ECE 4309

# Basics of computer networks and systems - part 1

Dr. Valerio Formicola

CalPolyPomona

# Reference about this material

A. Tanenbaum – Computer networks:
https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188/9780137523214

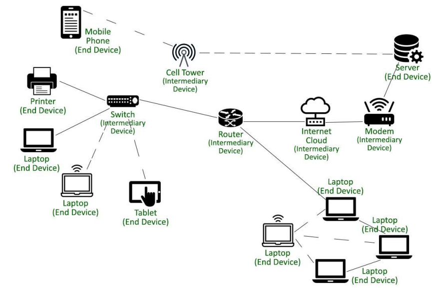
https://www.geeksforgeeks.org/computer-network-tutorials/?ref=lbp

And others…

# Computer Networking

- Computer Networking is the practice of connecting computers together to enable communication and data exchange between them. In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily.
- Elements of a computer network:
  - **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, or other devices, like Equipment for Data Communication (e.g., Modem, Switch, Router, Bridge, Wireless Access Point, etc.)
  - **Links:** wires or cables or free space (wireless networks)

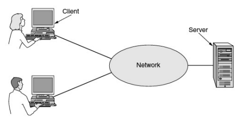
Computer network




Observation: A computer is also known as a ***host***, but as a part of a computer network it is known as a ***node***

# Communication models

- Client - Server



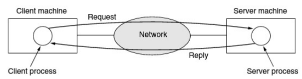




**Figure 1-2.** The client-server model involves requests and replies.

Peer to Peer (P2P)

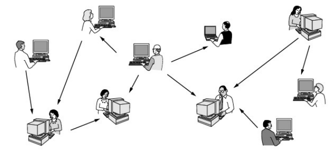
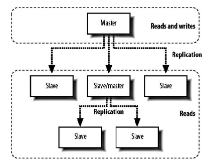
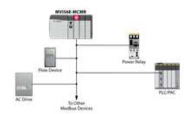


**Figure 1-3.** In a peer-to-peer system there are no fixed clients and servers.

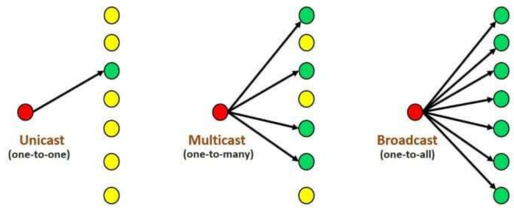
Master-Slave (industry)



# Content fruition models

Who can access to messages/stream of data/signals as a receiver



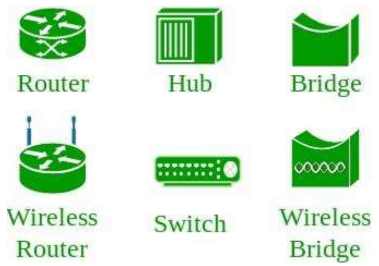

Question: What fruition models are flowed by AM/FM Radio and public TV?

# Key concepts in communications

- **Connection-oriented communication: it's** like the old telephone system (Plain Old Telephone Service), there is a dedicated channel between source and destination. Data (e.g., the voice signal) arrives following one unique path established at the beginning, i.e., a "connection".
- **Connection-less communication:** it's like the postal service. The message contains information of source and destination and it's forwarded to the destination step-by-step.
  Two mails towards the same destination might follow similar but different paths.

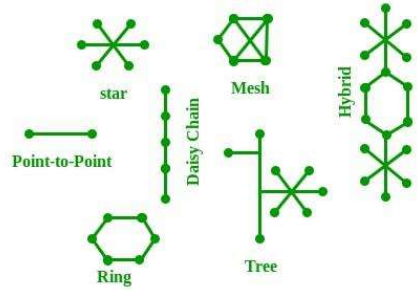
## Network devices/nodes

- In addition to the computers, networks are done of devices/mediums which help in the communication between two different devices or nodes; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



# Network Topology

- The Network Topology is the layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.



# Network scales

| 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 |

**Figure 1-6.** Classification of interconnected processors by scale.

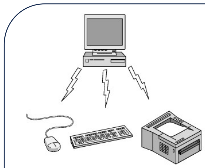


**Figure 1-7.** Bluetooth PAN configuration.

Personal Area Network, PAN
(e.g., Bluetooth)

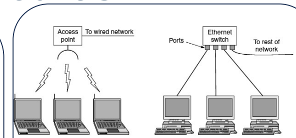



**Figure 1-8.** Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

Local Area Network, LAN
(e.g., Ethernet or WiFi LAN)

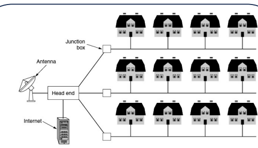
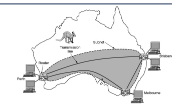
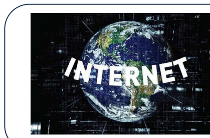



**Figure 1-9.** A metropolitan area network based on cable TV.

Metropolitan Area Network, MAN
(e.g., Network Broadcasting)

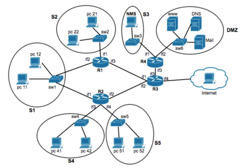



Wide Area Network

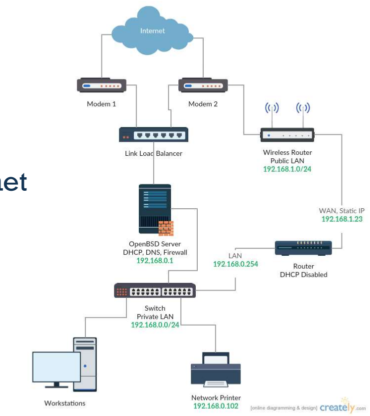


# Internet is the network of networks

- Usually, your device is connected to a private Local Area Network (LAN) and traverses many sub-nets (sub-networks) to arrive on a public network or directly to Internet

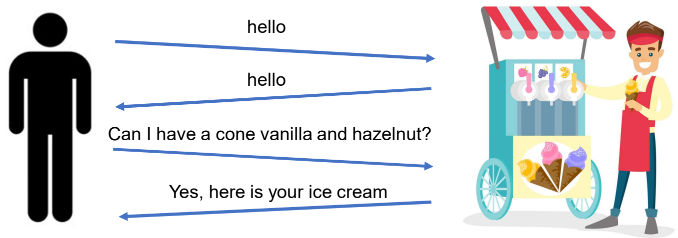


Examples of local networks connected to Internet



# Protocol

- **Protocol:** A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of a communication model.
  Example of *telecommunication models in computer networks*: **ISO/OSI, TCP/IP**
  Examples of *protocols* that implement what is described in the model
  (with some small differences): TCP, IP, UDP, ARP, DHCP, FTP, and so on.



# Typical protocol *primitives**

- Note: they are not necessarily present in any protocol or not necessarily use these names

| 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 |

**Figure 1-17.** Six service primitives that provide a simple connection-oriented service.

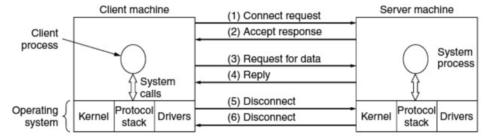



**Figure 1-18.** A simple client-server interaction using acknowledged datagrams.

*Primitives: functions that are used to implement a service

# Why do we need communication protocols?

- In the absence of protocols, devices would not be able to understand the electronic signals that they send while communicating over network connections.
  - You need to **identify** who is the sender and who is the (intended) receiver of a message, especially in *shared medium* of communication (e.g., air), i.e., a physical medium that is used by multiple nodes at the same time
  - Each **physical transmission medium** (cable, air, wire, etc.) needs a different way to transmit digital signals (0s, 1s), and recognize a 0 or 1 (e.g., light, electromagnetic frequencies in air, electric signals in wires, etc.)
  - Protocols help sender and receiver to understand if a **message is lost, sent out of sequence, duplicated, corrupted, etc. during transmission.**
  - Sender might be too fast **(congestion)** than the receiver or to slow and they need to agree on the ***transmission rate***

# Net. communication model: ISO/OSI

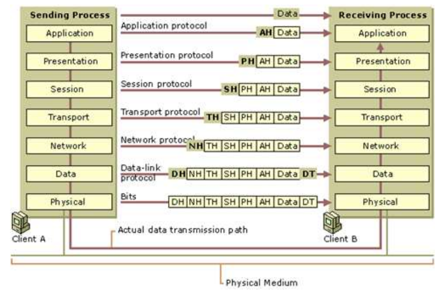
- OSI stands for Open Systems Interconnection. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer. The OSI has been developed by the International Organization For Standardization and it is 7 layer architecture. Each layer of OSI has different functions and each layer has to follow different protocols. The 7 layers are as follows:

Onion model:

- Physical Layer
- Data link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

xH: x layer header

xT: x layer trailer



# What is exchanged between two nodes (aka, hosts)?

- *Onion model:* Each layer provides some mechanisms to allow the communication
  - At sender side: you add layers
  - At receiver side: you remove layers
- Very often we say two nodes exchange *packets*: i.e., nodes are the entities that exchange *packet units*
- **PDU** is generically Protocol Data Unit, and can be associated to the corresponding layer Transport PDU (TPDU), Session PDU (SPDU), etc.

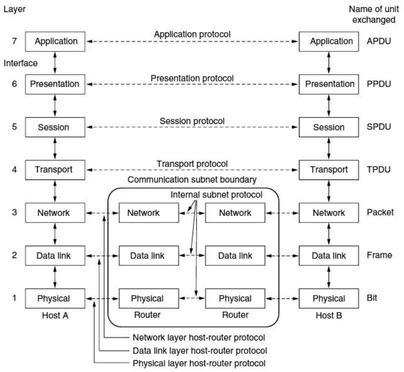
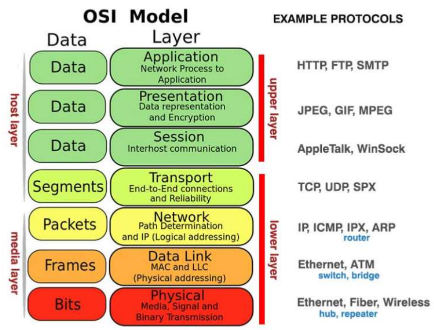



**Figure 1-20.** The OSI reference model.

# Examples of protocols and networking devices



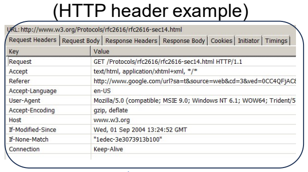

Networking devices typical for each layer

| | |
|---|---|
| Application layer | Application gateway |
| Transport layer | Transport gateway |
| Network layer | Router |
| Data link layer | Bridge, switch |
| Physical layer | Repeater, hub |

# Example of headers

- Based on the services to be provided by a layer, some "fields" are added to the PDU (i.e., data) coming from the layer above

Application layer, i.e., app data
(HTTP header example)

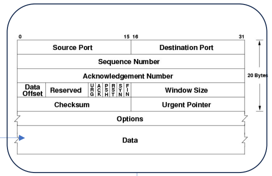

URL: http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

Request Headers | Request Body | Response Headers | Response Body | Cookies | Initiator | Timings

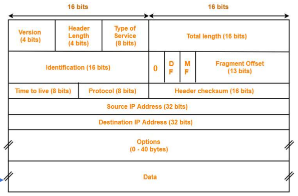
| Key | Value |
|---|---|
| Request | GET /Protocols/rfc2616/rfc2616-sec14.html HTTP/1.1 |
| Accept | text/html, application/xhtml+xml, */* |
| Referer | http://www.google.com/url?sa=t&source=web&cd=3&ved=0CC4QFjAC8 |
| Accept-Language | en-US |
| User-Agent | Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5 |
| Accept-Encoding | gzip, deflate |
| Host | www.w3.org |
| If-Modified-Since | Wed, 01 Sep 2004 13:24:52 GMT |
| If-None-Match | "1edec-3e3073913b100" |
| Connection | Keep-Alive |

*Http* (Hypertext Transfer Protocol)
is the application layer protocol
to request (client) or send (server) web pages

Transport layer protocol
TCP (Transmission Control Protocol)




Network layer protocol
IP (Internet Protocol)



# ISO/OSI model

| | | |
|---|---|---|
| 7 | Application Layer | Human-computer interaction layer, where applications can access the network services |
| 6 | Presentation Layer | Ensures that data is in a usable format and is where data encryption occurs |
| 5 | Session Layer | Maintains connections and is responsible for controlling ports and sessions |
| 4 | Transport Layer | Transmits data using transmission protocols including TCP and UDP |
| 3 | Network Layer | Decides which physical path the data will take |
| 2 | Data Link Layer | Defines the format of data on the network |
| 1 | Physical Layer | Transmits raw bit stream over the physical medium |

# Application layer

- The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

# Presentation Layer and Session Layer

- **Presentation Layer**
  - The presentation layer prepares data for the application layer. Unlike the lower layers, which are mostly concerned with moving bits around, the presentation layer is concerned with the syntax and semantics of the information transmitted.
    It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end.
    For example, the presentation layer tells if the code used for representing a character in a text message is ASCII, ASCII extended, pictures/videos are in MPEG 1, 2, etc.
    The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

- **Session Layer**
  - The session layer creates communication channels, called *sessions*, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

# Transport Layer

Transport Layer is used to provide a service for a direct communication between two *applications* with a dedicated data channel.
The transport layer takes application data (actually, application + presentation + session) and breaks it into "segments" (TPDU) on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer (the layer right on top). The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device (*congestion control*), and error control, checking if application data was received incorrectly and if not, requesting it again.

# Network Layer

The network layer has two main functions. One is breaking up segments into network *packets and* reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol (IP) addresses) to route packets to a destination node.

The *network layer* creates a virtual connection (virtual data path)
between two hosts (computers) because they might not be physically connected (most often they are not)

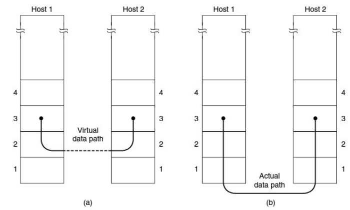



**Figure 3-2.** (a) Virtual communication. (b) Actual communication.

# Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

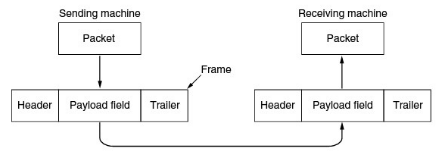
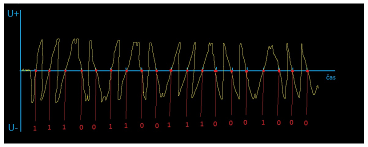



**Figure 3-1.** Relationship between packets and frames.

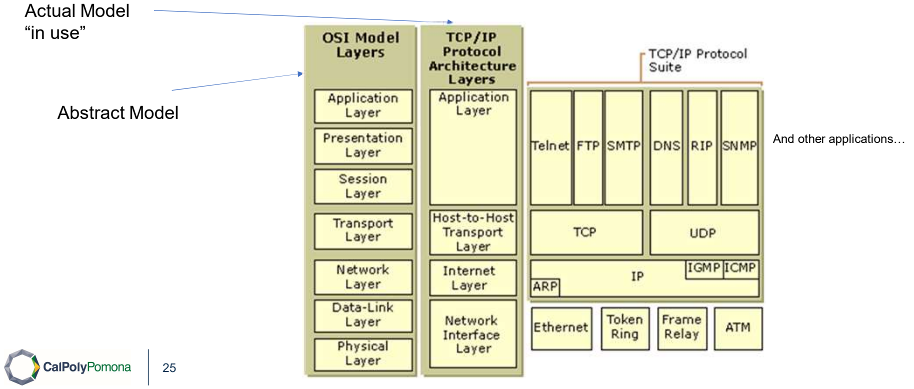
# Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

The electromagnetic signal (light, voltage, current, radio wave, etc.) and depends on the medium considered.



# The OSI model is not actually followed 100%, and we use the TCP/IP model



# Difference between TCP/IP and ISO/OSI model

- The Transfer Control Protocol/Internet Protocol (TCP/IP) is older than the OSI model and was created by the US Department of Defense (DoD). A key difference between the models is that TCP/IP is simpler, collapsing several OSI layers into one:
- OSI layers 5, 6, 7 are combined into one Application Layer in TCP/IP
- OSI layers 1, 2 are combined into one Network Access Layer in TCP/IP – however TCP/IP does not take responsibility for sequencing and acknowledgement functions, leaving these to the underlying transport layer.

Other important differences:

- TCP/IP is a functional model designed to solve specific communication problems, and which is based on specific, standard protocols. OSI is a generic, protocol-independent model intended to describe all forms of network communication.
- In TCP/IP, most applications use all the layers, while in OSI simple applications do not use all seven layers. Only layers 1, 2 and 3 are mandatory to enable any data communication.

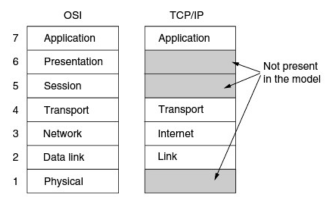



**Figure 1-21.** The TCP/IP reference model.

# Communication standards

• IEEE's 802 committee has standardized many kinds of LANs

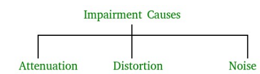
| Number | Topic |
|---|---|
| 802.1 | Overview and architecture of LANs |
| 802.2 ↓ | Logical link control |
| 802.3 * | Ethernet |
| 802.4 ↓ | Token bus (was briefly used in manufacturing plants) |
| 802.5 | Token ring (IBM's entry into the LAN world) |
| 802.6 ↓ | Dual queue dual bus (early metropolitan area network) |
| 802.7 ↓ | Technical advisory group on broadband technologies |
| 802.8 † | Technical advisory group on fiber optic technologies |
| 802.9 ↓ | Isochronous LANs (for real-time applications) |
| 802.10 ↓ | Virtual LANs and security |
| 802.11 * | Wireless LANs (WiFi) |
| 802.12 ↓ | Demand priority (Hewlett-Packard's AnyLAN) |
| 802.13 | Unlucky number; nobody wanted it |
| 802.14 ↓ | Cable modems (defunct: an industry consortium got there first) |
| 802.15 * | Personal area networks (Bluetooth, Zigbee) |
| 802.16 * | Broadband wireless (WiMAX) |
| 802.17 | Resilient packet ring |
| 802.18 | Technical advisory group on radio regulatory issues |
| 802.19 | Technical advisory group on coexistence of all these standards |
| 802.20 | Mobile broadband wireless (similar to 802.16e) |
| 802.21 | Media independent handoff (for roaming over technologies) |
| 802.22 | Wireless regional area network |

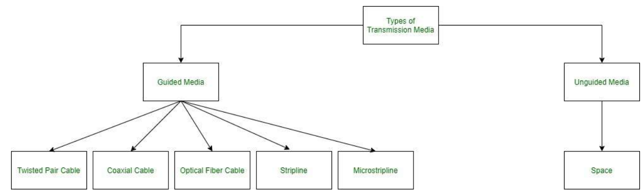
**Figure 1-38.** The 802 working groups. The important ones are marked with *. The ones marked with ↓ are hibernating. The one marked with † gave up and disbanded itself.

# Closer look at layers and protocols

# Physical Layer (1/3)

- Solves the problem of transmitting bits as signals in different kinds of transmission media
- Each transmission medium has a limited distance possible



# Physical Layer (2/3)

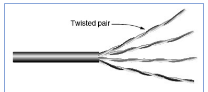



Figure 2-3. Category 5 UTP cable with four twisted pairs.

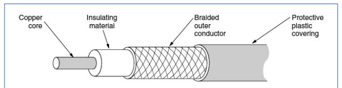



Figure 2-4. A coaxial cable.

Optical fiber

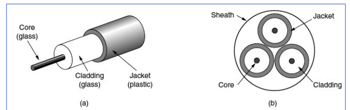



Figure 2-8. (a) Side view of a single fiber. (b) End view of a sheath with three fibers.

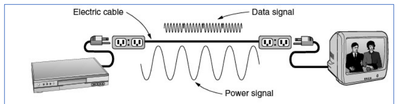
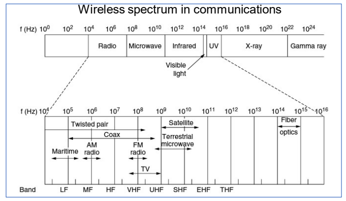



Figure 2-5. A network that uses household electrical wiring.

Power line communication (PLC)

Wireless spectrum in communications



# Physical Layer (3/3)

Baseband Transmission

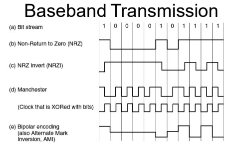


Figure 2-20. Line codes: (a) Bits, (b) NRZ, (c) NRZI, (d) Manchester, (e) Bipolar or AMI.

Passband Transmission (PSK, ASK, QAM, …)

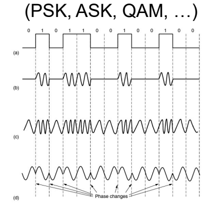


Figure 2-22. (a) A binary signal. (b) Amplitude shift keying. (c) Frequency shift keying. (d) Phase shift keying.

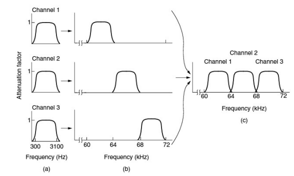


Figure 2-25. Frequency division multiplexing. (a) The original bandwidths. (b) The bandwidths raised in frequency. (c) The multiplexed channel.

FDM Transmission

Time Division Multiplexing

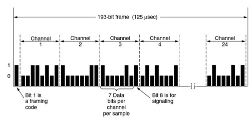


Figure 2-37. The T1 carrier (1.544 Mbps).

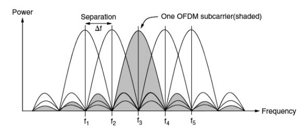
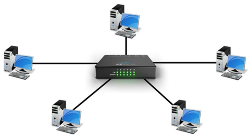


Figure 2-26. Orthogonal frequency division multiplexing (OFDM).

OFDM

# Physical level connecting devices

- Network **hub** is a device that might simply replicate an electrical signal reproposing the sequence of 0, 1s in input:
  - **Passive hubs** don't amplify the electrical signal of incoming packets before broadcasting them out to the network.
  - **Active hubs** perform amplification, much like a repeater.
  - **Intelligent Hub:** Provides additional features to the active hub. Also known as a manageable hub, as each port on the hub can be configured by the network operator according to the network requirement. All the ports of the hub can be configured, monitored, enable or disable.

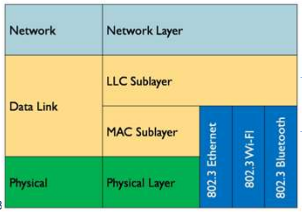


- A **wireless extender** is a smart repeater since it not simply replicates the signal, but it regenerates it from a new device

# Data link layer

Services:

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




LLC: Logical Link control
Responsible for flow control and error correction during physical transmission

MAC: Media Access Control
Responsible for providing a method to obtain access to the physical medium: addressing, physical channel selection (e.g., frequency), etc.

# Data link: MAC protocol *Ethernet (802.3)*

- Protocol used to communicate over a ***shared medium***
- All cables (coaxial, twisted pairs, fiber) are physically connected through a ***network switch***

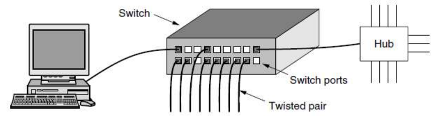



**Figure 4-18.** An Ethernet switch.


- All the devices can talk anytime but only one connection is possible in one time interval. To solve the problem of conflict in the use of the shared medium, there is a mechanism called **CSMA/CD** (Carrier Sensing Multiple Access/Collision Detection) that detects when the medium is occupied by other transmissions and waits for transmitting

| Name | Cable | Max. segment | Advantages |
|---|---|---|---|
| 100Base-T4 | Twisted pair | 100 m | Uses category 3 UTP |
| 100Base-TX | Twisted pair | 100 m | Full duplex at 100 Mbps (Cat 5 UTP) |
| 100Base-FX | Fiber optics | 2000 m | Full duplex at 100 Mbps; long runs |

| Name | Cable | Max. segment | Advantages |
|---|---|---|---|
| 1000Base-SX | Fiber optics | 550 m | Multimode fiber (50, 62.5 microns) |
| 1000Base-LX | Fiber optics | 5000 m | Single (10 μ) or multimode (50, 62.5 μ) |
| 1000Base-CX | 2 Pairs of STP | 25 m | Shielded twisted pair |
| 1000Base-T | 4 Pairs of UTP | 100 m | Standard category 5 UTP |


Figure 4-20. (a) A two-station Ethernet. (b) A multistation Ethernet.

CalPoly

# Data link: MAC protocols WiFi (802.11)

- Access Point mode or Ad-hoc network mode

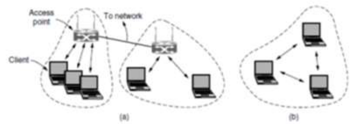



Figure 4-23. 802.11 architecture. (a) Infrastructure mode. (b) Ad-hoc mode.

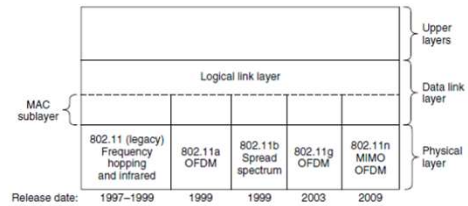



Figure 4-24. Part of the 802.11 protocol stack.

# Data link MAC frames (headers and trailers): Ethernet (802.3) and WiFi (802.11)

**Ethernet (802.3) Frame Format**

| 7 bytes | 1 byte | 6 bytes | 6 bytes | 2 bytes | 42 to 1500 bytes | 4 bytes | 12 bytes |
|---|---|---|---|---|---|---|---|
| Preamble | Start of Frame Delimiter | **Destination MAC Address** | **Source MAC Address** | Type | Data (payload) | CRC | Inter-frame gap |

**For TCP/IP communications, the payload for a frame is a packet**

**WiFi (802.11) Frame Format**

| 2 bytes | 2 bytes | 6 bytes | 6 bytes | 6 bytes | 2 bytes | 6 bytes | 0 to 2312 bytes | 4 bytes |
|---|---|---|---|---|---|---|---|---|
| Frame Control | Duration | MAC Address 1 (Destination) | MAC Address 2 (Source) | MAC Address 3 (Router) | Seq Control | MAC Address 4 (AP) | Data (payload) | CRC |

Each PHYSICAL device has ONE UNIQUE PHYSICAL ADDRESS called MAC address

# MAC Address

- 48-bit (6 bytes) version used in all IEEE 802 networks
  - Ethernet
  - 802.11 wireless networks (Wi-Fi)
  - Bluetooth
  - IEEE 802.5 Token Ring

- Commonly represented using Hexadecimal NUMBERS
- The Organization Unique Identifier (OUI) is the first 3 bytes of the MAC address and it's unique per vendor
  - E.g., the network card from Broadcomm has always the same set of first 3 bytes
- The Universally Administered Address is unique for each network card
- Together OUI + UAA = unique MAC address