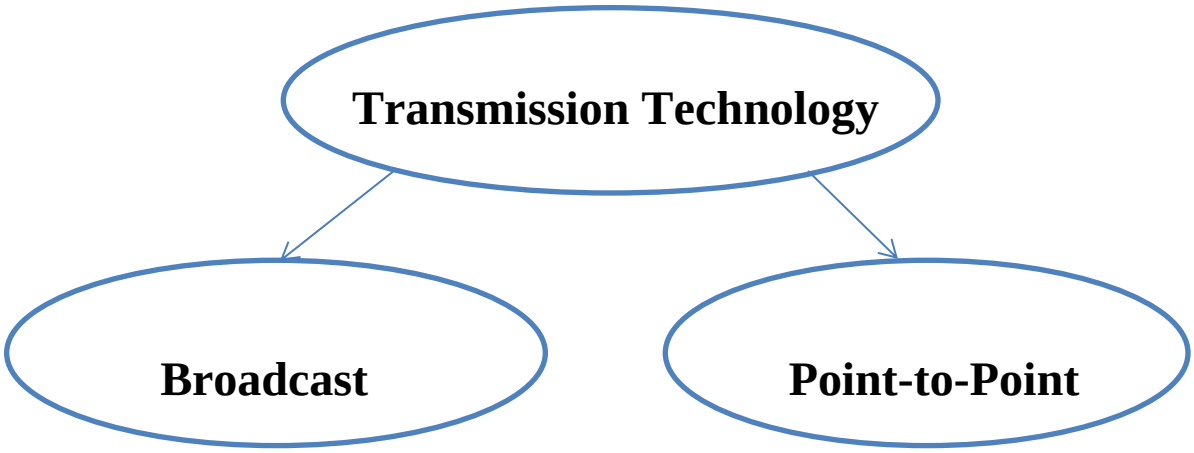
Section(2) Notes

Chapter(1): Introduction II

- 1.2 Network Hardware.
- 1.3 Network Software.
- 1.4 Reference Models.
- 1.5 Example Networks.
- 1.6 Network Standardization.
- Sheet (1).

1.2 Network Hardware:

- There is no generally accepted classification into which all computer networks fit.
- Two dimensions stand out as important: transmission technology and scale.
- There are two types of transmission technology that are in widespread use: **broadcast** links and **point-to-point** links.



- On a 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.
    1. If the packet is intended for the receiving machine, that machine processes the packet.
    2. If the packet is intended for some other machine, it is just ignored.
- Broadcast allow the possibility of addressing a packet to all destinations by using a special code in the address field.
- Example: Wireless network.

- Connect individual pairs of machines.
- To go from the source to the destination on a network made up of point-to-point links where packets may have to first visit one or more intermediate machines.
- The intermediate machines usually are multiple routes.

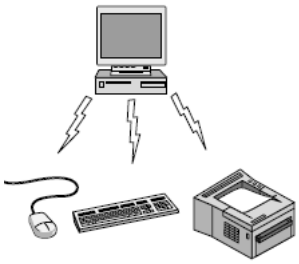
- Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting**.

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

1.2.1 Personal Area Networks (PAN):

- Example: Wireless network that connects a computer with its peripherals (monitor, keyboard, mouse, and printer).
- The short-range wireless technology used in this case is **Bluetooth**.
- Bluetooth networks use the master-slave paradigm.
- System unit (the PC) is normally the master, talking to the mouse, keyboard, etc., as slaves.
- The master jobs are to:
    1. Tells the slaves what addresses to use.
    2. When they can broadcast.
    3. How long they can transmit.
    4. What frequencies they can use.



1.2.2 Local Area Networks (LAN):

- A LAN is a privately owned network.
- LAN network 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:
    1. Let them share resources (e.g., printers).
    2. Exchange information.
- When LANs are used by companies, they are called **enterprise networks**.
- LAN network operates within and nearby a single building like a home, office or factory.
- Wireless LANs are very popular these days, especially in homes, older office buildings, **Why not the wired network?** Too much trouble to install cables.
- In **Wireless LANs**, every computer has a **radio modem** and **an antenna** that it uses to:
    1. Communicate with other computers.
    2. In most cases, each computer talks to a device in the ceiling called an **AP (Access Point), wireless router, or base station.**

- What (AP, Router, Base Station) for? Relays packets between the wireless computers and also between them and the Internet.
- If other computers are close enough, they can communicate directly with one another in a peer-to-peer configuration.
- There is a standard for wireless LANs called **IEEE 802.11**, popularly known as **WiFi.**
- WiFi runs at speeds anywhere from 11 to hundreds of Mbps.
- **Wired LANs** use a range of different transmission technologies. Most of them use **copper wires**, but some use **optical fiber**.
- Wired LANs advantages:
    1. Run at speeds of 100 Mbps to 1 Gbps, newer LANs can operate at up to 10 Gbps.
    2. Have low delay (microseconds or nanoseconds).
    3. Make very few errors.
- Compared to wireless networks, wired LANs exceed them in all dimensions of performance.
- LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing these bounds helps with the task of designing network protocols.
- The topology of many wired LANs is built from point-to-point links.
- Must common type of wired LAN is **Ethernet**.

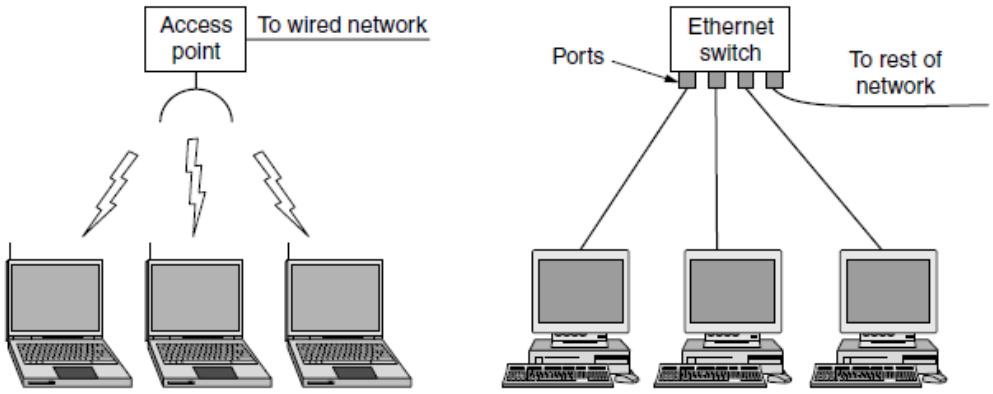
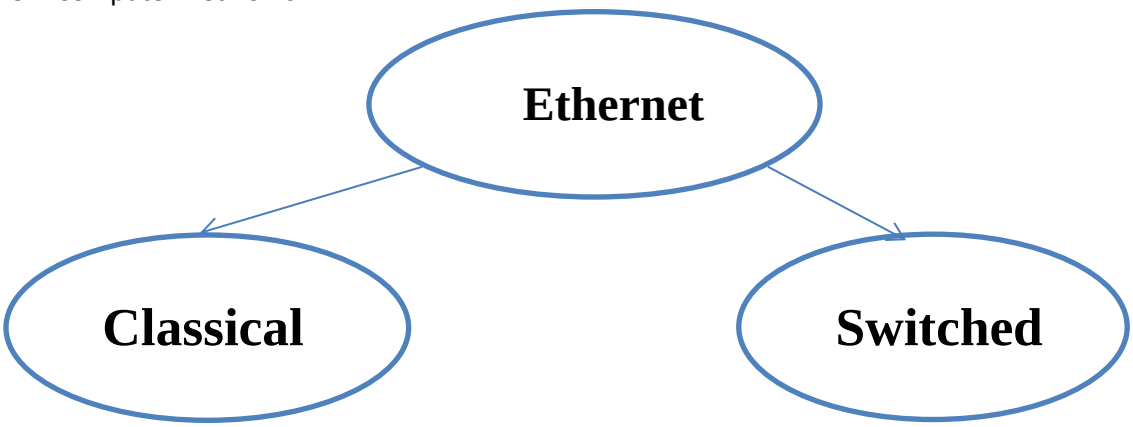


Figure 1-8. Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.



- Broadcast all the packets over a single linear cable.
- At most one machine could successfully transmit at a time.
- Distributed arbitration mechanism was used to resolve conflicts.
- This mechanism used a simple algorithm:
    1. Computers could transmit whenever the cable was idle.
    2. If two or more packets collided, each computer just waited a random time and tried later.

- Each computer connects to a box called a **switch** with a point-to-point link.
- A switch has multiple ports, each of which can connect to one computer.
- The job of the switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to.
- To build larger LANs, switches can be plugged into each other using their ports.
- What happens if you plug them together in a loop? The Algorithms will always solve any hardware possible problem.
- It is also possible to divide one large physical LAN into two smaller logical LANs by logical switches implemented by the SW and that's called **Virtual LAN** or **VLAN.**

- Both wireless and wired broadcast networks can be divided into **static** and **dynamic** designs, depending on **how the channel is allocated**.

Dynamic Allocation

Centralized

- A device in the middle of all computers which determines who goes next.
- The device might do this by accepting multiple packets and prioritizing them according to some internal algorithm.

Decentralized

- There is no central entity.
- Each machine must decide for itself whether to transmit.
- You might think that this approach would lead to chaos, but it does not. And that's because of the algorithm of course.

Static Allocation

- Static allocation would be to **divide time into discrete intervals** and use a round-robin algorithm, allowing each machine to broadcast only when its time slot comes up.
- This method disadvantage is the channel capacity waste when a machine has nothing to say during its allocated slot.
- Most systems attempt to allocate the channel dynamically

- LANs Advantages:
  1. It is likely that every appliance in the home will be capable of communicating with every other appliance, and all of them will be accessible over the Internet and this makes life easier.
  2. AND Help aging parents live safely in their own homes.

- LANs Disadvantages:
  1. The networked devices have to be very easy to install.
  2. The network and devices have to be foolproof in operation, and this not possible and the user will need to hire a technical in case of developing or fixing.
  3. It costs a lot.
  4. Security and reliability.

- Wired LAN is better because it is more secure.
- A third option is to use **Power-line networks** which will be provided by the internet connection by connecting any devices in the Network as TV.
- The difficulty is how to carry both power and data signals at the same time? Part of the answer is that they use different frequency bands.

1.2.3 Metropolitan Area Networks (MAN):

1. MANs cover a region of city**.**
2. Example: the cable television networks available in many cities.
3. Television signals and Internet being fed into the centralized **cable headend** for subsequent distribution to people's homes.
4. Cable television is not the only MAN, though. Recent developments in high speed wireless Internet access have resulted in another MAN, which popularly known as **WiMAX**.

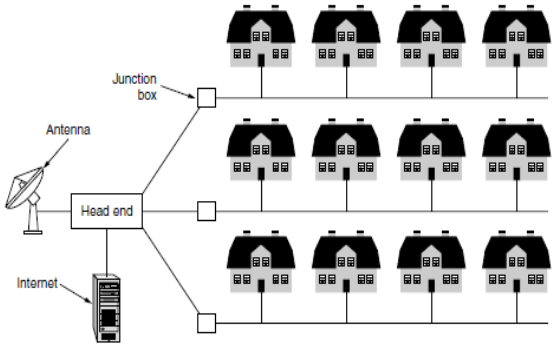


Figure 1-9. A metropolitan area network based on cable TV.

1.2.4 Wide Area Networks (WAN):

- Spans a large geographical area, often a country or continent.

Wired WANs

- Example: Company with its branches.
- Wired WANs consist of:
  1. Hosts: Computers.
  2. Subnets: transmission lines, switching elements.
- Subnets are collection of routers and communication lines that moved packets from the source host to the destination host.
- The job of the subnet is to carry messages from host to host, just as the telephone system.

Transmission lines

- Move bits between Machines.
- Examples: Copper, Optical Fiber.

Switching elements

- They are specialized computers that connect two or more transmission lines.
- Examples: Switches, routers.

Wireless WANs

- Example: Satellite System, cellular telephone network.
- In Satellite system each computer on the ground has an antenna through which it can send data to and receive data from to a satellite in orbit.
- Each cellular base station covers a distance much larger than a wireless LAN, with a range measured in kilometers rather than tens of meters.
- The base stations are connected to each other by a backbone network that is usually wired.
- The data rates of cellular networks are often on the order of 1 Mbps, much smaller than a wireless LAN that can range up to on the order of 100 Mbps.

5. Differences between LANs and WANs:
   - Usually in a WAN, the hosts and subnet are owned and operated by different people.
   - In WAN, routers will usually connect different kinds of networking technology.
   - A final difference is in what is connected to the subnet This could be:
     1. Individual computers, as was the case for connecting to LANs.
     2. Or it could be entire LANs.

- There are two varieties of WANs:
    1. Rather than lease dedicated transmission lines, a company might connect its offices to the Internet **(Virtual Private Network – VPN).** The advantages of this it provides flexible reuse of a resource (Internet connectivity).

    2. That the subnet may be run by a different company. The subnet operator is known as a **network service provider.** The subnet operator will also connect to other networks that are part of the Internet. Such a subnet operator is called an **ISP (Internet Service Provider).**

6. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, **via other routers**.
7. There may be many paths in the network that connect these two routers. How the network makes the decision as to which path to use? The network uses algorithms to solve such a problem such as:
    1. Routing algorithm: makes the decision as to which path to use.
    2. Forwarding algorithm: How each router makes the decision as to where to send a packet next.

1.2.5 Internetworks

Differences between Subnets, networks, and internetworks:

- **Subnets**: refers to the collection of routers and communication lines owned by the network operator.
- **Networks**: is formed by the combination of a subnet and its hosts.
- **Internetworking**: collection of computers interconnected by a single technology or connecting WANs or LANs with WANs under some conditions.
    1. If different organizations have paid to construct different parts of the network and each maintains its part.
    2. The underlying technology is different in different parts (e.g., broadcast versus point-to-point and wired versus wireless).

Gateway: a machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software.

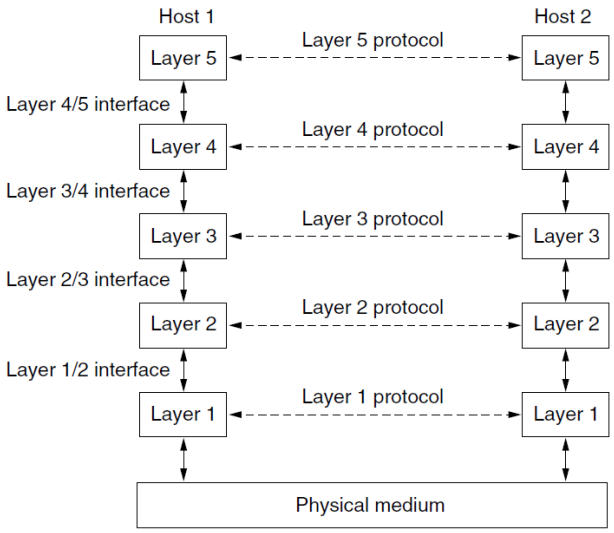
1.3 Network Software:

- The first computer networks were designed with the **hardware as the main concern** and the software as an afterthought.
- Network software is now highly structured.

1.3.1 Protocol Hierarchies:

- Most networks are organized as a stack of **layers** or **levels**, each one built upon the one below it.
- Each network can be distinguished from other networks by several features:
    - The number of layers.
    - The name of each layer.
    - The contents of each layer.
    - And the function of each layer.
- The purpose of each layer is to offer certain services to the higher layers.
- Information hiding is to provide a service by HW or SW to its users but keeps the details of its internal state and algorithms hidden from them. For instance,
    - Abstract data types.
    - Data encapsulation.
    - Object-oriented programming.

- The information hiding mechanism is also valid in networks field as each network divided into layers and each layer shielding from the details of how the offered services are actually implemented.
- **Protocol** is an agreement between the communicating parties on how communication is to proceed.
- **Peers** are (human, SW, HW) who are communicating by using the protocol to talk to each other.
- **Virtual communication** is the communication between layer n from any network and the layer n in any other network.
- No data are directly transferred from layer n on one machine to layer n on another machine.
- Each layer passes data and control information to the layer immediately below it.
- Below last layer is **the physical medium** through which actual communication occurs.
- **Interface** defines which primitive operations and services the lower layer makes available to the upper one.
- How to make it simpler to replace one layer with a completely different protocol or implementation?
    1. Minimizing the amount of information that must be passed between layers.
    2. Clear-cut interfaces (defining clean interfaces between the layers).



- Different hosts use different implementations of the same protocol.
- The protocol can change in some layer without the layers above and below it even noticing.
- **Network architecture** is a set of layers and protocols.
- The specification of 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.
- Neither the details of the implementation nor the specification of the interfaces is part of the architecture because these are hidden away inside the machines and not visible from the outside.
- It is not necessary that the interfaces on all machines in a network be the same, provided that each machine can correctly use all the protocols.

- **Protocol stack** is a list of the protocols used by a certain system, one protocol per layer.

1.3.2 Design Issues for the Layers:

Reliability | **Network Evaluation** | **Recourse Allocation** | **Security**

- **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.
- Reliability is concerned by very important aspects:
    1. How it is possible that we find and fix these errors that will occur due to fluke electrical noise, random wireless signals, hardware flaws or software bugs?

Error Detection

- Finding errors in received information uses codes
- Information that is incorrectly received can then be retransmitted until it is received correctly.

Error correction

- Where the correct message is recovered from the possibly incorrect bits that were originally received.

- Both of these mechanisms work by adding redundant information.
- Both are used at low layers, to protect packets sent over individual links, and high layers, to check that the right contents were received.

2. How to find a working path through a network. Often there are multiple paths between a source and destination? **Routing**.

Network Evaluation

- There are two main strategies work for the concerns of the evolution of the network:
  1. **Protocol layering**: it supports change by dividing the overall problem and hiding implementation details.
  2. **Addressing** or **naming:** is to identifying the senders and receivers that are involved in a particular message.

- **Scalability** is a feature the Designs will have it if it continues to work well when the network gets larger.

Recourse Allocation

- **Statistical multiplexing** is to share network bandwidth dynamically, according to the short-term needs of hosts or sharing based on the statistics of demand.
- Allocation problem can be:
  1. **Flow control:** the problem that occurs at every level to keep a fast sender from swamping a slow receiver with data and the feedback mechanism from the receiver to the sender is often used.
  2. **Congestion:** oversubscribed because too many computers want to send too much traffic, and the network cannot deliver it all.
- **Quality of service** is the name given to mechanisms that reconcile these competing demands.

Security

- Mechanisms that provide **confidentiality** defend against this threat, and they are used in multiple layers.
- Mechanisms for **authentication** prevent someone from impersonating someone else. They might be used to tell fake banking Web sites from the real one.
- Mechanisms for **integrity** prevent surreptitious changes to messages.

1.3.3 Connection-Oriented Versus Connectionless Service:

- Layers can offer two different types of service:

Connection-oriented

- Modeled after the telephone system.
- to use a connection-oriented service:
1. Establish the connection.
2. Use the connection.
3. Release the connection.

- It acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end.

- **Negotiation** can happens in the beginning about the parameters to be used, such as maximum message size, quality of service required, and other issues.
- One side makes a proposal and the other side can accept it, reject it, or make a counterproposal.

Connectionless

- Modeled after the postal system.
- Each message carries the full destination address.
- Each one is routed through the intermediate nodes inside the system.
- **Store-and-forward switching** is when nodes receive a message in full before sending it to the next node.

- **Cut-through switching** is when transmission of a message at a node starts before it is completely received by the node.
- When two messages are sent to the same destination, the first one sent will be the first one to arrive.

- Each kind of service can further be characterized by its reliability.

- A reliable service is implemented by having the receiver acknowledge the receipt of each message so the sender is sure that it arrived.
- Reliable connection-oriented service has two minor variations:
1. Message sequences: There is a need for boundaries between messages
2. Byte streams: There is **NO** need for boundaries between messages.

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

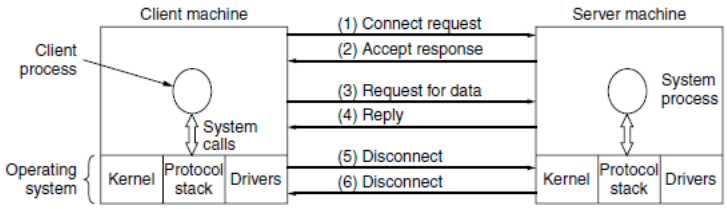
- A reliable service is implemented by having the receiver acknowledge the receipt of each message so the sender is sure that it arrived.
- For some applications, the transit delays introduced by acknowledgements are unacceptable such voice over IP.
- **Datagram:** Unreliable (meaning not acknowledged) connectionless service.
- **Acknowledged datagram:** Reliable connectionless service.
- **Request-Reply service:** this service the sender transmits a single datagram containing a request; the reply contains the answer.

1.3.4 Service Primitives:

- **Primitives** (operations) specify the services by a set of available to user processes to access the service. They tell the service to perform some action or report on an action taken by a peer entity.
- The primitives for connection-oriented service are different from those of connectionless service and they depend on the nature of the service being provided.
- The table describes the primitives of the connection-oriented services.

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

- These primitives might be used for a request-reply interaction in a client-server environment.



- Protocol stack is located in the operating system; the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.

1.3.5 The Relationship of Services to Protocols:

- Services and protocols are distinct concepts.
- *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.

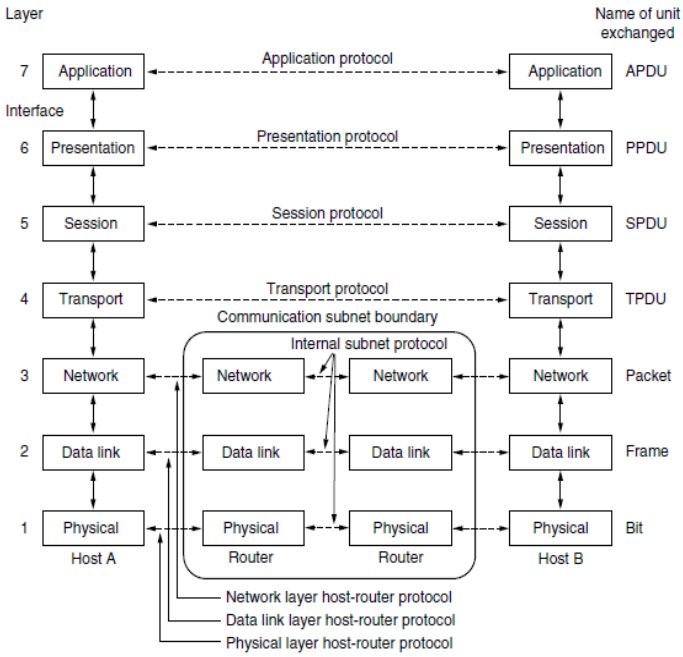
- *Protocol* is:
  - A set of rules governing the format and meaning of the packets.
  - Or messages that are exchanged by the peer entities within a layer.
  - Entities use protocols to implement their service definitions. They are free to change their protocols at will, provided they do not change the service visible to their users.

1.4 REFERENCE MODELS:

- There are two important network architectures that we going to study:
  1. **OSI reference model**: it isn't used any more, the model itself is actually quite general and still valid.
  2. **TCP/IP reference model:** it has the opposite properties, the model itself is not of much use but the protocols are widely used.

1.4.1 The OSI Reference Model:

- Model is based on a proposal developed by the International Standards Organization (ISO).
- The model is called the ISO OSI (Open Systems Interconnection) because it deals with connecting open systems.
- Connecting open systems is systems that are open for communication with other systems.
- The principles that were applied to arrive at the final network architecture are:
  1. A layer should be created where a different abstraction is needed.
  2. Each layer should perform a well-defined function.
  3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
  4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
  5. The number of layers **should be large enough** that distinct functions need not be thrown together in the same layer out of necessity and **small enough** that the architecture does not become unwieldy.



- Note that the OSI model itself is not network architecture because it does not specify the exact services and protocols to be used in each layer.

Physical Layer

- Concerned with transmitting raw bits over a communication channel.

Data Link Layer

- 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 transmits the frames sequentially.
- Possible issues May face this layer:
  1. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an **acknowledgement frame.**
  2. How to keep a fast transmitter from drowning a slow receiver in data? By some algorithms that let the transmitter know when the receiver can accept more data.
  3. How to control access to the shared channel in the broadcast networks? **Medium access control** sub-layer deals with this problem.

Network Layer

- The **network layer** controls the operation of the subnet.
- Possible issues May face this layer:
    1. How packets are routed from source to destination?
        a. Routes can be based on static tables that are ‘‘wired into’’ the network and rarely changed.
        b. Or they can be updated automatically to avoid failed components.
        c. They can also be determined at the start of each conversation.
        d. They can be highly dynamic, being determined anew for each packet to reflect the current network load.
    2. Handling congestion (sending too many packets in the same time)?
    3. The quality of service provided (delay, transit time...).
    4. The probability of using differ protocols between networks.

Transport Layer

- **Transport layer** is to:
    1. Accept data from above it.
    2. Split it up into smaller units if need be.
    3. Pass these to the network layer.
    4. Ensure that the pieces all arrive correctly at the other end.
    5. Determines what type of service to provide to the session layer.
- There are two types of transport connection which are:
    1. **Error-free point-to-point channel** that delivers messages or bytes in the order in which they were sent.
    2. Transporting of isolated messages **with no guarantee about the order of delivery**, and the broadcasting of messages to multiple destinations.
- The type of service is determined when the connection is established.
- The transport layer is a true end-to-end layer; it carries data all the way from the source to the destination.

Session Layer

- The session layer allows users on different machines to establish **sessions** between them.
- Services that are offered by this layer:
    1. **Dialog control** (keeping track of whose turn it is to transmit).
    2. **Token management** (preventing two parties from attempting the same critical operation simultaneously).
    3. **Synchronization** (check-pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).

Presentation Layer

- **Presentation layer** is concerned with the syntax and semantics of the information transmitted.
- The presentation layer manages abstract data structures and allows higher-level data structures to be defined and exchanged.

Application Layer

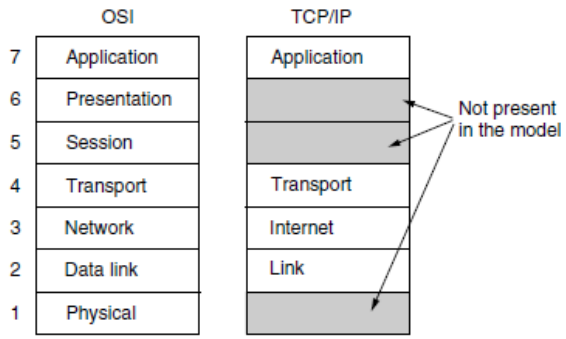
- Contains a variety of protocols that are commonly needed by users.
- Example: HTTP.
- HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide.
- The importance of HTTP appears when a browser wants a Web page, it sends the name of the page it wants to the server hosting the page using HTTP. The server then sends the page back.
- Other application protocols are used for:
    1. File transfer.
    2. Electronic mail.
    3. Network news.

1.4.2 The TCP/IP Reference Model:

- It is a **Packet-switching network** based on a connectionless layer that runs across different networks.

Link Layer

- Describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.



Internet Layer

- The linchpin that holds the whole architecture together.
- Its job is to permit hosts to inject packets into any network and have they 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.
- Examples of these protocols in this layers:
    - **IP (Internet Protocol).**
    - Companion protocol called **ICMP (Internet Control Message Protocol)** that helps it function.
- Possible issues May face this layer:
    1. Packet routing.
    2. Congestion.

Transport Layer

- It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer.
- Two end-to-end transport protocols have been defined here:
    1. **TCP** (**Transmission Control Protocol**) is a **reliable connection-oriented** protocol that allows **a byte stream** originating on one machine to be delivered without error on any other machine in the internet.
    2. **UDP (User Datagram Protocol),** is an **unreliable, connectionless** protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.

- It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery.

Application Layer

- The TCP/IP model does not have session or presentation layers.
- Application layer simply include any session and presentation functions that they require.
- This layer contains many protocols such as:
  - File transfer (FTP).
  - Electronic mail (SMTP).
  - Domain Name System (DNS).

1.4.3 The Model Used in This Book:

- The strength of **the OSI reference model** is the **model** itself and the strength of the **TCP/IP reference model** is the **protocols** so, we will use the hybrid model.
- **The physical layer** specifies how to transmit bits across different kinds of media as electrical (or other analog) signals.
- **The link layer** is concerned with how to send finite-length messages between directly connected computers with specified levels of reliability.
- Examples of its protocols: Ethernet and 802.11.
- **The network layer** deals with how to combine multiple links into networks, and networks of networks.
- Examples of its protocols: IP protocol.
- **The transport layer** strengthens the delivery guarantees of the Network layer, usually with increased reliability, and provides delivery abstractions.
- Examples of its protocols: TCP.
- **The application layer** contains programs that make use of the network. Many, but not all, networked applications have user interfaces, such as a Web browser.
  - Examples of its protocols: HTTP.

5	Application
4	Transport
3	Network
2	Link
1	Physical

1.4.4 A Comparison of the OSI and TCP/IP Reference Models:

In Common

- Both are based on the concept of a stack of independent protocols.
- The functionality of the layers is roughly similar.
- In both models, the layers above transport are application-oriented users of the transport service.

Differences

- Three concepts are central to the OSI model:
  1. Services.
  2. Interfaces.
  3. Protocols.

1.4.5 A Critique of the OSI Model and Protocols:

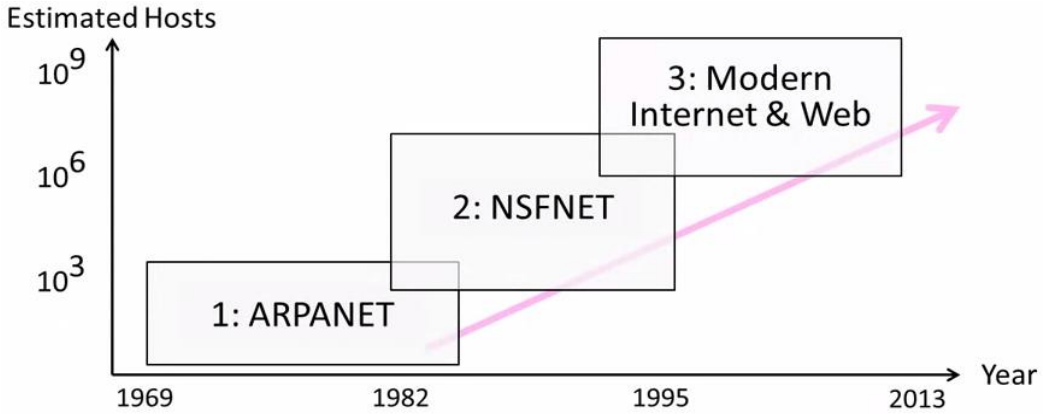
- It appeared for many experts in the field that the OSI model and its protocols were going to take over the world and push everything else out of their way. This did not happen. Why?
  1. Bad timing.
  2. Bad technology.
  3. Bad implementations.
  4. Bad politics.

1.4.6 A Critique of the TCP/IP Reference Model:

1. The model does not clearly distinguish the concepts of services, interfaces, and protocols.
2. The TCP/IP model is not at all general and is poorly suited to describing any protocol stack other than TCP/IP.
3. The link layer is not really a layer at all in the normal sense of the term as used in the context of layered protocols.
4. The TCP/IP model does not distinguish between the physical and data link layers.
5. The IP and TCP protocols were carefully thought out and well implemented, many of the other protocols were ad hoc, generally produced by a couple of graduate students hacking away until they got tired.

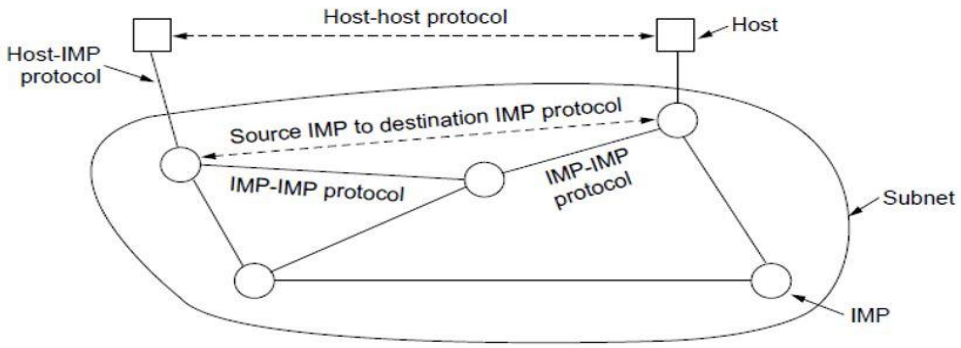
1.5 Example Networks:

1.5.1 Internet



1.5.1.1 ARPANET "a precursor to the internet"

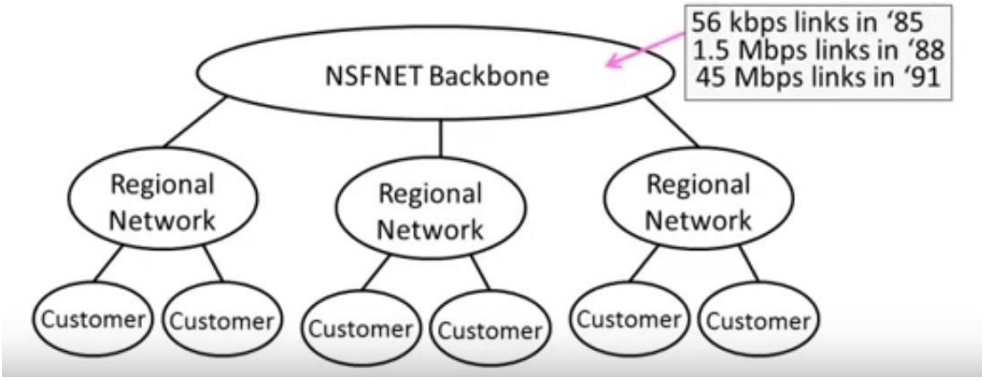
- Based on **switching techniques** "**the structure of telephone system**" developed by Kleinrock-Davies, and **decentralized control concept** developed by Baran. @1960
- Earlier design @1969, consisted of **4 connected nodes**. Motivated for **resources sharing**, by DoD, USA.
  - First application was **mail**.
- @1974, Cerf-Kahn deployed the **TCP/IP protocols** for usage instead of internetworking, as it was hard to build a concrete technology "network" using different networking techniques.
  - Easier for deployment, just setting up the new host. Thus, #of host increased rapidly.



The original ARPANET design

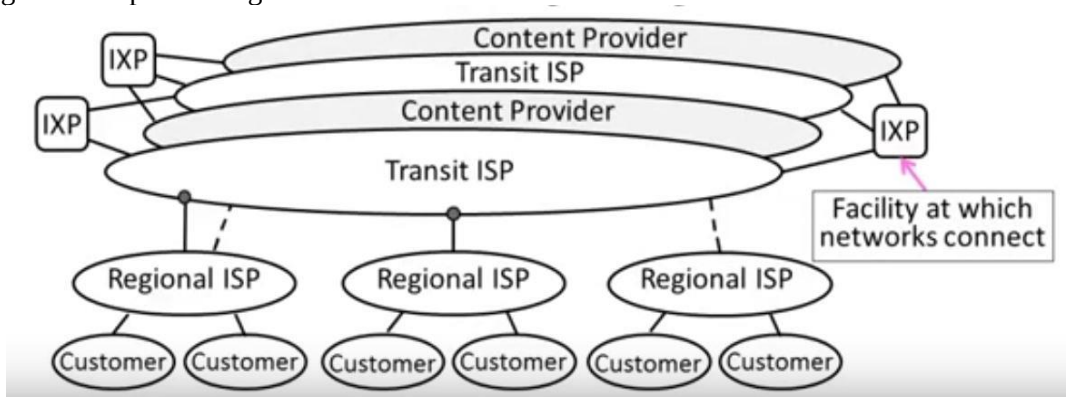
1.5.1.2 NSFNET

- NSFNET'85: supported **educational** and **research networks**. Initially supercomputer sites, later it became the backbone network.
- Classic internet protocol raised up as a consequence,
  - TCP: Transport, - DNS: Naming, - Berkeley Socket: API,
  - BGP: Routing.
- Later, it evolved to the PCs and Ethernet LANs.



1.5.1.3 Modern Internet

- Large competitor ISPs "Internet Service Providers" connected to IXP "Internet eXchange Point" facilities.
- Large content providers got connected to the IXPs.



- Web launched, needed to develop Content Distribution Networks "CDNs".
- As most transferred bits are video streams, we went through Wireless.

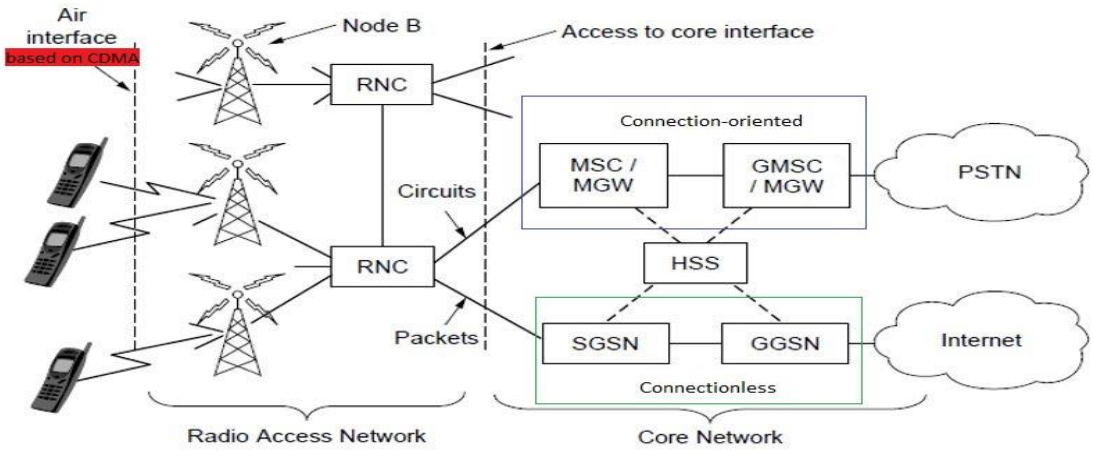
1.5.2 Mobile

1.5.2.1 1G technology Released @1982, serviced an **analog voice** communication, defined by **AMPS**.

1.5.2.2 2G technology Released @1991, serviced a **digital voice** communication supporting higher capacity and text messages, defined by **GSM**.

1.5.2.3 3G technology Released @2001, services a **digital voice** communication + **broadband digital data**, defined by **ITU**.

- Supports stationary and walking users @2Mbps & moving vehicles @384Kbps.
- By using **UMTS** "Universal Mobile Telecommunication System" (**WCDMA** "Wideband Code Division Multiple Access"), we reached 14Mbps for downstreaming & 6Mbps for upstreaming.
- Was based on **Antennas** & **Radios**, where each operator (provider) shall buy a license of portion of **radio spectrum** to transmit on. But, radio spectrum is narrow (limited bandwidth).
- Then, we deployed **Cellular network** where each coverage area is divided to cells each have a base station. Within a cell, users are assigned **different channels** so no interference occurs. This allows **spectrum reusability**.



Architecture of the UMTS 3G mobile phone network.

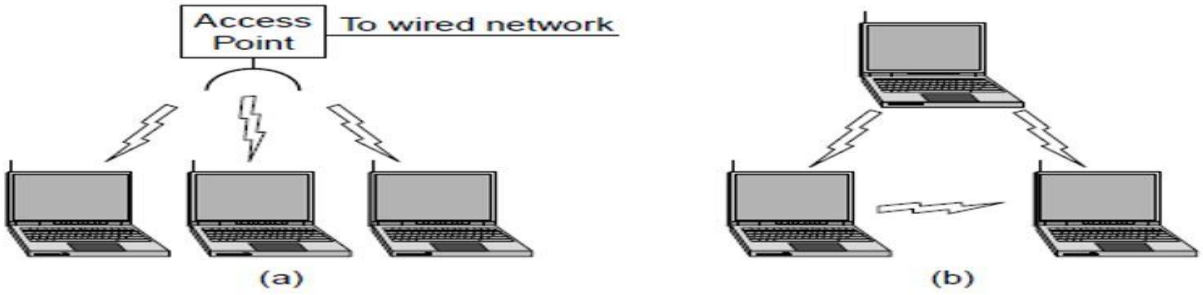
- Support mobility & network handover/handoff between cellular base stations:
  - Soft handover, like in CDMA based network where user connect to new station before disconnecting the old one.
  - Hard handover, user disconnect old station then connect to the new one.
- Components:
  - Radio Network Controller "RNC", to control how the spectrum is used.
  - Core Network, control traffic transmission.
    + Connection-oriented: circuit switching [MSC ⟶ GMSC ⟶ PSTN].
    + Connectionless: packet switching [SGSN ⟶ GGSN ⟶ Internet].
  - HSS "Home Subscriber Server", to localize and profile user's info for authentication & authorization.

1.5.2.3 4G technology an advance of 3G defined by LTE "Long Term Evolution" technology.

➢ **Note that,** 2G and further technologies depended on a handset "device" + a SIM (Subscriber Identity Module) chip.

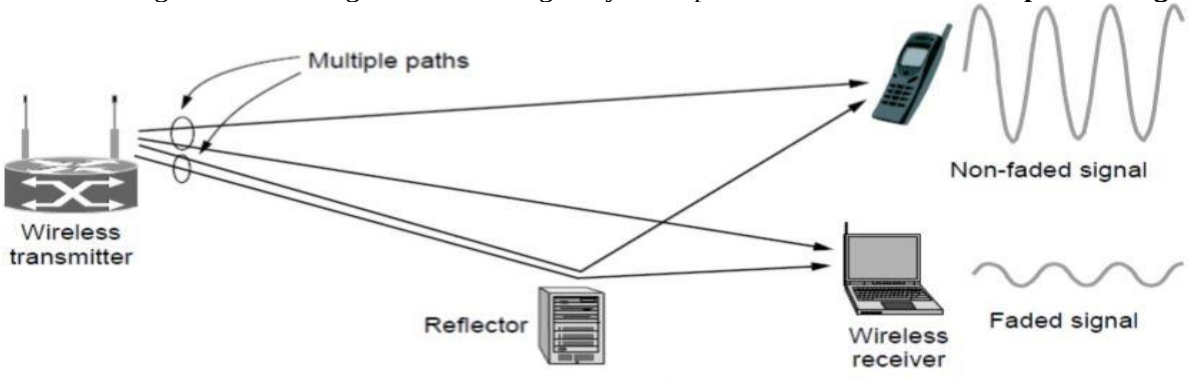
1.5.3 Wireless 802.11

- Earlier, each company had its radio brand/protocol, and no 2 of the brands were compatible.
- @1990s, standard wireless 802.11 "Wi-Fi" was released. [Why ".11"? as LAN standards ".1 ~ .10"]
  - We needed to find a worldwide available frequency band, so used the (unlicensed bands) **ISM** "Industrial-Scientific-Medical" with ranges [902~928MHz, 2.4~2.5GHz, 5.725~5.825GHz].
- Wireless network consists of clients (computers) + infrastructure "Base point/Access point" connected to the network.
  - Can be utilized to ad-hoc connection between clients, if they're close to each other.



(a) Wireless network with an access point.
(b) Ad hoc network.

- Frequencies used, radio signals can be reflected off solid objects so that multiple echoes of a transmission may reach a receiver along different paths. The echoes can cancel or reinforce each other, causing the received signal to oscillate greatly. This phenomenon is called **multipath fading**.

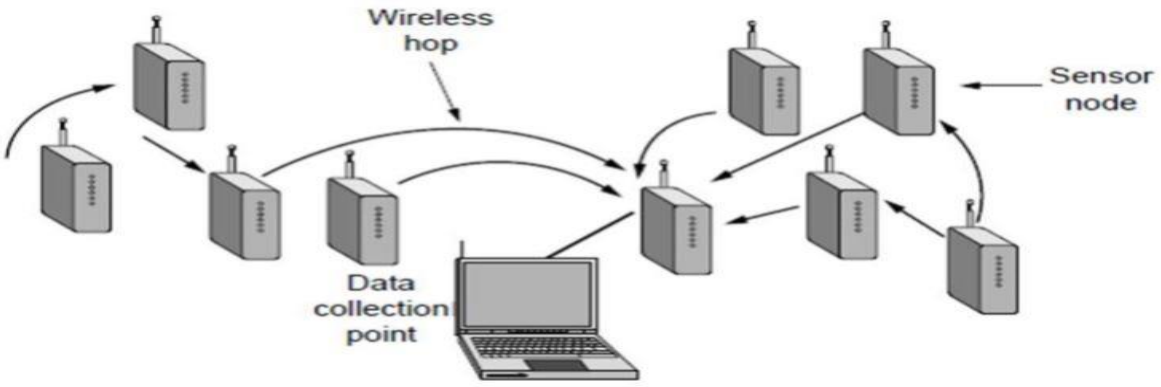


Multipath fading

- 802.11a (@1999) and 802.11g (@2003) standards used **OFDM** (Orthogonal Frequency Division Multiplexing) modulation. It divides a wide band of spectrum into many narrow slices over which different bits are sent in parallel, so they can avoid path diversity.
- CSMA "Carrier Sense Multiple Access" technique is used to **avoid collision**, with ALOHA extension to make users wait random intervals before retransmission.
- Multi-connected cells networks using **Ethernet switching** are deployed to avoid **handoff** problem.
- For extra security, we use WEP & WPA2 encryption techniques.

1.5.4 RFID "Radio Frequency IDentification"

- Tags on objects to be tracked.
  - Active: power source @tag.
  - Passive: power source @reader.
- Designed according to usage within different frequencies:
  - UHF (902~928MHz band): driving licenses, shipments.
  - HF (~13.56MHz): credit cards.
  - LF: animal tracking, Like in Sensors Network using multi-hops design.



Multihop topology of a sensor network

- It suffers collision, multiple correspondence, and privacy tracking & invasion.

1.6 Network Standardization:

Networking standards define the rules for data communications that are needed for interoperability of networking technologies and processes. Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.
During data communication, a number of standards may be used simultaneously at the different layers. The commonly used standards at each layer are:

1. **Application layer :** HTTP, HTML, POP, H.323, IMAP
2. **Transport layer:** TCP, SPX
3. **Network layer:** IP, IPX
4. **Data link layer:** Ethernet IEEE 802.3, X.25, Frame Relay
5. **Physical layer:** RS-232C (cable), V.92 (modem)

- **Types of standards:**

1. **De facto:** These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP had started as a de facto standard.
2. **De jure:** These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

- **Standards Organizations:**

1. International Standards Organization (ISO)
2. International Telecommunication Union (ITU)
3. Institute of Electronics and Electrical Engineers (IEEE)
4. American National Standards Institute (ANSI)
5. Internet Research Task Force (IETF)
6. Electronic Industries Association (EIA)

Please refer to the summary section in reference.

Sheet (1) Answers

Ex.1:

1- Better interactive interfaces, easy to connect.
2- Easy growing up.
3- More reliable, multiple points of failure.
4- Cheaper.

Ex.2: probability a host transmits = p, probability a host wats = $1 - p$
Here, we have 3 options to occur:

- One host transmits, others wait -> $P_w = n * p * (1-p)^{n-1}$
- All host wait -> $P_w = (1-p)^n$;
- Collision occurs -> P_c

$$P_c = 1 - [P_w + P_w] = 1 - [n * p * (1-p)^{n-1} + (1-p)^n]$$

Ex.3:

Advantages:

1- Break-up problems is system to minor problems.
2- Define a standard communication method “protocol”.
3- Change the protocols without affecting upper or lower layers.

Disadvantages:

1- Low performance, due to limited bandwidth against the overload on data by adding extra headers at each layer.
2- Low reliability, due to faults or delays in each layers.

Ex.4:

No, they totally different.

- A message stream is used when we need to keep track of “know” exact boundaries of a message. ex.: file sharing.
- A byte stream is used when there’s no need to know the boundaries or we just read the message as a block, ex.: movies download “torrent”.

Ex.5: $M - byte$ message, n layers, $h - byte$ header/layer

$$total\ size\ of\ message\ = M\ +\ n * h(bytes)$$

$$fraction\ of\ headers\ = \frac{n*h}{M + n*h}$$

Ex.6:

- TCP "**T**ransmission **C**ontrol **P**rotocol": connection-oriented
- UDP "**U**ser **D**atagram **P**rotocol": connectionless

Ex.7:

- Packet-by-packet acknowledgements: are used if we suspect the reliability of a network, and it tends to lose data.
- One acknowledgment at end: if network is reliable, and we want to save bandwidth.

Ex.8:

- Bad view: gives too much info. about user, which is insecurity and may used against user either through government or hackers.
- Good view: offers help to user in emergencies, and supports user's network via different transmission towers.

Ex.9:

$1600 \times 1200\ pixels, 3\ bytes/pixel = 3 \times 8\ bits/pixel$

$$total\ image\ size\ = 1600 \times 1200 \times 3 \times 8 =\ 46{,}080{,}000\ bits$$

$$t_{delay}\ = \frac{images\ size}{network\ speed}$$

@$56 - kbps$channel: $t_{delay}\ = \frac{46{,}080{,}000}{56{,}000} =\ 822.857\ sec.$

@$56 - kbps$channel: $t_{delay}\ = \frac{46{,}080{,}000}{1{,}000{,}000} =\ 46.08\ sec.$

@$56 - kbps$channel: $t_{delay}\ = \frac{46{,}080{,}000}{10{,}000{,}000} =\ 4.608\ sec.$

@$56 - kbps$channel: $t_{delay}\ = \frac{46{,}080{,}000}{100{,}000{,}000} =\ 0.4608\ sec.$

@$56 - kbps$channel: $t_{delay}\ = \frac{46{,}080{,}000}{1{,}000{,}000{,}000} =\ 46{,}08\ msec.$

Ex.10:

Advantages:

- Communications easier, as it's used by all users.
- Have economical benefits, as it's standardized and n need to develop several protocols.

Disadvantages:

- Hard to change or replace by another developed one.
- Poor standards due to the frequent archiving with political compromises and restrictions.

Ex.11:

No changes occur, as implementation changing doesn't affect services provided by a layer to the upper one.