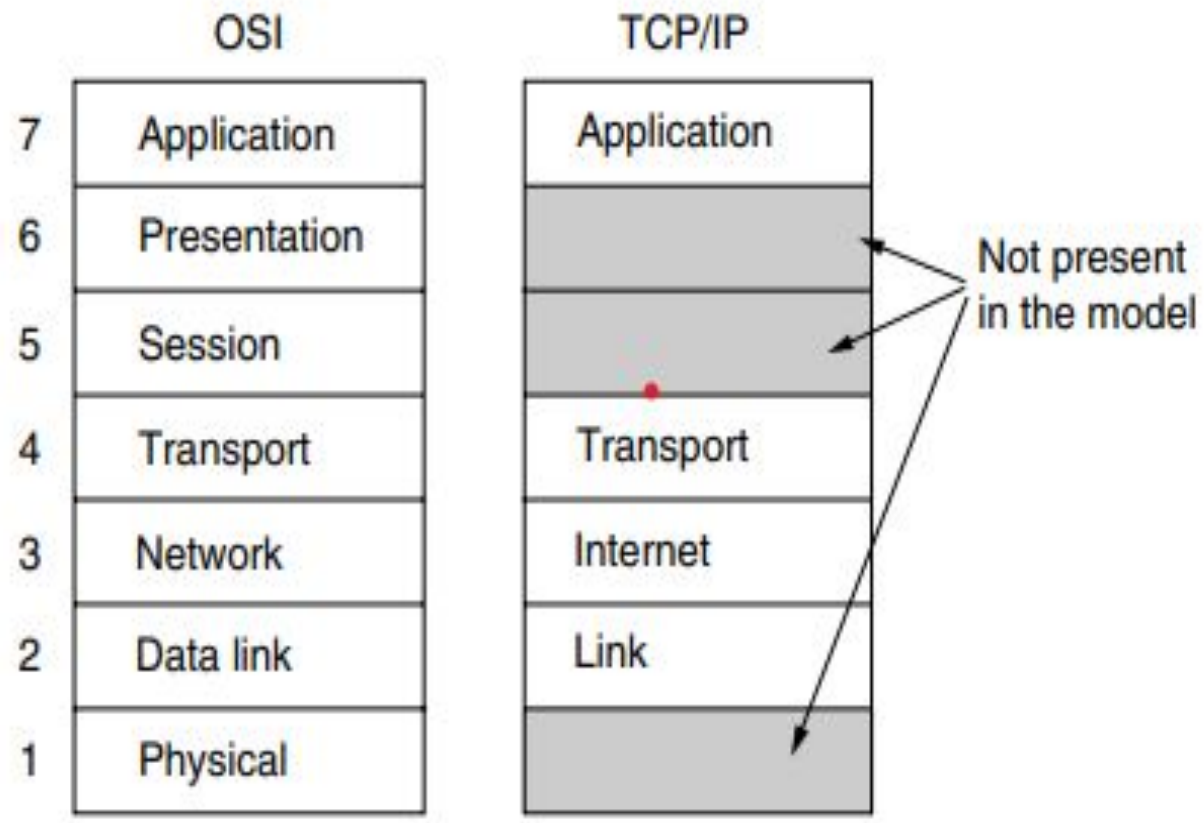
The TCP/IP Reference Model

- The TCP/IP reference model is a four layered architecture.
- It is the network model used in current internet architecture.
- Developed by Dept. Of Defense (DoD). Aim is to connect multiple N/w

The Link Layer

The lowest layer in the model, the link layer describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.

It uses Physical address, flow Control, congetion control and error control.



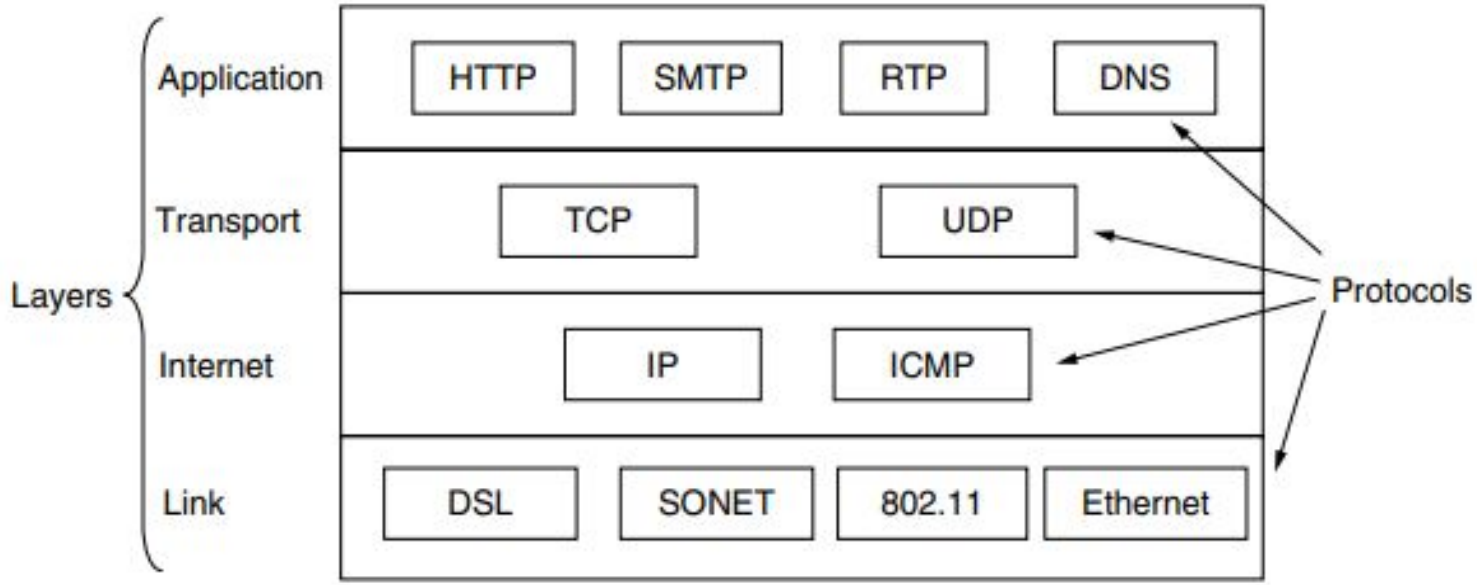
The Internet Layer

- Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network).
- They may even arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.
- The internet layer defines an official packet format and protocol called IP (Internet Protocol), plus a companion protocol called ICMP (Internet Control Message Protocol) that helps it function.
- The job of the internet layer is to deliver IP packets where they are supposed to go.

Transport Layer

- Similar to OSI Transport layer
- Here there are two main protocols used TCP and UDP((User Datagram Protocol),
- TCP is an reliable connection oriented protocol which can handle flow control
- UDP is an unreliable, connection less protocol, which focuses on prompt delivery

than accurate delivery.



The Application Layer

- The TCP/IP model does not have session or presentation layers.
- Applications simply include any session and presentation functions that they require.
- It contains all the higher-level protocols.
- The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP). Many other protocols have been added to these over the years.

What are the differences ??

- 7 layer V/S 4 layer
- In OSI reference model, Model was defined before the implementation of protocols.
- In TCP/IP reference model, after the implementation of protocol, model will be defined.
- OSI reference model has separate session and presentation layer
- TCP/IP reference model, session and presentation layer are included in application layer
- OSI reference model is Theoretical model

GUIDED TRANSMISSION MEDIA

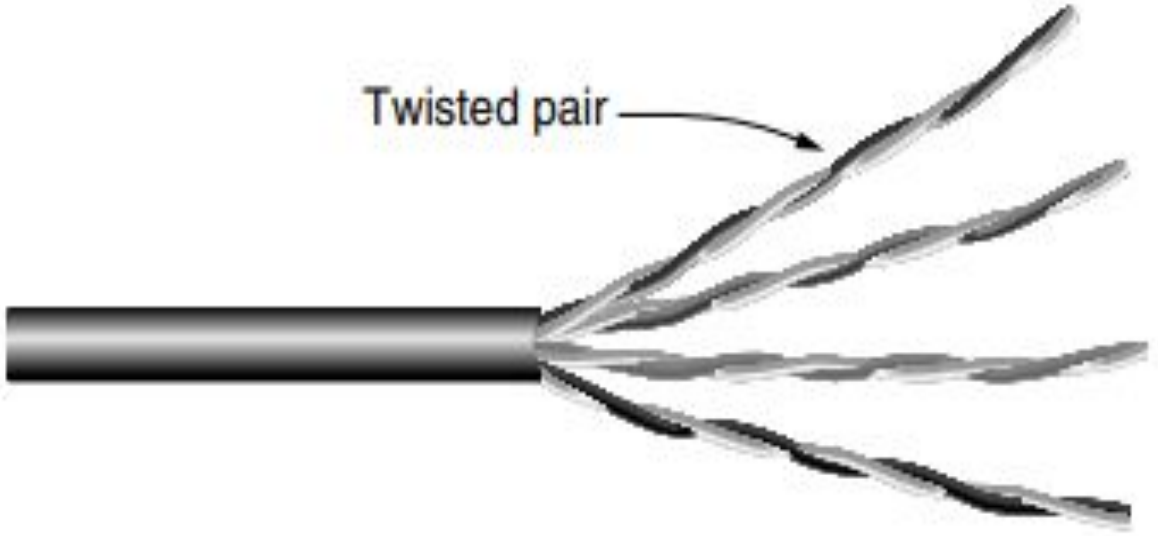
- The purpose of the physical layer is to transport bits from one machine to another.
- Various physical media can be used for the actual transmission with its own bandwidth, delay, cost, and ease of installation and maintenance.
- Media are roughly grouped into guided media, such as copper wire and fiber optics, and unguided media, such as terrestrial wireless, satellite, and lasers through the air.

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 (e.g., recordable DVDs)
- Physically transport the tape or disks to the destination machine, and read them back in again.
- bandwidth or cost per bit transported is the key factor compared to geosynchronous communication satellite

Twisted Pairs

- One of the oldest and still most common transmission media is twisted pair.
- A twisted pair consists of two insulated copper wires, typically about 1 mm thick.
- The wires are twisted together in a helical form, twisting is done because two parallel wires constitute a fine antenna. When the wires are twisted, the waves from different twists cancel out, so the wire radiates less effectively.

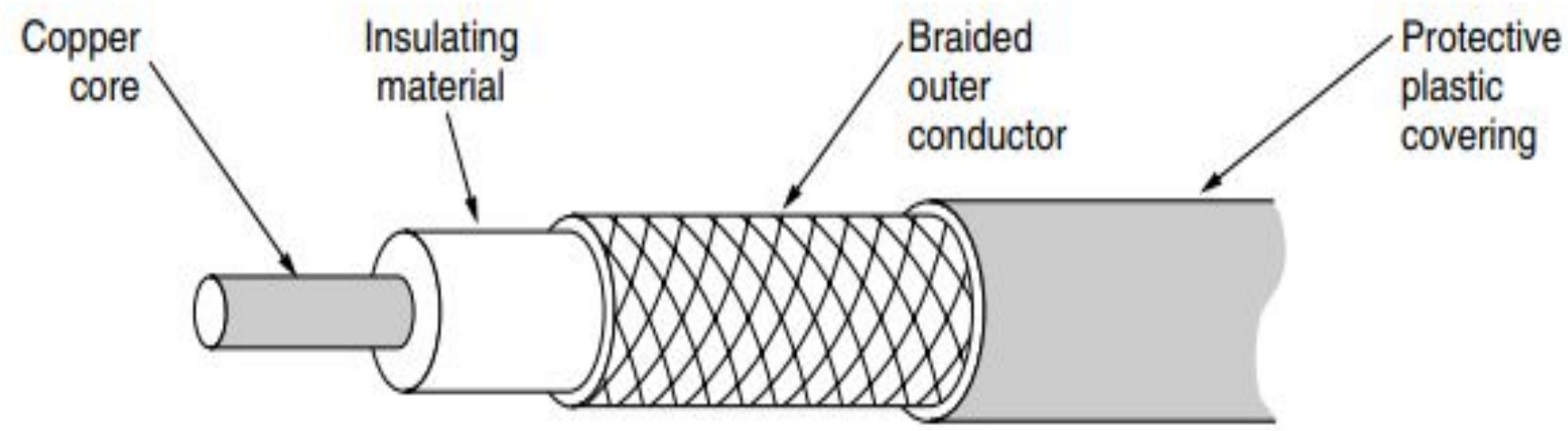


- The most common application of the twisted pair is the telephone system.
- Nearly all telephones are connected to the telephone company (telco) office by a twisted pair.
- For longer distances the signal becomes too attenuated and repeaters are needed.
- Twisted pairs can be used for transmitting either analog or digital information.
- The bandwidth depends on the thickness of the wire and the distance traveled, but several megabits/sec can be achieved for a few kilometers in many cases.
- Twisted-pair cabling comes in **several varieties**. One is ***Category 5*** cabling, or ***"Cat 5."*** consists of two insulated wires gently twisted together with four such pairs.

- Links that can be used in both directions at the same time, like a two-lane road, are called full-duplex links
- links that can be used in either direction, but only one way at a time are called half-duplex links.
- links that allow traffic in only one direction, called simplex links.
- Cat 5 replaced earlier Category 3 cables with a similar cable that uses the same connector, but has more twists per meter. More twists result in less crosstalk and a better-quality signal over longer distances.
- New wiring is more likely to be Category 6 or even Category 7.
- Some cables in Category 6 and above are rated for signals of 500 MHz and can support the 10-Gbps.

Coaxial Cable

- Coaxial cable has better shielding and greater bandwidth than unshielded twisted pairs, so it can span longer distances at higher speeds
- One kind, 50-ohm cable, is commonly used when it is intended for digital transmission from the start.
- The other kind, 75-ohm cable, is commonly used for analog transmission and cable television.



- The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity.
- The bandwidth possible depends on the cable quality and length.
- Modern cables have a bandwidth of up to a few GHz.
- Coaxial cables used to be widely used within the telephone system for long-distance lines but have now largely been replaced by fiber optics.
- Coax is still widely used for cable television and metropolitan area networks.

Fiber Optics

- Fiber optics are used for long-haul transmission in network backbones, highspeed LANs (although so far, copper has always managed catch up eventually), and high-speed Internet access such as FttH (Fiber to the Home)
- An optical transmission system has three key components: the light source, the transmission medium, and the detector.
- A pulse of light indicates a 1 bit and the absence of light indicates a 0 bit. The transmission medium is an ultra-thin fiber of glass.
- The detector generates an electrical pulse when light falls on it.
- By attaching a light source to one end of an optical fiber and a detector to the other, we have a unidirectional data transmission system.
- It accepts an electrical signal, converts and transmits it by light pulses, and then reconverts the output to an electrical signal at the receiving end.

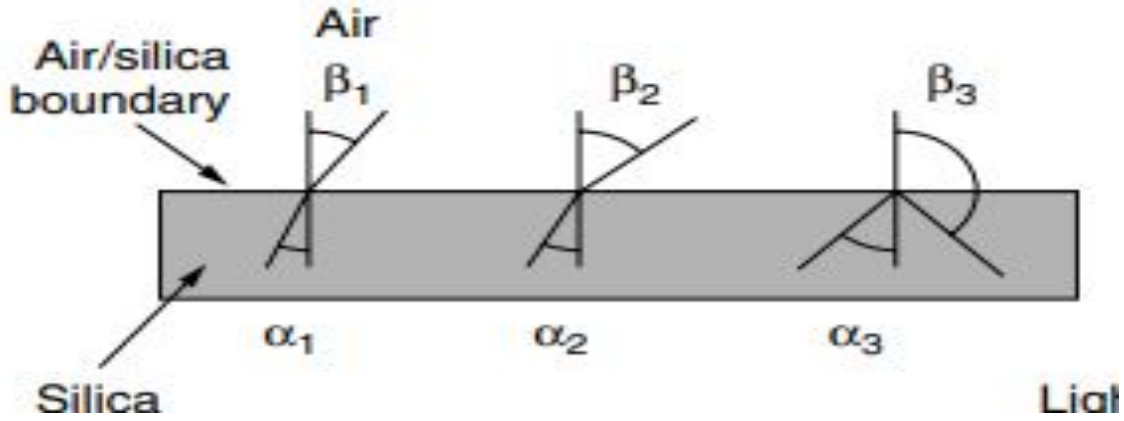
- When a light ray passes from one medium to another—for example, from fused silica to air—the ray is refracted (bent) at the silica/air boundary, as shown.
- Here we see a light ray incident

on the boundary at an angle α1

emerging at an angle β1.

The amount of refraction depends

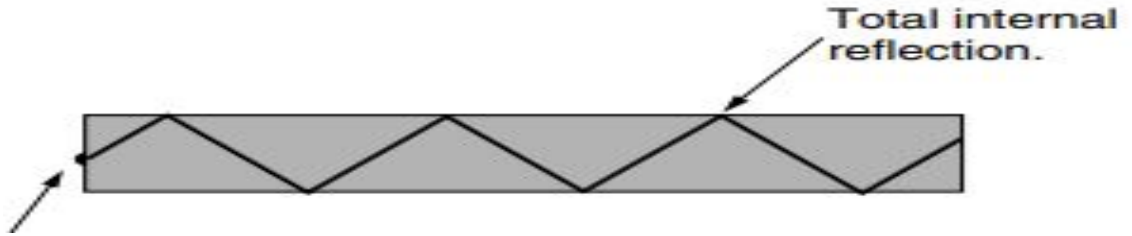
on the properties of the two media.



- For angles of incidence above a certain critical value, the light is refracted back into the silica; none of it escapes into the air.
- Thus, a light ray incident at or above

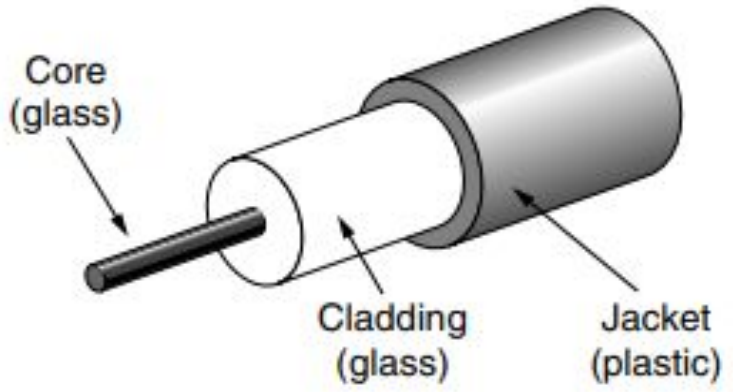
the critical angle is trapped inside the

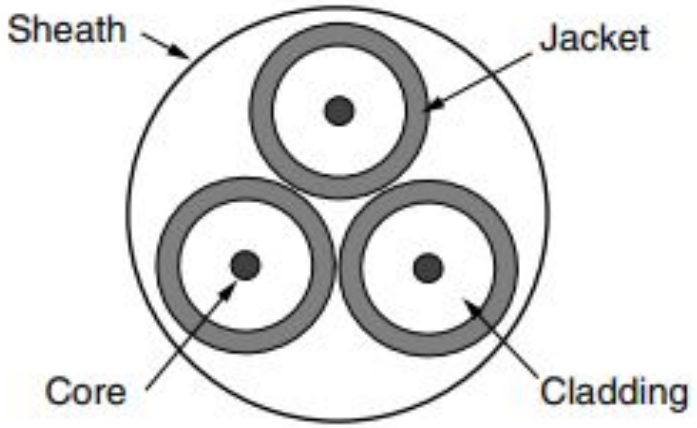
fiber can propagate for many kilometers



Fiber Cables

- Fiber optic cables are similar to coax, except without the braid.
- At the center is the glass core through which the light propagates.





- In multimode fibers, the core is typically 50 microns in diameter, about the thickness of a human hair. In single-mode fibers, the core is 8 to 10 microns.
- The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core.
- Next comes a thin plastic jacket to protect the cladding. Fibers are typically grouped in bundles, protected by an outer sheath.

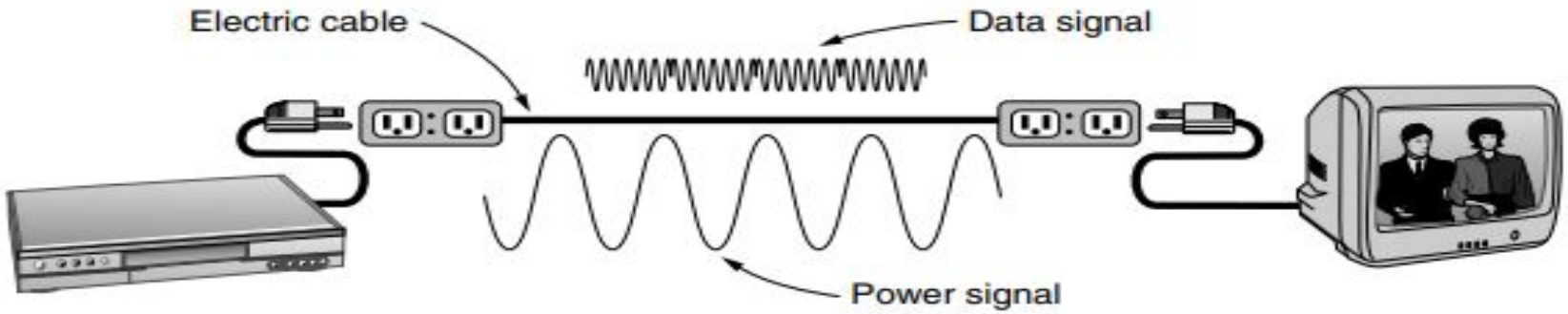
- Two kinds of light sources are typically used to do the signaling. These are LEDs (Light Emitting Diodes) and semiconductor lasers.
- They have different properties,

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

- The receiving end of an optical fiber consists of a photodiode, which gives off an electrical pulse when struck by light.
- The response time of photodiodes, which convert the signal from the optical to the electrical domain, limits data rates to about 100 Gbps

Power Lines

- The use of power lines for data communication is an old idea.
- Power lines have been used by electricity companies for low-rate communication such as remote metering for many years, as well in the home to control devices.
- In recent years there has been renewed interest in high-rate communication over these lines, both inside the home as a LAN and outside the home for broadband Internet access.



- Simply plug a TV and a receiver into the wall, which you must do anyway because they need power, and they can send and receive movies over the electrical wiring

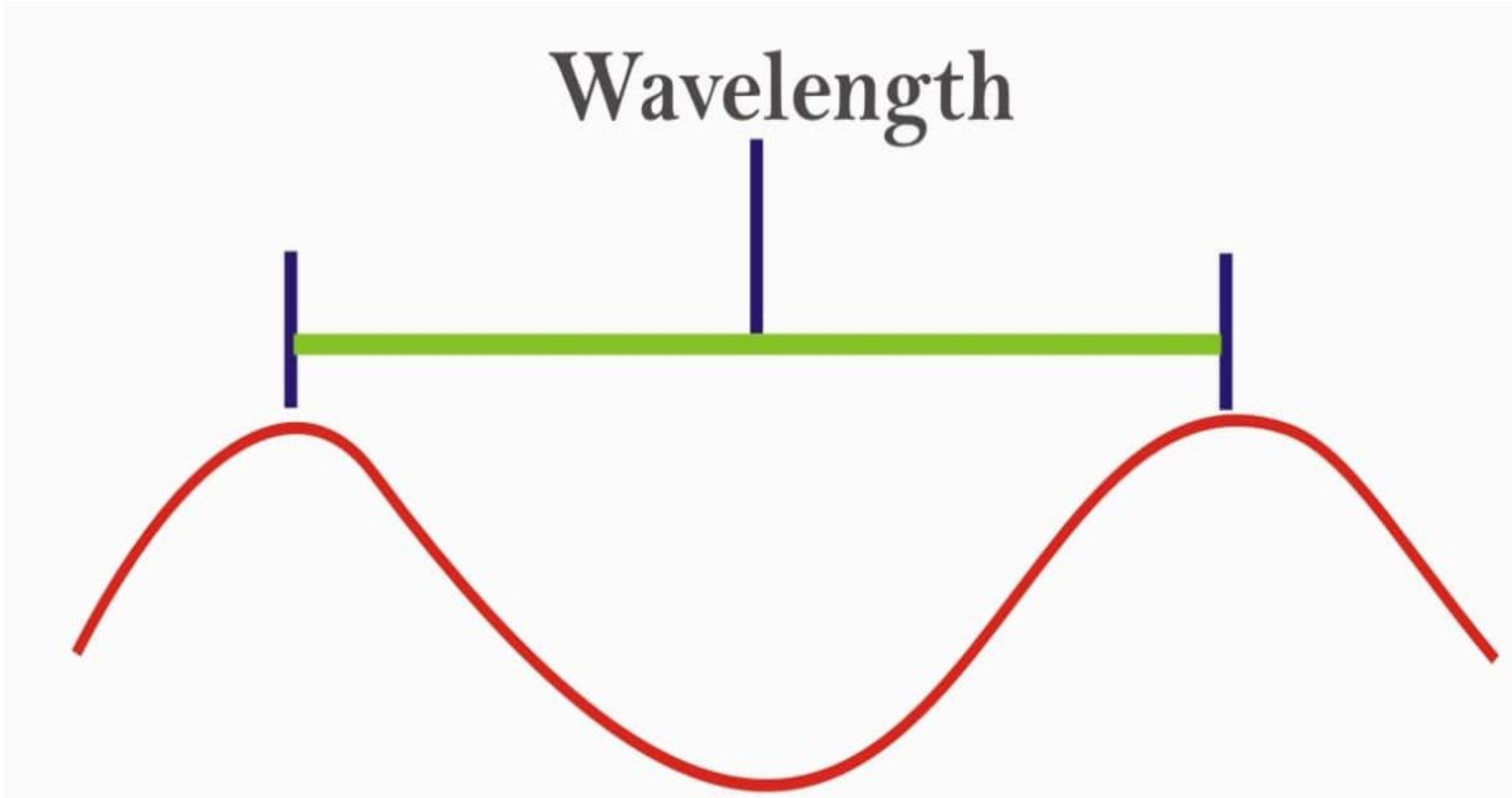
- The data signal is superimposed on the low-frequency power signal as both signals use the wiring at the same time.

WIRELESS TRANSMISSION

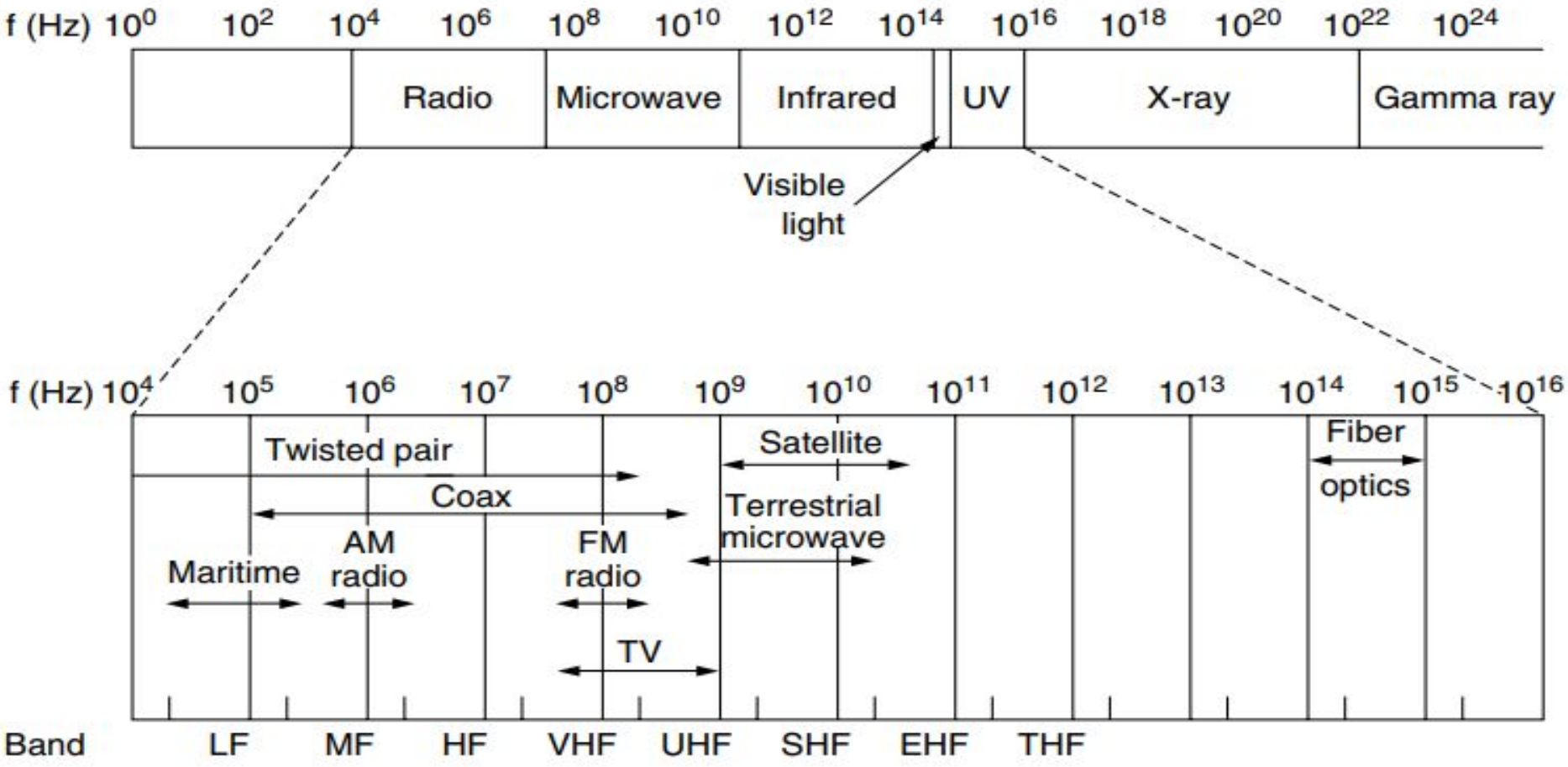
- People who need to be online all the time. For these mobile users, twisted pair, coax, and fiber optics are of no use.
- They need to get their ‘‘hits’’ of data for their laptop, notebook, shirt pocket, palmtop, or wristwatch computers without being tethered to the terrestrial communication infrastructure.
- For these users, wireless communication is the answer.

The Electromagnetic Spectrum

- When electrons move, they create electromagnetic waves that can propagate through space (even in a vacuum).
- The number of oscillations per second of a wave is called its frequency, f, and is measured in Hz.
- The distance between two consecutive maxima (or minima) is called the wavelength λ (lambda)
- 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.
- All wireless communication is based on this principle.
- In a vacuum, all electromagnetic waves travel at the same speed, no matter what their frequency.
- This speed, usually called the speed of light, c, is approximately $3 \times {}_{10}8$ m/sec, or about 1 foot (30 cm) per nanosecond.


Wavelength

- In copper or fiber the speed slows to about 2/3 of this value and becomes slightly frequency dependent.
- The fundamental relation between f, λ, and c (in a vacuum) is λf = c.
- The electromagnetic spectrum is shown



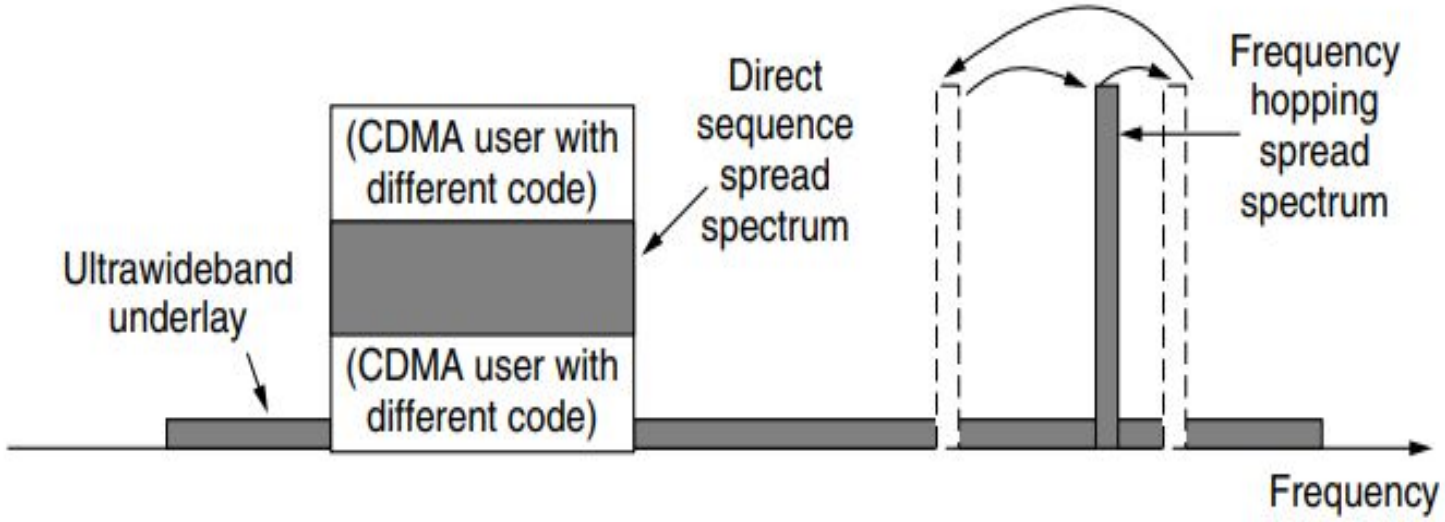
- The radio, microwave, infrared, and visible light portions of the spectrum can all be used for transmitting information by modulating the amplitude, frequency, or phase of the waves.
- Ultraviolet light, X-rays, and gamma rays would be even better, due to their higher frequencies, but they are hard to produce and modulate, do not propagate well through buildings, and are dangerous to living things.
- The bands listed at the bottom of Fig. are the official ITU (International Telecommunication Union) names and are based on the wavelengths
- The terms LF, MF, and HF refer to Low, Medium, and High Frequency, respectively, higher bands were later named the Very, Ultra, Super, Extremely, and Tremendously High Frequency bands.

- Most transmissions use a relatively narrow frequency band, they concentrate their signals in this narrow band to use the spectrum efficiently and obtain reasonable data rates by transmitting with enough power.
- In some cases, a wider band is used, with three variations.

1. frequency hopping spread spectrum
2. direct sequence spread spectrum
3. UWB (UltraWideBand)

- In frequency hopping spread spectrum, the transmitter hops from frequency to frequency hundreds of times per second.
- It is popular for military communication
- It makes transmissions hard to detect and next to impossible to jam.
- Example Bluetooth and older versions of 802.11.

- Direct sequence spread spectrum, uses a code sequence to spread the data signal over a wider frequency band.
- It is widely used commercially as a spectrally efficient way to let multiple signals share the same frequency band.
- These signals can be given different codes, a method called CDMA (Code Division Multiple Access).
- UWB (UltraWideBand) sends a series of rapid pulses, varying their positions to communicate information.
- The rapid transitions lead to a signal that is spread thinly over a very wide frequency band.
- UWB is defined as signals that have a bandwidth of at least 500 MHz or at least 20% of the center frequency of their frequency band.

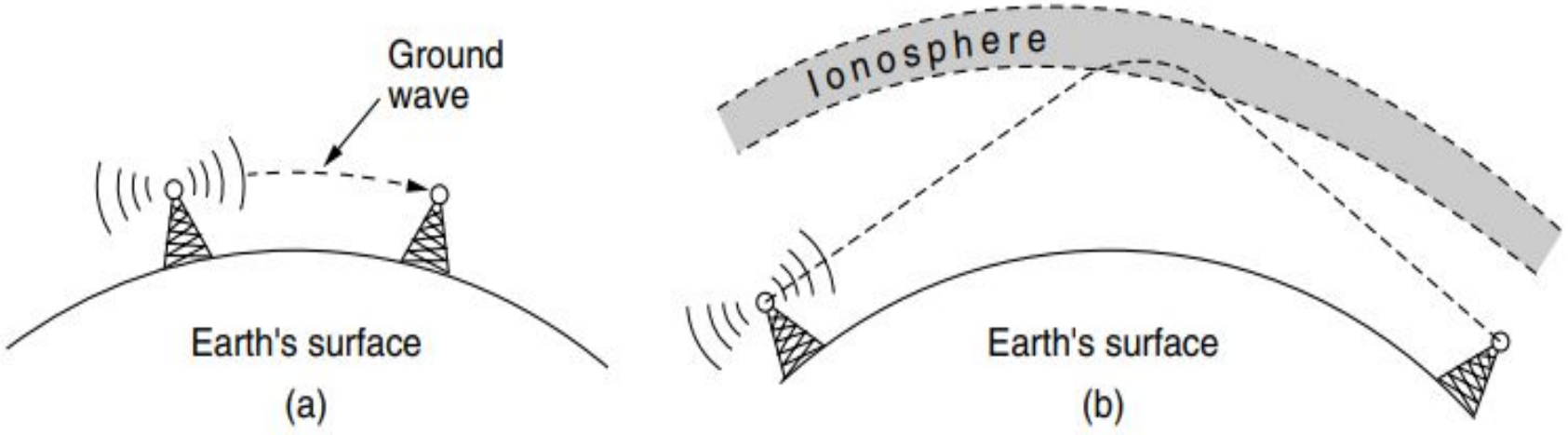


- With this much bandwidth, UWB has the potential to communicate at high rates.
- Because it is spread across a wide band of frequencies, it can tolerate a substantial amount of relatively strong interference from other narrowband signals.

Radio Transmission

- Radio frequency (RF) waves are 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. (travel in all directions from the source)
- The properties of radio waves are frequency dependent. At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source.
- This attenuation is called path loss.
- At all frequencies, radio waves are subject to interference from motors and other electrical equipment.

- In the VLF, LF, and MF bands, radio waves follow the ground, as illustrated in Fig(a)



- These waves can be detected for perhaps 1000 km at the lower frequencies, less at the higher ones.
- In the HF and VHF bands, the ground waves tend to be absorbed by the earth. However, the waves that reach the ionosphere, a layer of charged particles circling the earth at a height of 100 to 500 km, are refracted by it and sent back to earth, as shown in Fig(b)
- The military also communicate in the HF and VHF bands.

Infrared Transmission

- Unguided infrared waves are widely used for short-range communication. The remote controls used for 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.
- Well is also a plus, It means that an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings: you cannot control your neighbor's television with your remote control.
- Therefore, no government license is needed to operate an infrared system, in contrast to radio systems

Light Transmission

- A more modern application is to connect the LANs in two buildings via lasers mounted on their rooftops
- Optical signaling using lasers is inherently unidirectional, so each end needs its own laser and its own photodetector.
- This scheme offers very high bandwidth at very low cost and is relatively secure because it is difficult to tap a narrow laser beam.
- Wind and temperature changes can distort the beam and laser beams also cannot penetrate rain or thick fog, although they normally work well on sunny days.
- Many of these factors are not an issue when the use is to connect two spacecraft.

- Convection currents can interfere with laser communication systems. A bidirectional system with two lasers is pictured here.