Systems and Control Eng. Dept.

Computer Networks

Fourth Year Class

Lecture 1

Fundamentals of Data Networks

Abdulhameed N. Hameed

Chapter 1: Introduction

Introduction

- Data communications and networking
  - Change the way we do business and the way we live
  - Business decisions have to be made more quickly
  - Decision depends on immediate access to accurate information
  - Business today rely on computer networks and internetworks
  - Before we ask how quickly we can get hooked up, we need to know:
    - How networks operate
    - What types of technologies are available
    - Which design best fills which set of needs

1.1 Data Communications

Communication:

- Means sharing information
  - Local (face to face) or remote (over distance)
- Telecommunication
  - Telephone, telegraph and television
  - Means communication at a distance
  - Tele is Greek for far

Data Communications

Data:

- Refers to information
  - Presented in any form

Data communication : is the exchange of data between two devices via some form of transmission medium (wire cable).

Data Communications

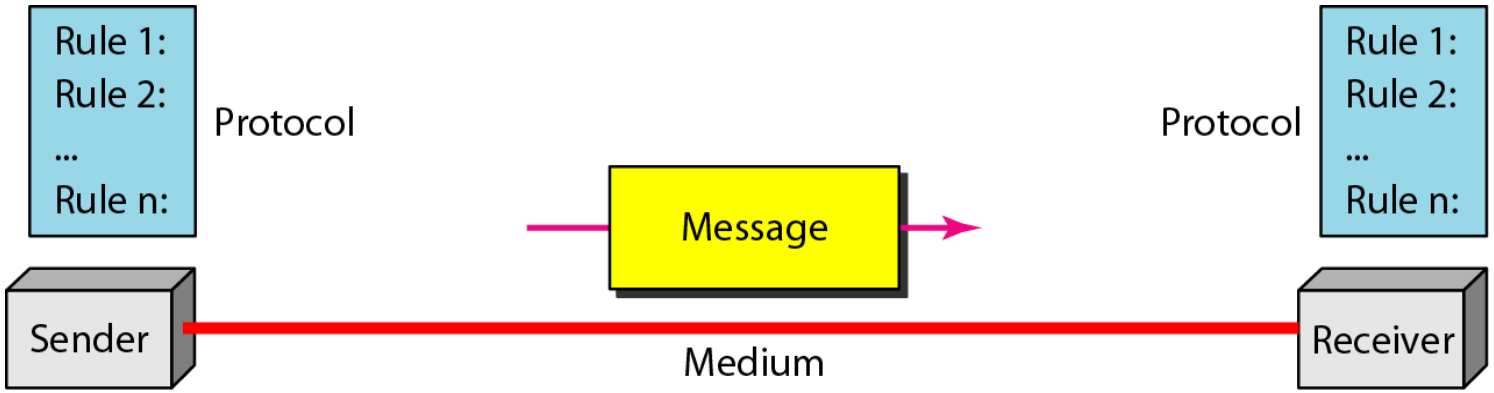
- Communication system made up of a combination of hardware and software
- Effectiveness of data communication system depends on:
  1. Delivery : The system must deliver data to correct destination. Data received by the indented user only
  2. Accuracy: The system must deliver data accurately (no change).
     - Data changed & uncorrected is unusable

Data Communications

3. Timeliness: The system must deliver data in timely manner
   - Data arrived late are useless
   - In the same order (video and audio) & without delay (Real time transmission).
4. Jitter: Variation in the packet arrival time (uneven quality in the video is the result).

Components

- A data communication system is made up of five components

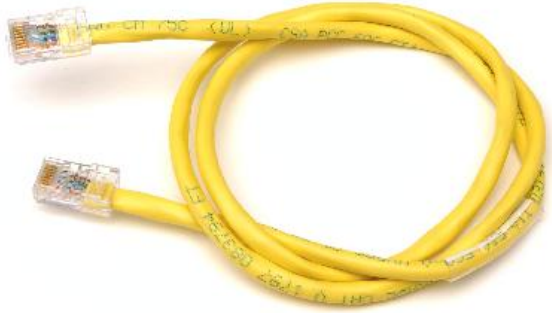


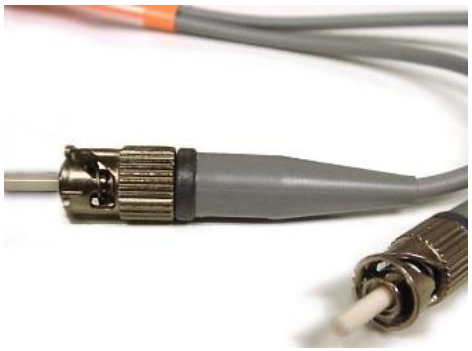
Components

1. Message: the information (data) to be communicated
   - Consist of text, numbers, pictures, audio, or video
2. Sender: the device that sends the data message
   - Computer, workstation, telephone handset, video camera, …
3. Receiver: the device that receives the message
   - Computer, workstation, telephone handset, television, ….

Components

4. Medium: The physical path by which a message travels from sender to receiver
   - twisted pair, coaxial cable, fiber-optic, radio waves

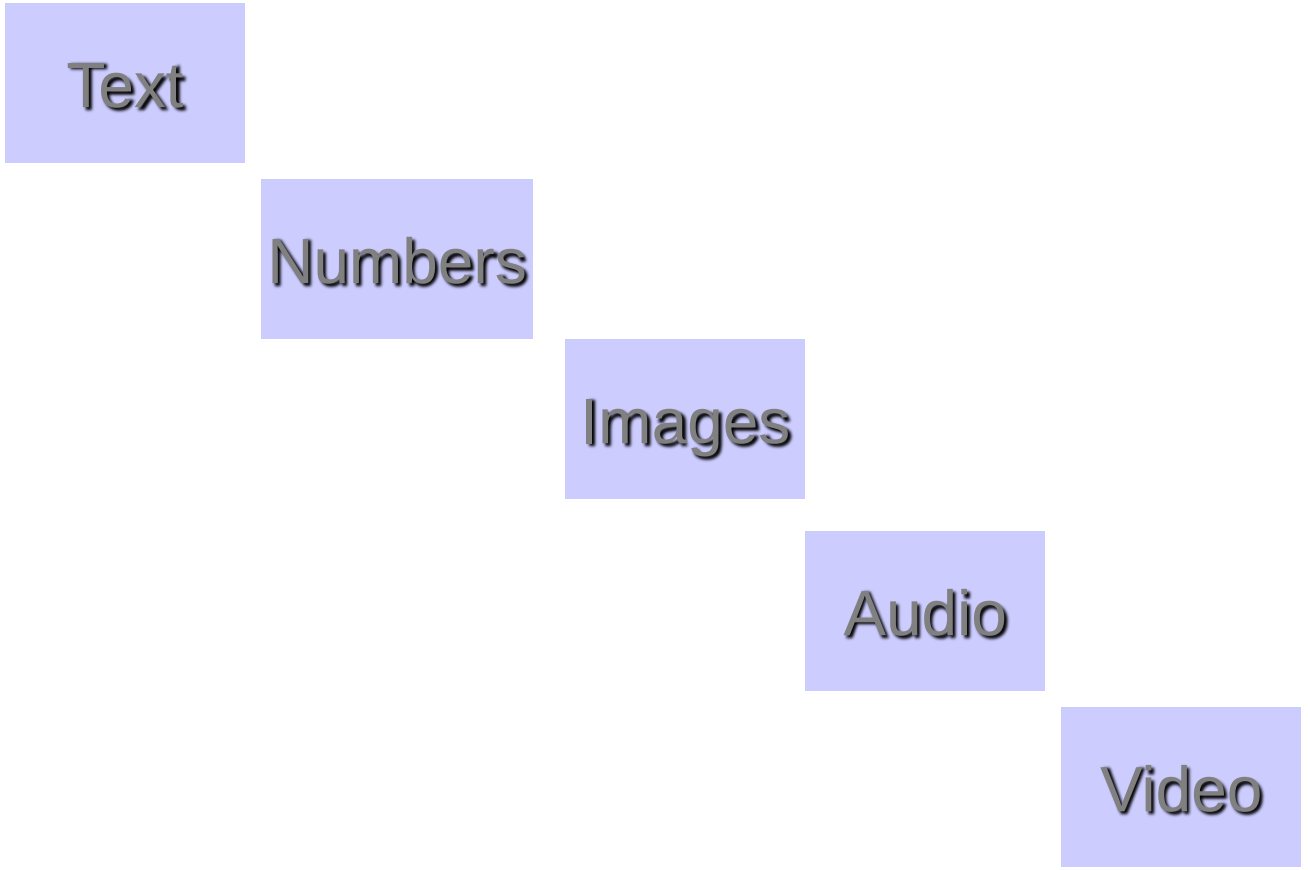




Components

5. Protocol: a set of rules that govern data communications
   - An agreement between the communicating devices
   - Devices may be connected but not communicating (no protocol)
   - Arabic speaker with Japanese speaker

Data Representation



Data Representation

- Text:
  - Sequence of bits (0s or 1s)
  - Different sets of patterns to represent text symbols (each set is called: *code*)
  - Example of coding system is: **Unicode**
  - Unicode uses: 32 bits to represent a symbol or character in any language

Data Representation

- Numbers:
  - Represented by bit patterns
  - The number is directly converted to a binary number.

Data Representation

- Images:
  - Represented by bit patterns
  - A matrix of pixels
  - Resolution: size of the pixels
  - High resolution: more memory is needed
  - Each pixel is assigned a bit pattern
    - 1-bit pattern (black and white dots image)
    - 2-bit pattern (4 levels of gray)
    - RGB (color images)

Data Representation

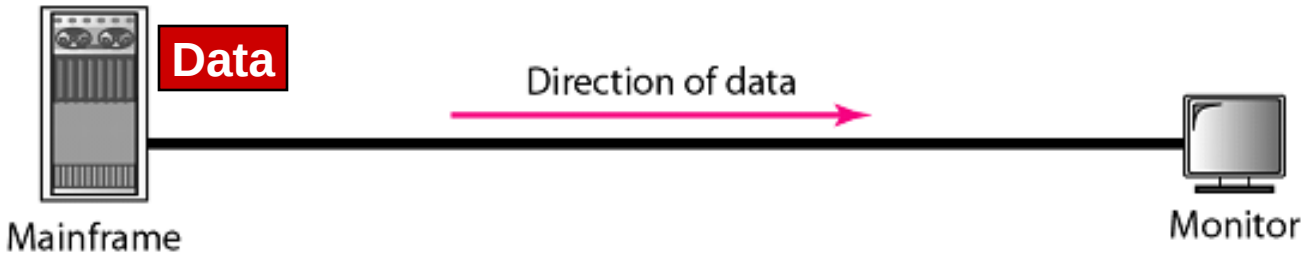
- Audio:
  - Continuous not discrete
  - Change to digital signal
- Video:
  - Recording or broadcasting of a picture or movie
  - Change to digital signal

Data Flow

- Communication between two devices can be:
  - Simplex
  - Half-Duplex
  - Full-Duplex

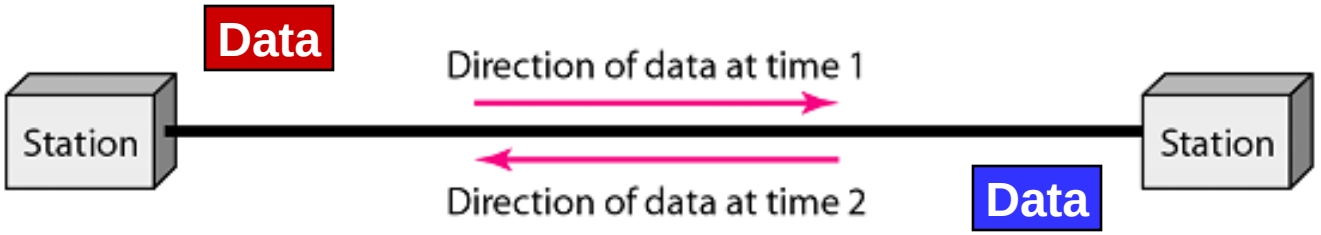
Data Flow

- Simplex (one way street)
  - The communication is unidirectional
  - Only one device on a link can transmit; the other can only receive
  - Use the entire capacity of the channel to send data
  - Example: Keyboards, Monitors



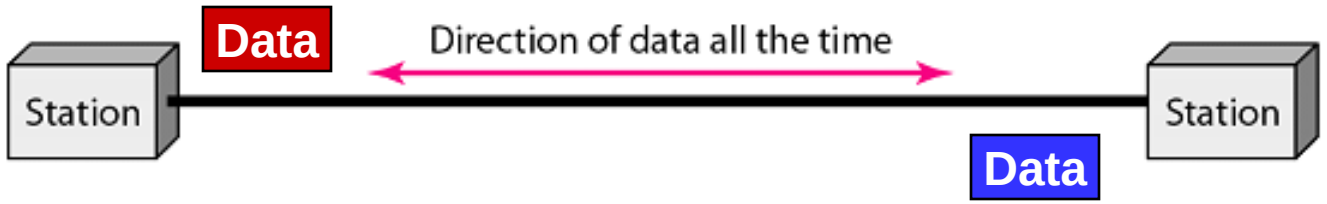
Data Flow

- Half-Duplex (one-lane with two-directional traffic)
  - Each station can both transmit and receive, but not at the same time
  - When one device is sending, the other can only receive, and vice versa
  - The entire capacity of a channel is taken over by the transmitting device
  - Example: Walkie-talkies



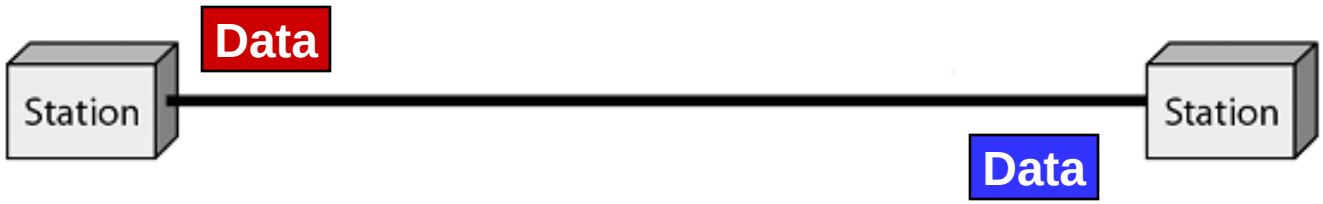
Data Flow

- Full-Duplex (Duplex) (two-way street)
  - Both stations can transmit and receive at same time
  - Signals going in either direction sharing the capacity of the link
  - Sharing can occur in two ways:
    - Link has two physically separate transmission paths
      - One for sending and the other for receiving
    - The capacity of the channel is divided between signals travelling in both directions
  - Example: Telephone network



Exercise

- What mode of data flow the following exhibits shows?



- Answer: Full-Duplex

Computer Networks

Fourth Year Class

Lecture 2

Networks

Abdulhameed N. Hameed

1.2 Networks

- Network : Is the interconnection of a set of devices capable of communication.

Devices divided into :

- **Hosts** such as computer, Laptop, printer, cellular phone
- **Connecting devices** such as a router, and switch

Networks

- Network Criteria
  - Network must meet a certain number of criteria
  - The most important of the network criterions are:
    - Performance
    - Reliability
    - Security

Networks

Performance

- Performance depends on :

  1- Number of users: large number slow response time.

  2- Type of transmission medium: fiber-optic cabling faster than others cables.

  3- Capabilities of the connected hardware: affect both the speed and capacity of transmission.

  4- Efficiency of the software: process data at the sender and receiver and intermediate affects network performance.

Networks

- Performance
  - Performance is evaluated by two networking metrics:
    - Throughput (high): a measure of how fast we can actually send data through a network
    - Delay (low)

Networks

- Reliability
  - Reliability is measured by:
    1. Frequency of failure
    2. Recovery time of a network after a failure
    3. Network's robustness in a disaster: protect by good back up network system

Networks

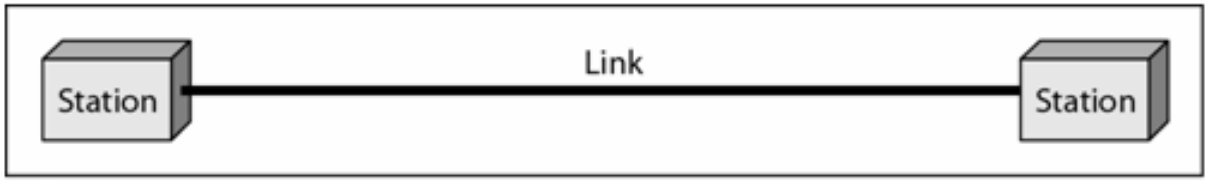
- Security
  - Protecting data from unauthorized access
  - Protecting data from damage and development
  - Implementing policies and procedures for recovery from breaches and data losses (Recovery plan)

Networks

- Physical Structures:
  - Type of connection
    - Network: Two or more devices connected through links
    - Link: Communication pathway that transfers data from one device two another
    - Two devices must be connected in some way to the same link at the same time. Two possible types:
      - Point-to-Point
      - Multipoint

Networks

- Point-to-Point
  - Dedicated link between two devices
  - Entire capacity of the link is reserved for transmission between those two devices
  - Use an actual length of wire or cable



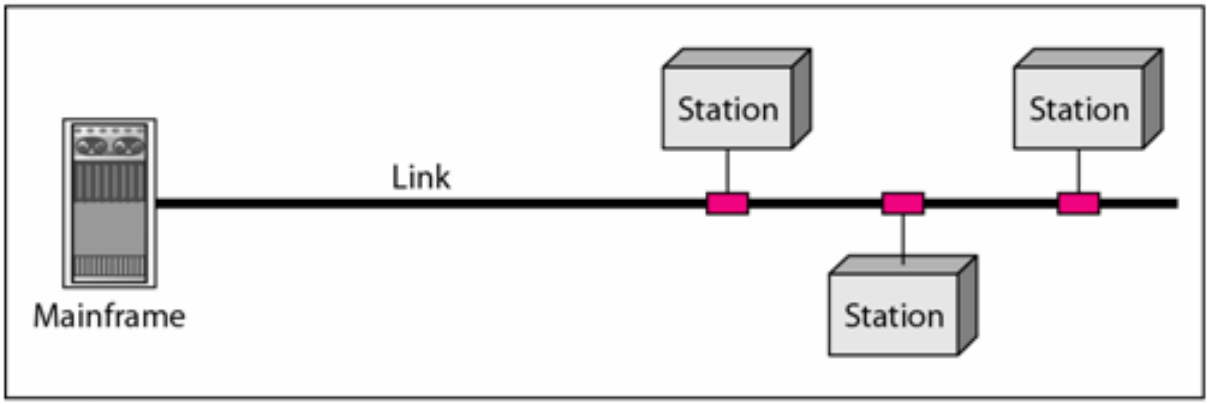
a. Point-to-point

Networks

- Point-to-Point
  - Other options, such as microwave or satellite is possible
  - Example: Television remote control

Networks

- Multipoint (multidrop)
  - More than two devices share a single link
  - Capacity is shared
  - Channel is shared either spatially or temporally
    - Spatially shared: if devices use link at same time
    - Timeshare: if users must take turns

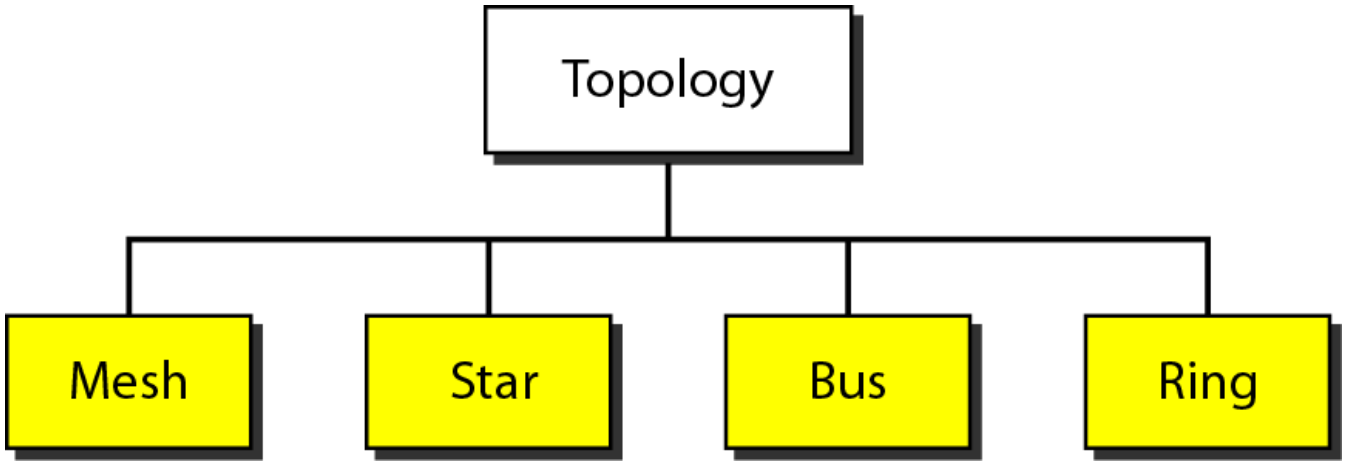


b. Multipoint

Networks

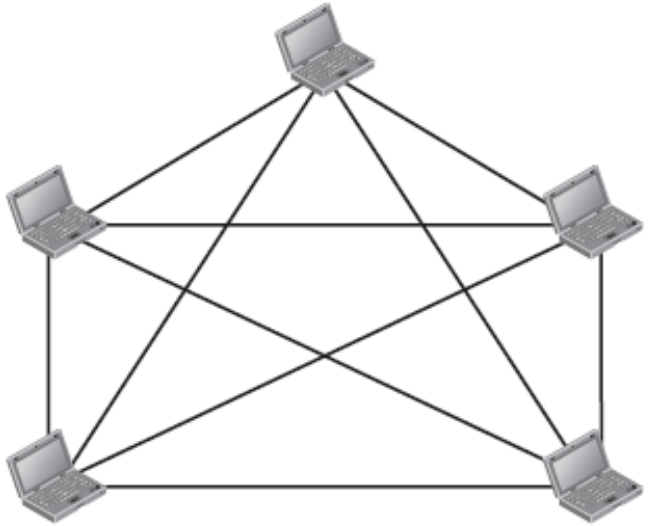
- Physical Topology
  - The way a network is laid out physically
  - Two or more links form a topology
  - The topology of a network is the geometric representation of the relationship of all the links and linking devices (nodes) to one another.
  - Four topologies : Mesh, Star, Bus, and Ring

Physical Topology



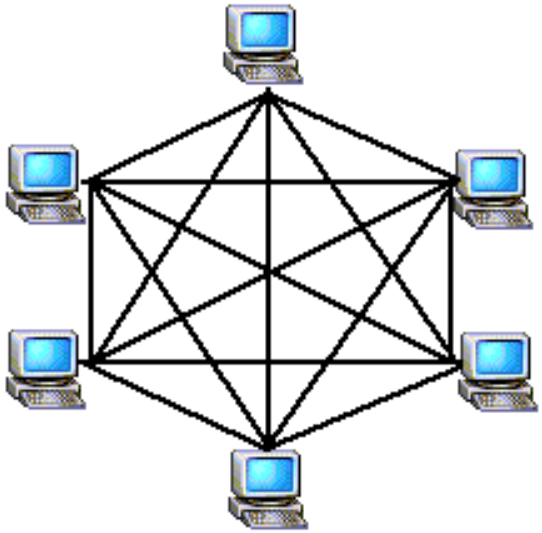
Physical Topology

- Mesh
  - Every device has a dedicated point-to-point link to every other device.
  - The term dedicated means that the link carries traffic only between the two devices it connects.



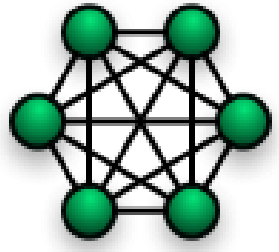
Physical Topology

- Mesh
  - To link ***n*** devices fully connected mesh has:
    n (n - 1) / 2 physical links (Full-Duplex)
  - Every Device on the network must have
    n - 1 ports



Physical Topology

- Mesh
  - Example:



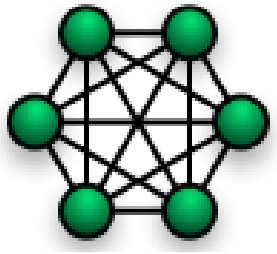
8 devices in mesh has links: n(n-1) / 2

number of links = 8 (8-1)/2 = **28**

number of ports per device = n – 1 = 8 –1 = **7**

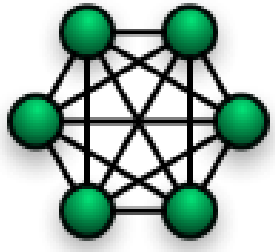
Physical Topology

- Mesh
  - Advantages
    - Each connection carry its own data load (no traffic problems)
    - A mesh topology is robust
    - Privacy or security
    - Fault identification and fault isolation



Physical Topology

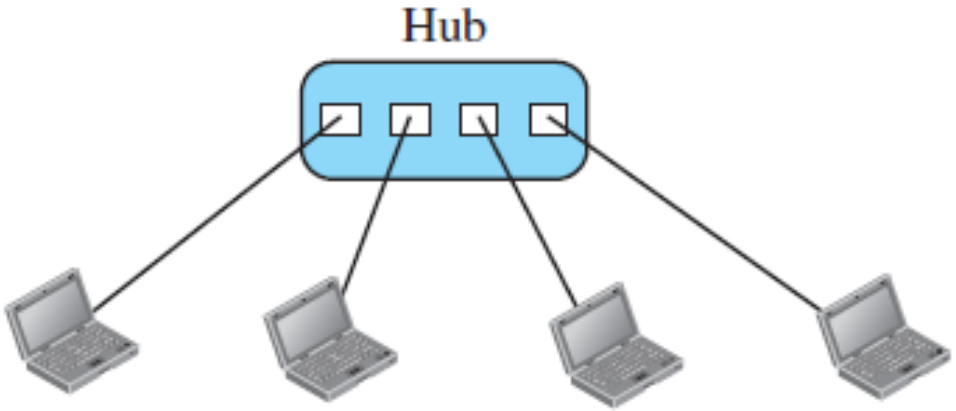
- Mesh:
  - Disadvantages
    - Installation and reconnection are difficult
    - Sheer bulk of the wiring can be greater than the available space
    - Big amount of cabling
    - Big number of I/O ports
    - Hardware connect to each I/O could be expensive



- Mesh topology is implemented in a limited fashion; e.g., as backbone of hybrid network

Physical Topology

- Star:
  - Dedicated point-to-point to a central controller (Hub)
  - No direct traffic between devices
  - The control acts as an exchange



Physical Topology

- Star
  - Advantages
    - Less expensive than mesh (1 Link + 1 port per device)
    - Easy to install and reconfigure
    - Less cabling
    - Additions, moves, and deletions required one connection
    - Robustness : one fail does not affect others
    - Easy fault identification and fault isolation

Physical Topology

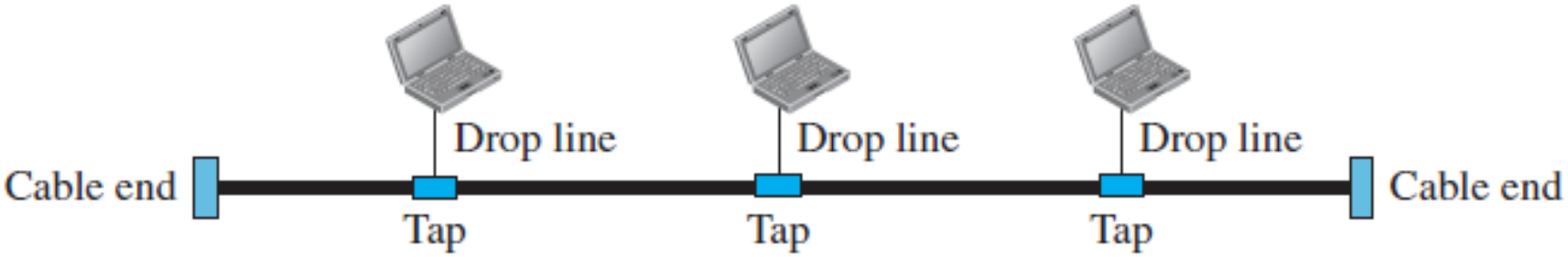
- Star
  - Disadvantages
    - Dependency of the whole topology on one single point (hub)
    - More cabling than other topologies (ring or bus)
- Used in LAN

Physical Topology

- Bus
  - It is multipoint
  - One long cable acts as a backbone
  - Used in the design of early LANS, and Ethernet LANs

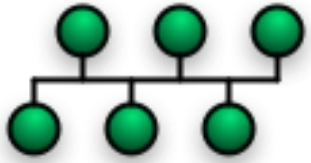
Physical Topology

- Bus
  - Nodes connect to cable by drop lines and taps
  - Signal travels along the backbone and some of its energy is transformed to heat
  - Limit of number of taps and the distance between taps



Physical Topology

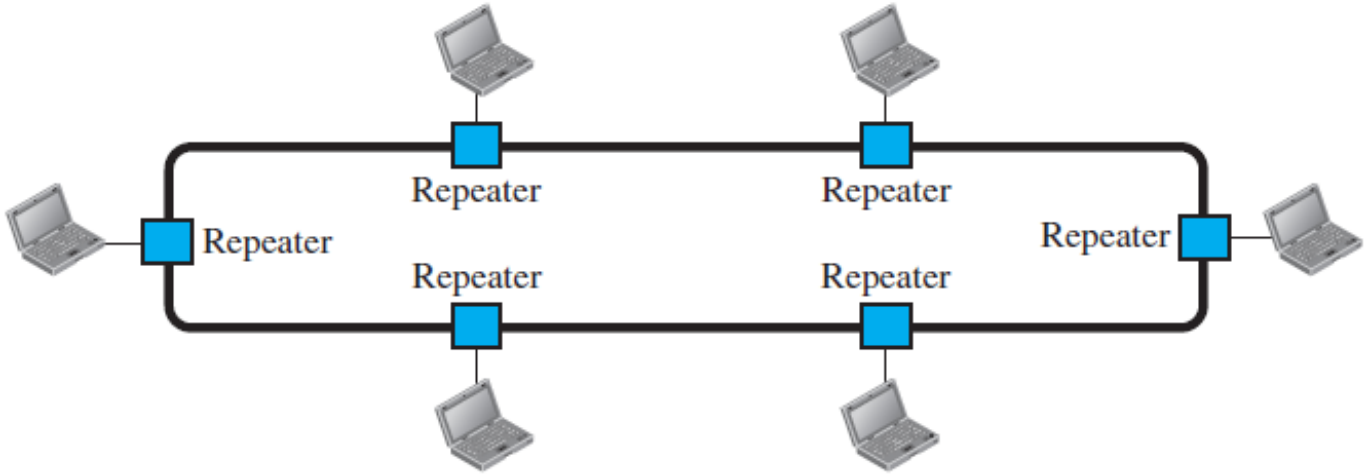
- Bus



  - Advantages
    - Ease of installation
    - Less cables than mesh, star topologies
  - Disadvantages
    - Difficult reconnection and fault isolation (limit of taps)
    - Adding new device requires modification of backbone
    - Fault or break in the bus cable stops all transmission
    - The damaged area reflects signals back in the direction of the origin, creating noise in both directions

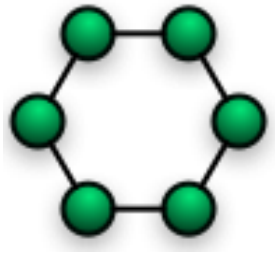
Physical Topology

- Ring
  - Each device has dedicated point-to-point connection with only the two devices on either side of it
  - A signal is passed along the ring in one direction from device to device until it reaches its destination
  - Each device incorporates a Repeater



Physical Topology

- Ring
  - Advantages
    - Easy of install and reconfigure
    - Connect to immediate neighbors
    - Move two connections for any moving (Add/Delete)
    - Easy of fault isolation
  - Disadvantage
    - Unidirectional
    - One broken device can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break



Physical Topology

- Hybrid Topology
  - Example: having a main star topology with each branch connecting several stations in a bus topology

Computer Networks

Fourth Year Class

Lecture 3

Categories of Networks

Abdulhameed N. Hameed

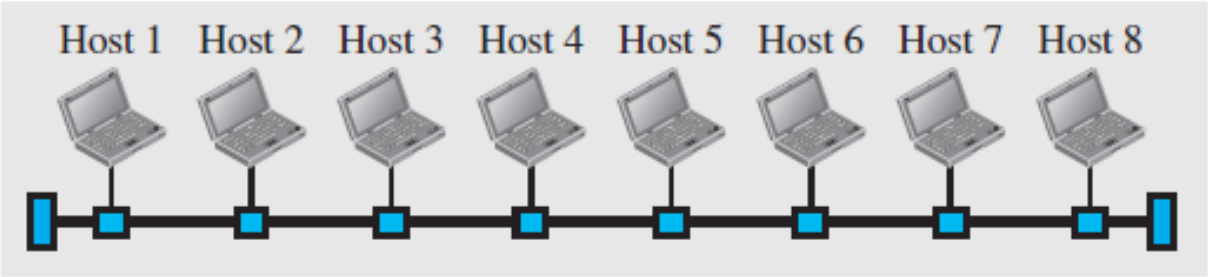
1.3 Categories of Networks

- Network Category depends on its size
- Two primary categories
  - **LAN**: Covers area < 2miles
  - **WAN**: Can be worldwide

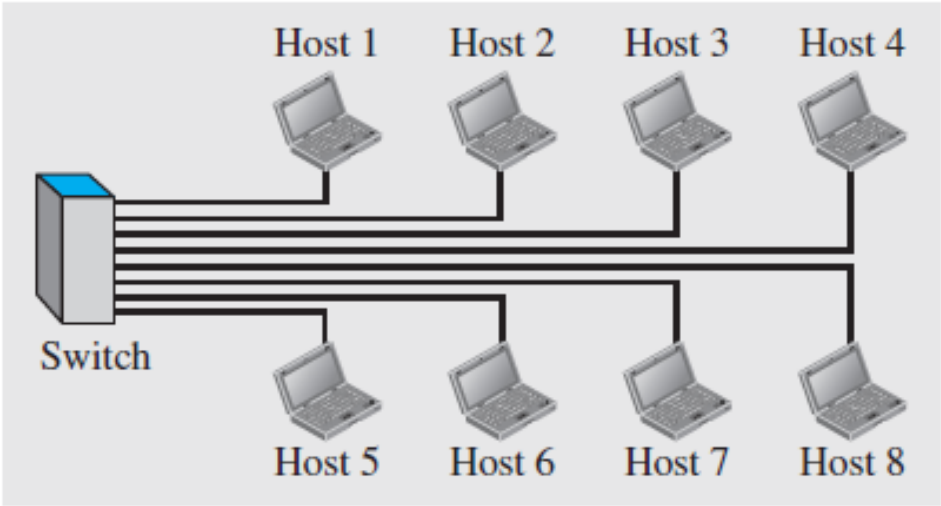
Local Area Network (LAN)

- Privately owned
- Links devices in the same office, building, or campus
- Simple LAN: 2 PCs & 1 printer in home or office
- Size is limited to a few kilometers
- Allow resources to be shared (hardware, software, or data)

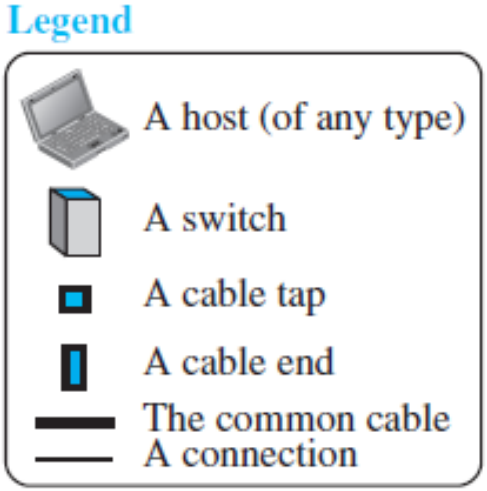
Local Area Network (LAN)



a. LAN with a common cable (past)



b. LAN with a switch (today)

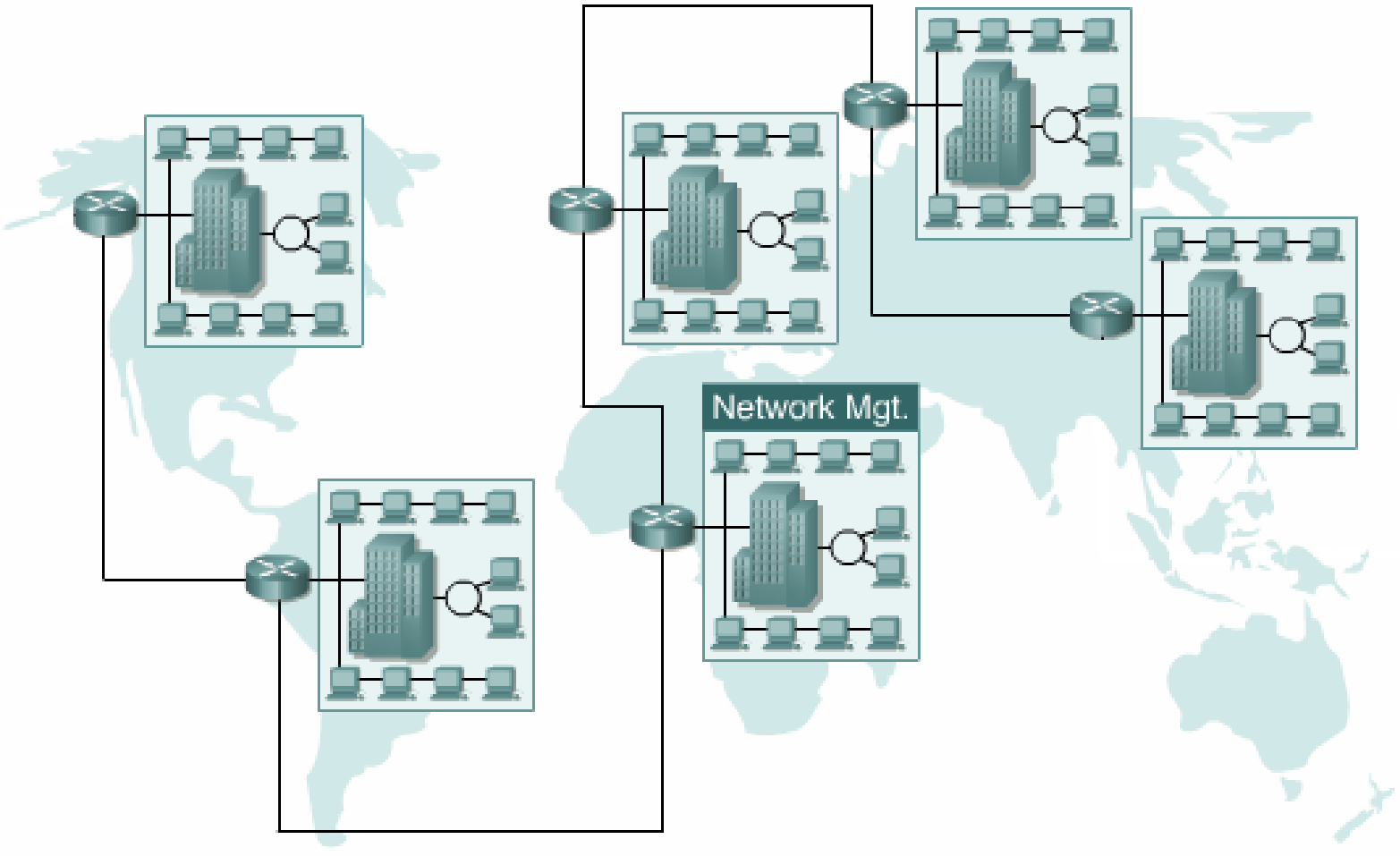


An isolated LAN in the past and today

Wide Area Networks (WAN)

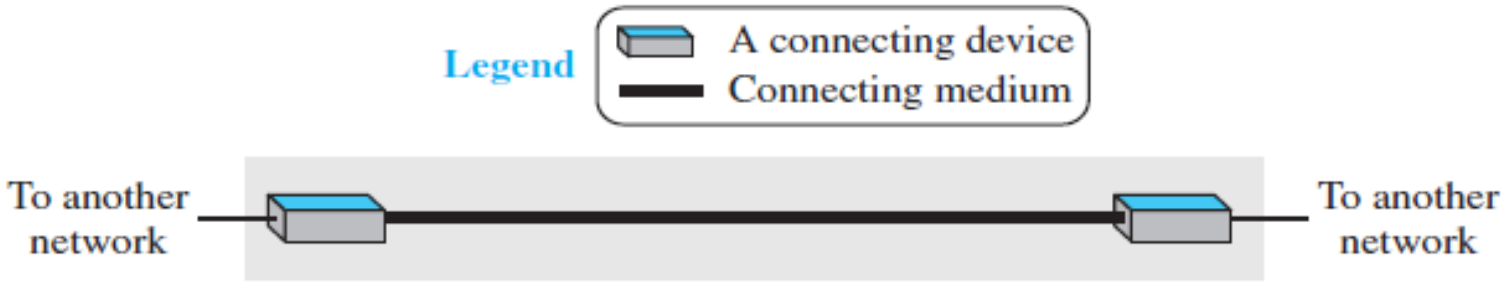
- A wide area network (WAN) is also an interconnection of devices capable of communication.
- Provides long-distance transmission of data over large geographic areas (town, state, country, or even the world).
- WAN is normally created and run by communication companies and leased by an organization that uses it.

Wide Area Networks (WAN)



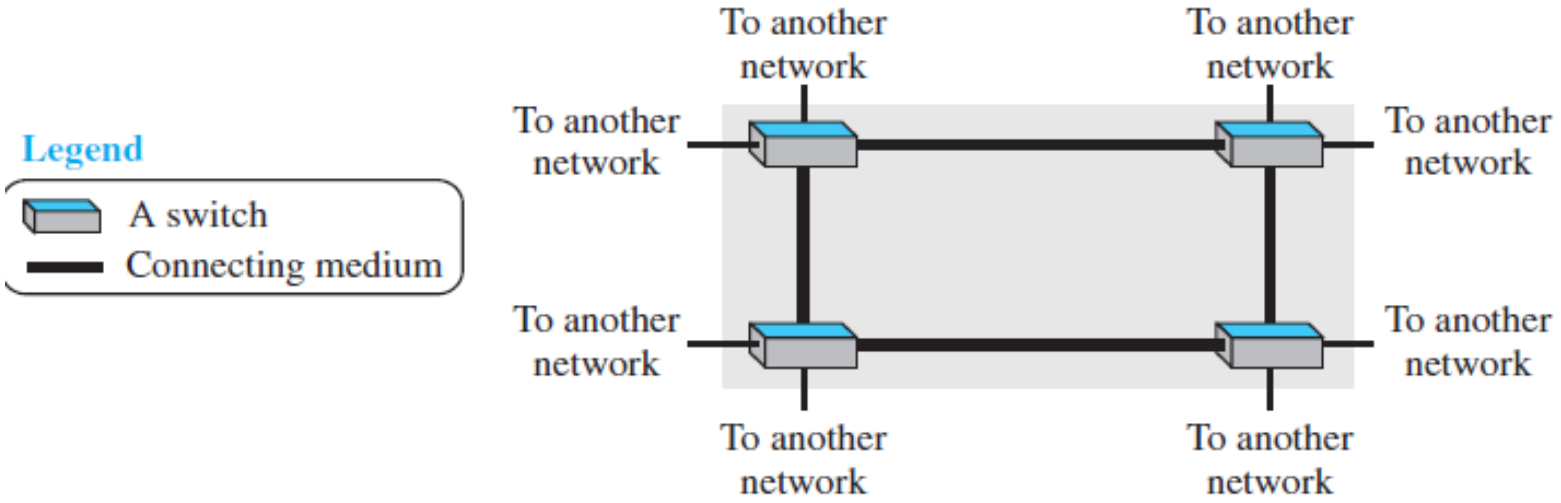
Wide Area Networks (WAN)

- Two examples of WAN are used today:
- Point-to-point WAN:
- A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).



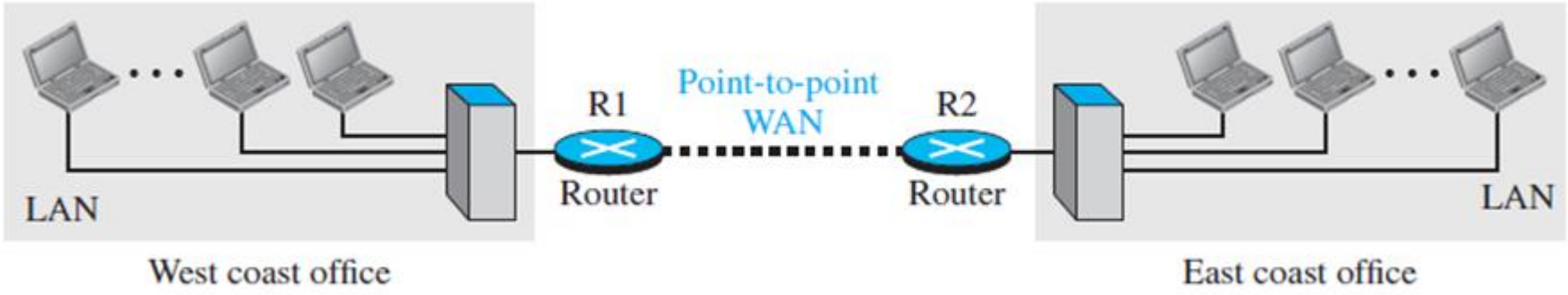
Wide Area Networks (WAN)

- Switched WAN
  - A switched WAN is a network with more than two ends.
  - Backbone of the Internet
- Combination of several point-to-point WANs that are connected by switches



Interconnection of Networks: Internetworks

- Two or more networks connected together make an internetwork, or internet.

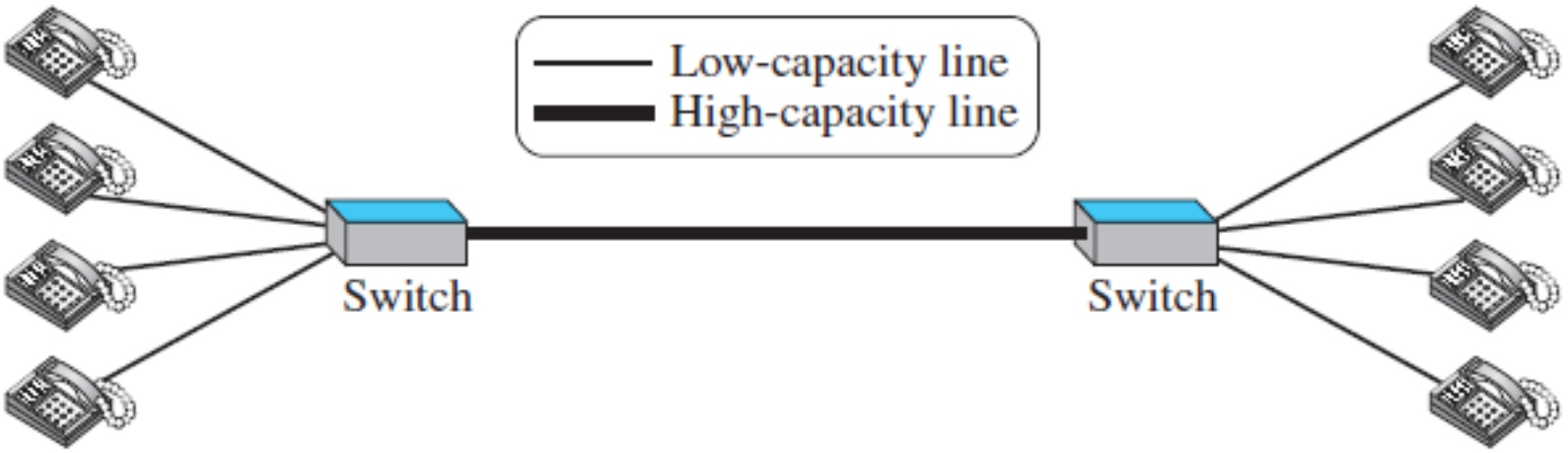


Network Switching

- An internet is a switched network in which a switch connects at least two links together. A switch needs to forward data from a network to another network when required. The two most common types of switched networks are:
- Circuit-switched networks
- Packet-switched networks

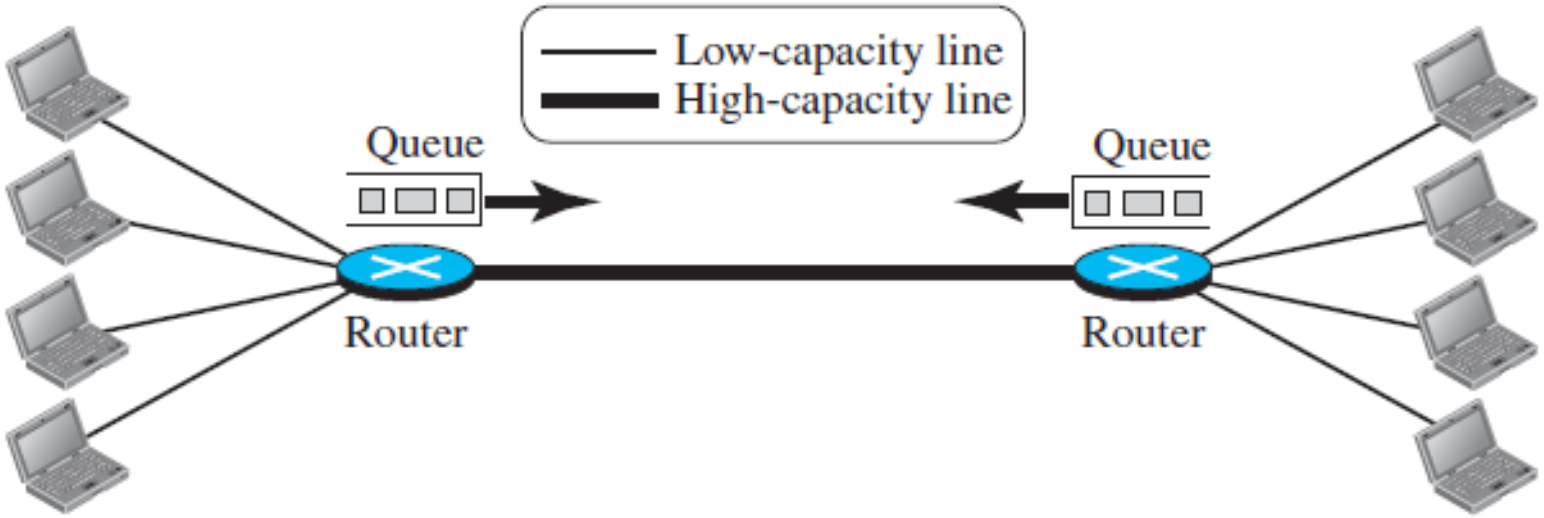
Circuit-Switched Network

- In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive.



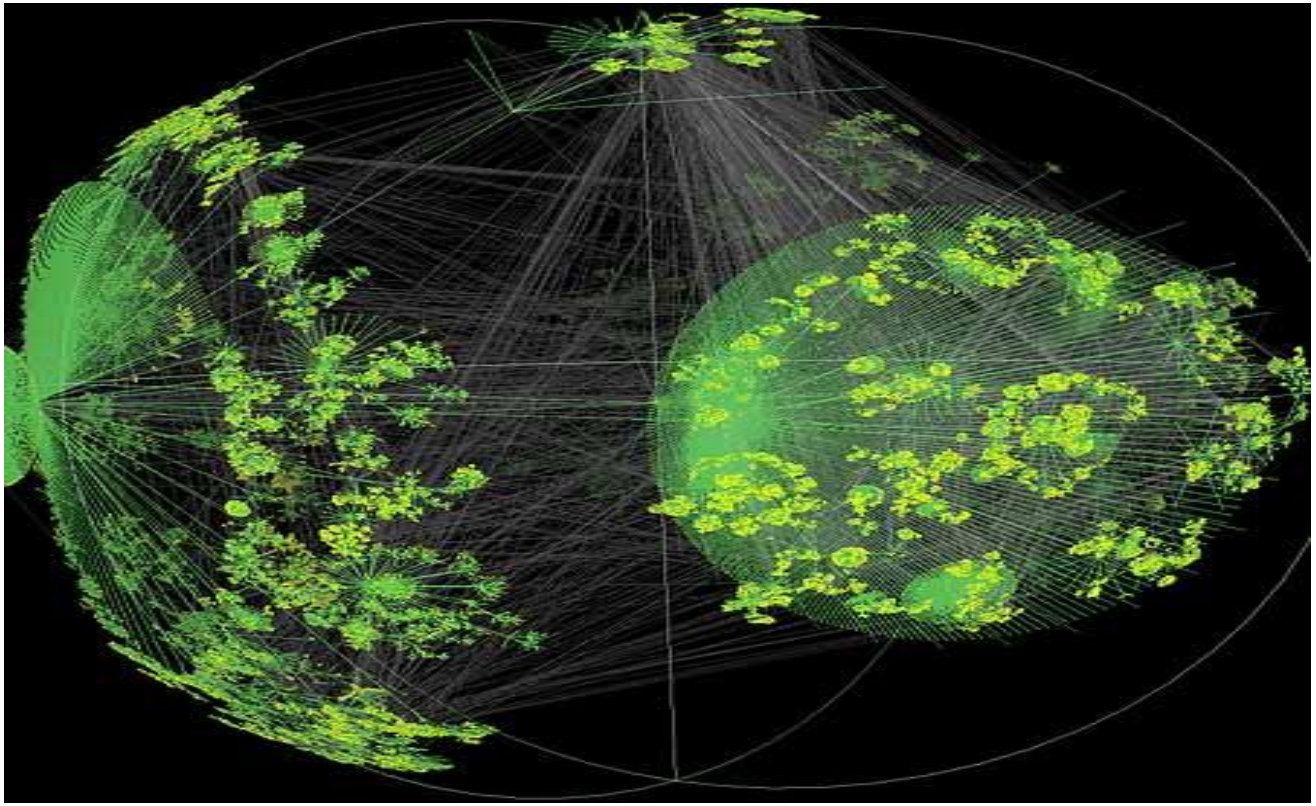
Packet-Switched Network

- In a computer network, the communication between the two ends is done in blocks of data called **packets.**
- packet-switched network is more efficient than a circuit switched network, but the packets may encounter some delays.



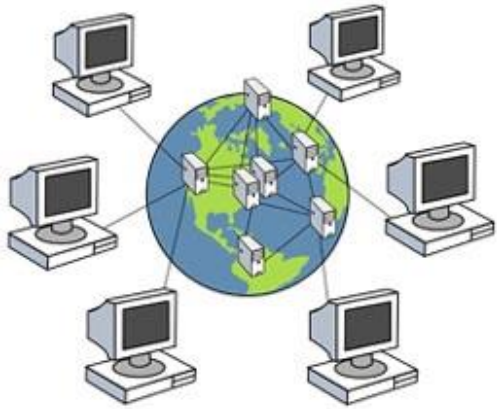
The Internet

- An internet is two or more networks that can communicate with each other.
- The Internet is a collaboration of more than hundreds of thousands of interconnected networks.



Accessing the Internet

- Using Telephone Networks
  - Dial-up service
  - DSL Service
- Using Cable Networks
- Using Wireless Networks
- Direct Connection to the Internet



Systems and Control Eng. Dept.

Computer Networks

Fourth Year Class

Lecture 4

Network Models

Abdulhameed N. Hameed

Lecture Outline

1. Protocol Layering
2. TCP/IP Protocol Suite
3. OSI Model

2-1 PROTOCOL LAYERING

A protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.

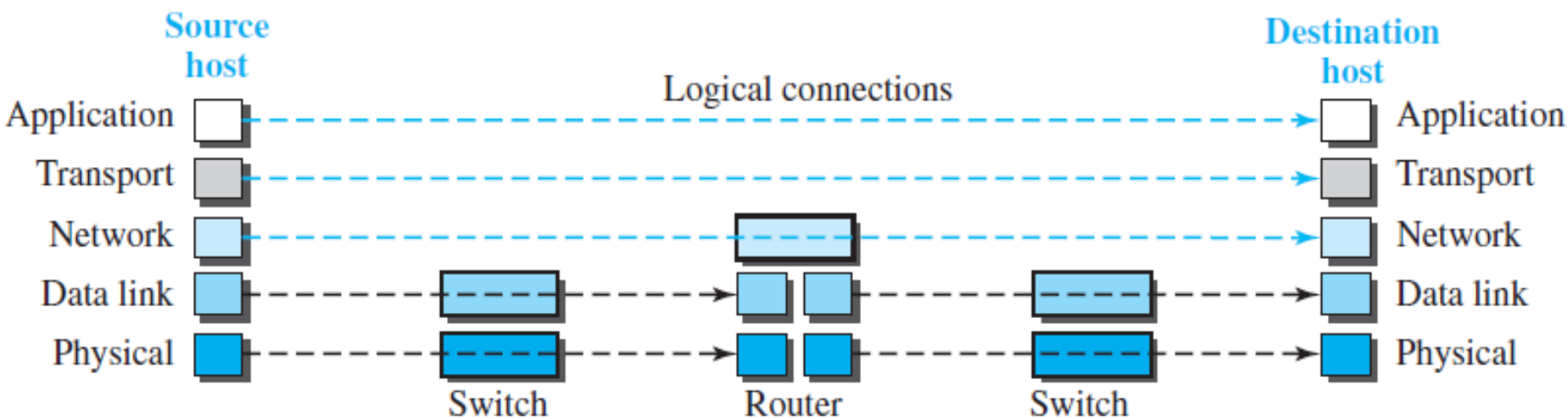
When communication is simple, we may need only one simple protocol; when the communication is complex, we need a protocol at each layer, or protocol layering.

Why Use Layered Architecture?

- Layering helps us to divide a complex task into several smaller and simpler tasks
- Layered architecture is modular. For example, if a network function needs to be improved, only the layer that is carrying out this function needs to be updated. Other layers remain untouched.
- A layer can be treated as a black box with certain inputs and outputs. Other layers only need to know the inputs and outputs and not how the layer is functioning
- Some devices may not need the functions of all the layers. This means we do not have to implement the complete system in those devices that saves cost

Logical Connections

- logical connection between each layer means that we have layer-to-layer communication.
- logical connection help us better understand the task of layering.



TCP/IP PROTOCOL SUITE

- TCP/IP means (Transmission Control Protocol/Internet Protocol).
- TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today.
- TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.

Figure 2.4: Layers in the TCP/IP protocol suite

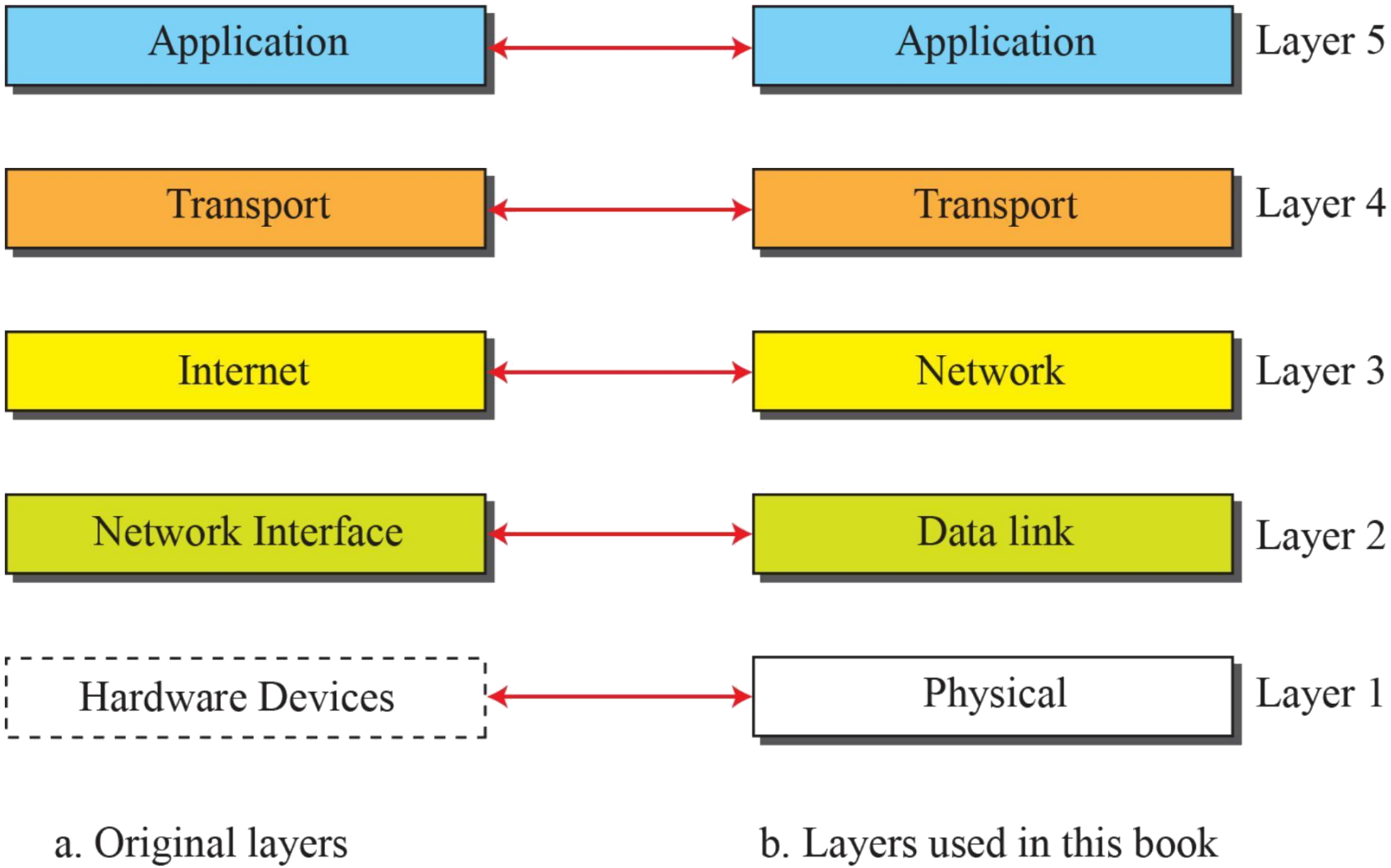


Figure 2.5: Communication through an internet

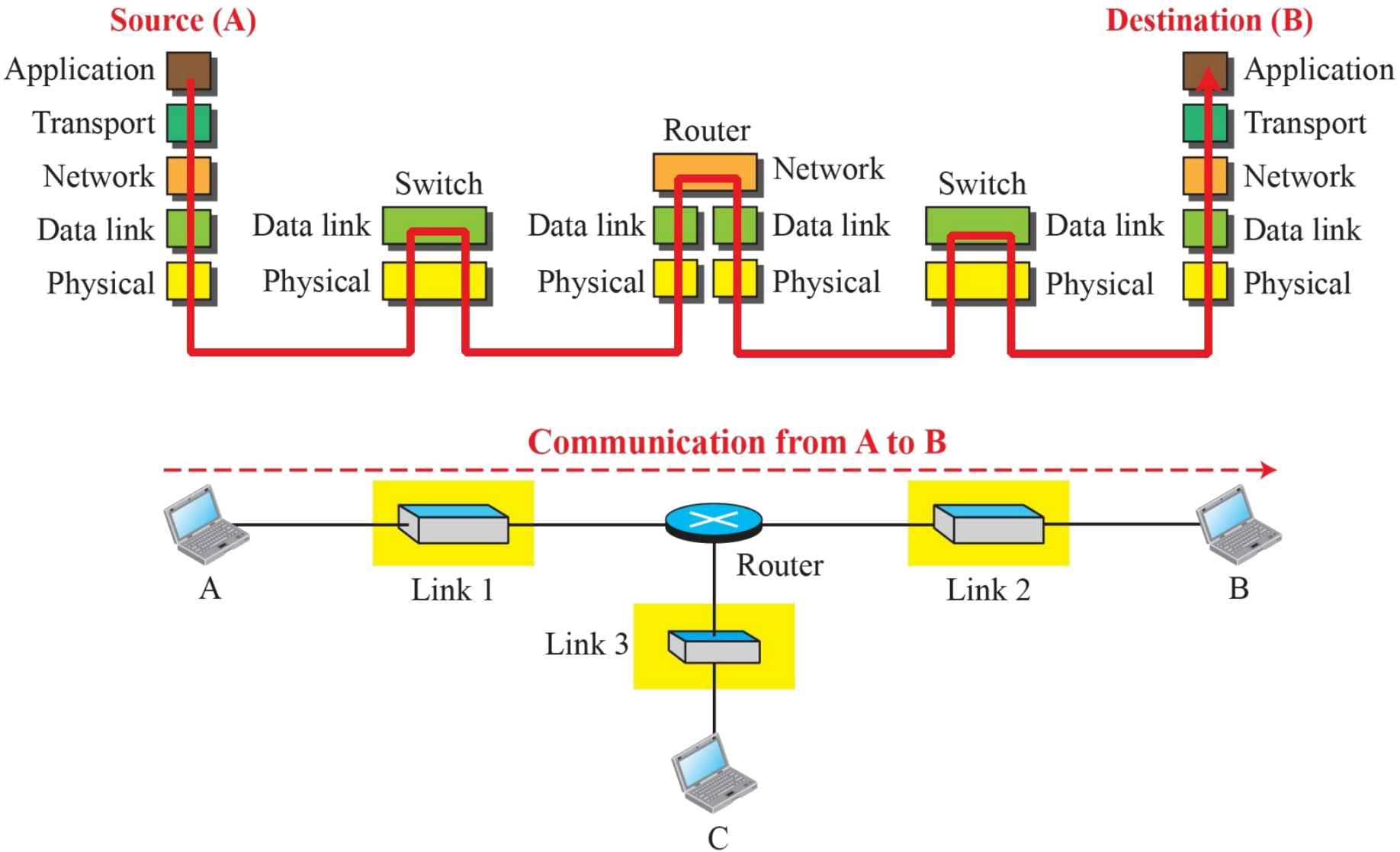


Figure 2.6: Logical connections between layers in TCP/IP

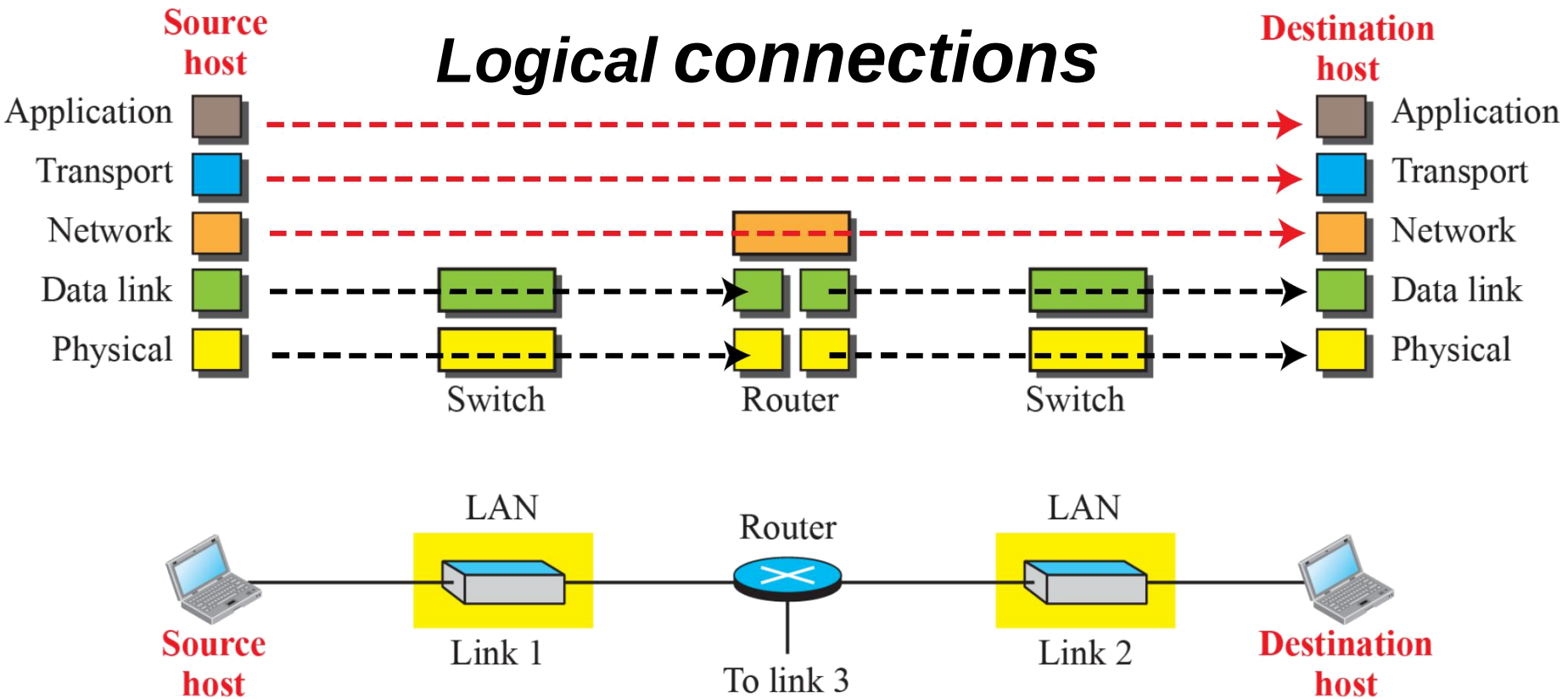
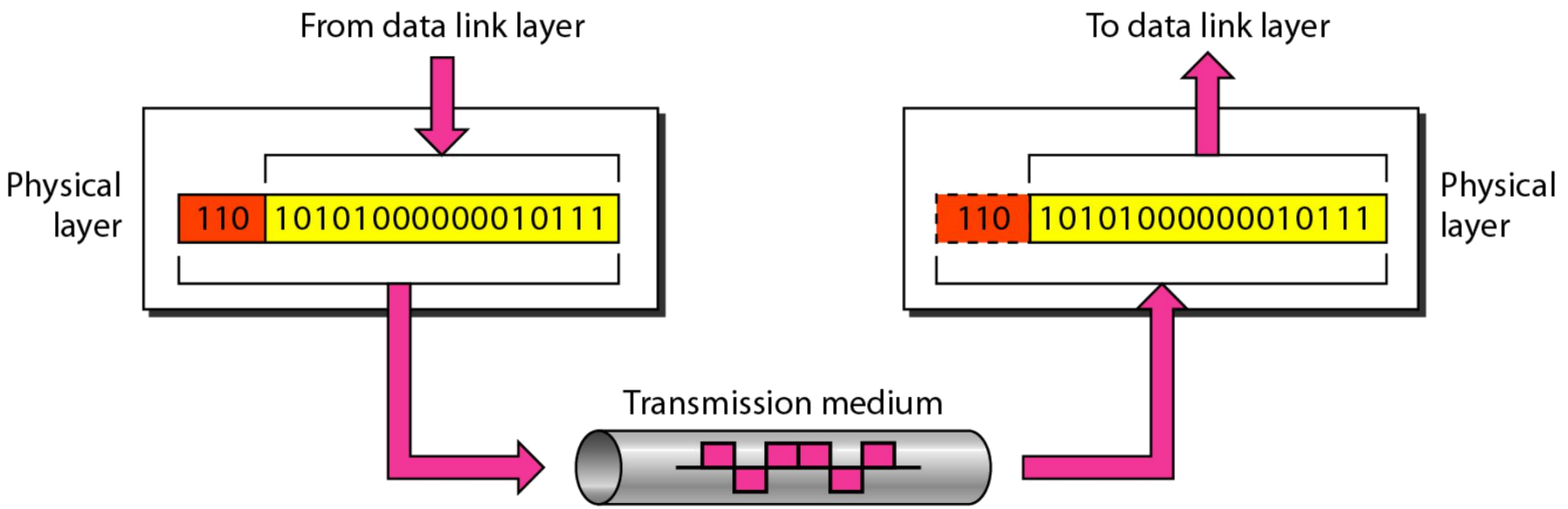


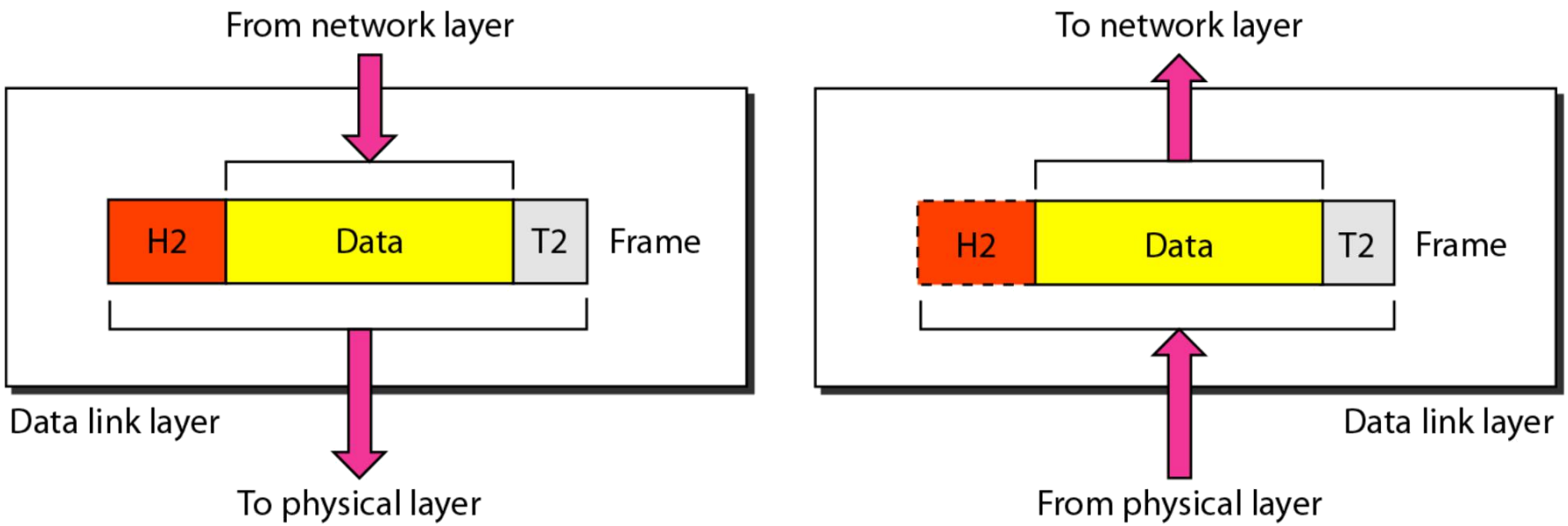
Figure 2.5 *Physical layer*



Physical Layer Tasks and Responsibilities

- Physical transmission medium (what type of medium is being used, cable, fiber optic, wireless, etc.).
- Representation of bits (how 0s and 1s are changed to signals).
- Synchronization of bits (sender and receiver clocks must be synchronized).
- Line configuration (type of link; point-to-point or multipoint).
- Physical topology (mesh, bus, ring, star, hybrid).
- Transmission mode (simplex, half-duplex, duplex).

Figure 2.6 *Data link layer*

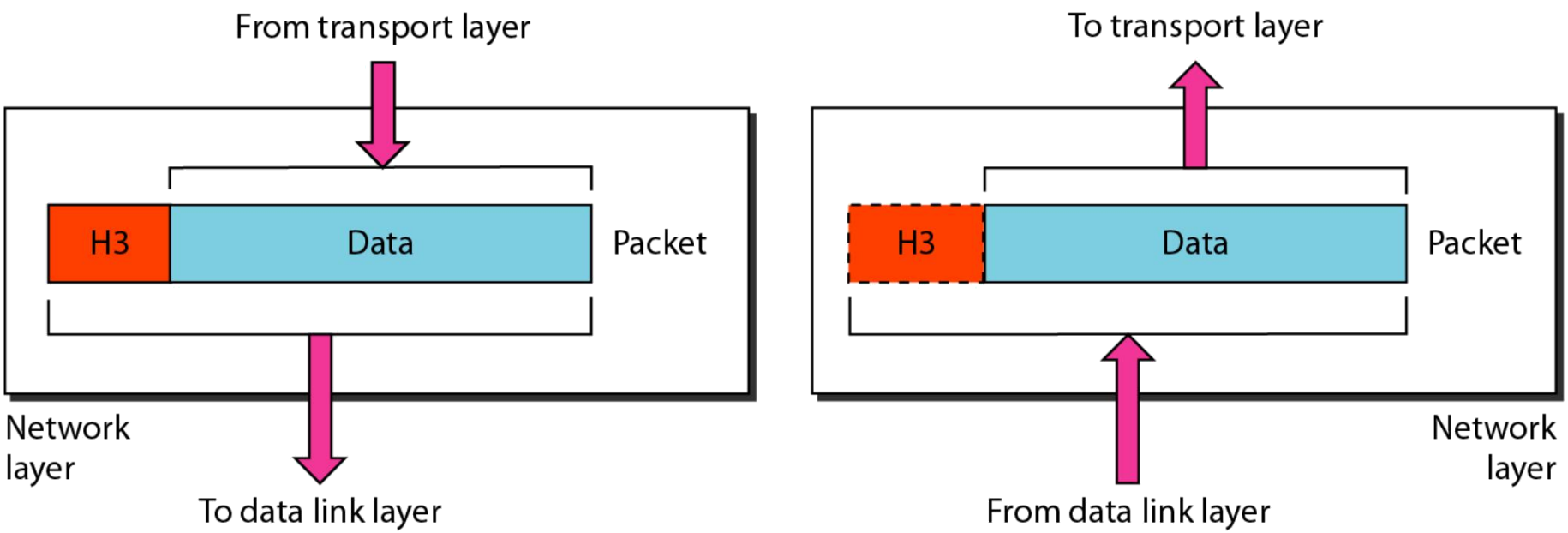


Data Link Layer Tasks and Responsibilities

- Framing
- Flow control
- Error control

Read further details on page 39

Figure 2.8 *Network layer*



Network Layer Tasks and Responsibilities

- Source to destination delivery (host- to-host)
- Logical addressing (the IP address)
- Routing
- This layer includes the main protocol, Internet Protocol (IP) that defines
  - the format of the packet (called "datagram" at the network layer)
  - Format and structure of the addresses used in this layer

Internet Protocol (IP)

- IP is the transmission mechanism used by the TCP/IP.
- IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services.
- IP transports data in packets called *datagrams*
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
- IP does not keep track of the routes and cannot reorder the datagrams.

Transport Layer Tasks and Responsibilities

- It accepts data from application layer, breaks up the data into smaller units (if needed), and sends these smaller units to the network layer
- At the destination, this layer combines the packets into their original state
- Data in transport layer called **segment** or **user datagram** depends on the protocol.

TCP and UDP

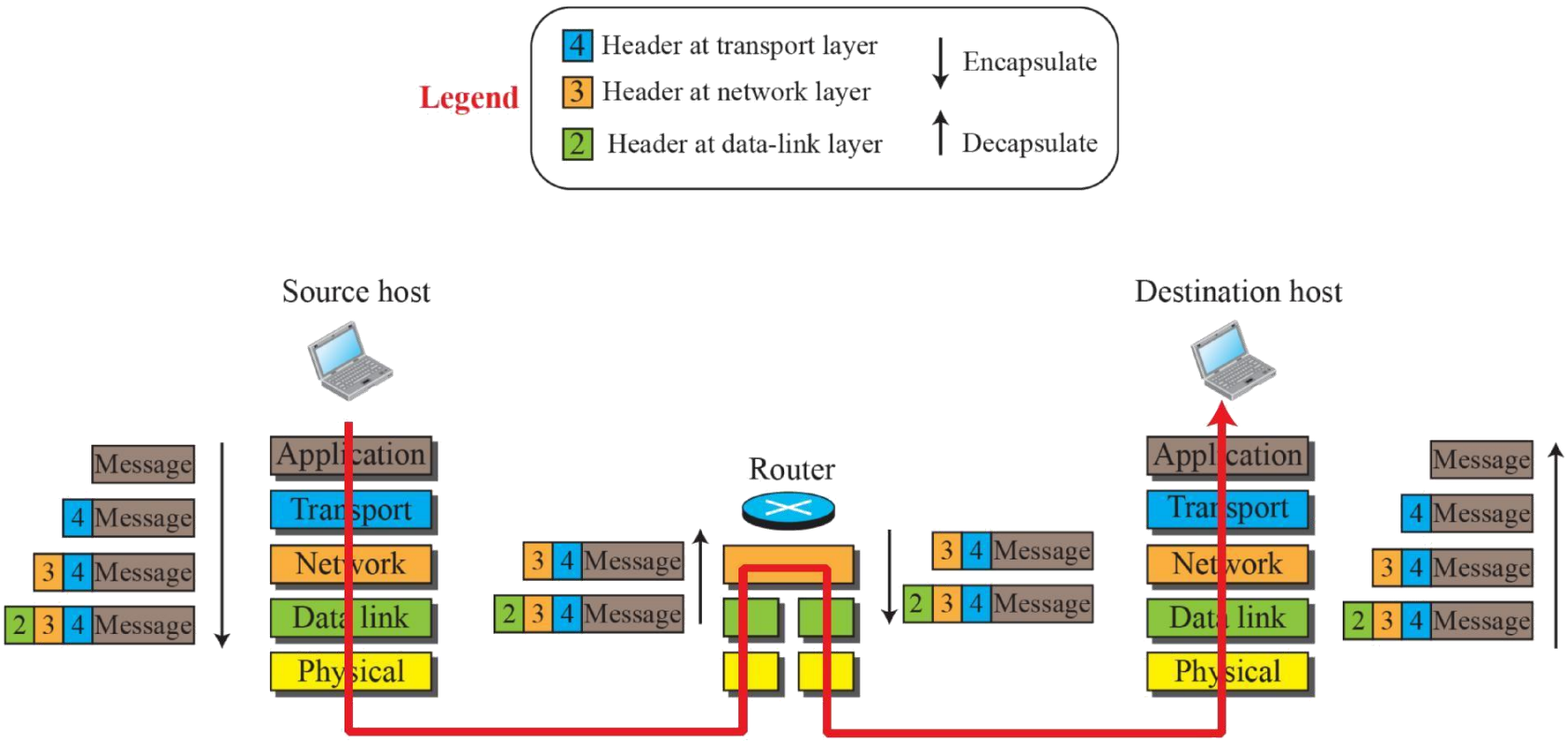
- Transport layer uses Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) depending upon the application requirements.
- TCP is a connection-oriented protocol that provides error control, flow control and congestion control.
- UDP is a connectionless protocol that transmits user datagrams without first creating a logical connection.

Application Layer Tasks and Responsibilities

- The application level provides user interfaces and services that directly support the user applications such as user interface, e -mail, file transfer, database access, etc.
- Communication at the application layer is between two processes(two programs running at this layer).
- There are many protocols at this layer that are commonly needed such as HTTP, WWW, FTP, TELNET, SSH, SNMP, DNS and IGMP.

Encapsulation and Decapsulation

Figure 2.8: ***Encapsulation / Decapsulation***



Encapsulation at the Source Host

- Data at the application layer is message.
- Transport layer adds header to the payload and the resulting packet is called “segment” (in TCP) and “user datagram” (in UDP).
- Network layer adds its own header and the packet is called “datagram”.
- Data-link layer adds its own header and the packet is called “frame”.

Decapsulation & Encapsulation at the Router

- Data-link layer decapsulates the datagram from the frame.
- The network layer only inspects the source and destination addresses in the datagram header and finds the next hop to which the datagram is to be delivered.
- Data-link layer of the next link encapsulates the datagram in a frame and passes to the physical layer for transmission.

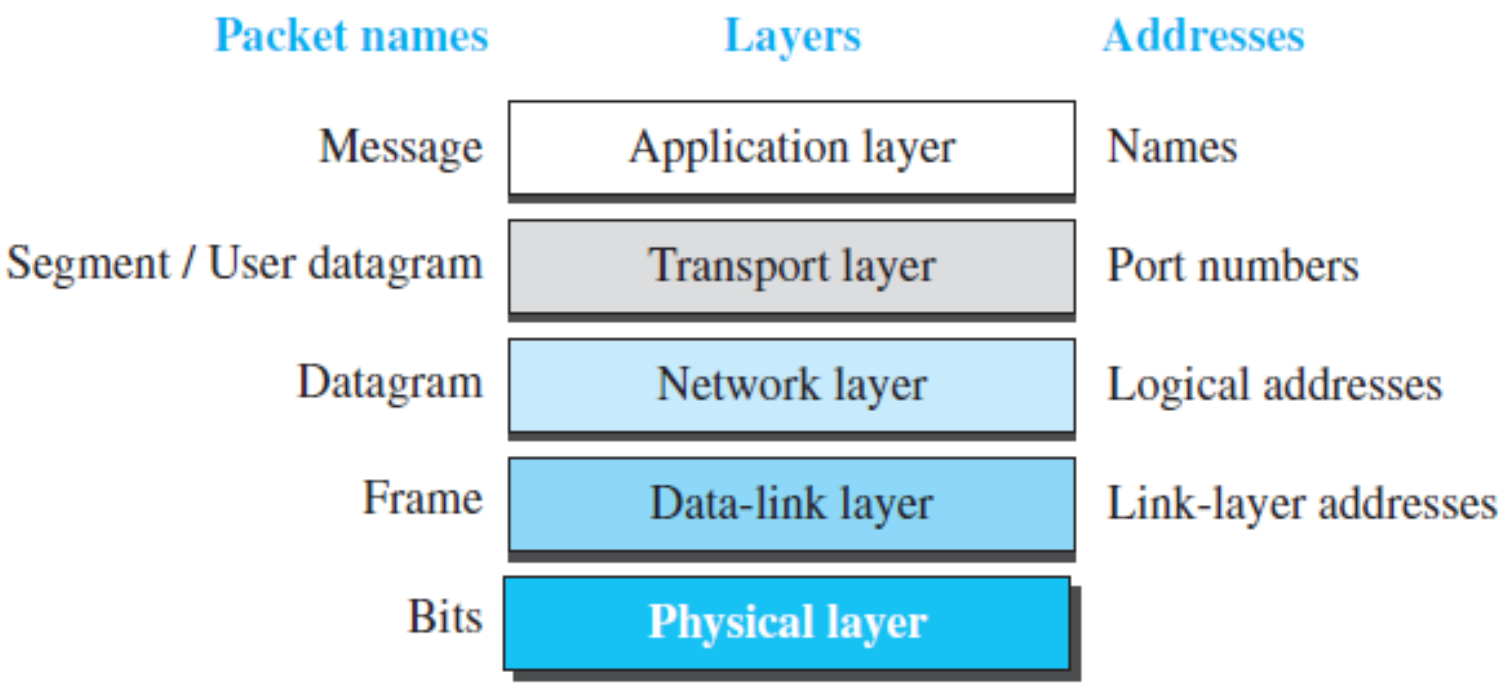
Decapsulation at the Destination Host

- At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer.

2.2.5 Addressing

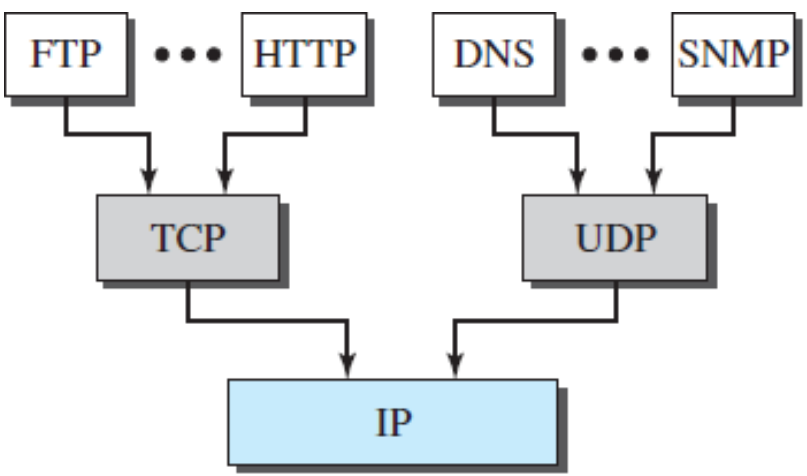
- **Any communication that involves two parties needs two addresses:**
  source address and destination address.

Figure 2.9: ***Addressing in the TCP/IP protocol suite***

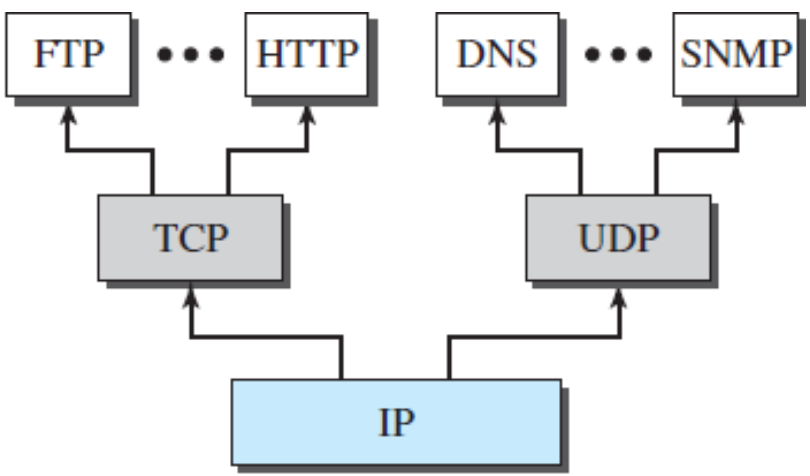


2.2.6 Multiplexing and Demultiplexing

- Multiplexing means that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time); demultiplexing means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time).



a. Multiplexing at source

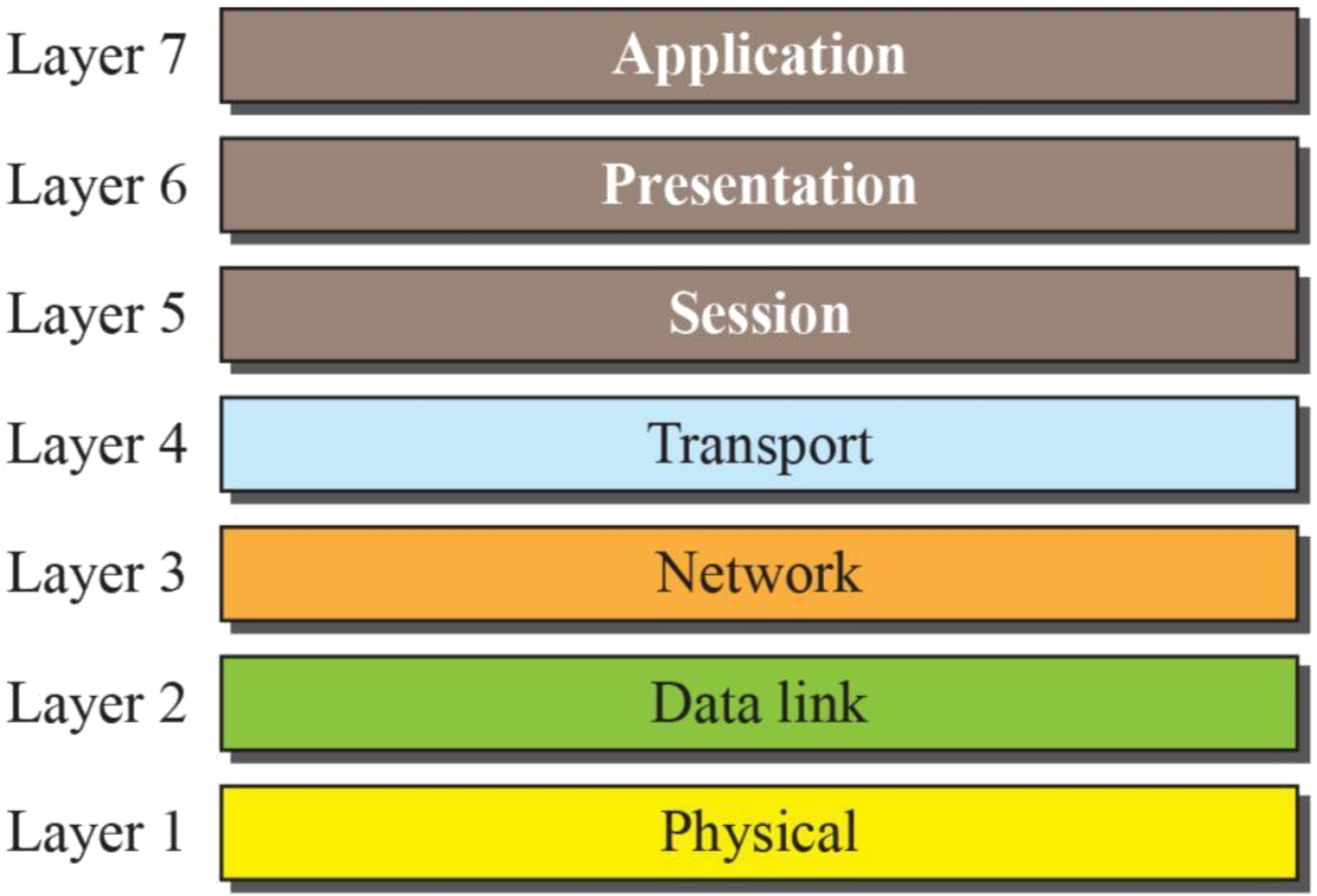


b. Demultiplexing at destination

2-3 THE OSI MODEL

- Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.
- It was first introduced in the late 1970s.

Figure 2.11: The OSI model



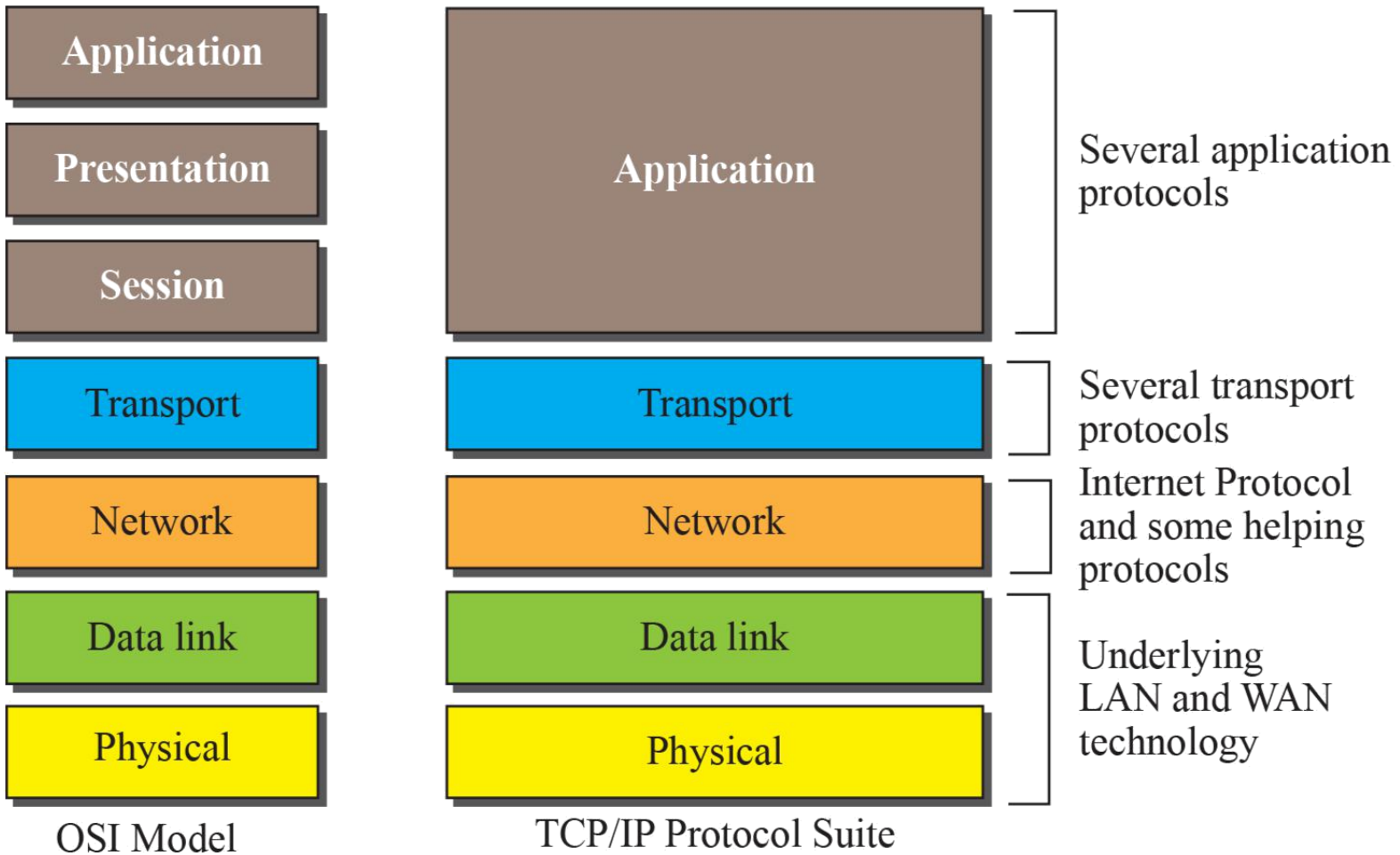
2.3.1 OSI versus TCP/IP

When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite.

These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model.

The application layer in the suite is usually considered to be the combination of three layers in the OSI model, as shown in Figure 2.12.

Figure 2.12: TCP/IP and OSI model



2.3.2 Lack of OSI Model's Success

OSI model could not replace TCP/IP for several reasons, but we describe only three, which are agreed upon by all experts in the field.

- **OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on it.**
- **Some layers in the OSI model were never fully defined.**
- **When OSI was implemented by an organization in a different application, it did not show a high level of performance.**

Systems and Control Eng. Dept.

Computer Networks

Fourth Year Class

Lecture 5

Transmission Media

Abdulhameed N. Hameed

Lecture Outline

1. **Transmission Media**
2. **GUIDED MEDIA**
3. **UNGUIDED MEDIA**

Transmission Media

- Transmission media is any thing that can carry information from source to destination.
- Transmission media are located below the physical layer and controlled by physical layer.
- Transmission media is usually free space, metallic cable, or fiber optic.

Transmission Media

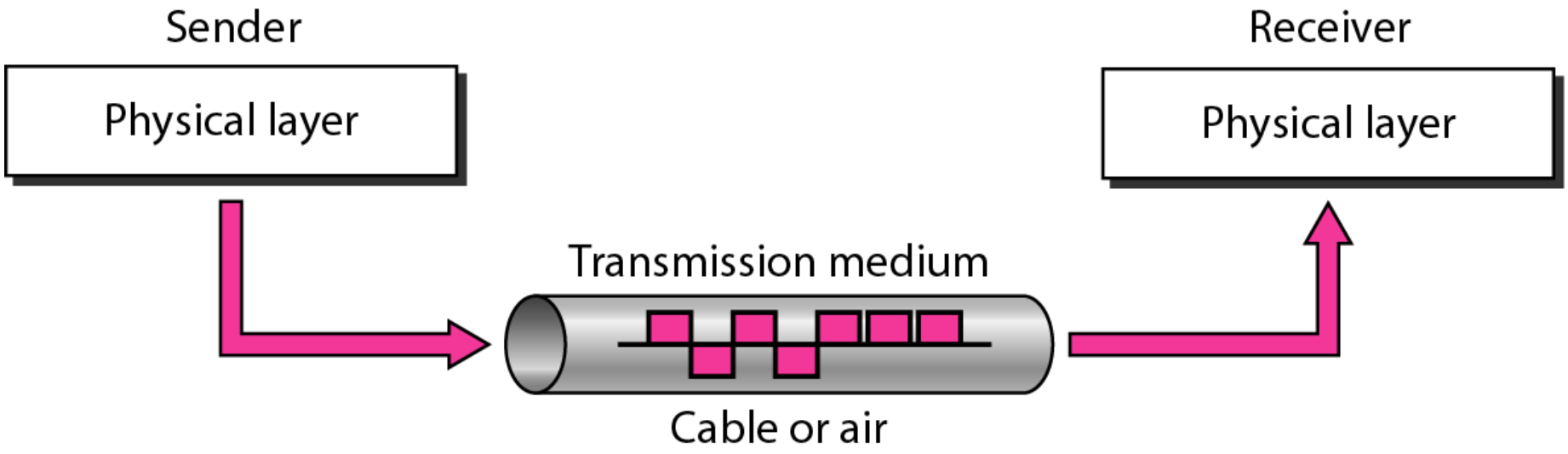


Figure 7.1 *Transmission medium and physical layer*

Transmission Media

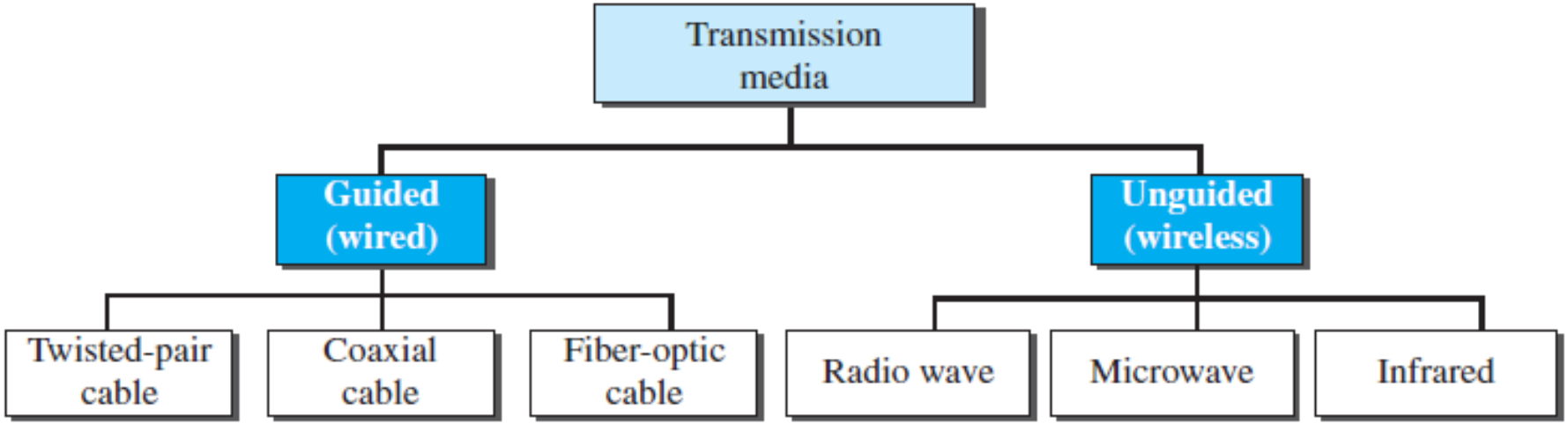


Figure 7.2 *Classes of transmission media*

Guided media

- Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- A signal traveling along any of these media is directed and contained by physical limits of the medium.

Twisted-pair cable

- It consists of two conductors each with its own plastic isolation.
- One used to carry signal , other is ground reference. The receiver use difference between two.

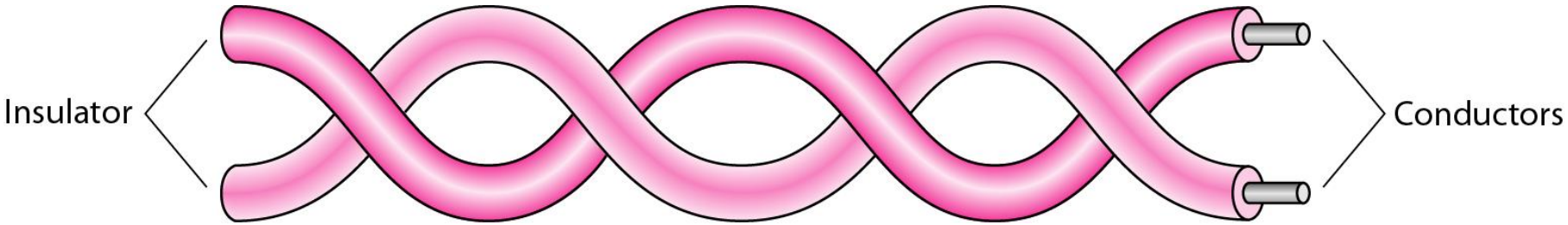


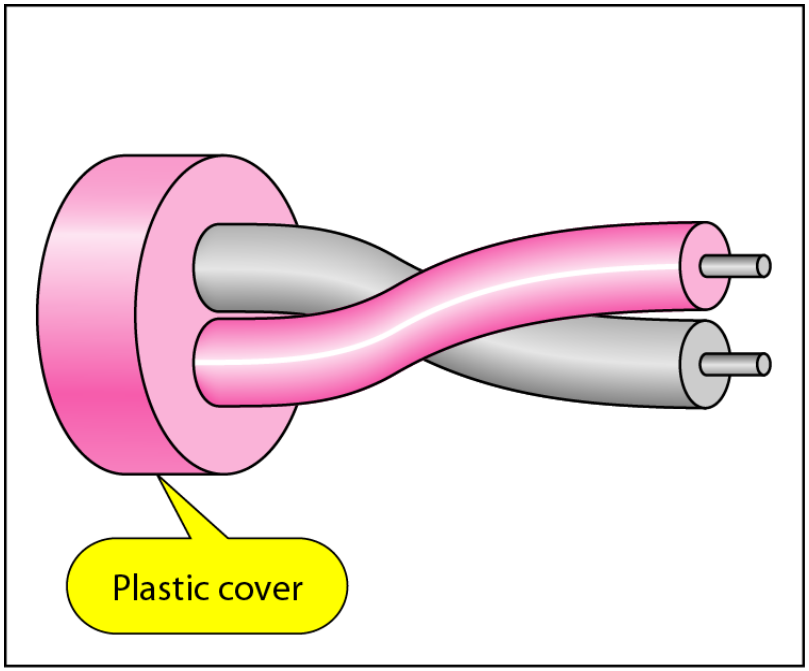
Figure 7.3 ***Twisted-pair cable***

Twisted-pair cable

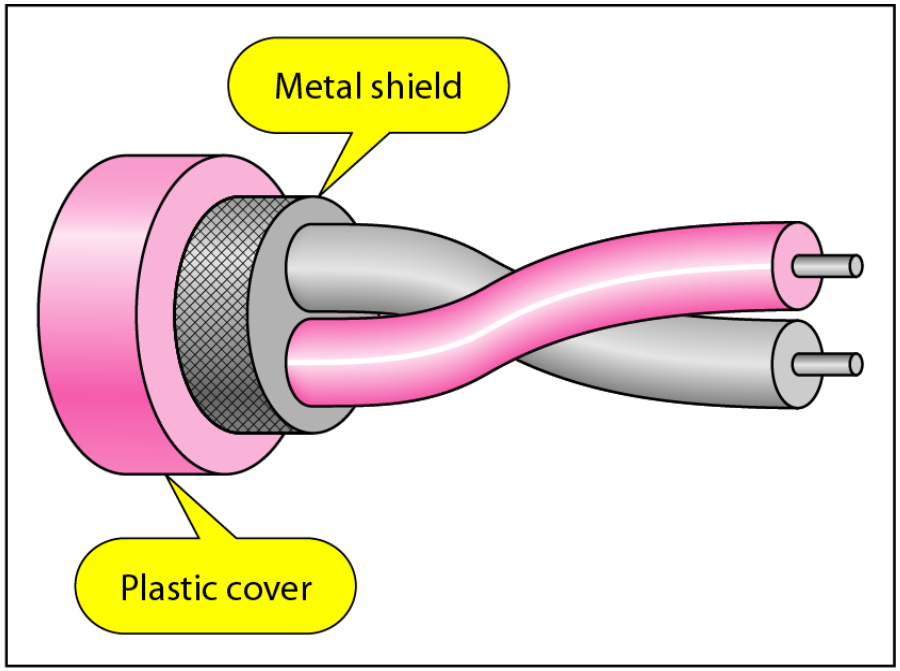
- If the two wires are parallel, the effect of unwanted signal is not the same in both wires, this results in a difference at the receiver.
- By twisting the pairs, a balance is maintained.
- For example, suppose one wire is close to noise and other is farther , in the next twist the reverse is true.
- Twisting make both wire are equally affected by external influences.

Twisted-pair cable type

- Unshielded twisted-pair (UTP)
- Shielded twisted-pair (STP)



a. UTP



b. STP

Figure 7.4 ***UTP and STP cables***

Table 7.1 *Categories of unshielded twisted-pair cables*

Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Twisted-pair cable

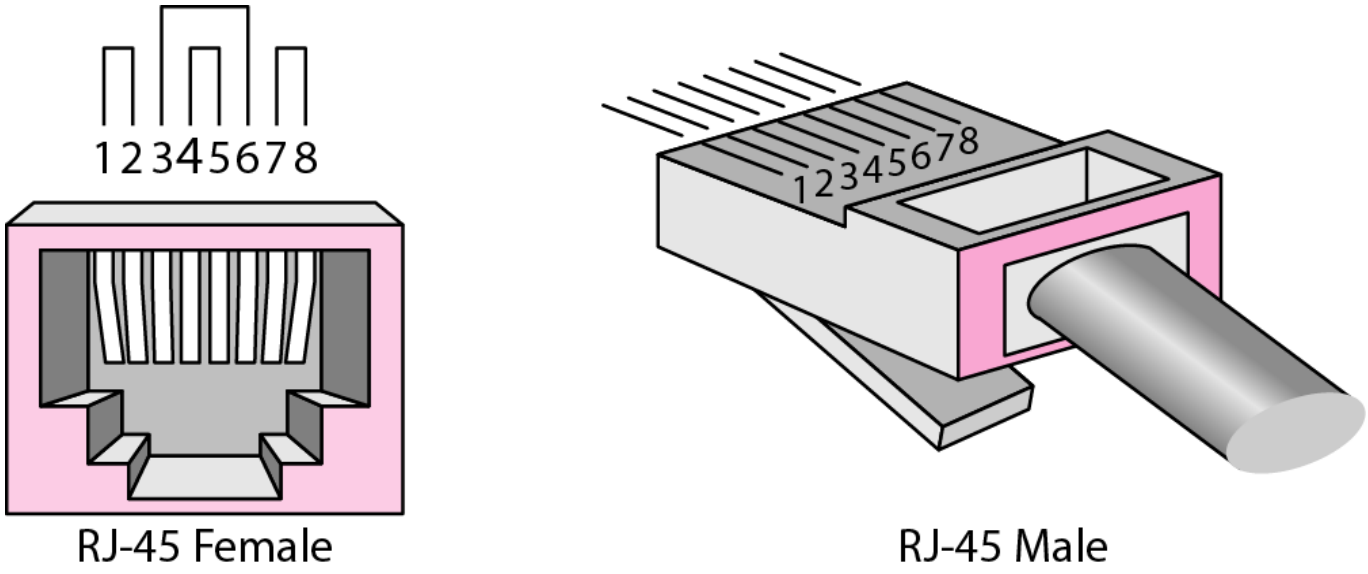
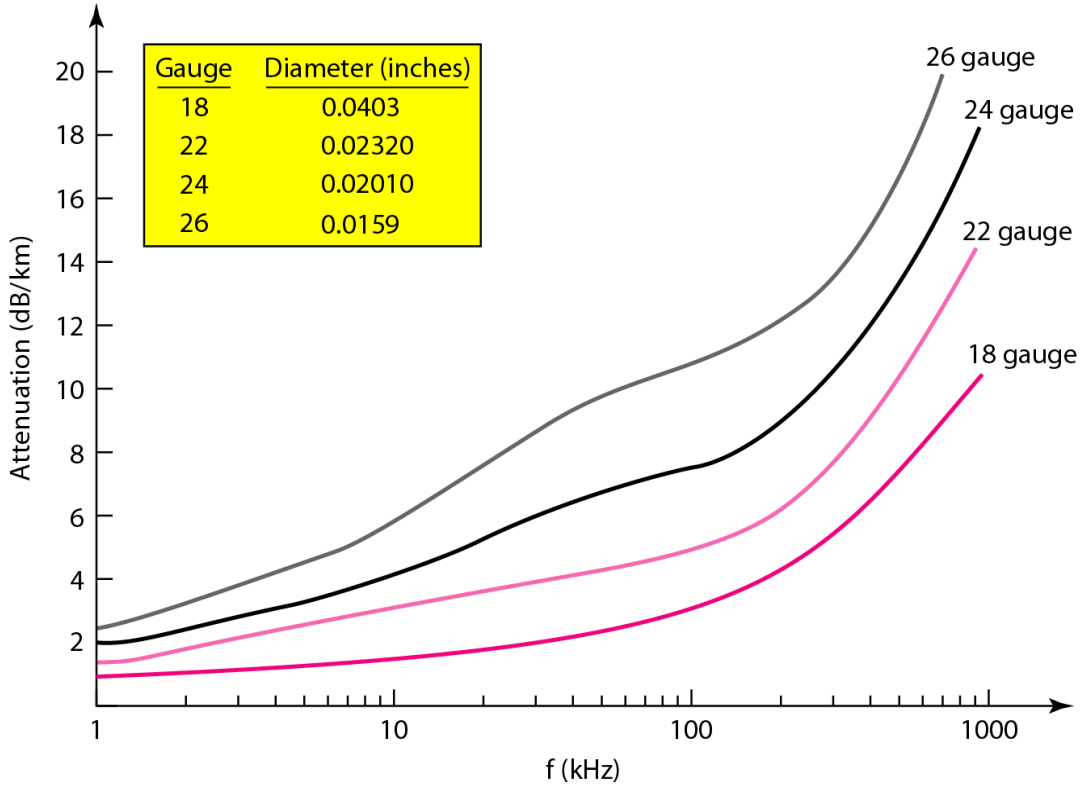


Figure 7.5 *UTP connector*

RJ stands for registered jack

Twisted-pair cable performance

- With increasing frequency , the attenuation sharply increase.



Coaxial cable

- Coaxial cable carries signals of higher frequency ranges than those in twisted-pair.
- Instead of having two wires, coax has central core conductor of solid wire enclosed in insulating sheath which in true encased in outer conductor of metal foil .
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.

Coaxial cable

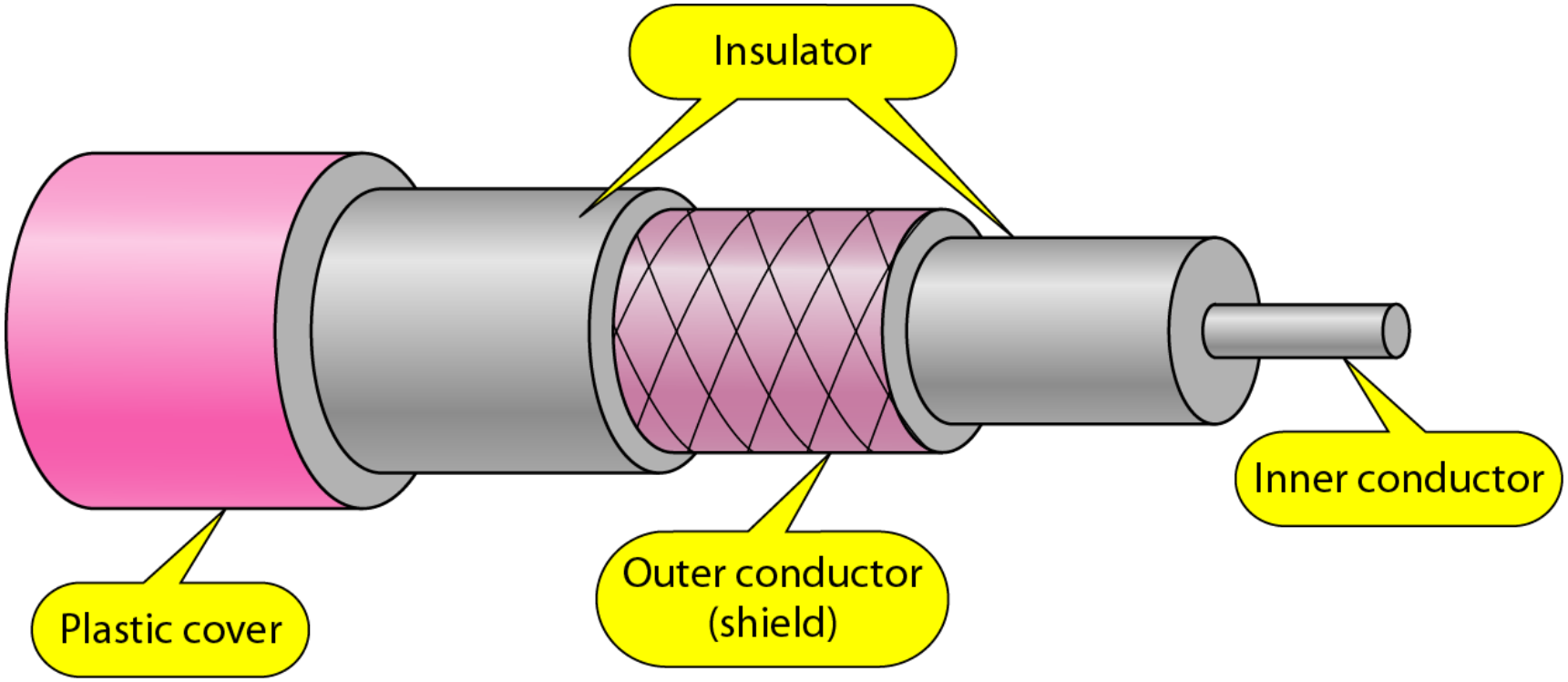


Figure 7.7 *Coaxial cable*

Coaxial cable

Table 7.2 *Categories of coaxial cables*

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Radio Government (RG)

Coaxial cable

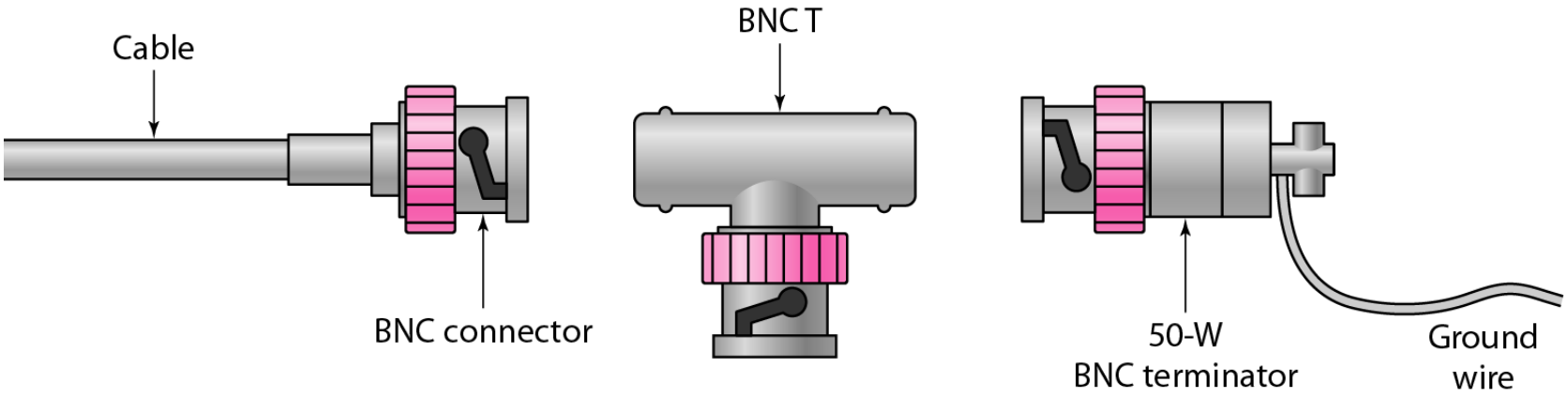


Figure 7.8 *BNC connectors*

Bayonet Neill-Concelman (BNC)

Coaxial cable

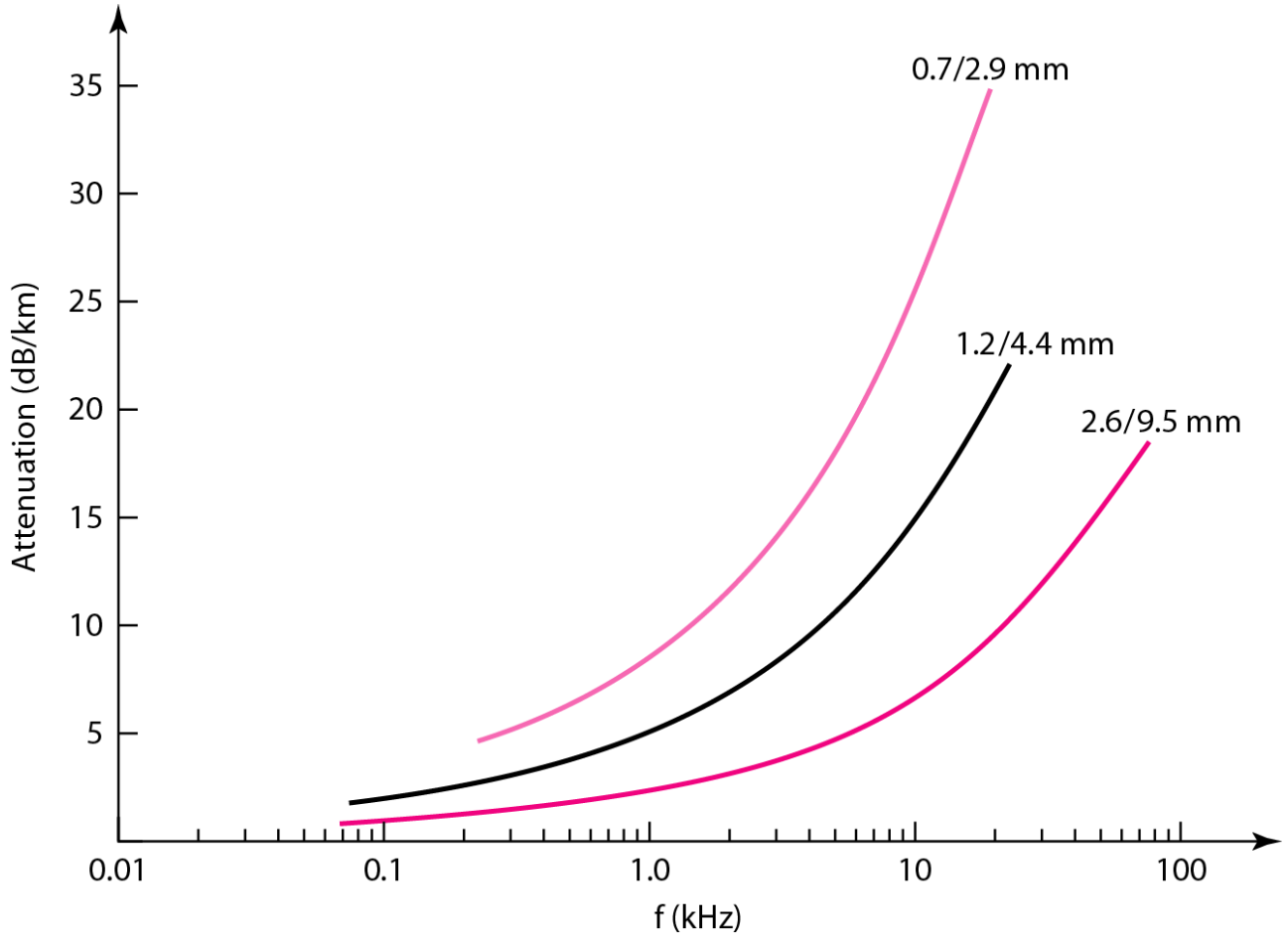


Figure 7.9 *Coaxial cable performance*

Coaxial cable

Coaxial cable performance

- Attenuation is much higher in coaxial cable than in twisted-pair cable.
- Coaxial cable has a much higher bandwidth
- The signal weakens rapidly and requires the frequent use of repeaters.

Coaxial cable

Coaxial Cable Applications

- Coaxial cable was widely used in analog telephone networks and digital telephone networks.
- Cabling TV networks.
- In traditional Ethernet LANs

Optical Fiber

- Light travels in straight line as long as it is moving through a single uniform substance.
- If a ray of light traveling through one substance suddenly enters another substance of difference density, the ray change direction.

Optical Fiber

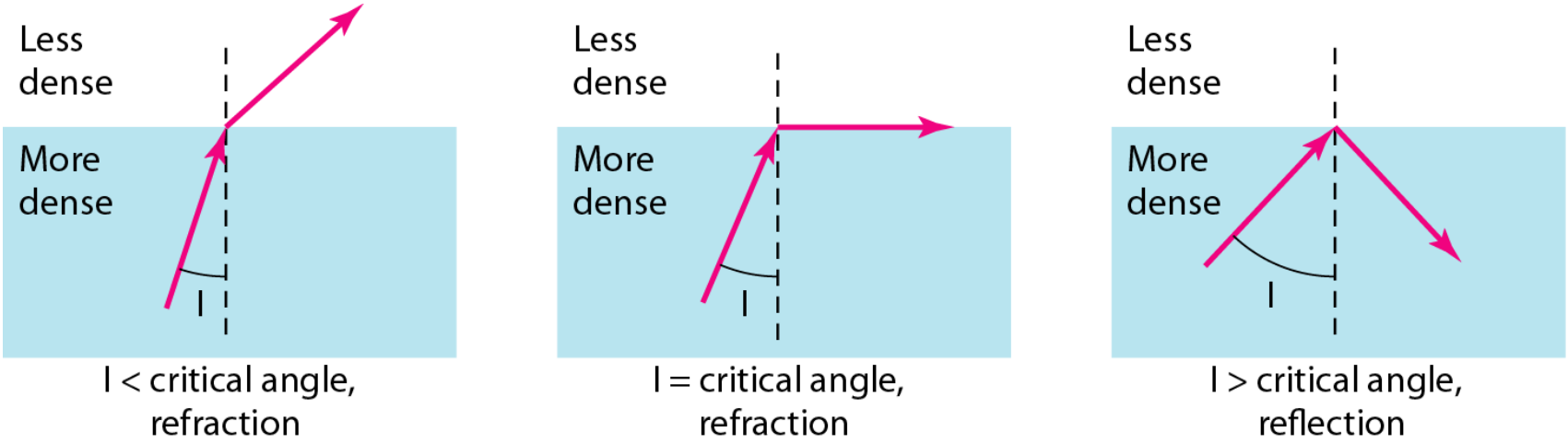


Figure 7.10 Fiber optics: ***Bending of light ray***

Optical Fiber

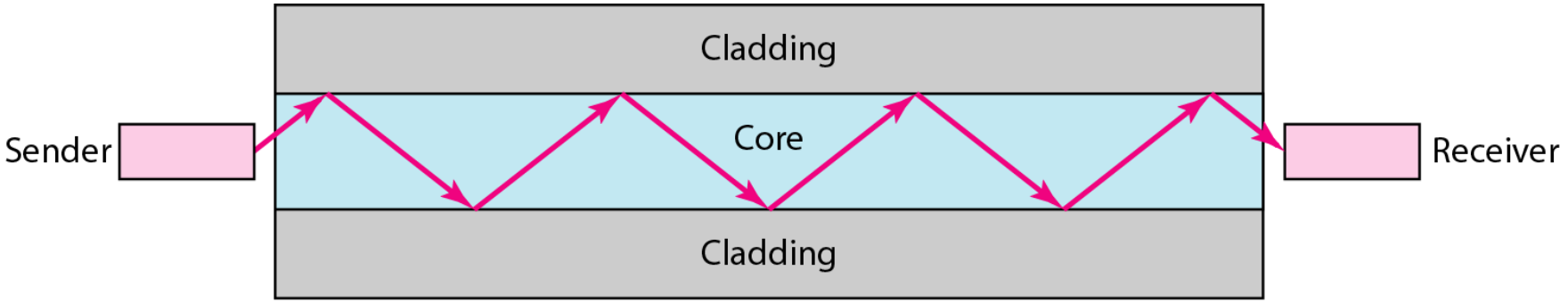


Figure 7.11 ***Optical fiber***

Propagation modes

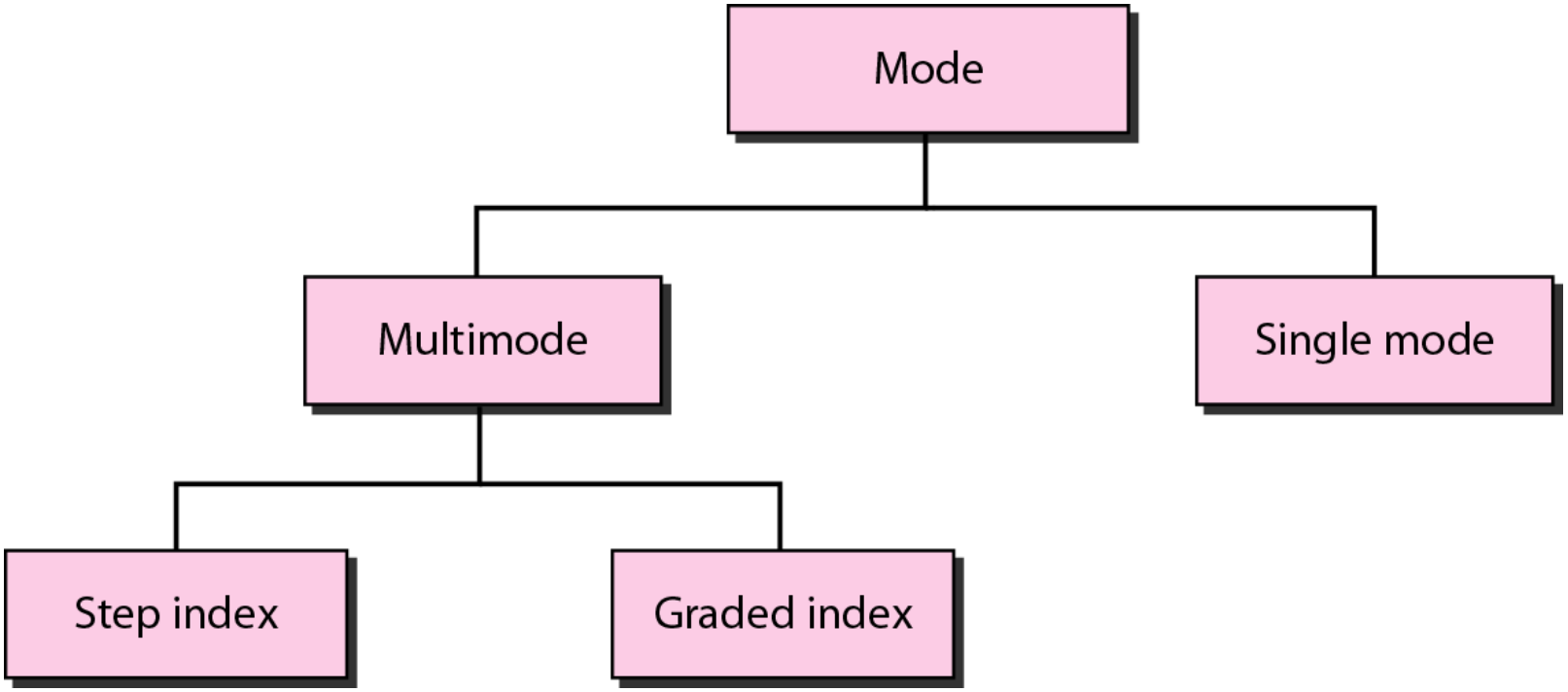
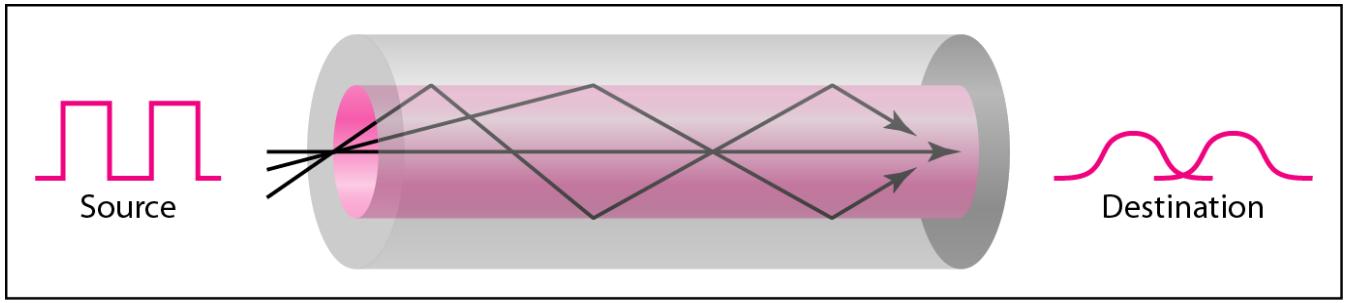
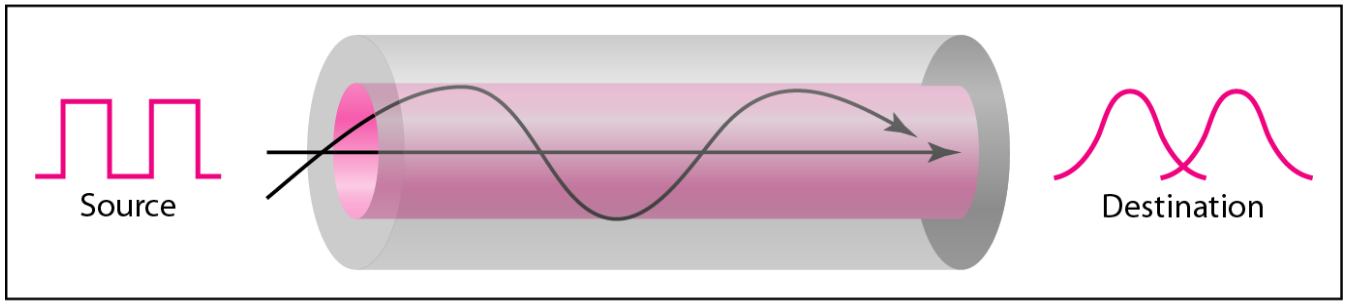


Figure 7.12 ***Propagation modes***

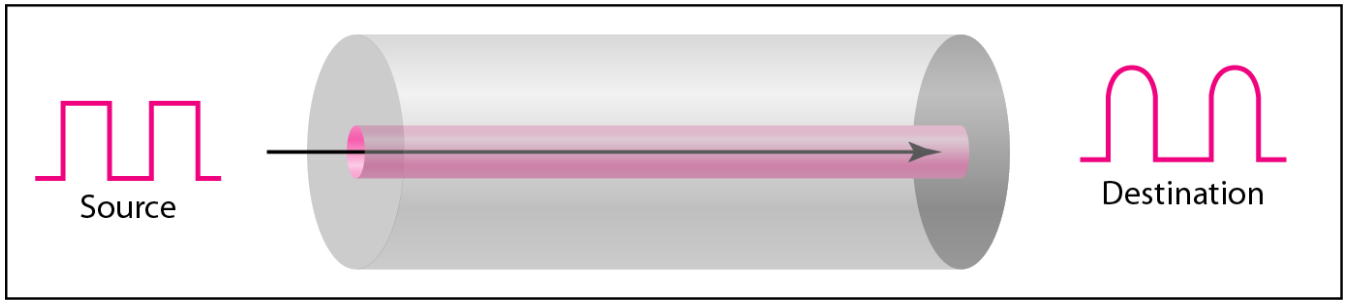
Figure 7.13 *Modes*



a. Multimode, step index



b. Multimode, graded index



c. Single mode

Optical Fiber

Table 7.3 ***Fiber types***

Type	*Core (μm)*	*Cladding (μm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

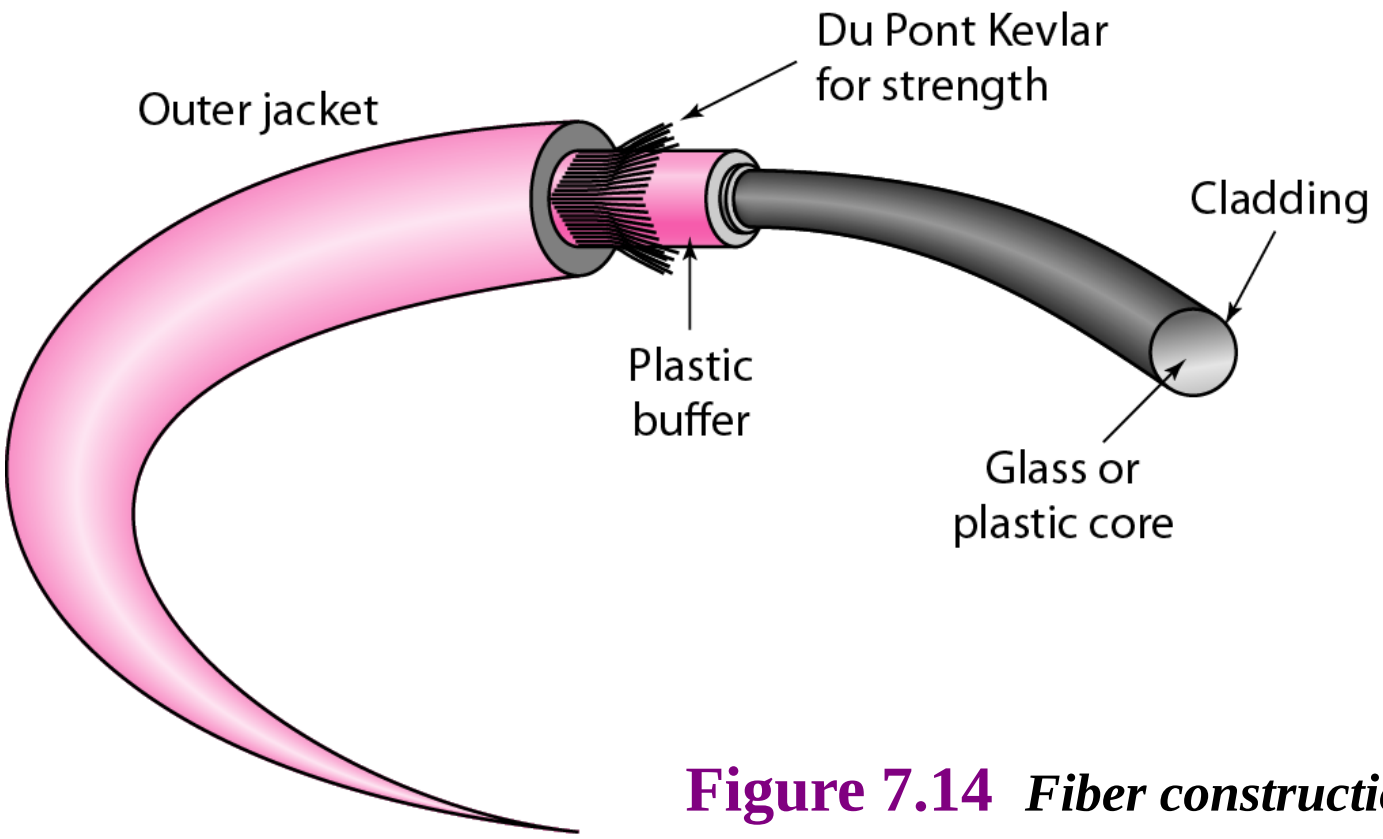


Figure 7.14 *Fiber construction*

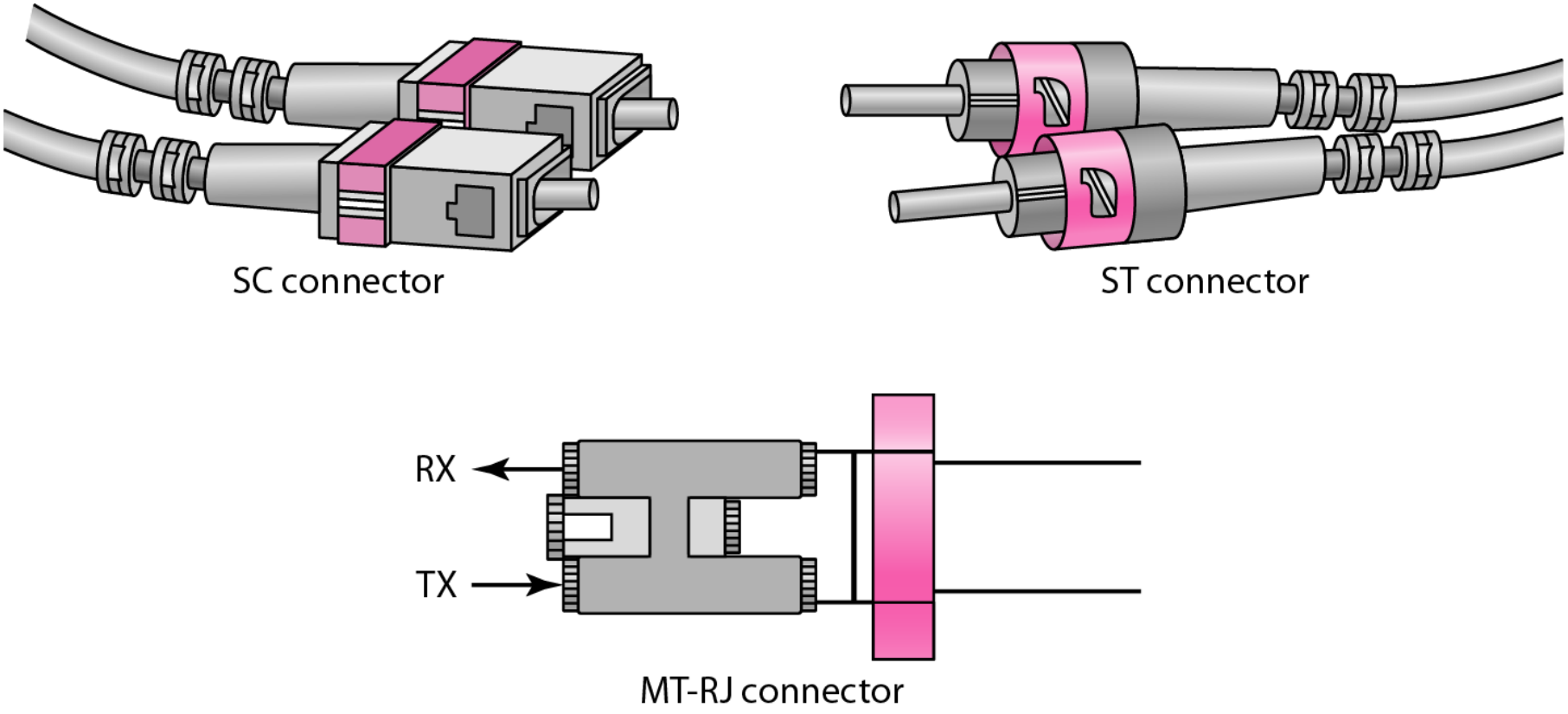
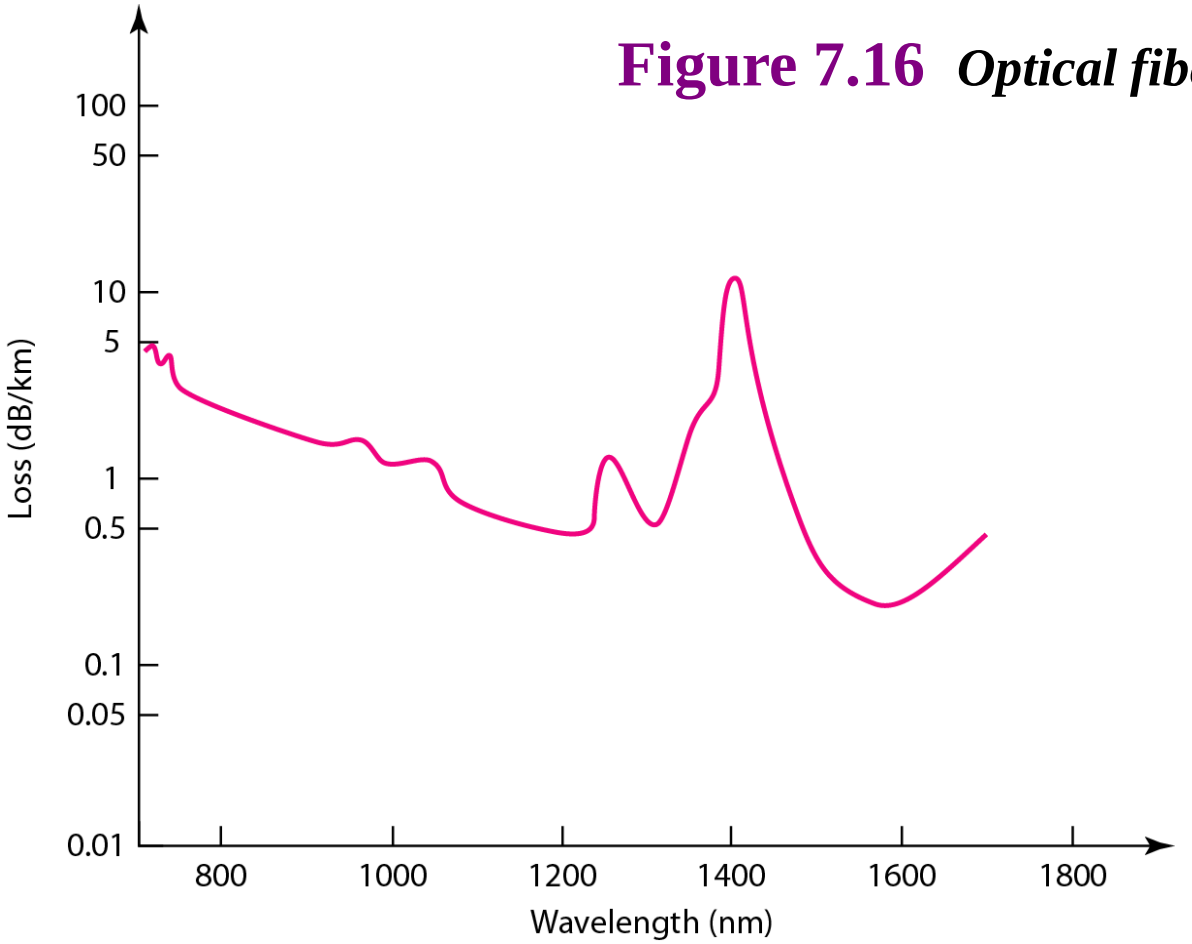


Figure 7.15 ***Fiber-optic cable connectors***

Figure 7.16 *Optical fiber performance*



Advantages/disadvantages

- Advantages
  - Higher bandwidth
  - Less signal attenuation
  - Immunity to electromagnetic interference
  - Resistance to corrosive materials
  - Light weight
  - Greater immunity to tapping
- Disadvantages
  - Installation and maintenance
  - Unidirectional light propagation
  - Cost

Unguided Media

- Unguided media transport electromagnetic waves without using a physical conductor.
- This type of communication is often referred to as wireless communication.
- Unguided signals can travel from the source to the destination in several ways: ground propagation, sky propagation, and line-of-sight propagation.

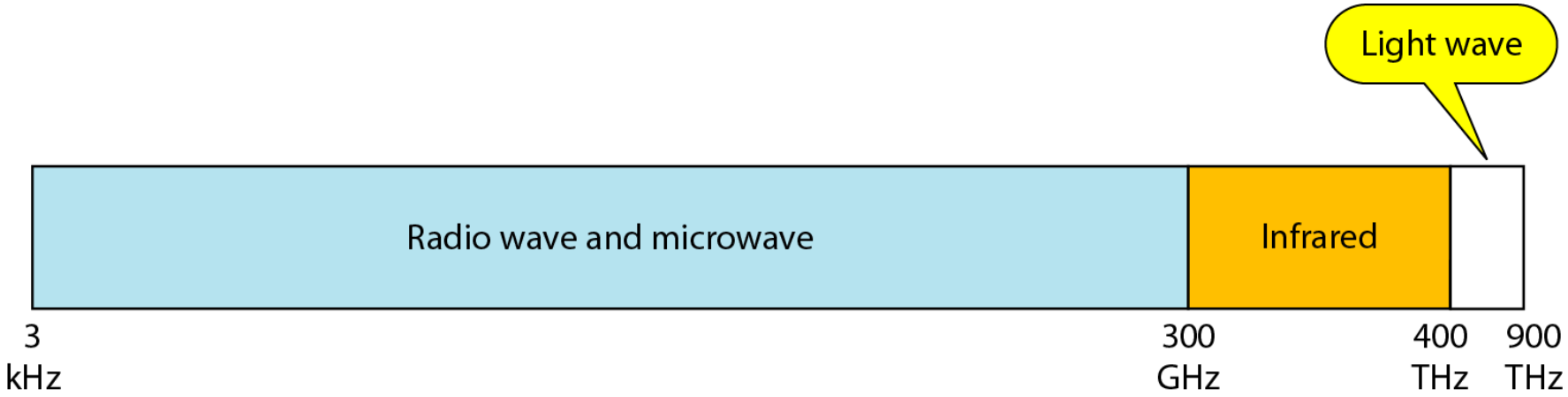
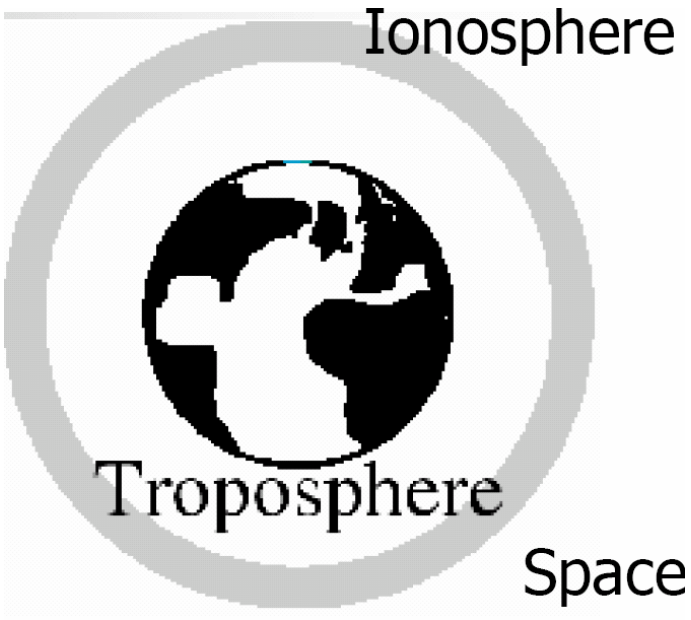


Figure 7.17 *Electromagnetic spectrum for wireless communication*

Earth Atmosphere

- Troposphere
  - 30 miles from earth
  - Air
  - Cloud, wind, weather
  - Jet plane travel
- Ionosphere
  - Between troposphere and space
  - Free electrically charged particles



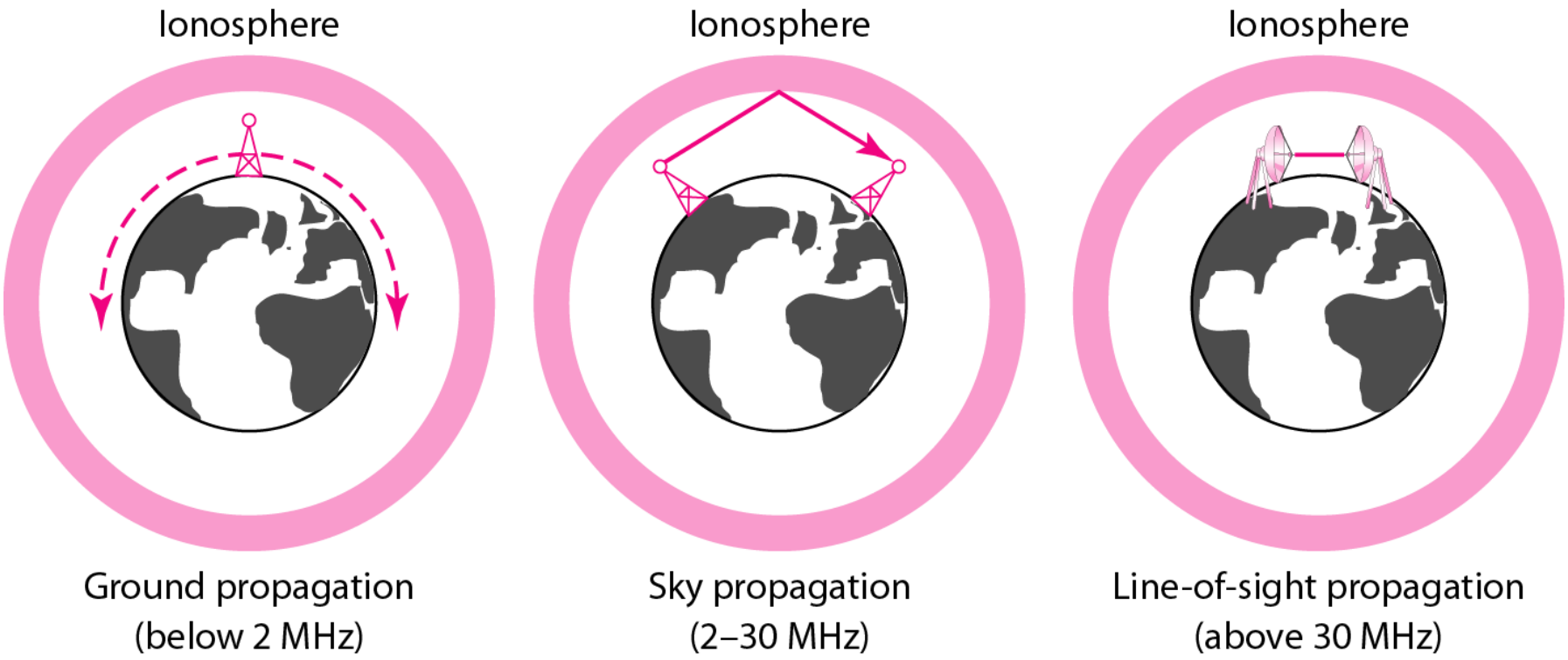
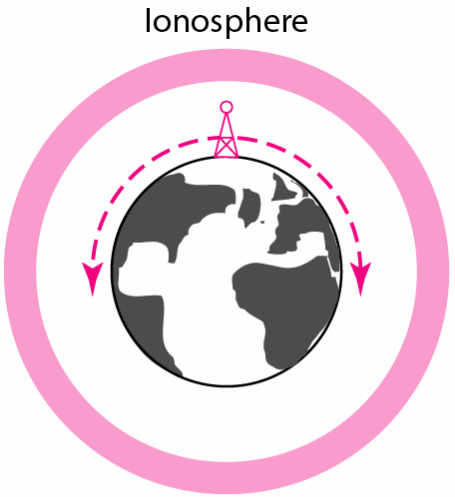


Figure 7.18 ***Propagation methods***

Ground propagation

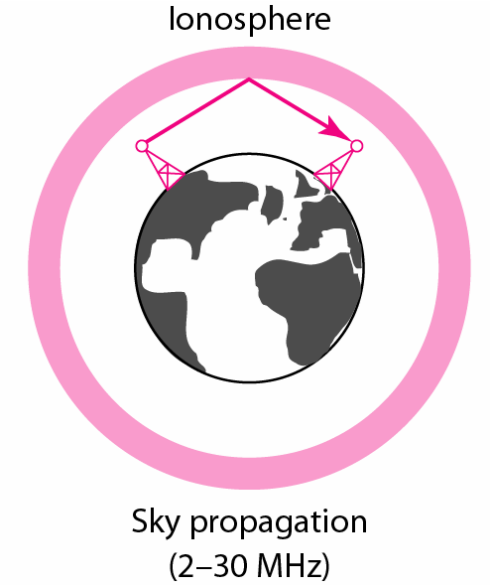
- Radio waves travels through the lowest portion of the atmosphere
- VLF (in range of 3KHz – 10 KHz)
  - Low attenuation
  - Atmosphere noise (heat & electricity)
  - For long-range radio navigation
- LF (in range of 30 KHz – 300 KHz)
  - For long-range radio navigation
  - Greater attenuation
- Distance depends on the amount of power in the signal



Ground propagation
(below 2 MHz)

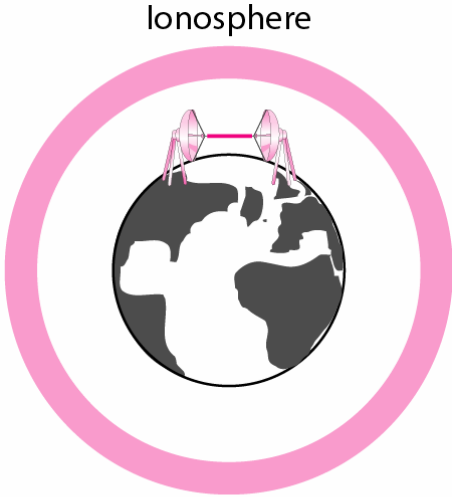
Sky propagation

- Higher frequency radio waves radiate upward into ionosphere where they reflect back to earth.
- Allows greater distance with lower output power



Line-of-sight propagation

- Very high frequency signals transmitted in straight lines from antenna to antenna
- Antenna must be directional
- This mode is tricky because radio transmissions cannot be completely focused



Line-of-sight propagation (above 30 MHz)

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite

Wireless transmission waves

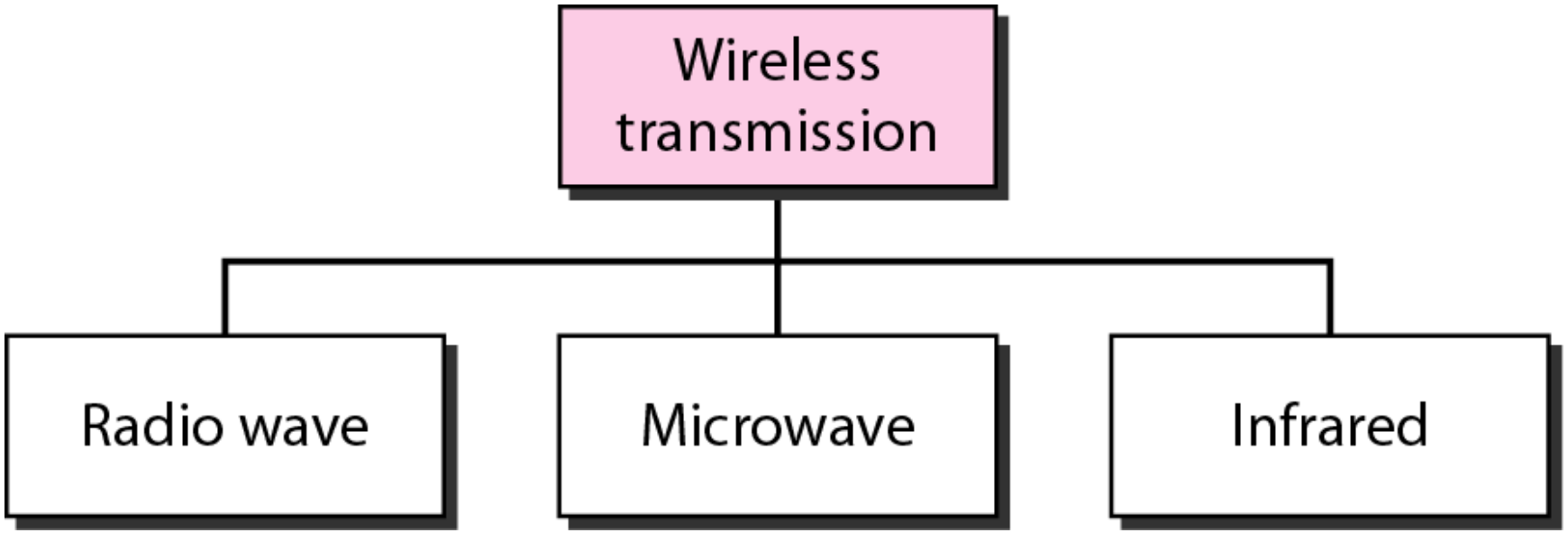


Figure 7.19 *Wireless transmission waves*

Radio waves

- Ranging from 3 KHz and 1 GHZ
- Omnidirectional, waves propagated in all directions
- Sender and receiver must not be aligned
- Propagate in sky mode
- With low frequencies can penetrate walls
- The radio wave band is relatively narrow

Radio waves

Radio waves are used for multicast communications, such as radio and television, and paging systems.
They can penetrate through walls.
Highly regulated.
Use Omni directional antennas.

Microwave

- Ranges from 1 and 300 GHz
  - They can be narrowly focused (use unidirectional antenna)
  - A pair of antenna can be aligned without interfering with another pair of aligned antennas
- Characteristics
  - Line-of-sight
  - Repeaters are needed for long distances
  - High frequency cannot penetrate walls
  - Microwave band is relatively wide, therefore wider subbands can be assigned, (higher data rate)

Microwave

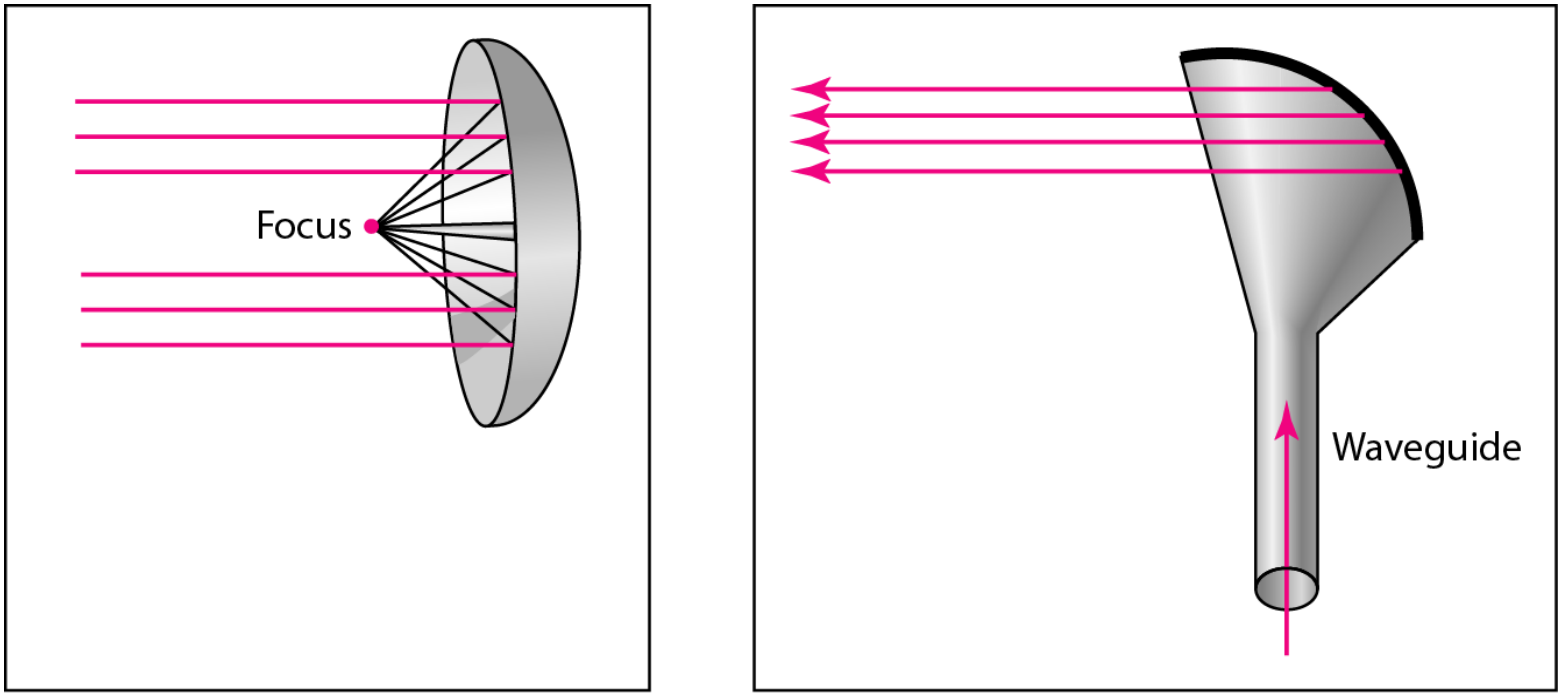


Figure 7.21 *Unidirectional antennas*

Microwave

Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

Infrared

- Ranges from 300 GHz to 400 GHz
- Used for short range communication
- High frequency
- Cannot penetrate walls
- Cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication

Infrared

Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation

Systems and Control Eng. Dept.

Computer Networks

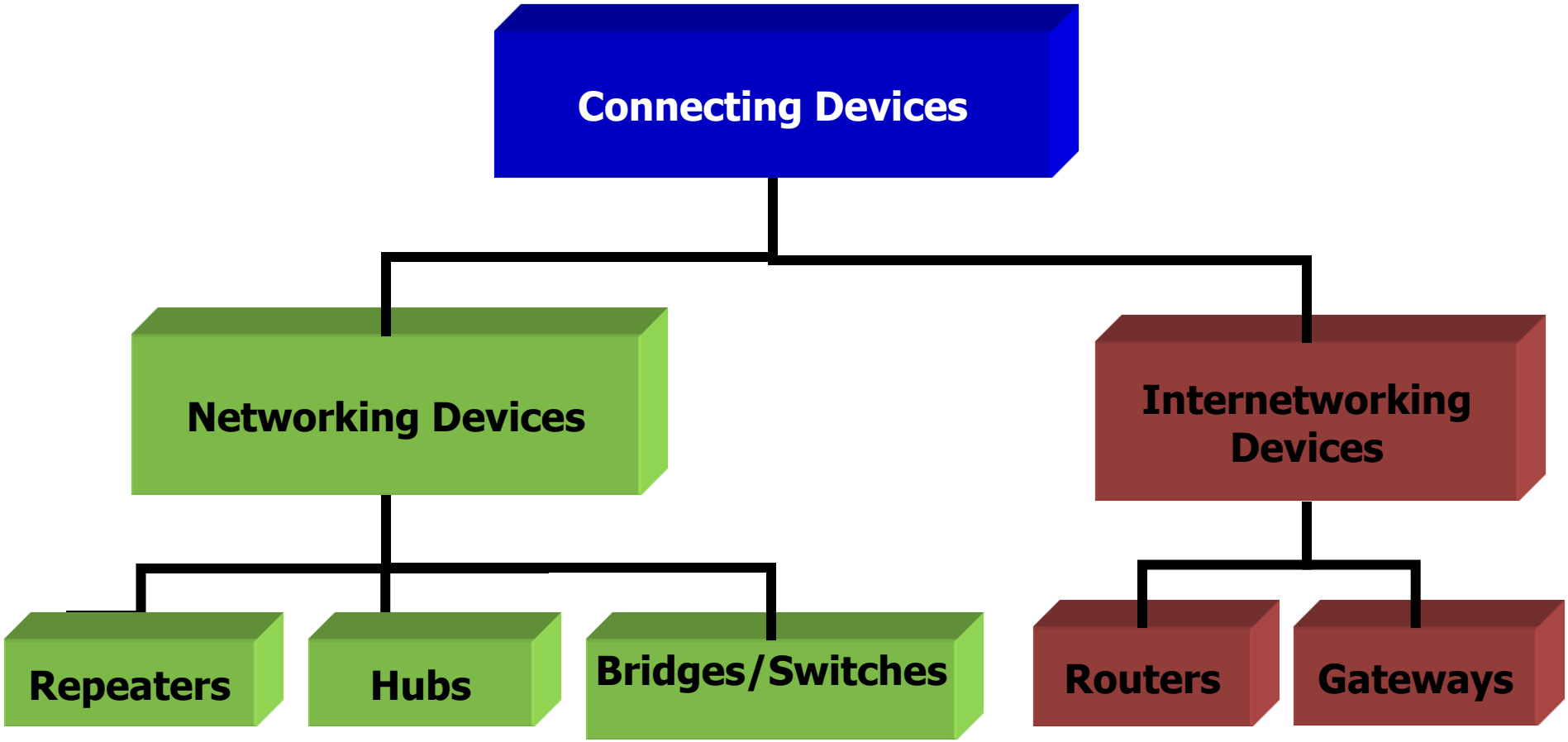
Fourth Year Class

Lecture 7

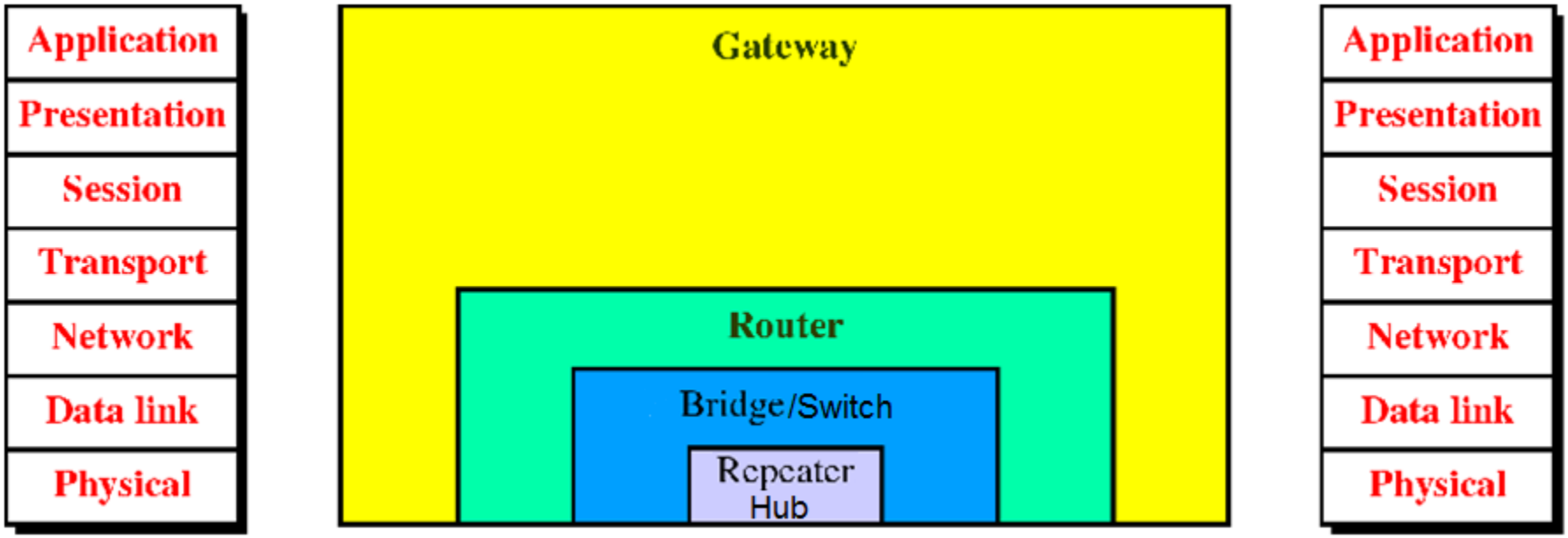
Connecting Devices

Abdulhameed N. Hameed

Connecting Devices



Five categories of connecting devices

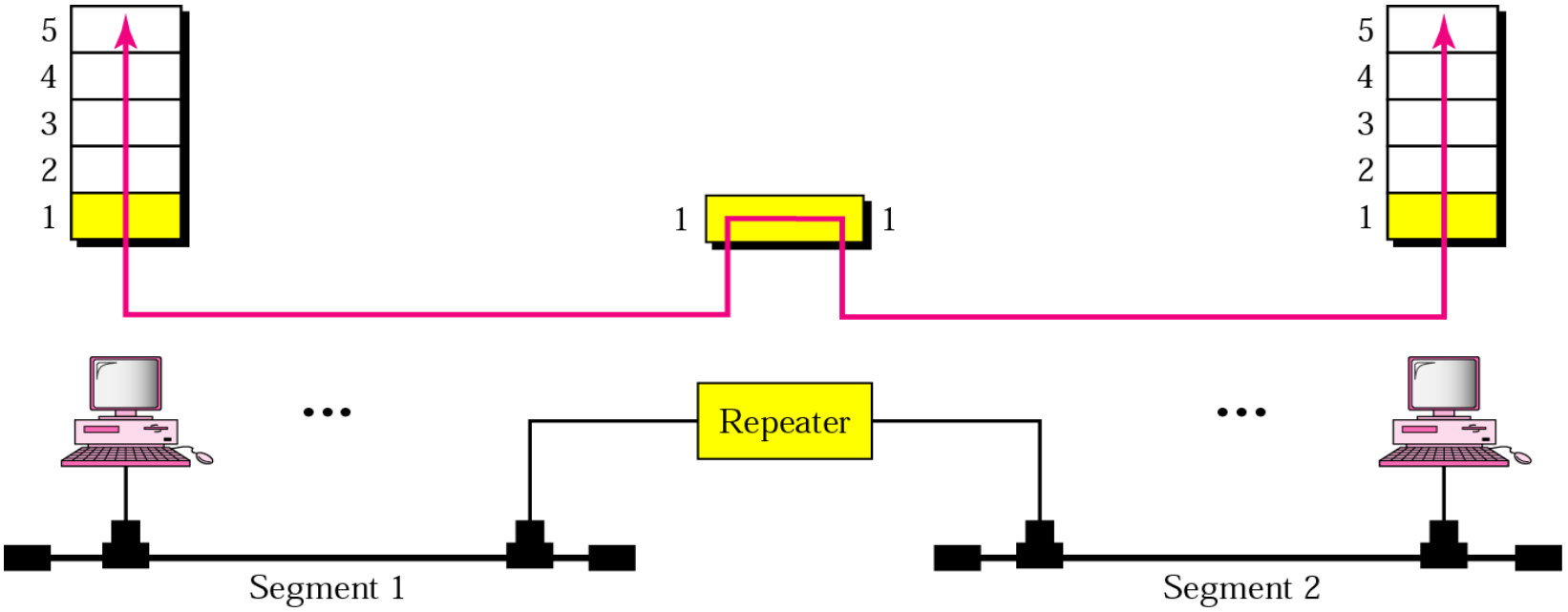


Repeaters

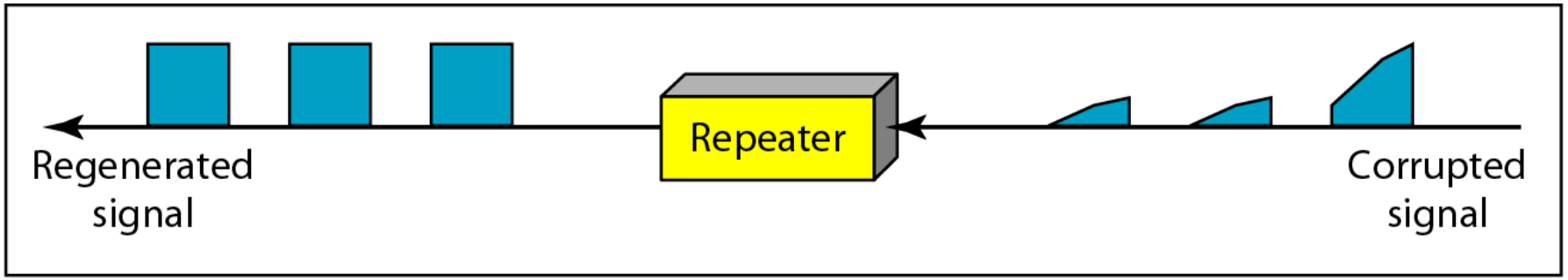
- Acts on the **physical layer**
- Operate on bits
- When a bit (0,1) arrives, the repeater receives it and **regenerates** it, then transmits it onto all other interfaces
- Used in LAN to **connect cable segments** and **extend** the **maximum cable length** ➔ extending the **geographical LAN range**
  - Ethernet 10base5 – Max. segment length 500m – 4 repeaters are used to extend the cable to 2500m.
  - Ethernet 10Base2- Max. segment length 185m - 4 repeaters are used to extend the cable to 925m.
- Repeaters do not implement any **access method**
  - If any two nodes on any two connected segments transmit at the same time **collision** will happen

Repeater

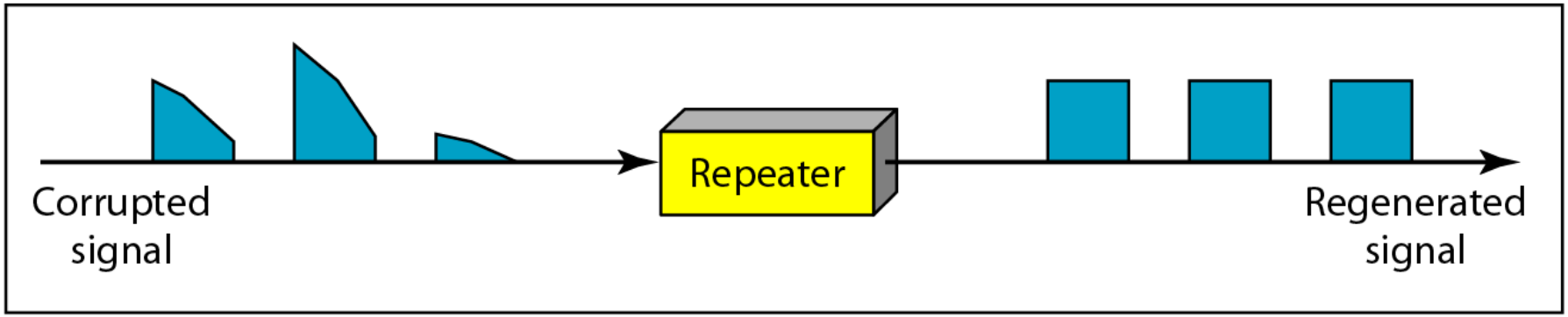
A repeater connecting two segments of a LAN



Function of a Repeater



a. Right-to-left transmission.

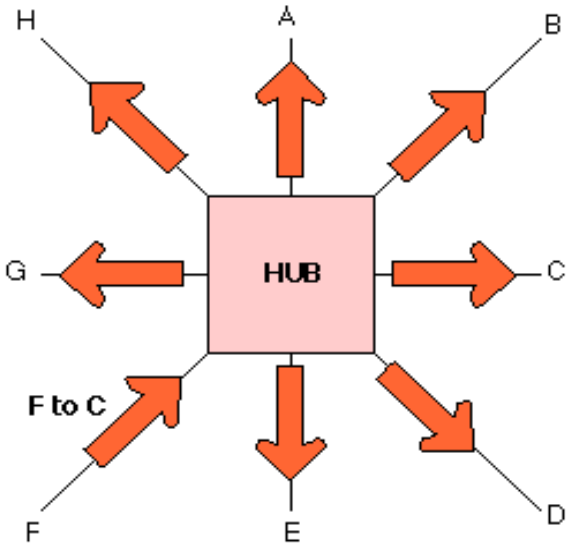


b. Left-to-right transmission.

Hubs

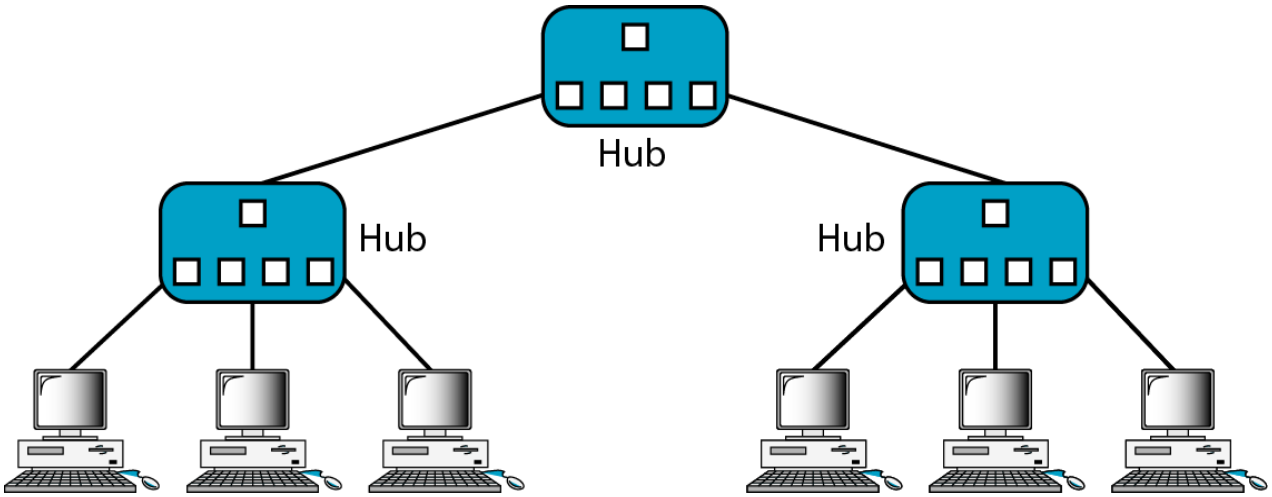
- Acts on the **physical layer**
- Operate on bits
- Also called **multiport repeater**
- Used to connect stations in a **physical star topology**
- Connection to the hub consists of **two pairs of twisted pair wire** one for **transmission** and the other for **receiving**.
- Hub receives a bit from an adapter and sends it to **all** the other adapters **without implementing any access method**.
- Does not do **filtering** (forward a frame into a specific destination or drop it) just it copy the received frame onto **all other links**
- The entire hub forms **a single collision domain**, and **a single Broadcast domain.**
  - **Collision domain**: is that part of the network when two or more nodes transmit at the same time collision will happen.
  - **Broadcast domain:** is that part of the network where the broadcast messages are reached. (**broadcast** is the transmission of a message to all hosts on the network simultaneously).
- Multiple Hubs can be used **to extend** the network length
- For 10BaseT and 100BaseT the maximum length of the connection between an adapter and the hub is 100 meters ➔ the maximum length between any two nodes is 200 m = maximum network length

Hubs



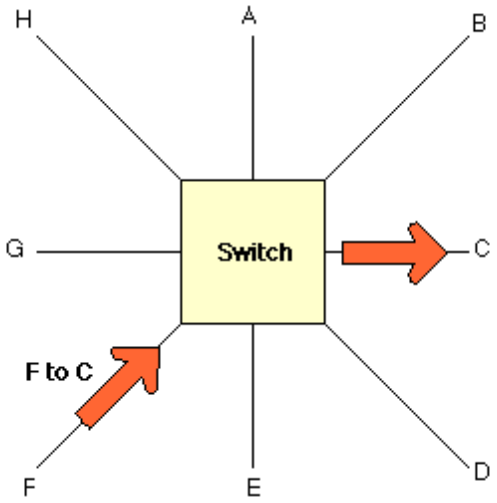
Interconnecting with hubs

- Backbone hub interconnects LAN segments
- **Advantage**:
  - Extends max distance between nodes
- **Disadvantages**
  - Individual segment collision domains become one large collision domain ➔ (**reduce the performance**)
  - Can't interconnect different Ethernet technologies(like 10BaseT & 100BaseT) because **no buffering** at the hub

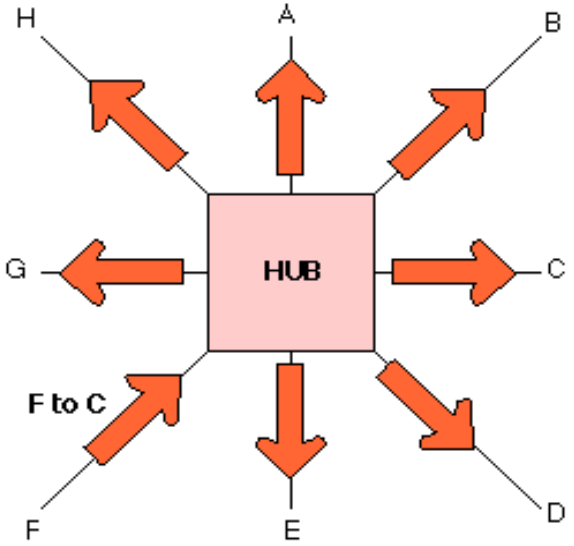


Here we have a single collision domain and a single broadcast domain

Bridges (Switches) Vs. Hubs



A Switch sending a packet from F to C



A Hub sending a packet form F to C.

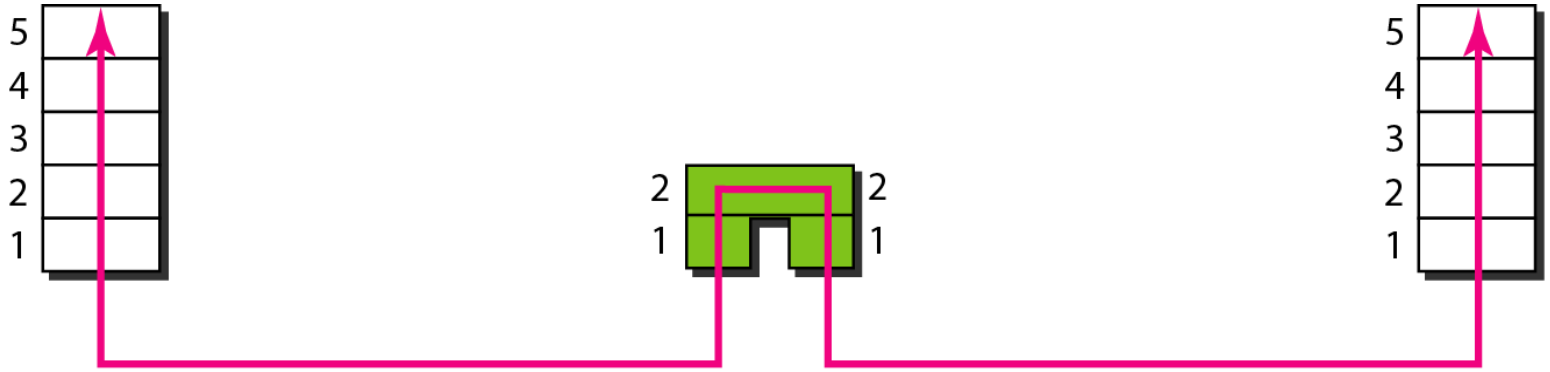
Bridges/Switches

- Acts on the **data link** layer (MAC address level)
- Operate on frames
- Used to **divide** (segment) the LAN into smaller LANs segments.
- Each LAN segment is a **separate collision domain**
- Bridge does not send the received frame to all other interfaces like hubs and repeaters, but it performs **filtering** which means:
  - Whether a frame should be **forwarded** to another interface that leads to the destination or **dropped**
- This is done by a bridge table (**forwarding table**) that contains entries for the nodes on the LAN
  - The bridge table is **initially empty** and **filled automatically** by **learning from frames movements** in the network
  - An entry in the bridge table consists of : node LAN (**MAC) Address, Bridge Interface to which the node is connected to**, **the record creation time**

Address	Interface	Time
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36
...	...	...

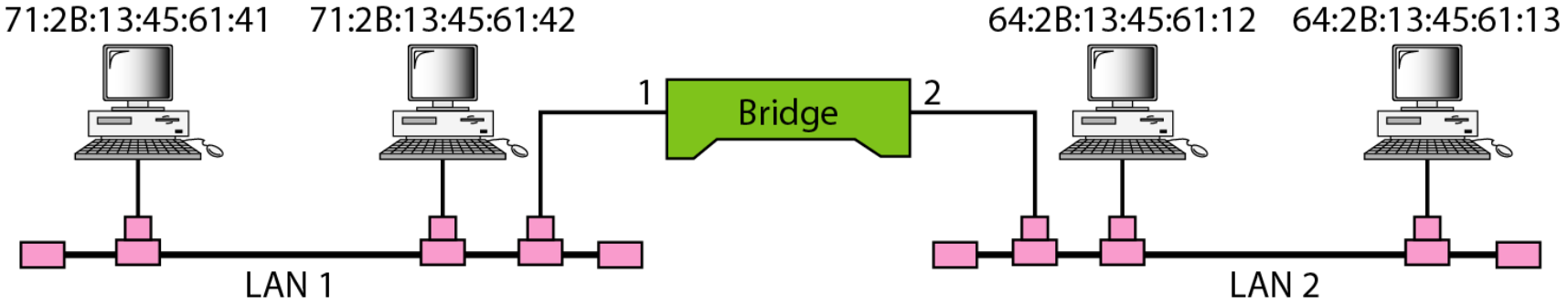
- A bridge runs **access method** before sending a frame onto the link not like the hub or repeater

A bridge/Switch connecting two or more LANs



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

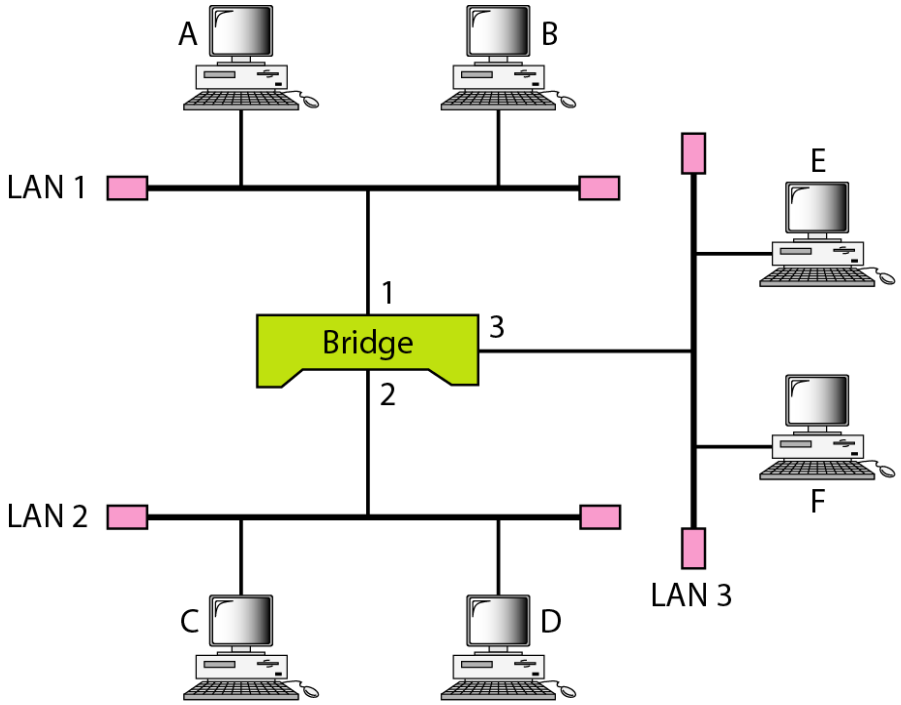
Bridge Table



Bridge/ Switch learning Process

- When the switch receives a frame, it compares the **source address** of the frame with each entry in the forwarding table
  - If **No match is found**, the switch will **add** to the table the frame **source address** and the **Interface** on which the frame **was received.**
  - If a **match is found**, the switch **updates** the **Interface number** on which the frame was received if **it is different** from the one in the table also it **updates** the **record time**
- Then, the switch compares the **destination address** of the frame with each entry in the **forwarding table (MAC table)**
  - If a match is found then
    - The switch compares the **interface number** on which the frame was received and the interface number in the table, if they are **different** the switch **forwards** the frame through the interface number stored in the table. Otherwise, if they are the **same** the switches **discards** (**drops**) the frame.
  - If no match is found, the switch **floods the frame** on **all interfaces** except the one on which the frame was received.

A learning switch and the process of learning



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

c. After E sends a frame to A

Address	Port
A	1
E	3
B	1

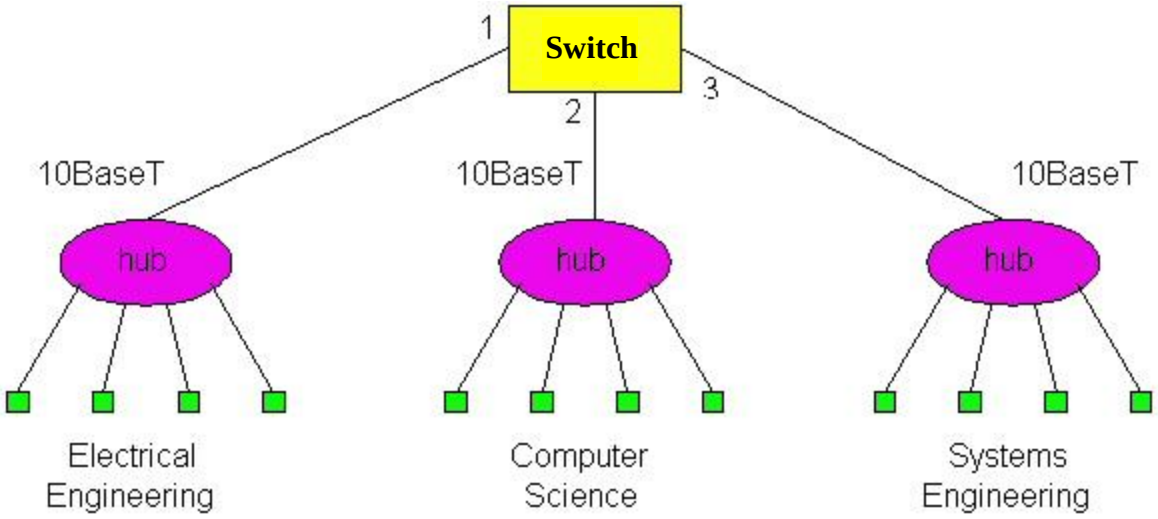
d. After B sends a frame to C

Switch learning Process Summary

Switching Process	Description
Learn Examining the Source MAC Address	• Switches examine all incoming frames for new source MAC address information to learn. • If the source MAC address is unknown, it is added to the table along with the port number. • If the source MAC address does exist, the switch updates the refresh timer for that entry. • By default, most Ethernet switches keep an entry in the table for 5 minutes.

Forward
Examining the Destination MAC Address
	• If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.
	• If the destination MAC address is a unicast address, the switch will look for a match in its MAC address table.
	  • If the destination MAC address is in the table, it will forward the frame out the specified port.
	  • If the destination MAC address is not in the table (i.e., an unknown unicast) the switch will forward the frame out all ports except the incoming port.

Example: how many collision domains in this network?

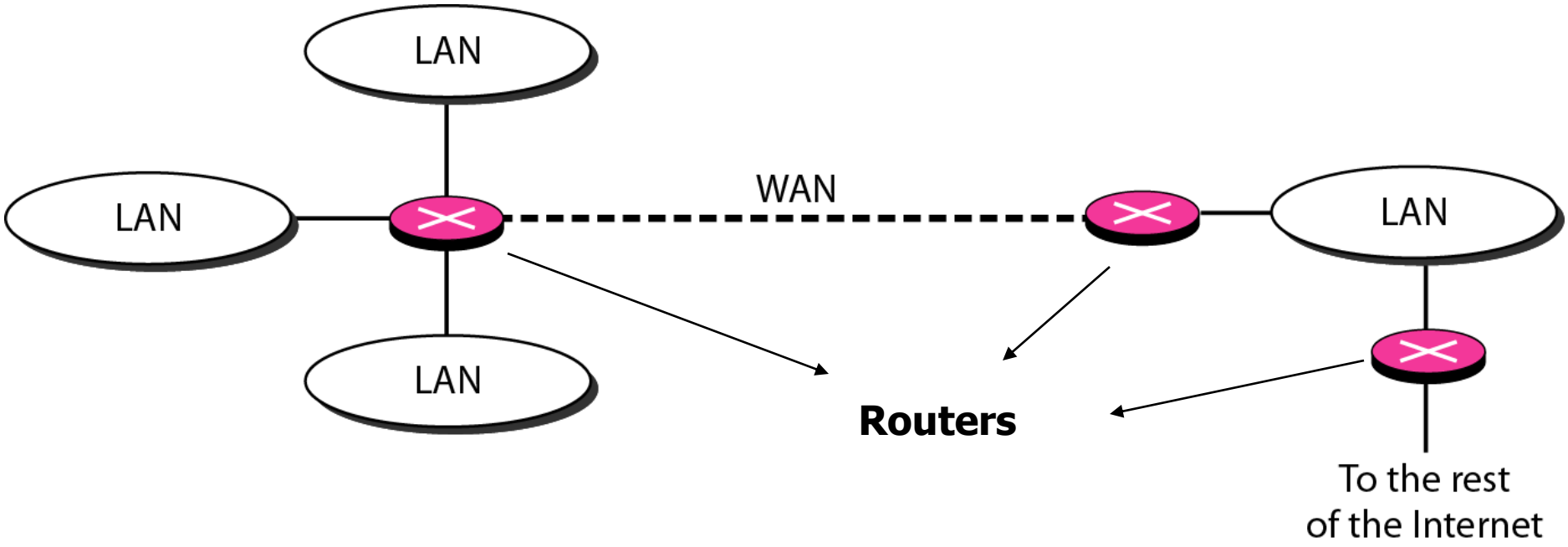


Three LANs connected through a switch (*three collision* domains are there)

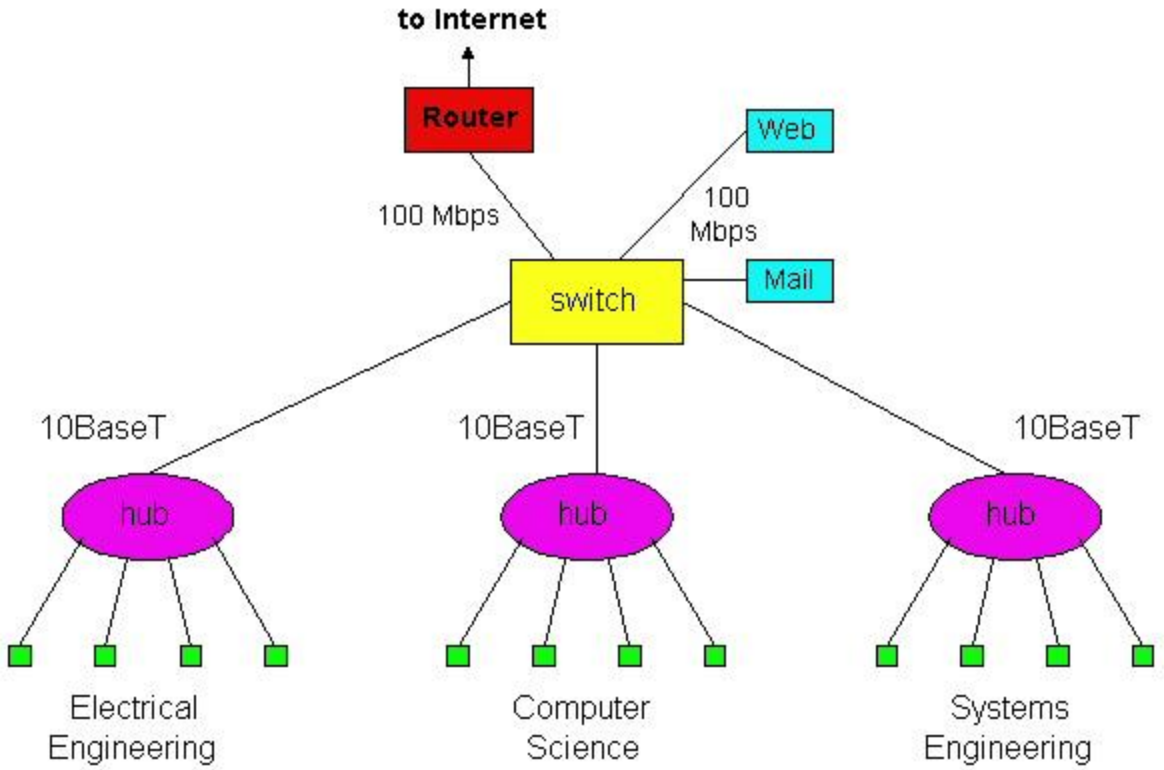
Routers

- Operates at network layer = deals with **packets** not **frames**
- Connect LANs and WANs with similar or different protocols together
- Switches and bridges **isolate collision domains** but forward broadcast messages to **all LANs** connected to them. Routers **isolate both** *collision* domains and *broadcast* domains
- Have **more than one** network address (an address to each connected network)
- Deals with global address (network layer address (IP)) not local address (MAC address)
- Routers **Communicate with each other** and exchange routing information
- Determine best route using **routing algorithm** by special software installed on them
- **Forward traffic if information on destination** is available otherwise **discard** it (not like a switch or bridge)

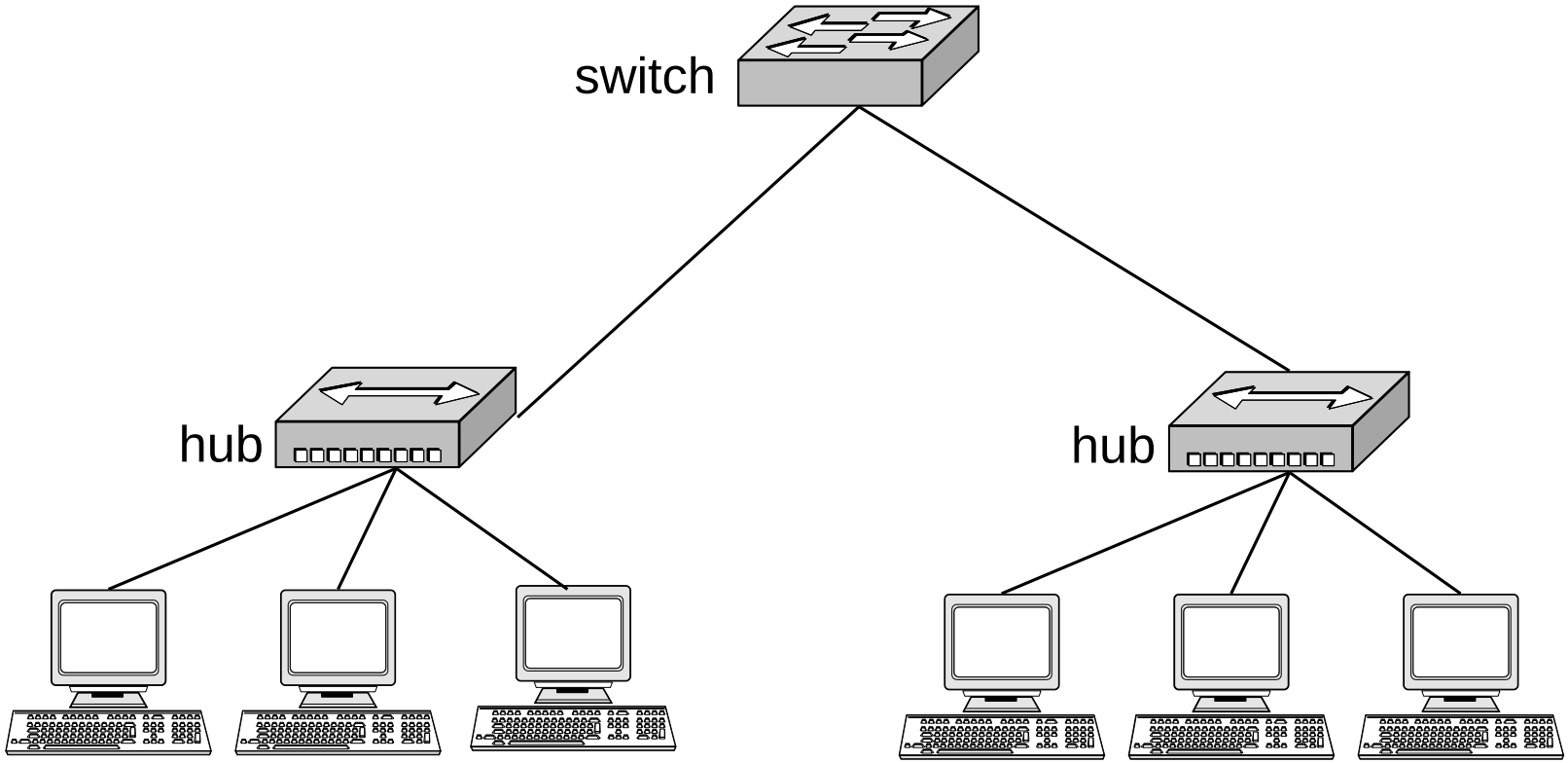
Routers connecting independent LANs and WANs



An Institutional Network Using Hubs, Ethernet Switches, and a Router



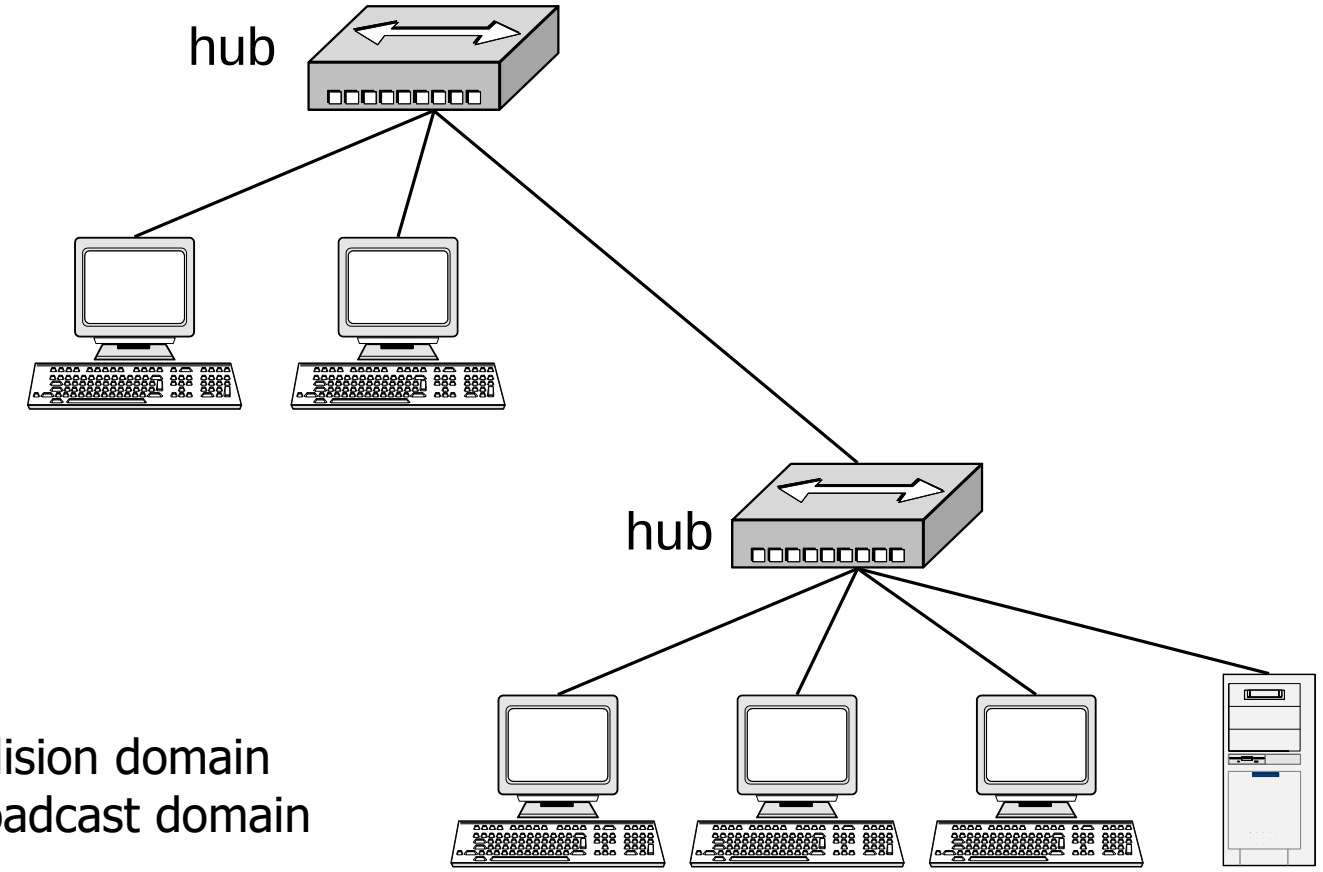
Identify the collision domains & broadcast domains:



_____collision domains

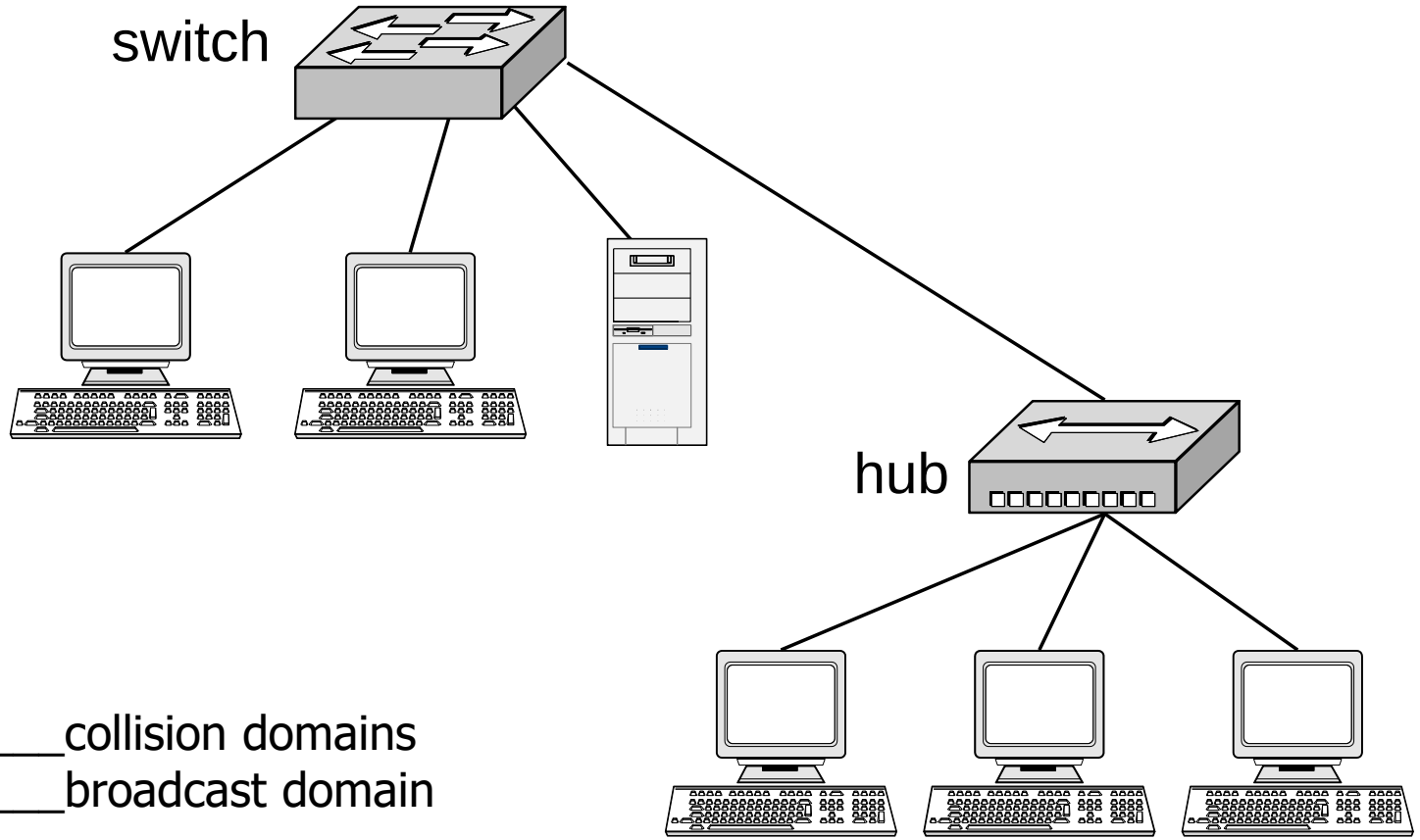
_____broadcast domain

Identify the collision domains & broadcast domains:



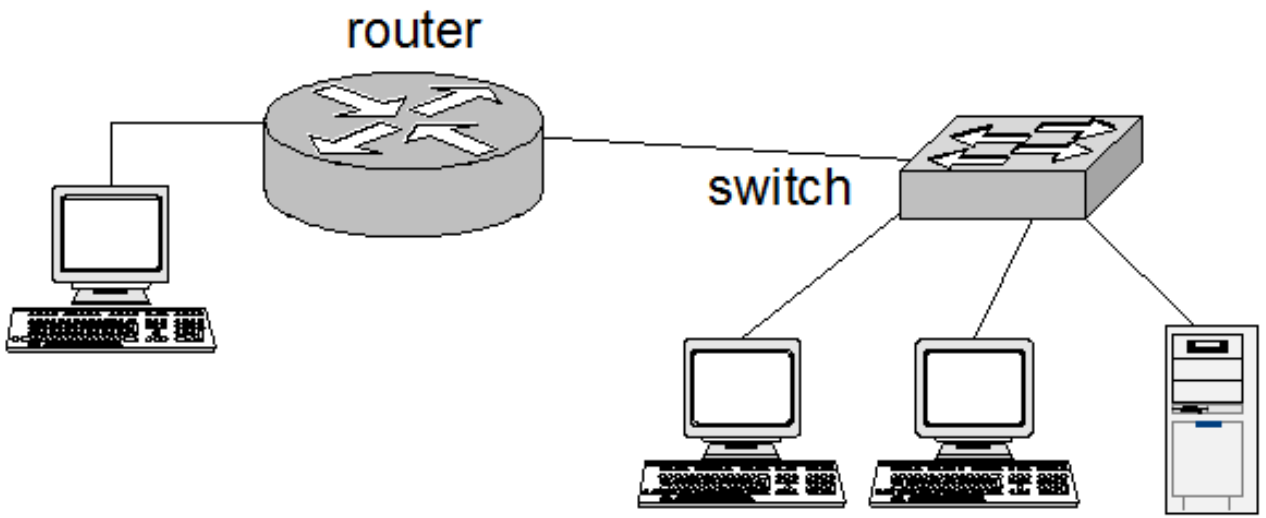
_____collision domain
_____broadcast domain

Identify the collision domains & broadcast domains:



_____collision domains
_____broadcast domain

Identify the collision domains & broadcast domains:



_____collision domains
_____broadcast domains

Systems and Control Eng. Dept.

Computer Networks

Fourth Year Class

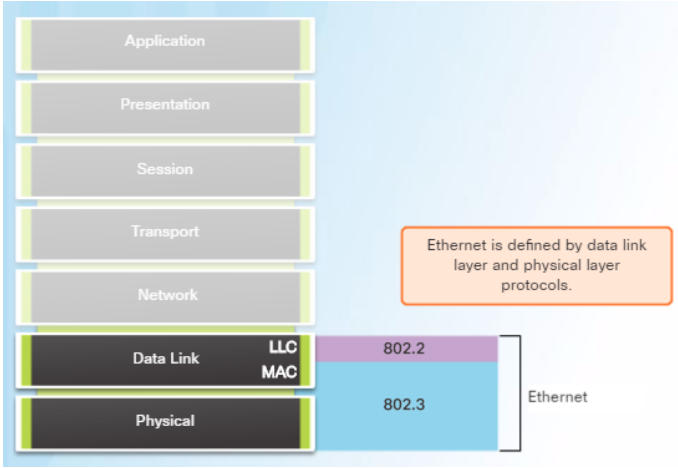
Lecture 8

Introduction to Data Link Layer

Abdulhameed N. Hameed

Ethernet Encapsulation

- Ethernet is the most widely used LAN technology today.
  - Defined in the IEEE 802.2 and 802.3 standards.
  - It supports data bandwidths of 10 Mb/s, 100 Mb/s, 1000 Mb/s (1 Gb/s), 10,000 Mb/s (10 Gb/s), 40,000 Mb/s (40 Gb/s), and 100,000 Mb/s (100 Gb/s).



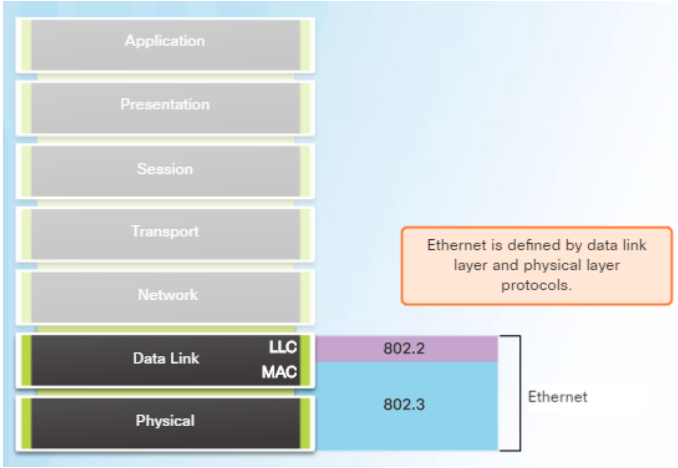
- Ethernet operates in the data link layer and the physical layer.

- Ethernet relies on the two separate sublayers of the data link layer to operate, the Logical Link Control (LLC) and the MAC sublayers.

Ethernet Encapsulation (Cont.)

- The Ethernet LLC sublayer handles the communication between the upper layers and the lower layers. It is implemented in software, and its implementation is independent of the hardware.

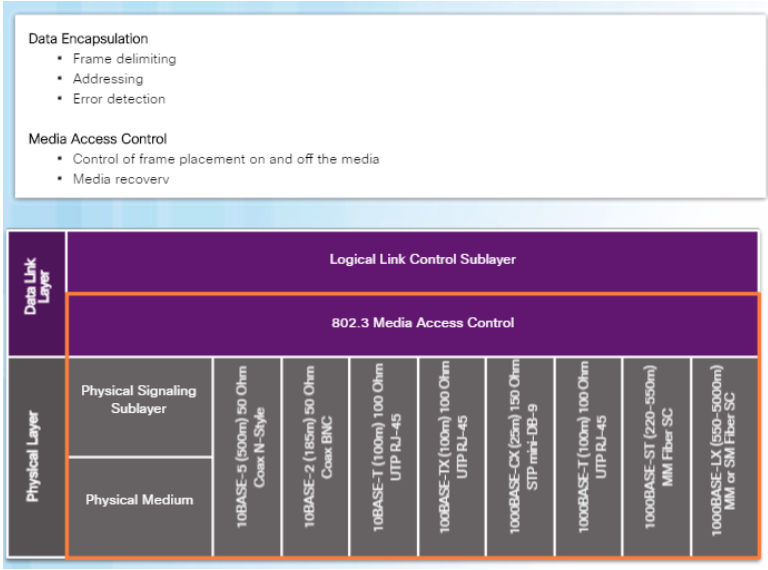
- The MAC sublayer constitutes the lower sublayer of the data link layer. MAC is implemented by hardware, typically in the computer NIC.



MAC Sublayer

- The MAC sublayer has two primary responsibilities:
  - Data encapsulation
  - Media access control

- Data encapsulation provides three primary functions:
  - Frame delimiting
  - Addressing
  - Error detection



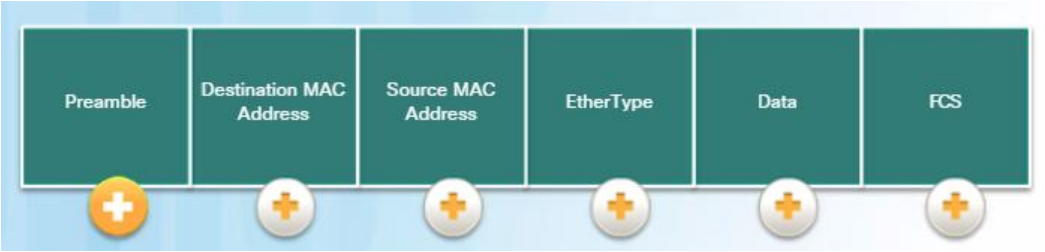
- Media access control is responsible for the placement of frames on the media and the removal of frames from the media. This sublayer communicates directly with the physical layer.

Ethernet Evolution

- Since 1973, Ethernet standards have evolved specifying faster and more flexible versions of the technology.
- Early versions of Ethernet were relatively slow at 10 Mbps.
- The latest versions of Ethernet operate at 10 Gigabits per second and faster.

Ethernet Frame Fields

- The minimum Ethernet frame size from Destination MAC address to FCS is 64 bytes and the maximum is 1518 bytes.



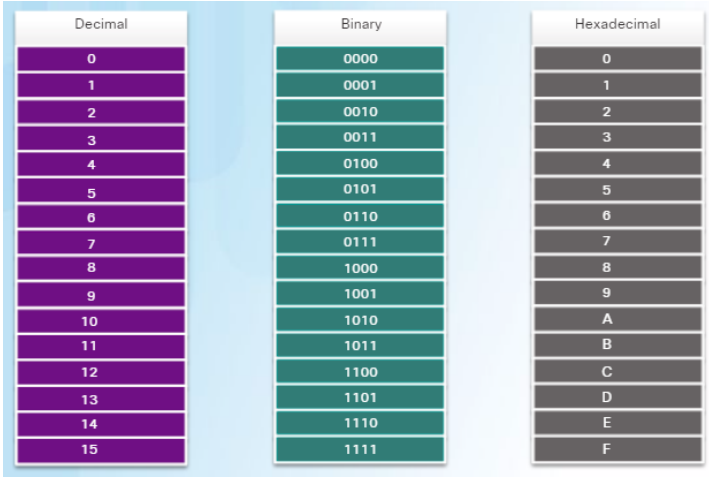
- Frames less than 64 bytes are called a “collision fragment” or “runt frame” and are automatically discarded by receiving stations. Frames greater than 1500 bytes of data are considered “jumbo” or “baby giant frames”.

- If the size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame.

MAC Addresses and Hexadecimal

- An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits (4 bits per hexadecimal digit).

- Hexadecimal is used to represent Ethernet MAC addresses and IP Version 6 addresses.
  - Hexadecimal is a base sixteen system using the numbers 0 to 9 and the letters A to F.
  - It is easier to express a value as a single hexadecimal digit than as four binary bits.
  - Hexadecimal is usually represented in text by the value preceded by 0x (E.g., 0x73).



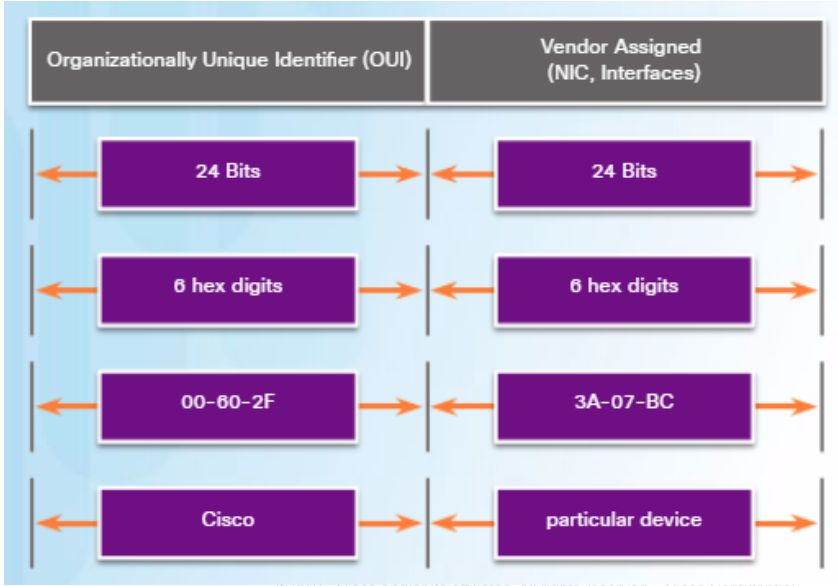
Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

- Convert the decimal or hexadecimal value to binary, and then to convert the binary value to either decimal or hexadecimal as needed.

MAC Addresses: Ethernet Identity

- MAC addresses were created to identify the actual source and destination.
  - The MAC address rules are established by IEEE.
  - The IEEE assigns the vendor a 3-byte (24-bit) code, called the Organizationally Unique Identifier (OUI).

- IEEE requires a vendor to follow two simple rules:
  - All MAC addresses assigned to a NIC or other Ethernet device must use that vendor's assigned OUI as the first 3 bytes.
  - All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes.

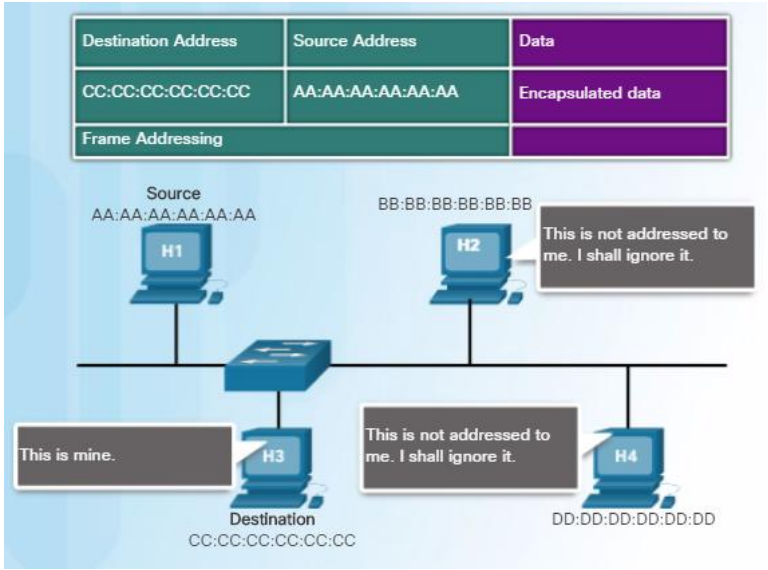


Frame Processing

- The MAC address is often referred to as a burned-in address (BIA) meaning the address is encoded into the ROM chip permanently. When the computer starts up, the first thing the NIC does is copy the MAC address from ROM into RAM.

- When a device is forwarding a message to an Ethernet network, it attaches header information to the frame.

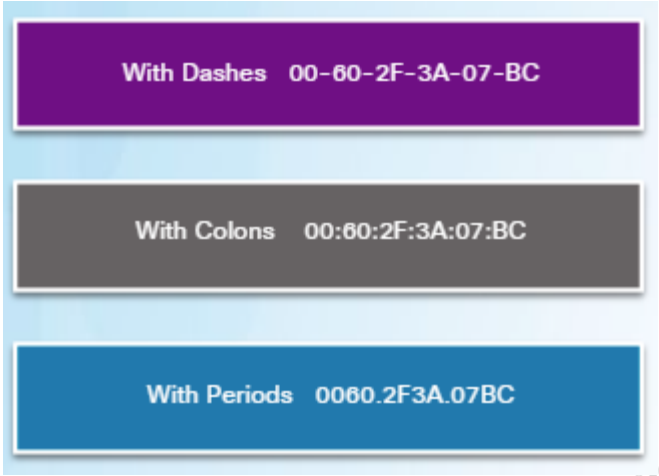
- The header information contains the source and destination MAC address.



MAC Address Representations

- Use the **ipconfig /all** command on a Windows host to identify the MAC address of an Ethernet adapter. On a MAC or Linux host, the **ifconfig** command is used.

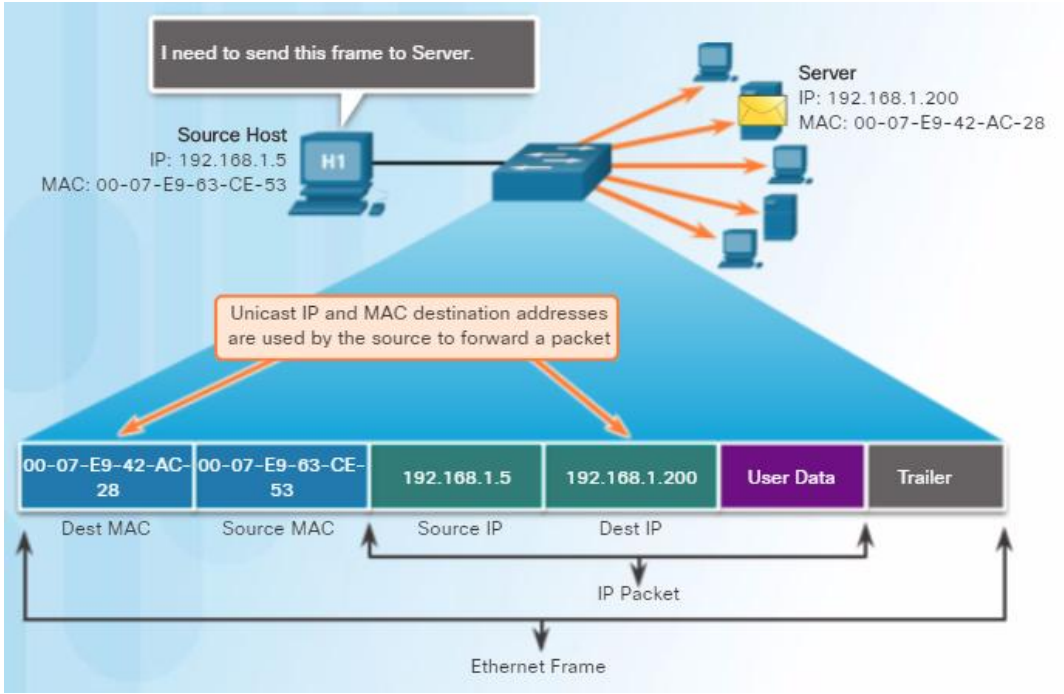
- Depending on the device and the operating system, you will see various representations of MAC addresses.



Unicast MAC Address

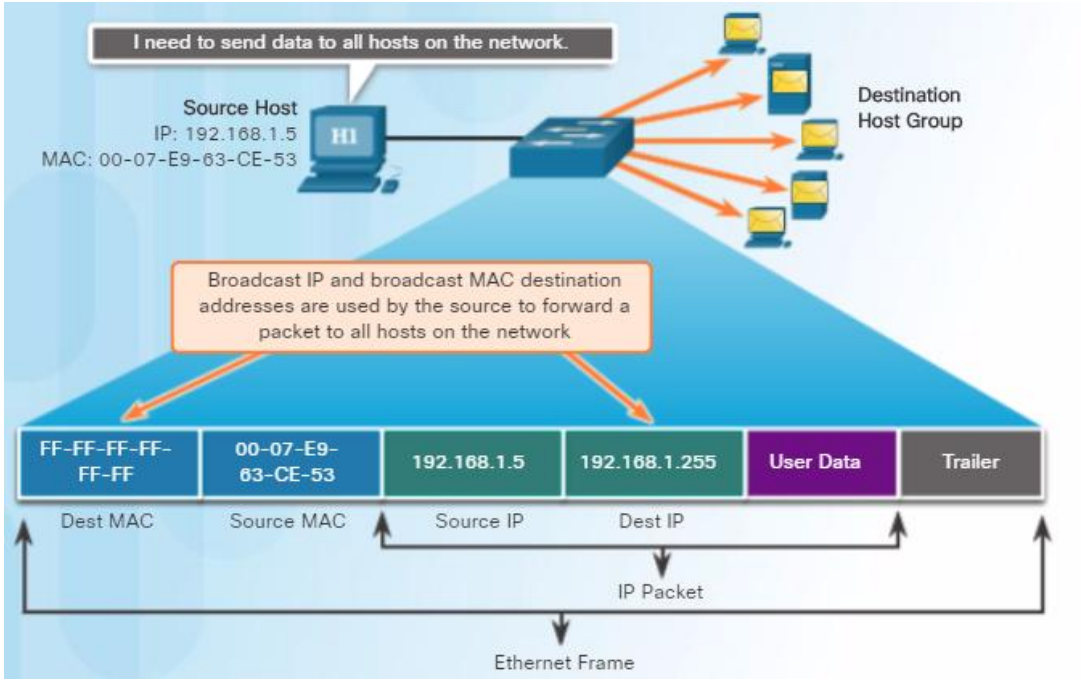
- A unicast MAC address is the unique address used when a frame is sent from a single transmitting device to a single destination device.

- For a unicast packet to be sent and received, a destination IP address must be in the IP packet header and a corresponding destination MAC address must also be present in the Ethernet frame header.



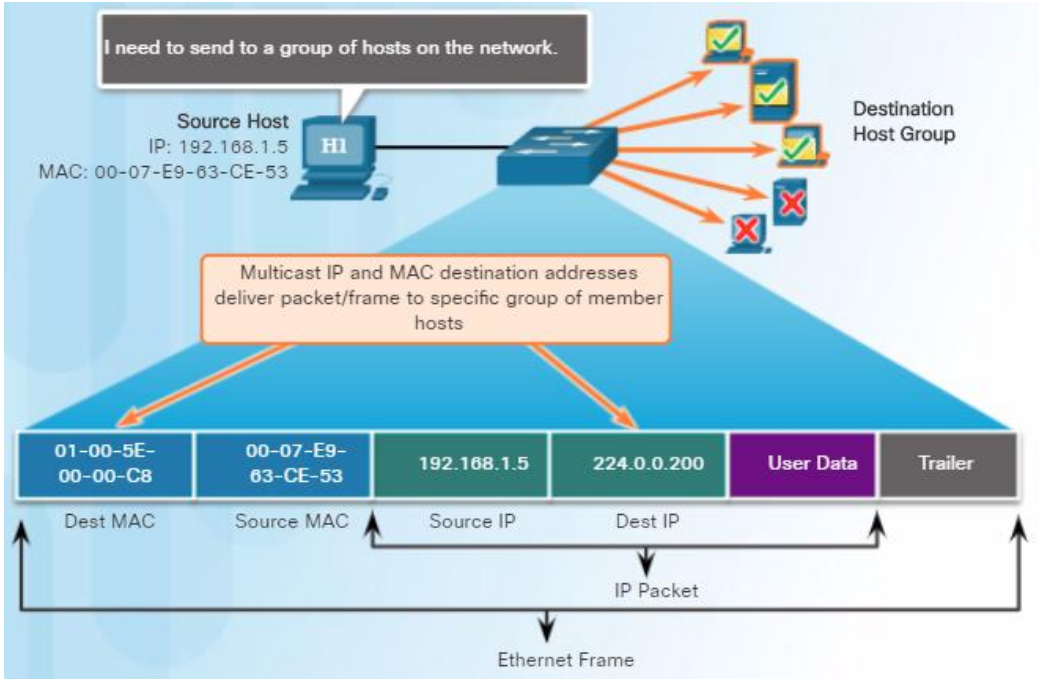
Broadcast MAC Address

- Many network protocols, such as DHCP and ARP, use broadcasts.
- A broadcast packet contains a destination IPv4 address that has all ones (1s) in the host portion indicating that all hosts on that local network will receive and process the packet.
- When the IPv4 broadcast packet is encapsulated in the Ethernet frame, the destination MAC address is the broadcast MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).



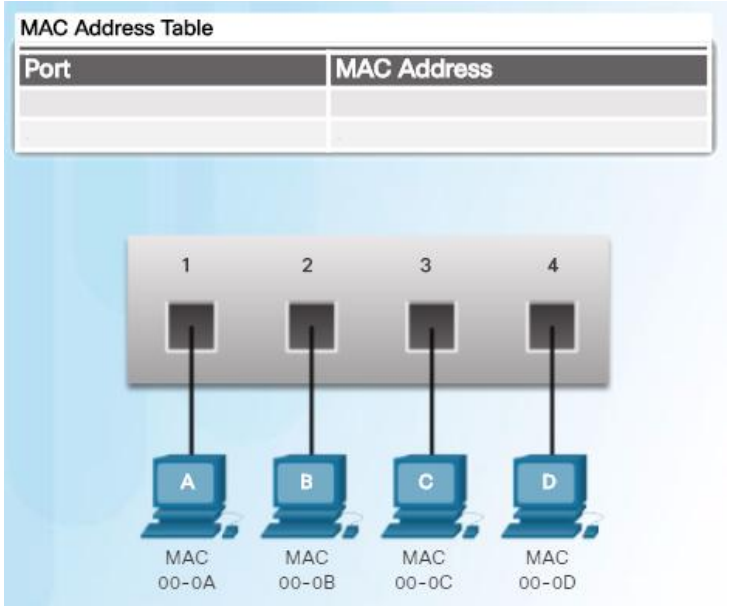
Multicast MAC Address

- Multicast addresses allow a source device to send a packet to a group of devices.
  - Devices in a multicast group are assigned a multicast group IP address in the range of 224.0.0.0 to 239.255.255.255 (IPv6 multicast addresses begin with FF00::/8).
  - The multicast IP address requires a corresponding multicast MAC address that begins with 01-00-5E in hexadecimal.



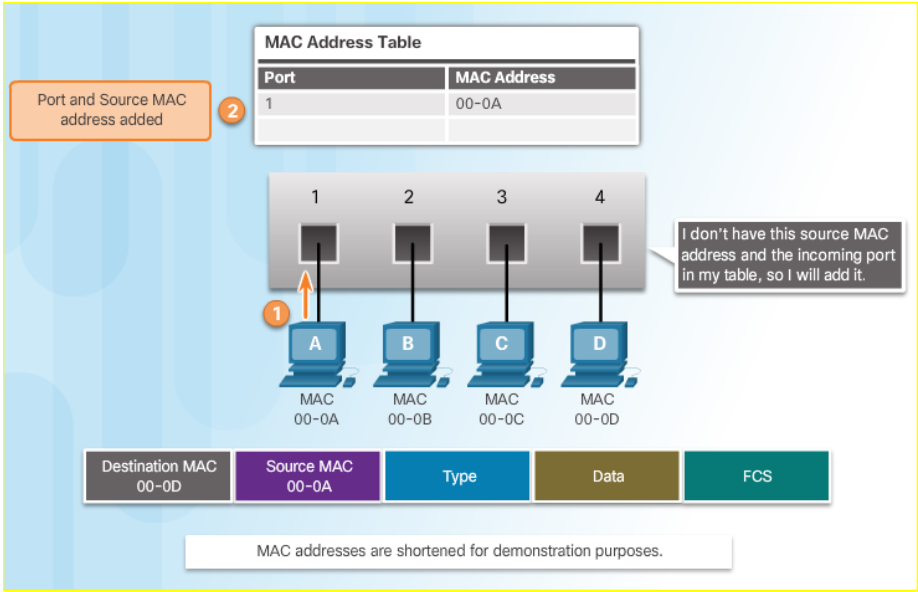
Switch Fundamentals

- A Layer 2 Ethernet switch makes its forwarding decisions based only on the Layer 2 Ethernet MAC addresses.
- A switch that is powered on, will have an empty MAC address table as it has not yet learned the MAC addresses for the four attached PCs.
- Note: The MAC address table is sometimes referred to as a content addressable memory (CAM) table.



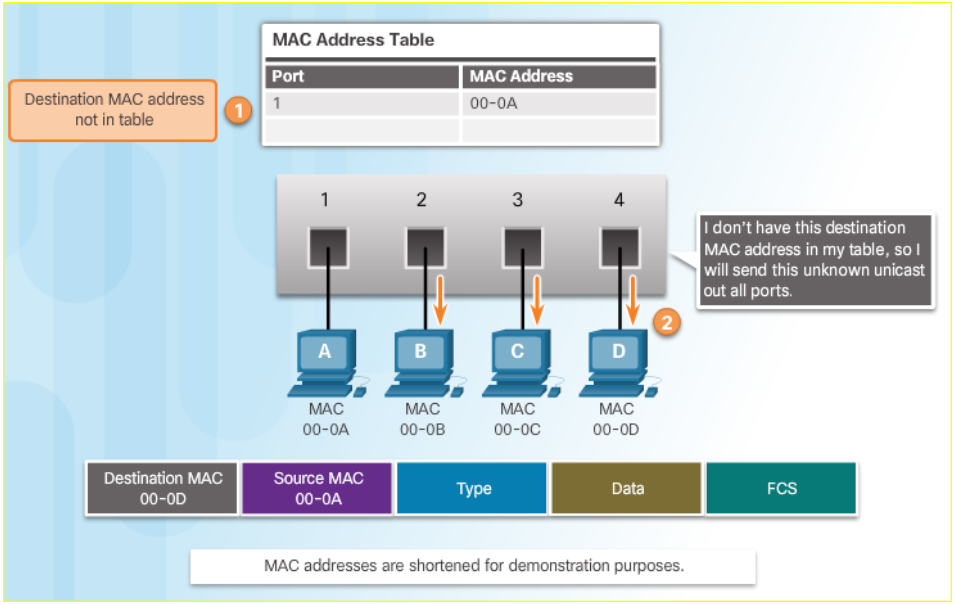
Learning MAC Addresses

- The switch dynamically builds the MAC address table. The process to learn the Source MAC Address is:
  - Switches examine all incoming frames for new source MAC address information to learn.
  - If the source MAC address is unknown, it is added to the table along with the port number.
  - If the source MAC address does exist, the switch updates the refresh timer for that entry.
  - By default, most Ethernet switches keep an entry in the table for 5 minutes.



Learning MAC Addresses (Cont.)

- The process to forward the Destination MAC Address is:
  - If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.
  - If the destination MAC address is a unicast address, the switch will look for a match in its MAC address table.
  - If the destination MAC address is in the table, it will forward the frame out the specified port.
  - If the destination MAC address is not in the table (i.e., an unknown unicast) the switch will forward the frame out all ports except the incoming port.



Learning MAC Addresses

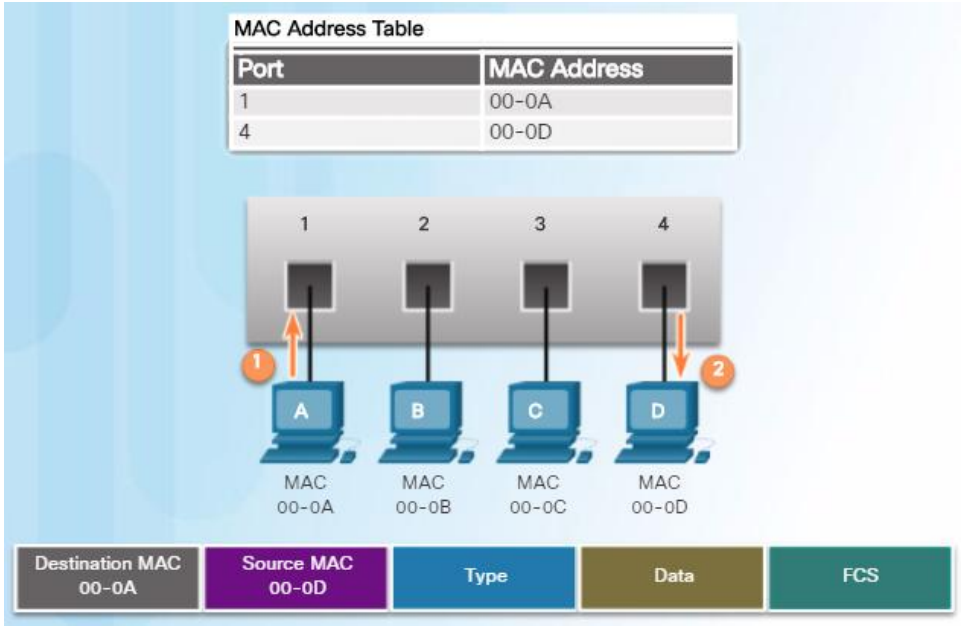
Switching Process	Description
Learn Examining the Source MAC Address	• Switches examine all incoming frames for new source MAC address information to learn. • If the source MAC address is unknown, it is added to the table along with the port number. • If the source MAC address does exist, the switch updates the refresh timer for that entry. • By default, most Ethernet switches keep an entry in the table for 5 minutes.

Forward
Examining the Destination MAC Address
	• If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.
	• If the destination MAC address is a unicast address, the switch will look for a match in its MAC address table.
	  • If the destination MAC address is in the table, it will forward the frame out the specified port.
	  • If the destination MAC address is not in the table (i.e., an unknown unicast) the switch will forward the frame out all ports except the incoming port.

Filtering Frames

- As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame.

- When the switch's MAC address table contains the destination MAC address, it is able to filter the frame and forward out a single port.



Systems and Control Eng. Dept.

Computer Networks

Fourth Year Class

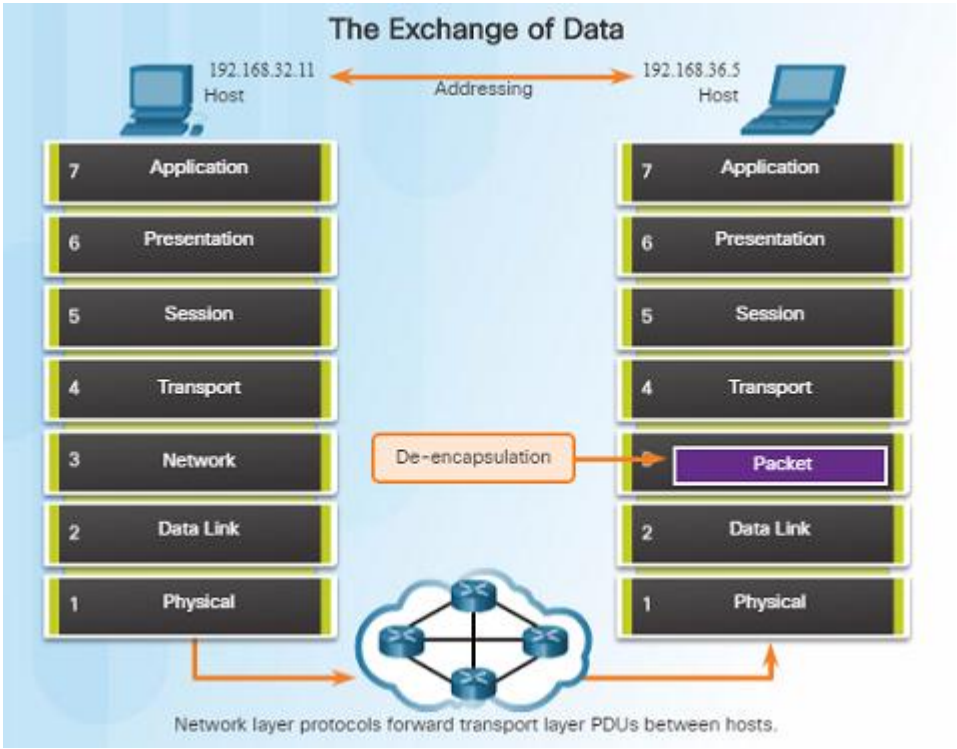
Lecture 9

Introduction to Network Layer

Abdulhameed N. Hameed

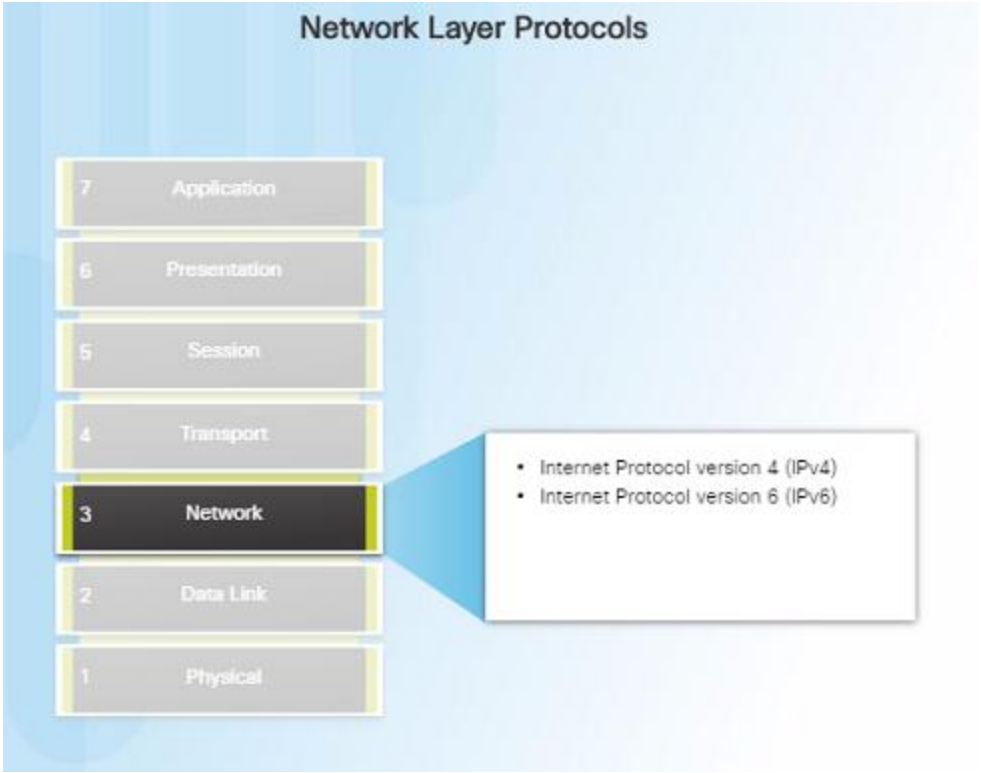
The Network Layer

- The network layer, which resides at OSI Layer 3, provides services that allow end devices to exchange data across a network.
- The network layer uses four processes in order to provide end-to-end transport:
  - Addressing of end devices – IP addresses must be unique for identification purposes.
  - Encapsulation – The protocol data units from the transport layer are encapsulated by adding IP header information including source and destination IP addresses.
  - Routing – The network layer provides services to direct packets to other networks. Routers select the best path for a packet to take to its destination network.
  - De-encapsulation – The destination host de-encapsulates the packet to see if it matches its own.



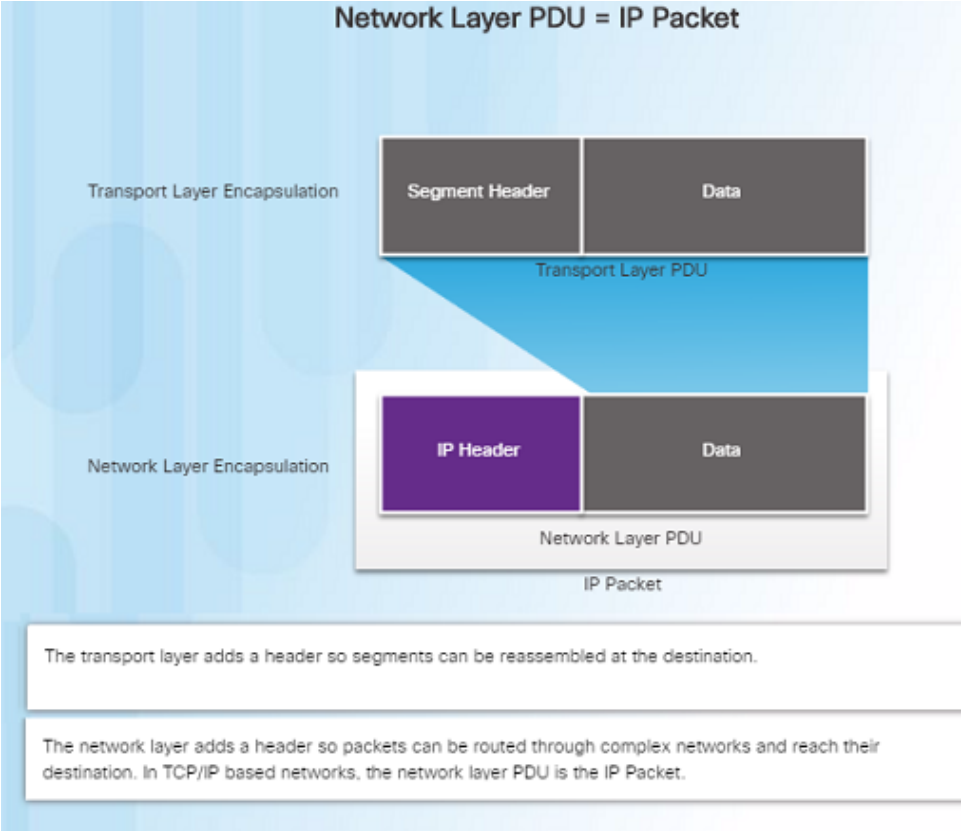
Network Layer Protocols

- There are several network layer protocols in existence; however, the most commonly implemented are:
  - Internet Protocol version 4 (IPv4)
  - Internet Protocol version 6 (IPv6)



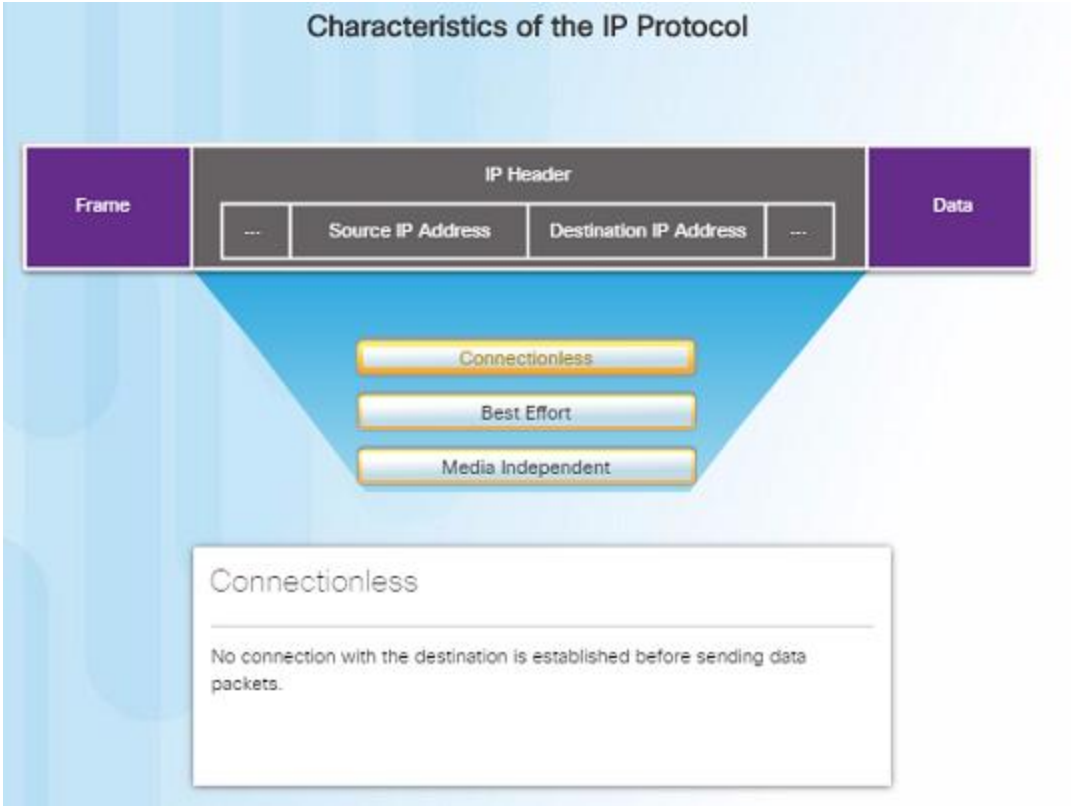
Encapsulating IP

- At the network layer, IP encapsulates the transport layer segment by adding an IP header for the purpose of delivery to the destination host.
- The IP header stays the same from the source to the destination host.
- Routers implement different network layer protocols concurrently over a network and use the network layer packet header for routing.



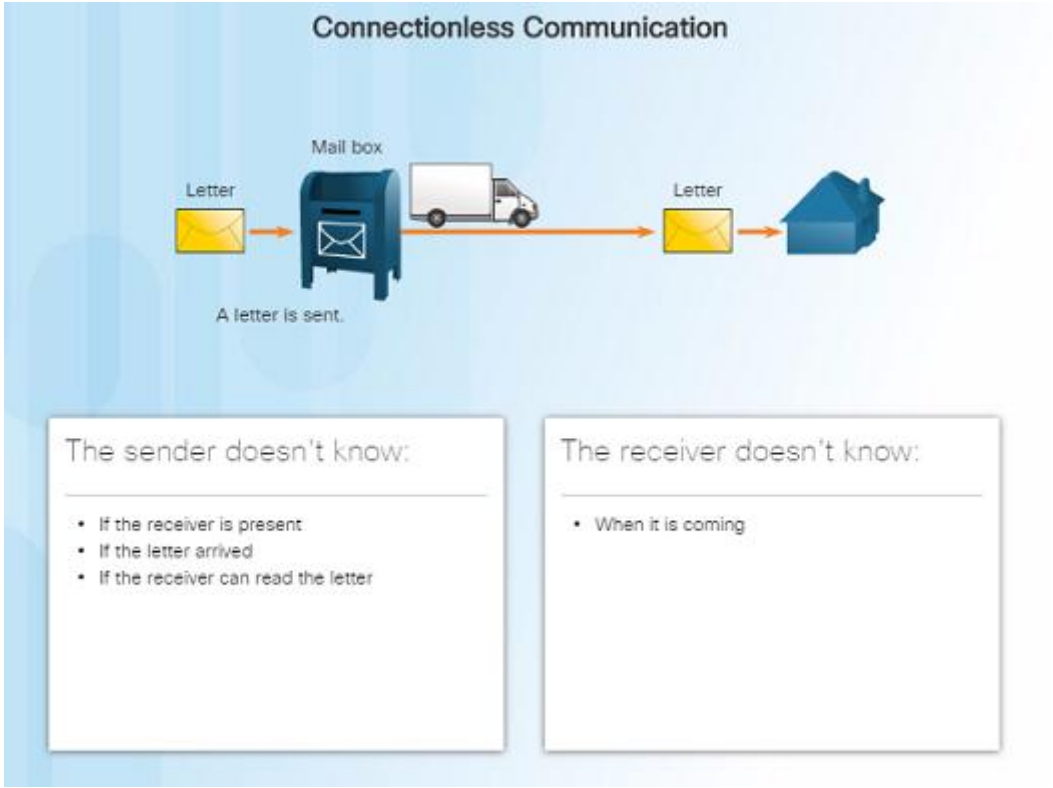
Characteristics of IP

- IP was designed as a protocol with low overhead – it provides only the functions required to deliver a packet from the source to a destination.
- An IP packet is sent to the destination without prior establishment of a connection
- IP was not designed to track and manage the flow of packets.
  - These functions, if required, are performed by other layers – primarily TCP



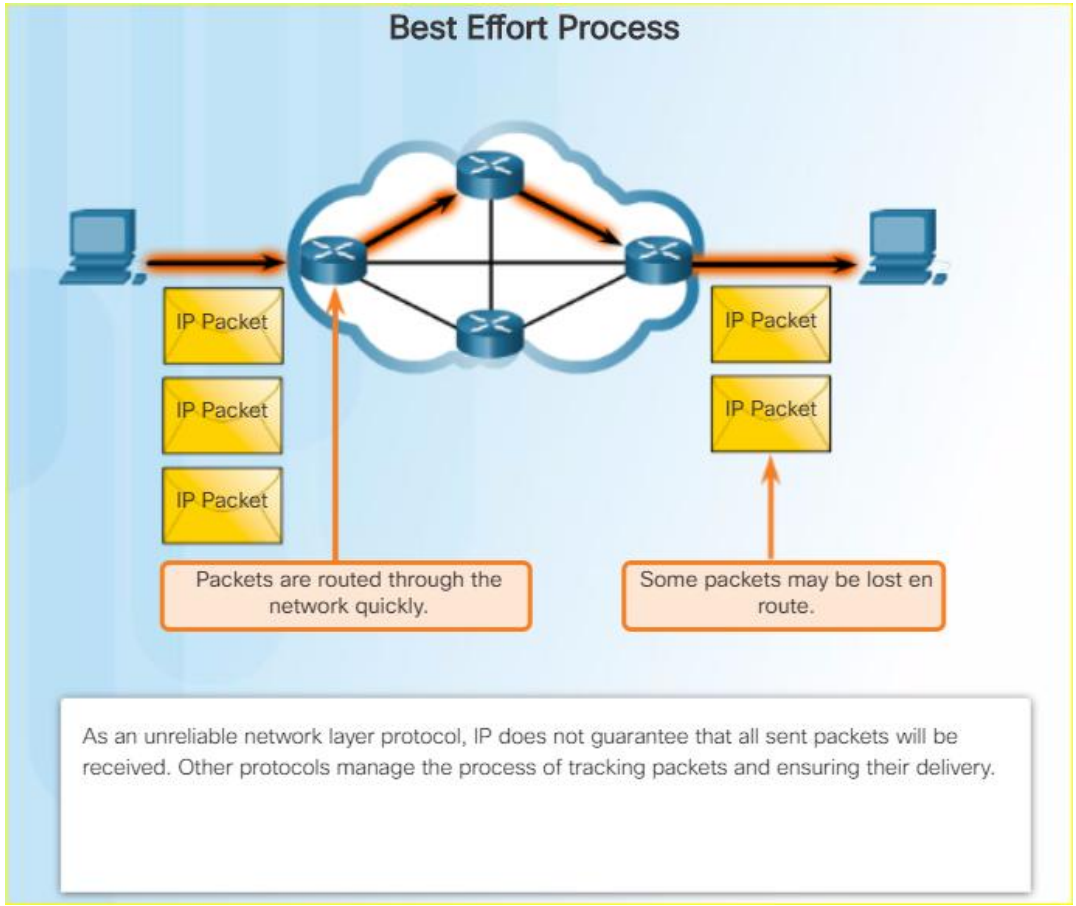
IP - Connectionless

- IP is a connectionless protocol:
  - No dedicated end-to-end connection is created before data is sent.
  - Very similar process as sending someone a letter through mail.
  - Senders do not know whether or not the destination is present, reachable, or functional before sending packets.
  - This feature contributes to the low overhead of IP.



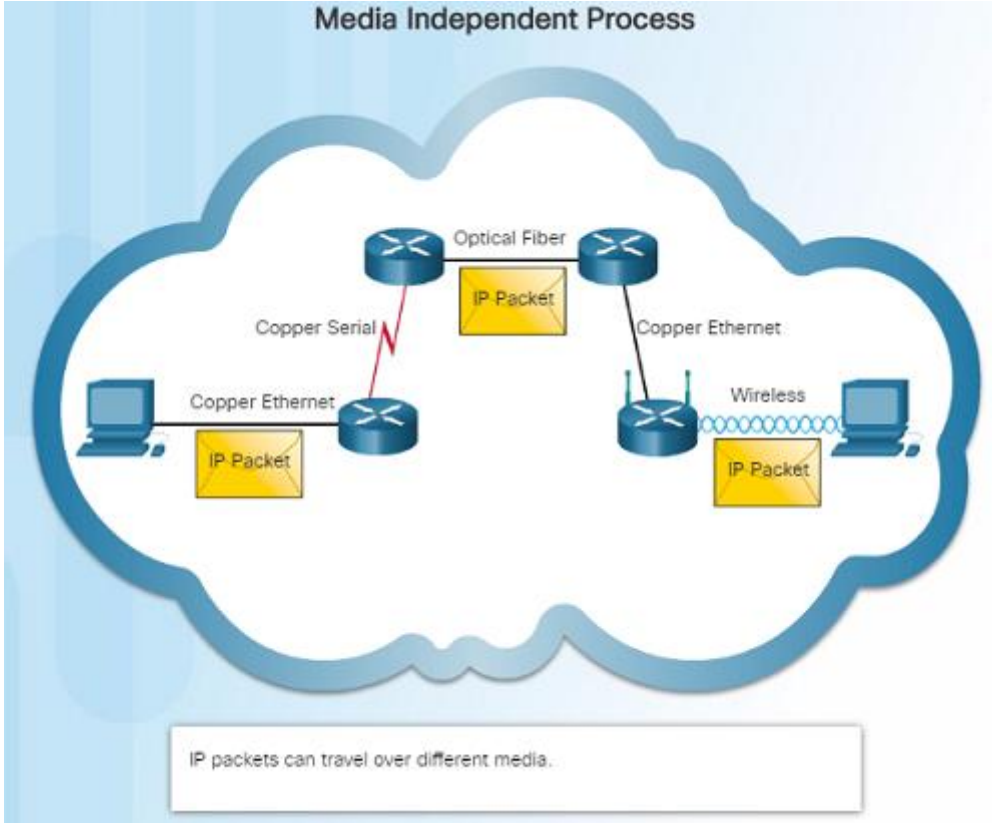
IP – Best Effort Delivery

- IP is a Best Effort Delivery protocol:
  - IP is considered “unreliable” because it does not guarantee that all packets that are sent will be received.
  - Unreliable means that IP does not have the capability to manage and recover from undelivered, corrupt, or out of sequence packets.
  - If packets are missing or not in the correct order at the destination, upper layer protocols/services must resolve these issues.



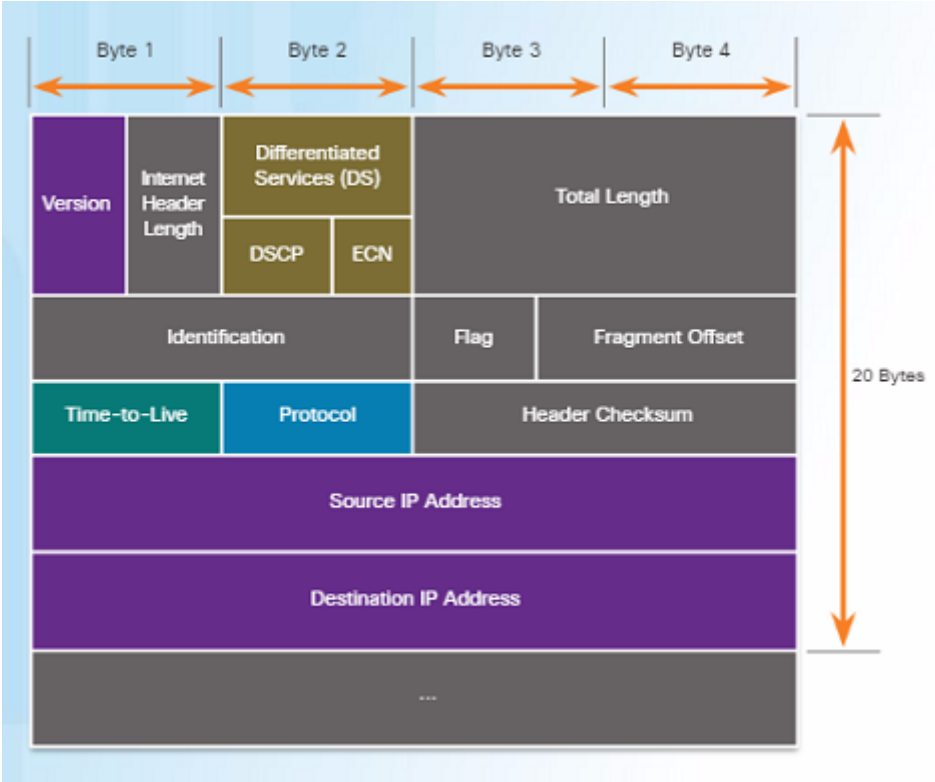
IP – Media Independent

- IP operates independently from the media that carries the data at lower layers of the protocol stack – it does not care if the media is copper cables, fiber optics or wireless.
- The OSI data link layer is responsible for taking the IP packet and preparing it for transmission over the communications medium.

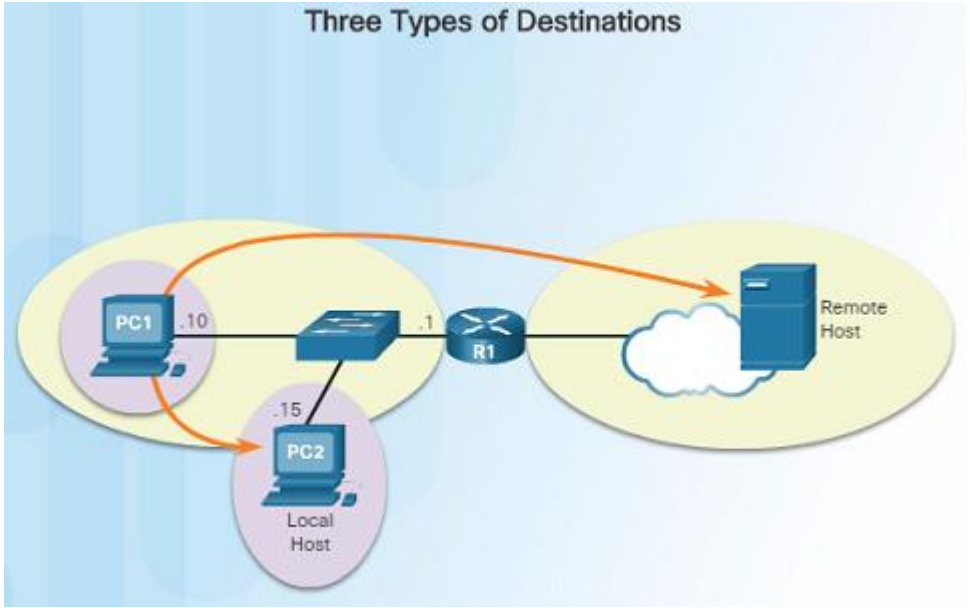


IPv4 Packet Header

- An IPv4 packet header consists of the fields containing binary numbers. These numbers identify various settings of the IP packet which are examined by the Layer 3 process.
- Significant fields include:
  - Version – Specifies that the packet is IP version 4
  - Differentiated Services or DiffServ (DS) – Used to determine the priority of each packet on the network.
  - Protocol – Used to identify the next level protocol.
  - Source IPv4 Address – Source address of the packet.
  - Destination IPv4 Address – Address of destination.

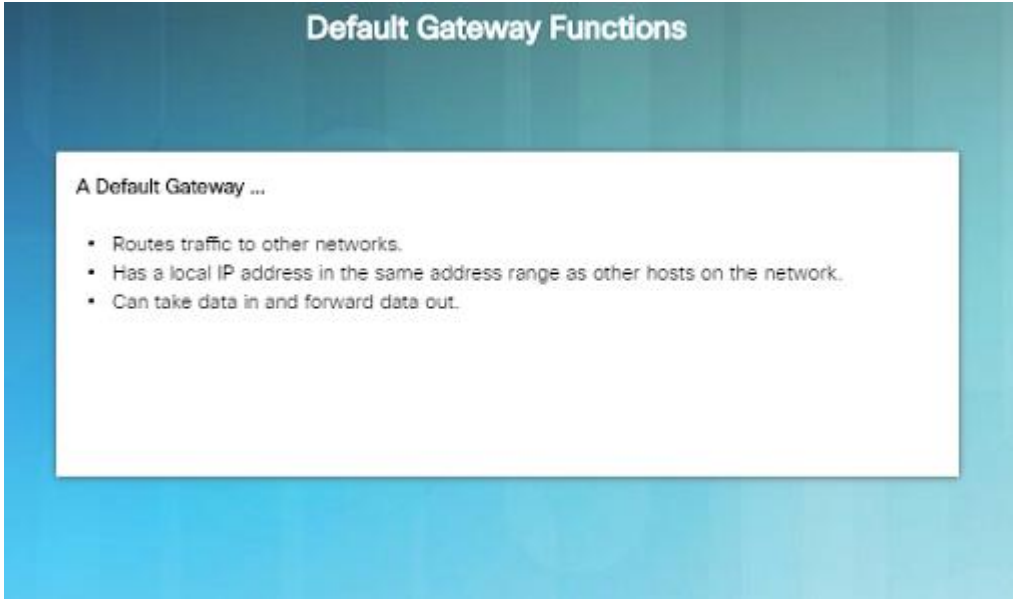


Host Forwarding Decision



- An important role of the network layer is to direct packets between hosts. A host can send a packet to:
  - Itself – A host can ping itself for testing purposes using 127.0.0.1 which is referred to as the loopback interface.
  - Local host – This is a host on the same local network as the sending host. The hosts share the same network address.
  - Remote host – This is a host on a remote network. The hosts do not share the same network address.
- The source IPv4 address and subnet mask is compared with the destination address and subnet mask in order to determine if the host is on the local network or remote network.

Default Gateway



- The default gateway is the network device that can route traffic out to other networks. It is the router that routes traffic out of a local network.
- This occurs when the destination host is not on the same local network as the sending host.

Systems and Control Eng. Dept.

Computer Networks

Fourth Year Class

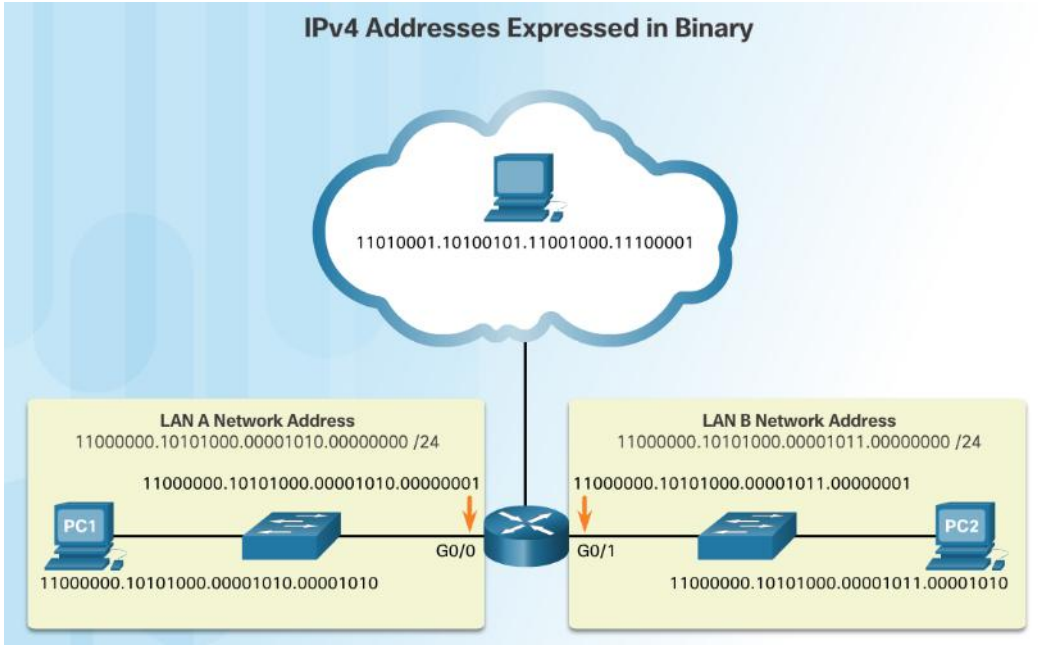
Lecture 10

IPv4 Network Addresses

Abdulhameed N. Hameed

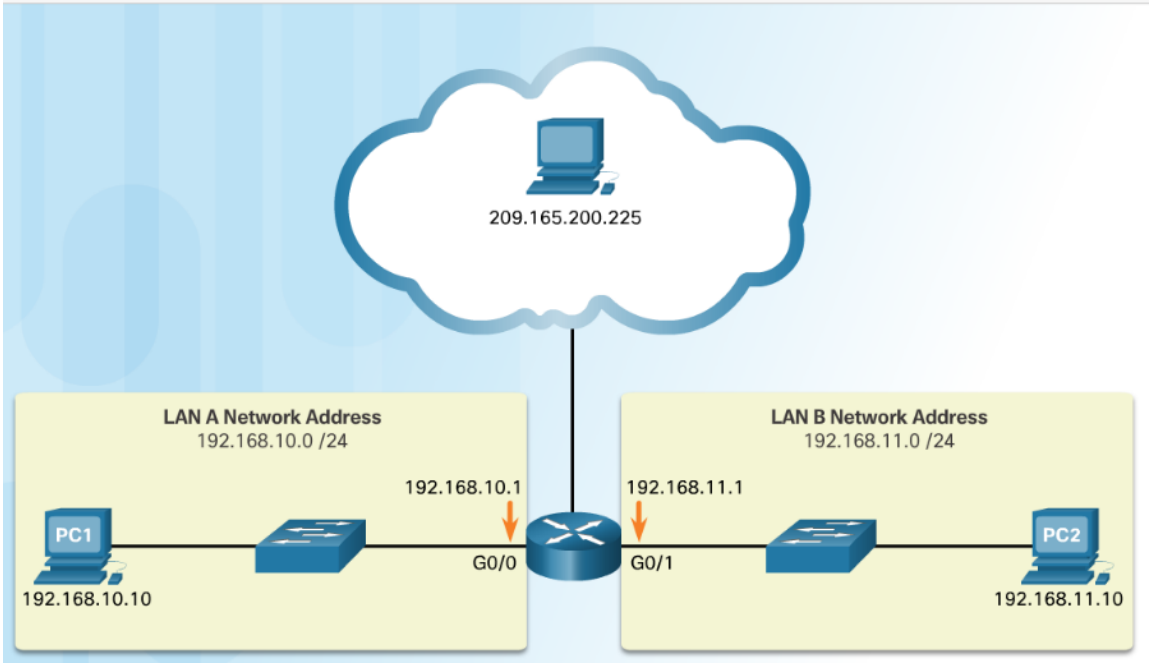
IPv4 Addresses

- An IP address is an address used to uniquely identify a device on an IP network.
- Binary numbering system consists of the numbers 0 and 1 called bits
  - IPv4 addresses are expressed in 32 binary bits divided into 4 8-bit octets



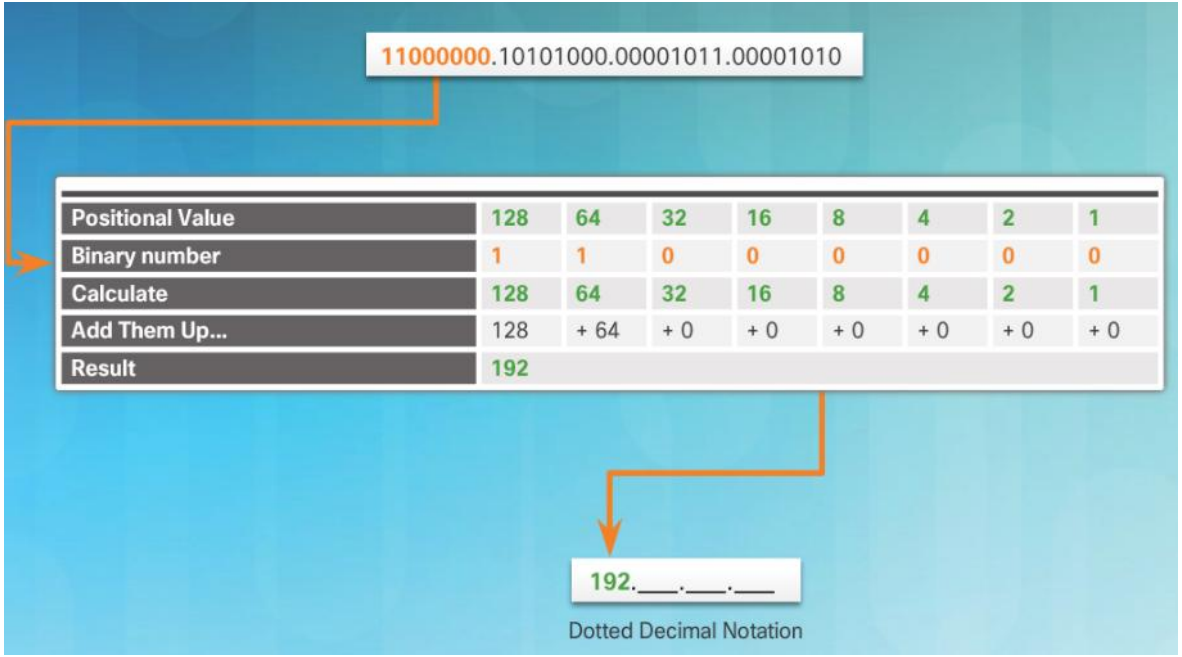
IPv4 Addresses (Cont.)

- IPv4 addresses are commonly expressed in dotted decimal notation



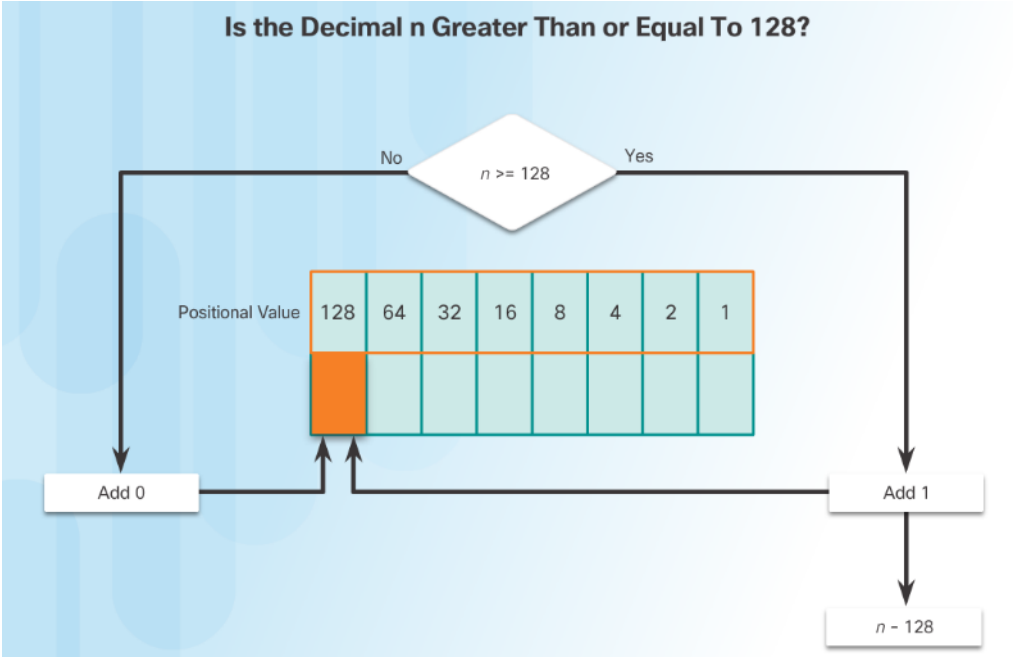
Binary to Decimal Conversion

- To convert a binary IPv4 address to decimal enter the 8-bit binary number of each octet under the positional value of row 1 and then calculate to produce the decimal.



Decimal to Binary Conversion

- To convert a decimal IPv4address to binary use the positional chart and check first if the number is greater than the 128 bit. If no a 0 is placed in this position. If yes then a 1 is placed in this position.
- 128 is subtracted from the original number and the remainder is then checked against the next position (64) If it is less than 64 a 0 is placed in this position. If it is greater, a 1 is placed in this position and 64 is subtracted.
- The process repeats until all positional values have been entered.



Decimal to Binary Conversion Examples

Example: 192.168.10.11

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

11000000 . _____ . _____ . _____

Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	1	0	1	0	1	0	0	0

11000000 . 10101000 . _____ . _____

Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	0

11000000 . 10101000 . 00001010 . _____

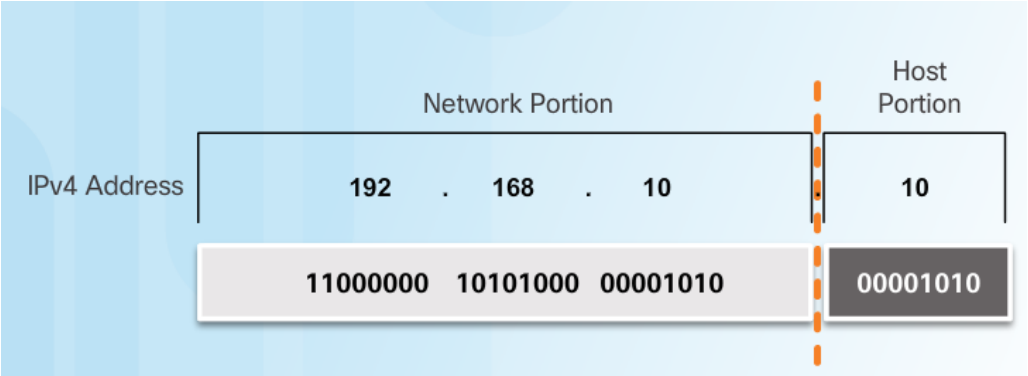
Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	1

11000000 . 10101000 . 00001010 . 00001011

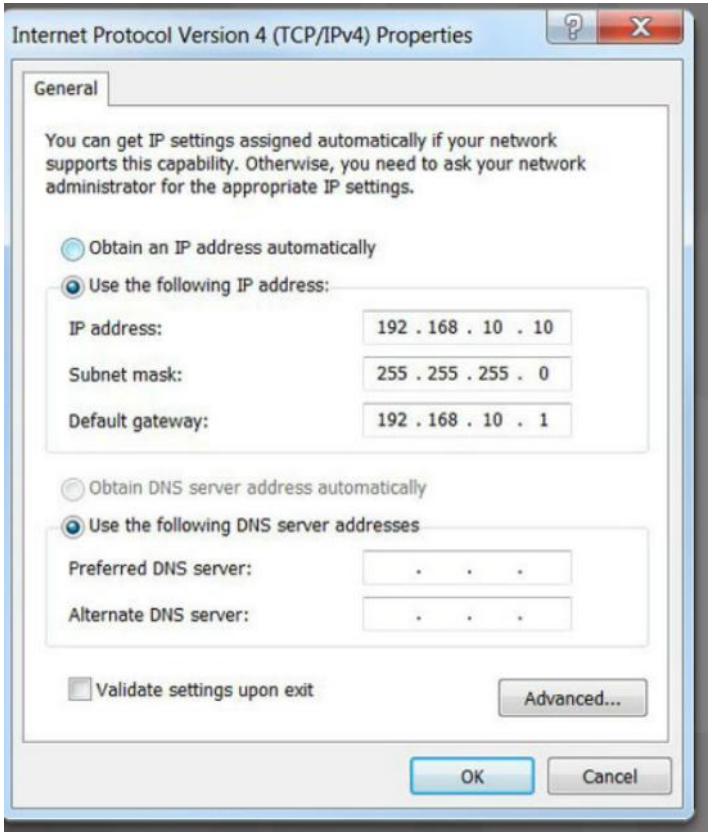
Network and Host Portions

- An IPv4 address is hierarchical.
  - Composed of a Network portion and Host portion.
- All devices on the same network must have the identical network portion.
- The Subnet Mask helps devices identify the network portion and host portion.



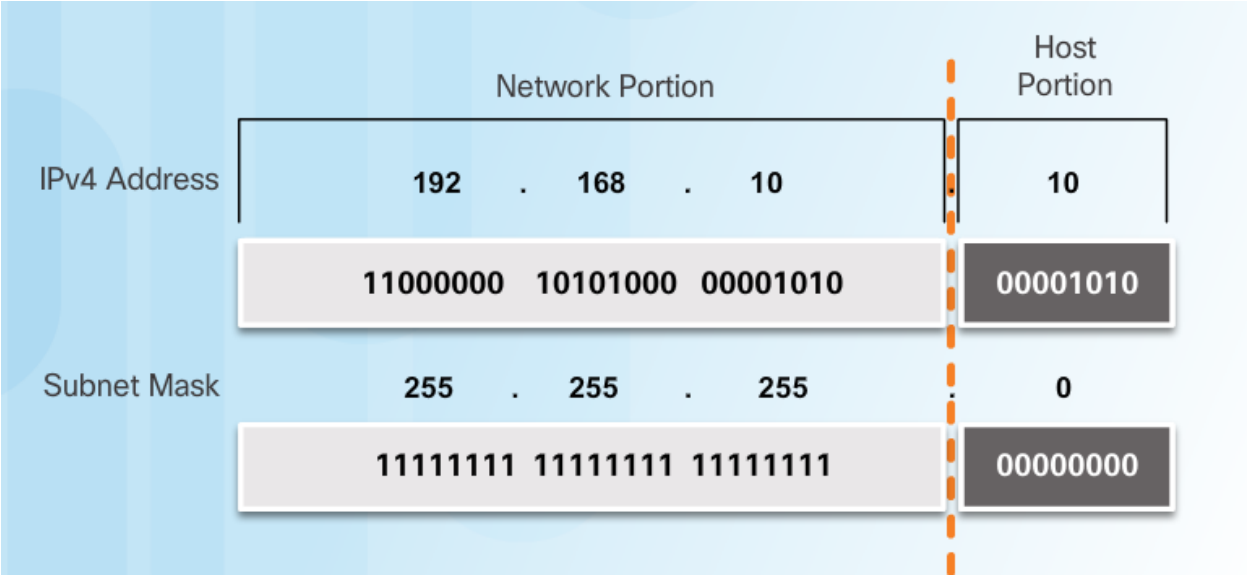
The Subnet Mask

- Three IPv4 addresses must be configured on a host:
  - Unique IPv4 address of the host.
  - Subnet mask - identifies the network/host portion of the IPv4 address.
  - Default gateway -IP address of the local router interface.

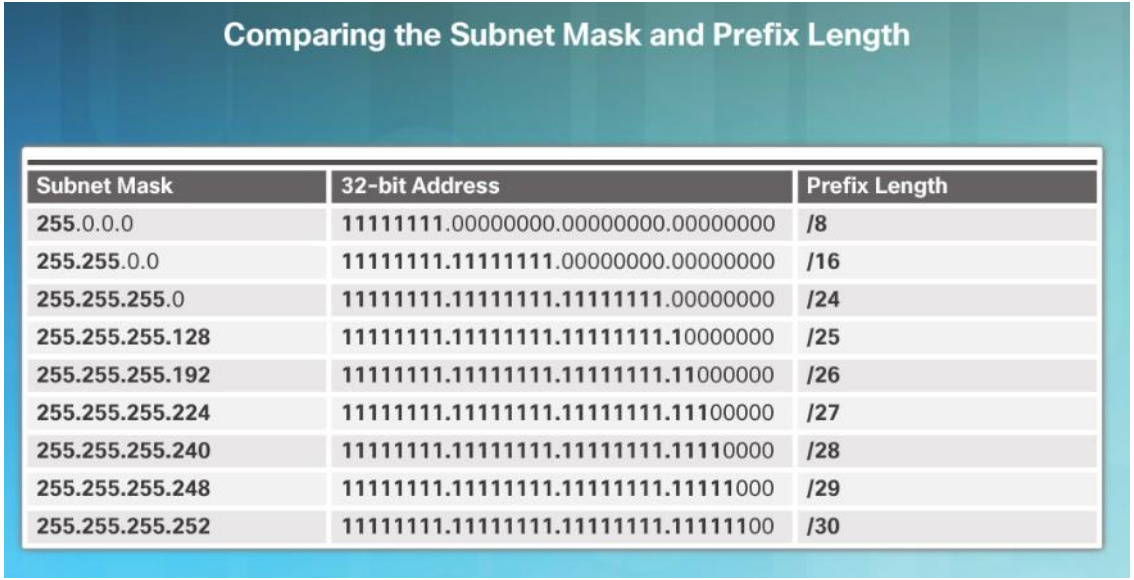


The Subnet Mask (Cont.)

- The IPv4 address is compared to the subnet mask bit by bit, from left to right.
- A 1 in the subnet mask indicates that the corresponding bit in the IPv4 address is a network bit.



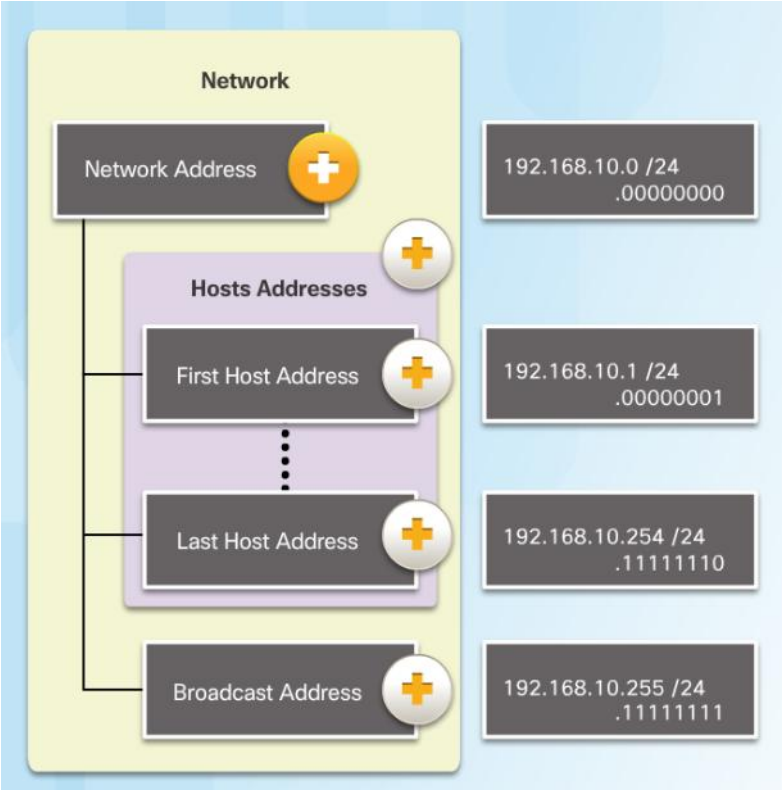
The Prefix Length



Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

- The Prefix Length:
  - Shorthand method of expressing the subnet mask.
  - Equals the number of bits in the subnet mask set to 1.
  - Written in slash notation, / followed by the number of network bits.

Network, Host, and Broadcast Addresses



- Types of Addresses in Network 192.168.10.0/24
  - Network Address - host portion is all 0s (.00000000)
  - First Host address - host portion is all 0s and ends with a 1 (.00000001)
  - Last Host address - host portion is all 1s and ends with a 0 (.11111110)
  - Broadcast Address - host portion is all 1s (.11111111)

Legacy Classful Addressing

Class A Specifics	
Address Block	0.0.0.0 - 127.0.0.0
Default Subnet Mask	/8 (255.0.0.0)
Maximum Number of Networks	128
Number of Host per Network	16,777,214
High order bit	0xxxxxxx.___.___.___

* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

Class B Specifics	
Address Block	128.0.0.0 - 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx.___.___.___

Class C Specifics	
Address Block	192.0.0.0 - 223.255.255.0
Default Subnet Mask	/24 (255.255.255.0)
Maximum Number of Networks	2,097,152
Number of Host per Network	254
High order bit	110xxxxx.___.___.___

- In 1981, Internet IPv4 addresses were assigned using classful addressing (RFC 790)
- Network addresses were based on 3 classes:
  - **Class A** (0.0.0.0/8 to 127.0.0.0/8) – Designed to support extremely large networks with more than 16 million host addresses.
  - **Class B** (128.0.0.0 /16 – 191.255.0.0 /16) – Designed to support the needs of moderate to large size networks up to approximately 65,000 host addresses.
  - **Class C** (192.0.0.0 /24 – 223.255.255.0 /24) – Designed to support small networks with a maximum of 254 hosts.