Basic Networking Concepts

NTNU

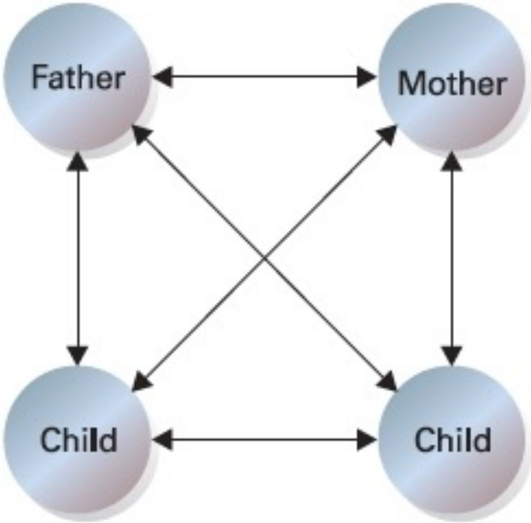
TTM4175 - Introduction to Communication Technology and Digital Security

Amir Taherkordi
{amirhost}@item.ntnu.no

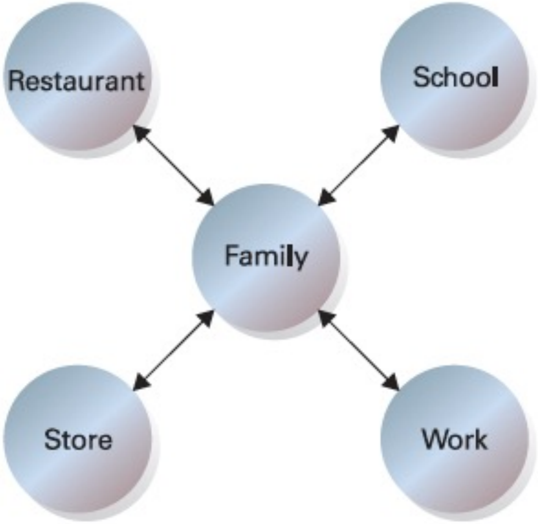
September 1, 2022

Networks in Our Daily Life

- Family network
  - related people share their resources and information
  - bi-directional

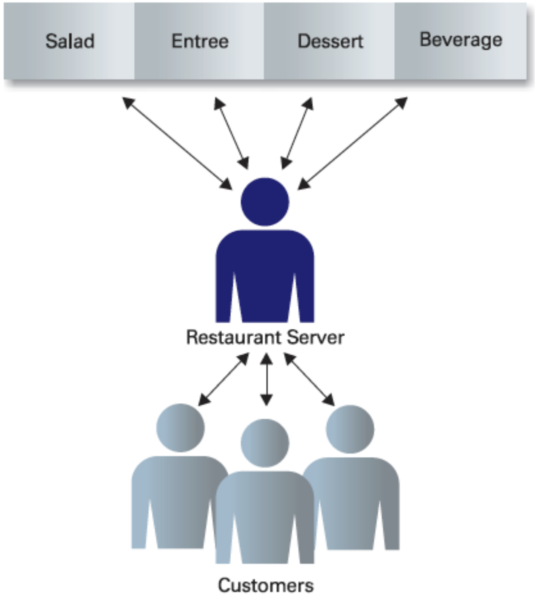


- Peer network
  - a community offers a wider array of resources
  - as simple as loaning a hammer to a neighbour, car-pooling
  - bi-directional among equals or peers

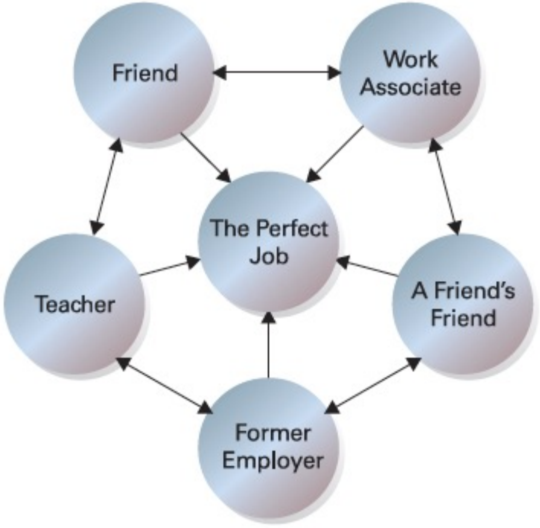


Examples

- Restaurant Network
  - a client-server model
  - you as customer: *client*
  - waiter: *server*

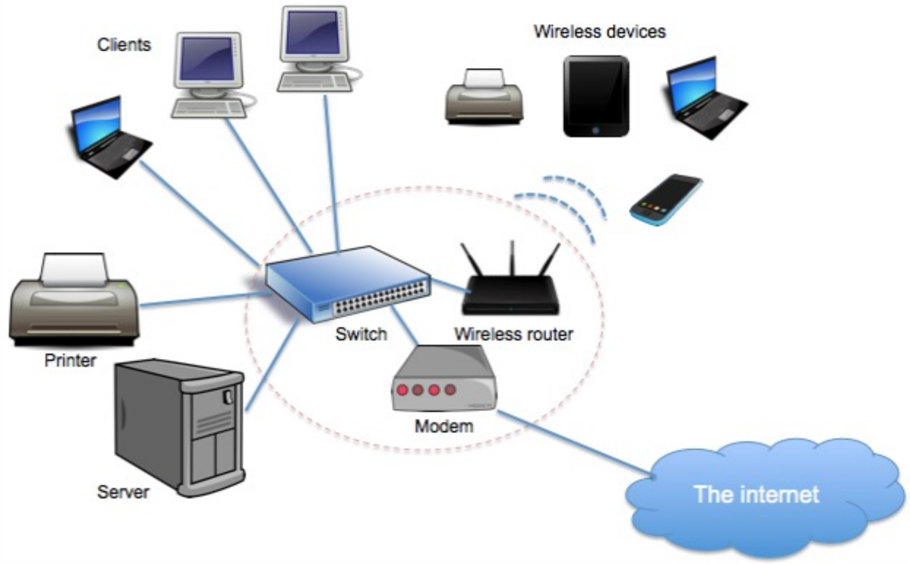


- Job contact network
  - a best way to find a job is to network
  - more people you meet, the better your chances of obtaining work.
  - A peer-to-peer network



Computer Networks

- A computer network:
  - consists of two or more *computing devices (nodes)* connected by *communication links.*
- A **node**: a computer, printer or any other device capable of sending or receiving data
  - e.g., server, printer, computer, security camera
  - *intermediary* devices
  - *end* devices: start or end of the communication
- A **communication link**: a wired or wireless link
  - only carrying the information

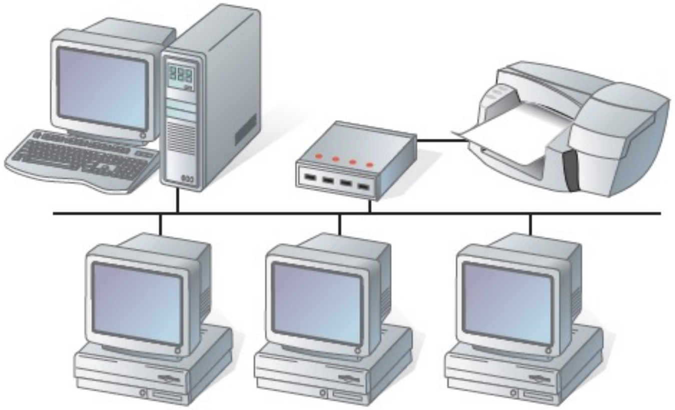


Computer Networks: Purposes

- Sharing information
  - e.g., company newsletters and announcements for employees
  - advertisements and purchase information for customers
- Sharing resources
  - *peripherals*: additional components attached to a computer like printers, scanners, and speakers
  - *storage*: users quickly ran out of space, sharing data with any user
  - *applications*: cost and space savings when computer users can centrally store their software applications
    - e.g., for creating text documents or playing computer games
  - other types of resources?

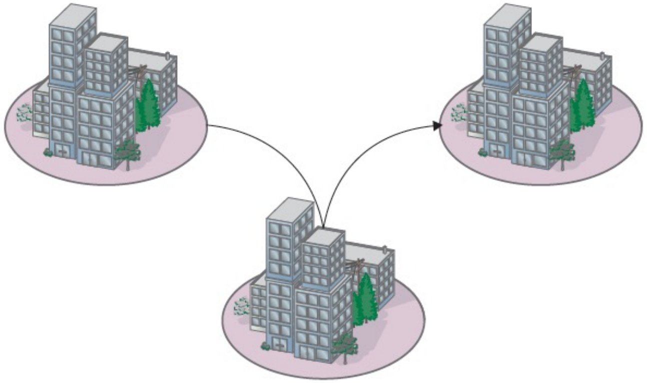
Classifying Computer Networks by Geography - 1

- According to the *geographical* boundaries the network spans
  - **Local Area Network (LAN)**
  - **Wide Area Network (WAN)**
  - **Metropolitan Area Network (MAN)**
- **LAN:** contained within a relatively small area, such as a classroom, school, or single building
  - **easy** to design and **troubleshoot**
  - all machines are connected to a **single cable**.
  - different types of **topologies** such as star, bus, ring, etc.
  - usually a **privately owned** network

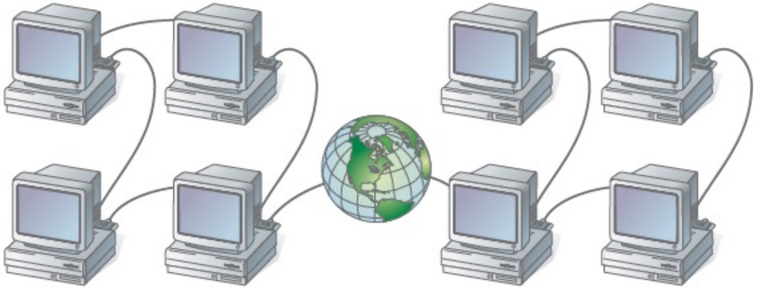


Classifying Computer Networks by Geography - 2

- **MAN:** When the network spans the distance of a metropolitan city, it can be referred to as MAN
  - similar technology as LAN
  - can be a single network such as cable TV network
  - or connecting a number of LANs to share resources LAN to LAN or device to device
  - not much popular today



- **WAN:** when the network spans a larger area
  - communication in WAN: leased telephone lines, satellite links and similar channels
  - mostly used to transfer large blocks of data between its users



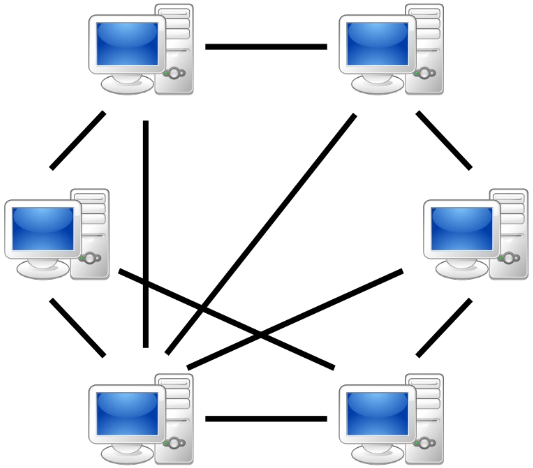
Classifying Computer Networks by Geography - 3

- Comparison

Parameters	LAN	MAN	WAN
Ownership of network	Private	Private or public	Private or public
Geographical area covered	Small	Moderate	Very large
Design and maintenance	Easy	Not easy	Not easy
Communication medium	Coaxial cable	Coaxial cables, PSTN, optical fibre, cables, wireless	PSTN or satellite links
Bandwidth	Low	Moderate	High
Datarates(speed)	High	Moderate	Low

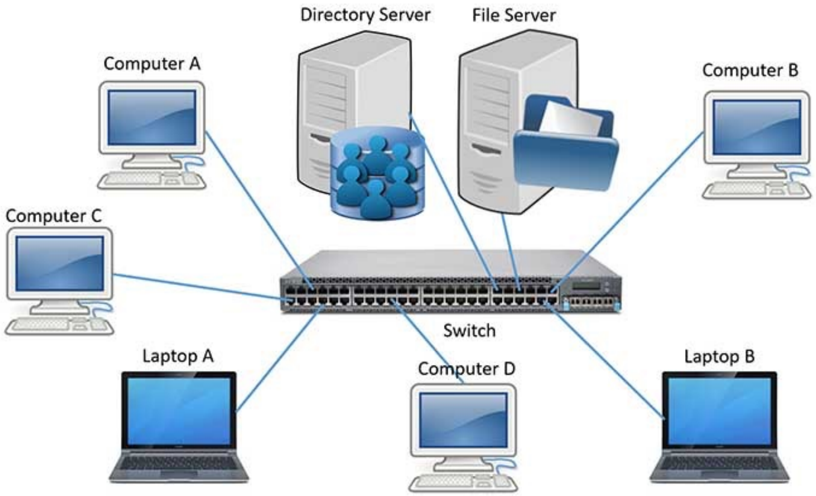
Classifying Computer Networks by Role - 1

- According to the *role of components* in the network
  - **Peer-to-peer** networks
  - **Client-server** networks
- Peer-to-peer (p2p) networks
  - each computer: responsible for making its **own resources** available to other computers in the network
  - each computer: responsible for setting up and maintaining its **own security** for these resources
  - do **not** have a **central** control system
  - no servers in p2p networks



Classifying Computer Networks by Role - 2

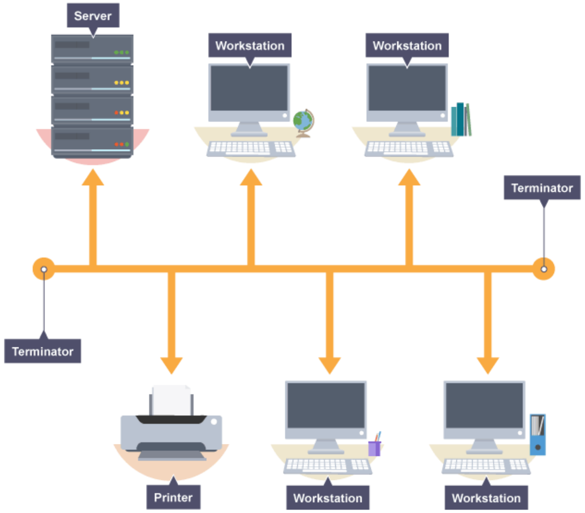
- Client-server networks
  - certain computers act as server and other act as clients.
  - a server: a computer providing the network resources and services to other computers
  - a client: the computer running a program that requests the service from a server
  - servers providing security and administration of the network
  - available network resources:
    - files, directories, applications and shared devices
    - centrally managed and hosted and then accessed by client



Classifying Computer Networks by Topology - 1

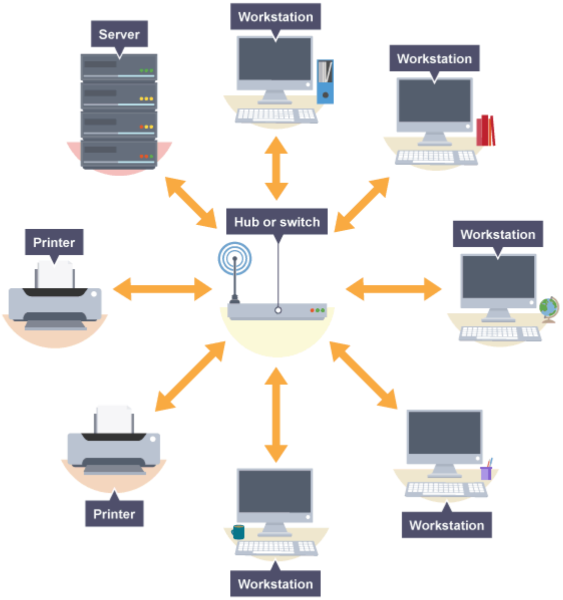
- Based on different ways of setting up a LAN (LAN topologies)
  - **Bus**
  - **Star**
  - **Ring**

- **Bus**
  - simple and low-cost
  - a single cable called a trunk(backbone, segment)
  - only one computer can send messages at a time
  - *Advantages*
    - easy to install
    - cheap to install - it does not require much cabling
  - *Disadvantages*
    - if the main cable fails or gets damaged, the whole network will fail
    - as more workstations are connected, the performance becomes slower because of data collisions
    - every workstation on the network 'sees' all of the data on the network: can be a security risk



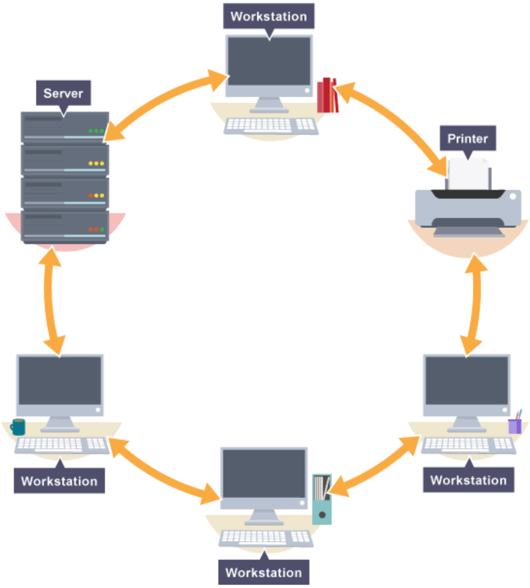
Classifying Computer Networks by Topology - 2

- **Star**
  - each device in the network has its own cable that connects to a switch or hub.
  - most popular way of setting up a LAN
  - *Advantages*
    - very reliable: if one cable or device fails, then all the others will continue to work
    - high performing as no data collisions can occur
  - *Disadvantages*
    - **expensive** to install as it uses the most cable, and cable is expensive
    - **extra hardware** is required - hubs or switches – which add to the cost
    - if a hub or switch **fails**, all the devices connected to it will have no network connection



Classifying Computer Networks by Topology - 3

- **Ring**
  - each device (e.g. workstation, server, printer) is connected in a ring: each one is connected to two other devices.
  - each data packet travels in one direction.
  - each device receives each packet in turn until the destination device receives it.
  - Every computer serves as a repeater to boost signals
  - *Advantages*
    - Quick data transfer (even if there are a large number of devices connected) as it only flows in one direction **without any data collisions**
  - *Disadvantages*
    - if the main cable fails or any device is faulty, then the whole network will fail.

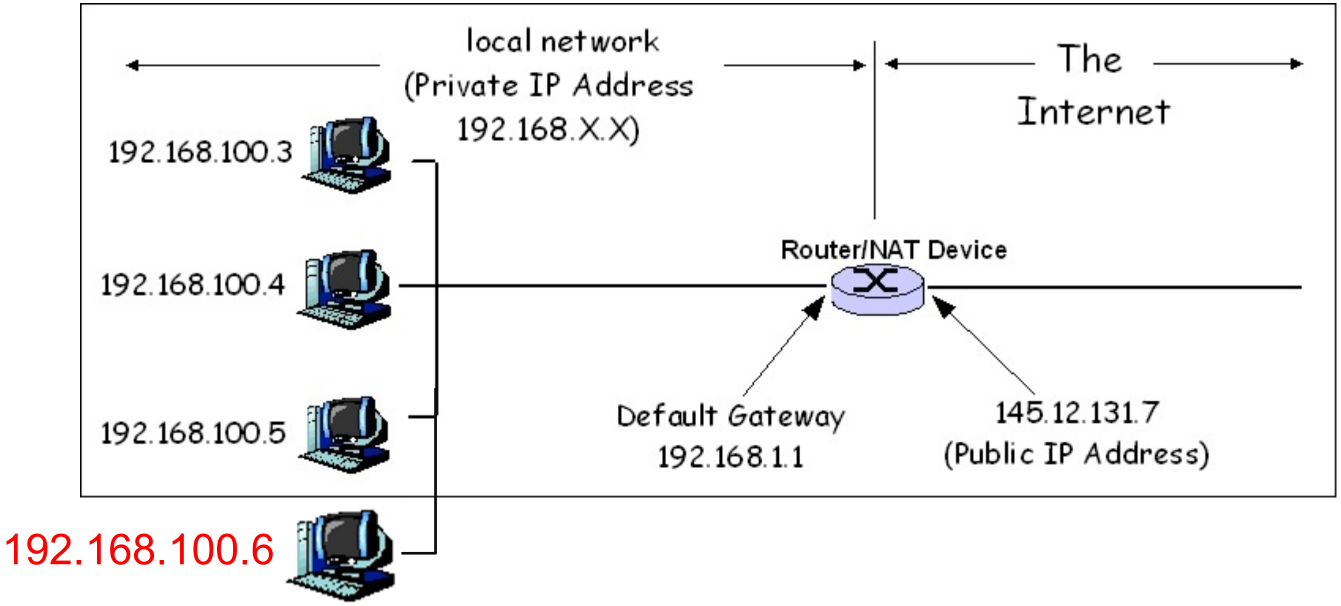


Addressing in Computer Networks

- If a node wants to communicate with other nodes?
  - How to find a node in the network?
  - It needs an address
- Generally three mechansims for addressing:
  - IP address
  - MAC address
  - Port number

IP Addressing - 1

- IP address: IP stands for Internet Protocol.
- IP is an important part in the Internet.
- IP address is a unique identifier assigned to each device connected to a computer network
- Example:



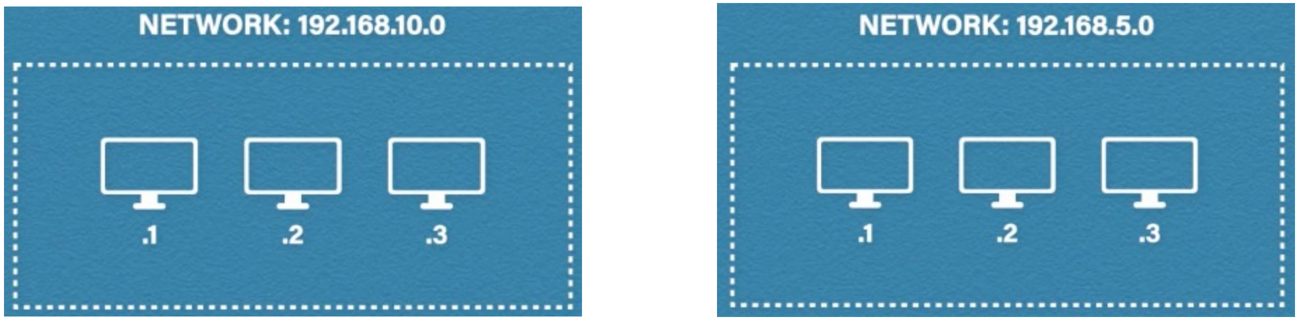
- IP addresses are logical
  - change the IP address based on the location of the device
  - assigned manually or dynamically

IP Addressing - 2

- An IP Address is unique and has four octets

192 • 168 • 10 • 3

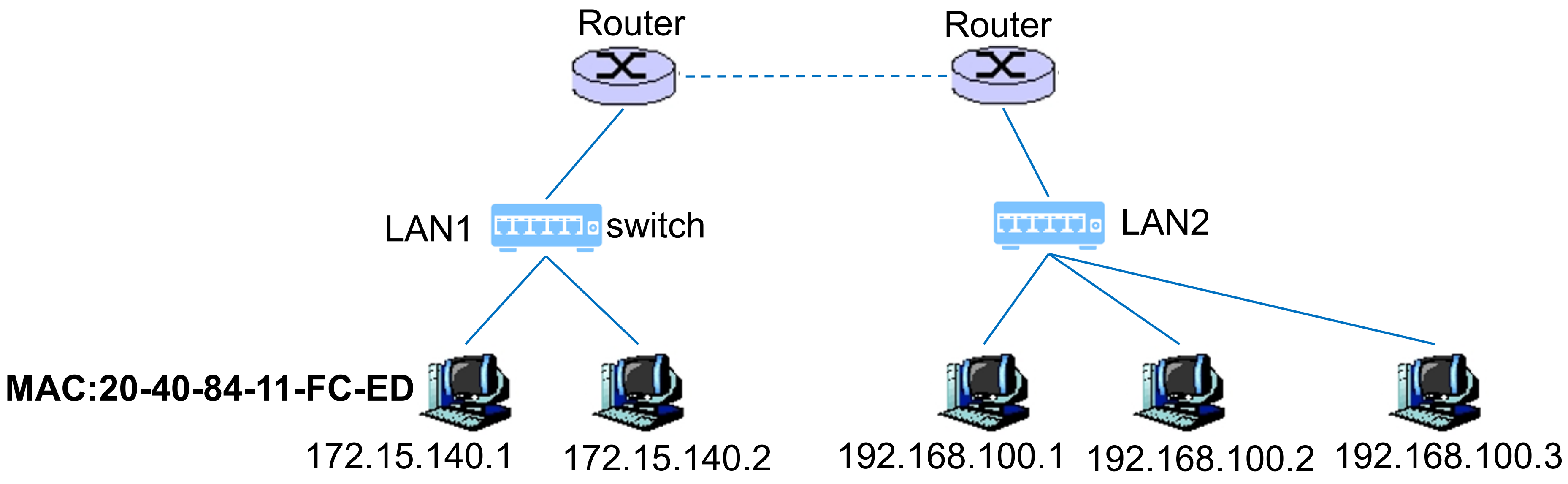
  - Say x.x.x.x and each of this x takes a value between 0 and 255.
  - the starting IP address will be 0.0.0.0 to 255.255.255.255.
  - the total number of bits in every IP address will be 32 bits.
  - address itself is separated into two parts: network and host



- Public and private IP addresses
  - public: given by Internet Service Provider (ISP)
  - private: by the router/wifi
- Static and dynamic IP addresses

MAC Address - 1

- MAC stands for Media Access Control.
- Every node in the LAN is identified with the help of MAC address only
- IP addresses: the location of the person.
  - Suppose, if a person is in London => his location is London.
  - So IP addresses are like the location of a person.
  - Wherever the person goes, his location gets changed.
- MAC addresses: the name of the person



MAC Address - 2

- IP addresses: logical addresses
  - which we can be changed
- MAC addresses
  - cannot be changed
  - normally be unique throughout the world.
- Why: because MAC address is assigned by the manufacturer.
- MAC addresses are represented in hexadecimal
  - e.g. , 20-40-84-11-FC-ED (48 bits)

Port Addressing - 1

- Example: a gift from a friend in Canada

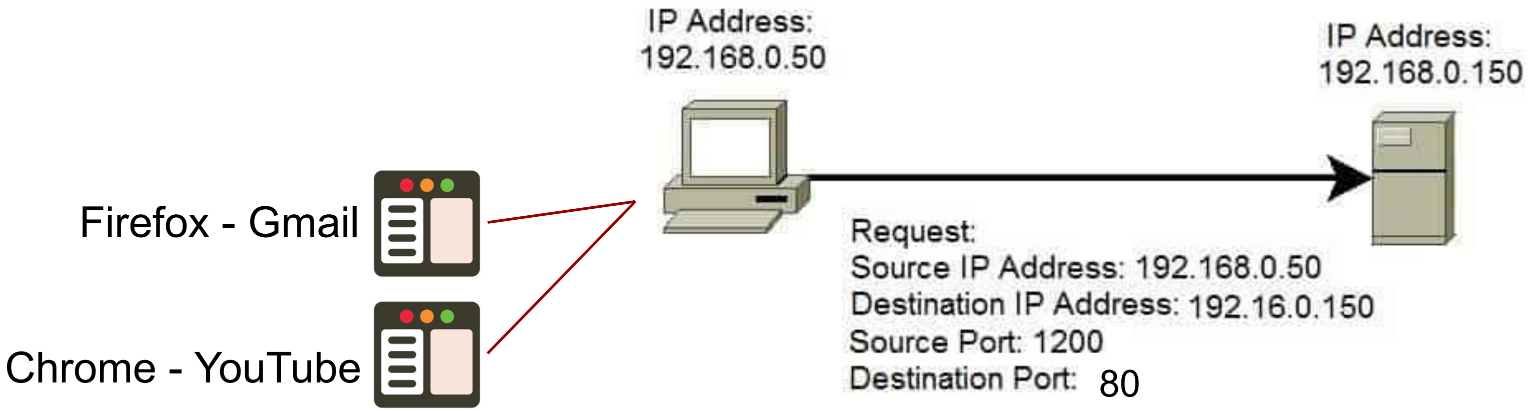
- Reaching our city?
  - It means reaching *our network:* done by IP address
- Reaching our apartment?
  - it means reaching the *right host:* done by MAC address
- Reaching the right person in the apartment?
  - It means reaching the *right process in the host:* done by **port address**

Port Addressing - 2

- In real communication, any device can be identified
  - with the help of IP address and MAC address
- But in the computer: many processes running

To which process that data has to reach is decided by the **port numbers** or **port address**.

- Port address/number:
  - every process in a node is uniquely identified using port number.
  - port number = communication end point
  - In general, the port numbers: 0 … 65535



Firefox - Gmail

Chrome - YouTube

IP Address:
192.168.0.50

IP Address:
192.168.0.150

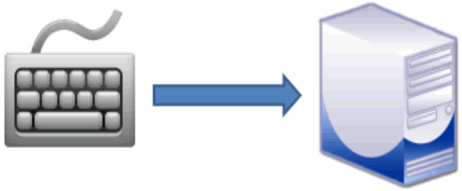
Request:
Source IP Address: 192.168.0.50
Destination IP Address: 192.16.0.150
Source Port: 1200
Destination Port: 80

Addressing – Key Points

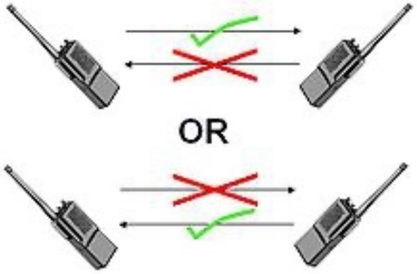
- Before sending the data
  - any node must attach the source IP address and destination IP address so that the **right network** is getting identified.
  - it should also attach source MAC address and destination MAC address so that the **right host** is identified.
  - It should also attach source port number and destination port number so that **the right process** from that particular host is identified.

Data Flow in Network Communication

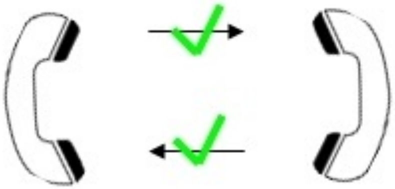
- **Data Flow**
  - Data communications: exchange of data between two nodes
- Data flow forms
  - *Simplex*
    - a unidirectional communication: one node transmits and other will receive.
    - e.g. a keyboard to a CPU. CPU does not send data to keyboard



  - *Half Duplex*
    - A a bidirectional communication: sending and receiving, but not at the same time
    - If one device is sending, the other device can receive, but not send.
    - e.g. walkie-talkie: talk and listen, but not at the same time.



  - *Full Duplex (Duplex)*
    - Communication: both directions simultaneously
    - devices can send or receive data at the same time.
    - e.g. telephone line: we can talk and listen simultaneously in a telephone line.



Network Protocols - Basics

- In any communication scheme, postal, SMS, Whatsapp, …, we have certain things in common:
  - source or sender
  - destination or receiver
  - channel or media
- this communication: always governed by certain *protocols*.

protocols are rules that govern the communications between two computers connected to the network.

- What if there are no protocols?
- If the guy speaks
  - at high speed which the destination cannot handle, this communication becomes useless.
  - different languages (maybe grammatically current, still …)
  - not giving time to other guy to respond

Network Protocols - Aspects

- There is a need for protocols
- More detailed definition:
  - formal **standards** and **policies** made up of **rules**, **procedures** and **formats** that defines communication between two or more devices over a network
- Protocol determines
  - **what** is communicated in the network
  - **how** it is communicated in the network
  - **when** it is communicated in the network
- Let's take a closer look at the human communication

Network Protocols – Inspired by Real World

- In human communication definitely
  - **a sender and a receiver**: maybe a single receiver and a group of receivers
  - the communication should involves **common language and grammar**.
  - speed **timing of delivery** of speech: very important in human communication
  - to ensure his words understandable by the lady: **confirmation or the acknowledgment** from the receiver

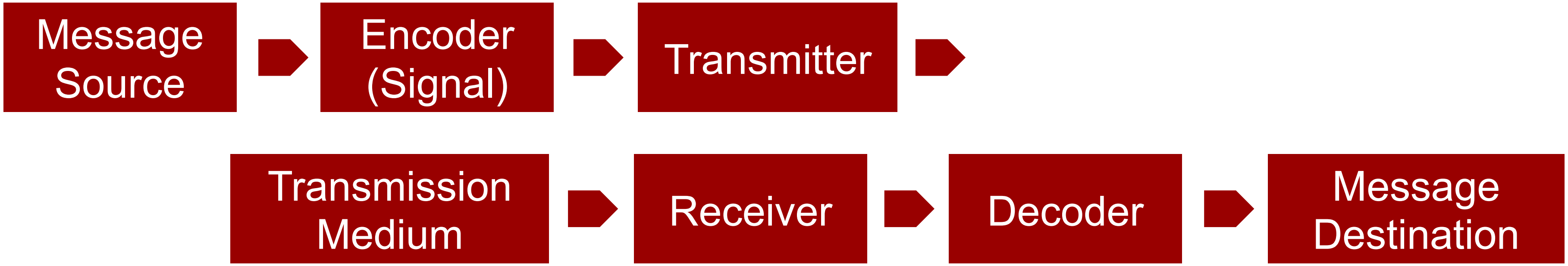
- Only then human communication can be effective.

Network Protocols - Parts

- The message should be **encoded, formatted and encapsulated** in a way that the destination can understand.
- **Timing** is very important in network communication.
- The **size** is very important.
  - because the link cannot carry big data.
  - If a low capacity link, this link cannot carry big data.
  - it has to be handled appropriately.
- **Delivery option:** whether the message is
  - only for one destination
  - or some group of destinations
  - or all the destinations in the network,

These all should be handled by protocols.

Message Encoding


Message Source
Encoder (Signal)
Transmitter
Transmission Medium
Receiver
Decoder
Message Destination

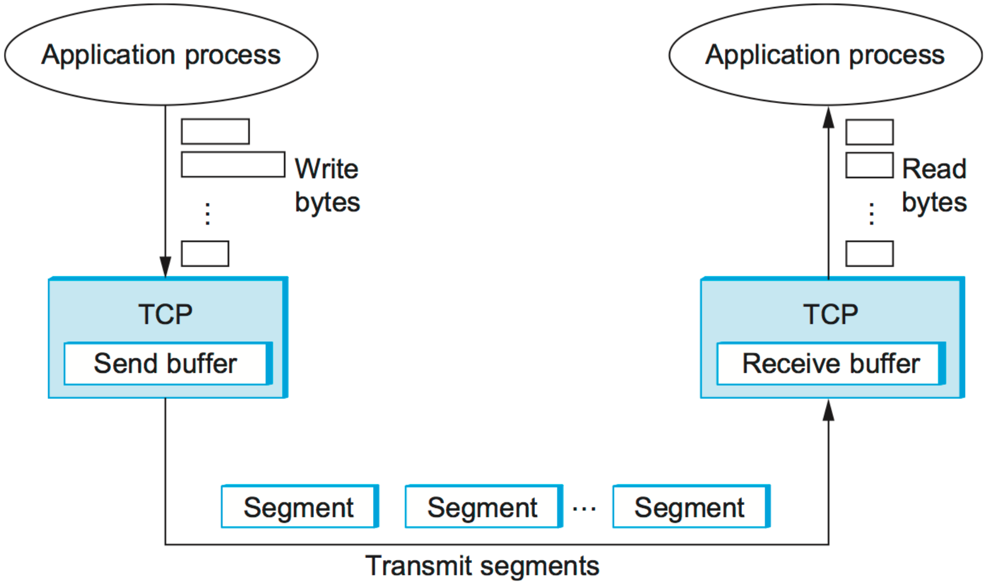
- Why encoder?
  - two kinds of transmission medium:
    - a wired medium
    - a wireless medium
  - The source needs to know to which medium it is connected to.
    - If a wired medium => the data has to be converted into signals
    - If a wireless medium => the sender have to encode the data in the form of waves.

Message Fromating and Encapsulation

- Formatting:
  - Both sender and receiver must mutually agree upon certain formats
- Encapsulation
  - when the receiver receives data: identify who has sent this data?
  - add information with the data to **identify** the **sender** and the **receiver**
- So we encapsulate certain things like the source information and the destination information with the data.

Message Size

- If there is a very big message: human breaks it into smaller parts or sentences.
- Likewise, our computer should do that.
- If the link capacity is very small, but the data to be transmitted is very big
  - The protocol should break it into smaller units which this transmission medium can handle.
- For example in TCP/IP protocol

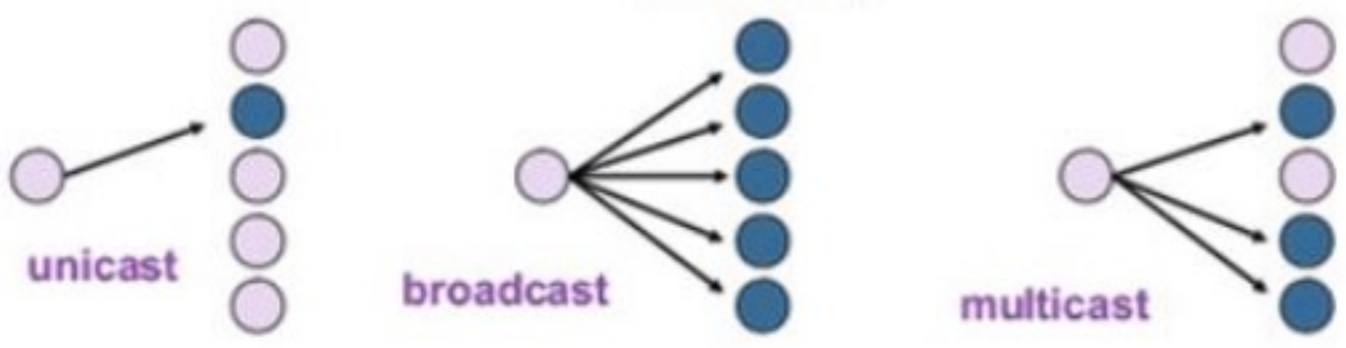


Message Timing

- Protocol should deal with
  - flow control
    - sender very fast VS. receiver is slow!
    - If no flow control: keep on sending data but not receiving the data
    - *flow control mechanism*: responsibility of the protocol
  - response timeout
    - sender is sending some data => the receiver has to acknowledge
    - if the *acknowledgment* is not received, the sender have to *wait* for a certain period of time
    - After he expiry of the time (timeout), the sender will re-transmit to ensure guaranteed delivery
    - waiting time for an acknowledgment: responsibility of protocol

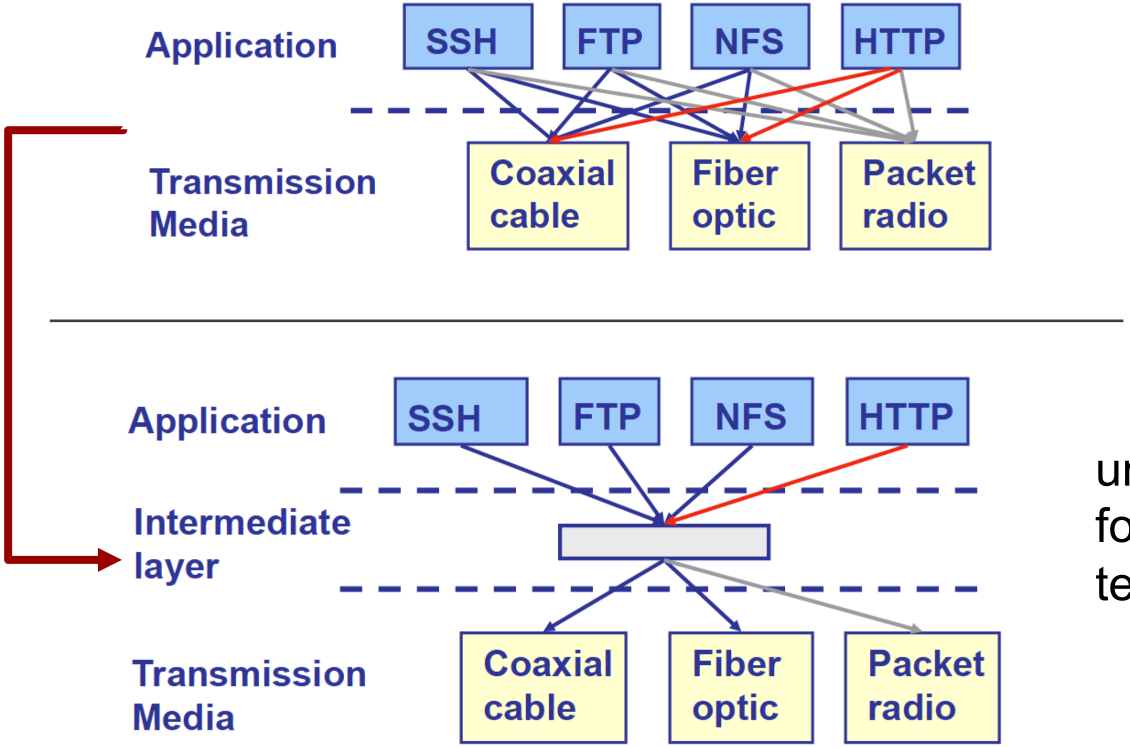
Delivery Options

- Three delivery options:
  - unicast
  - multicast
  - broadcast



Layering in Computer Networks

- Layering: decomposing the problem into more manageable components (layers).
- Why layering?



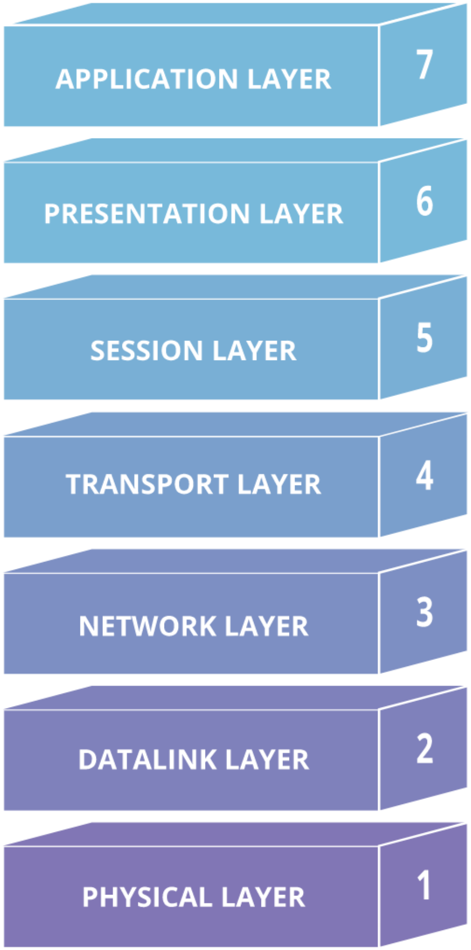
unique **abstraction** for various network technologies

Layering in Computer Networks

- Benefits:
  - Encapsulation
    - Functionality inside a layer: self-contained; one layer doesn’t need to reason about other layers
    - Decomposes problem of building network into more manageable components
    - it is easy to troubleshoot
  - Modularity
    - Can replace a layer without impacting other layers
    - Lower layers can be reused by higher layers
    - e.g. TCP and UDP both are layered upon IP

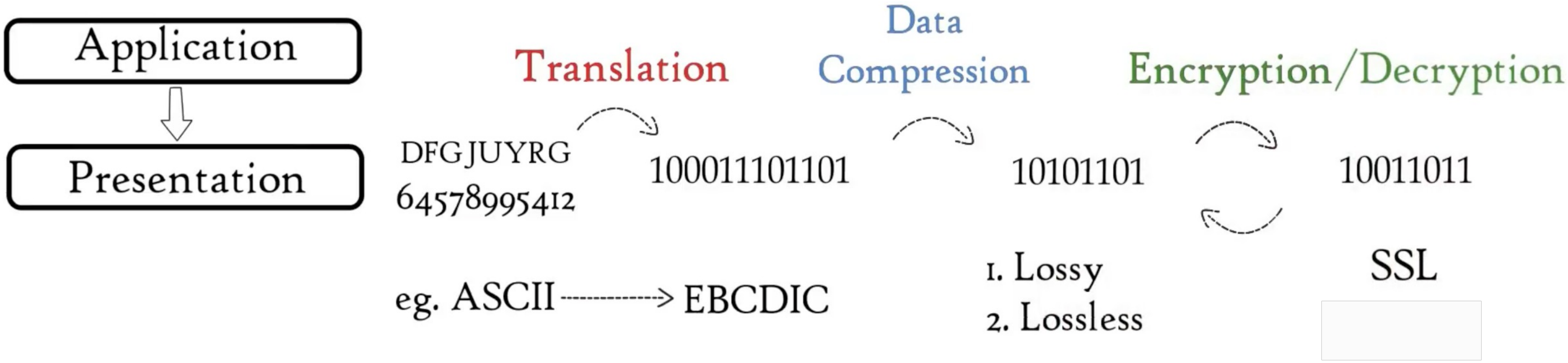
OSI Networking Model

- Open Systems Interconnection (OSI) model
  - a conceptual model
  - created by International Organization for Standardization
  - enables diverse communication systems to communicate using standard protocols
- *As a universal language for computer networking*
- OSI is not a protocol
  - guideline for communication



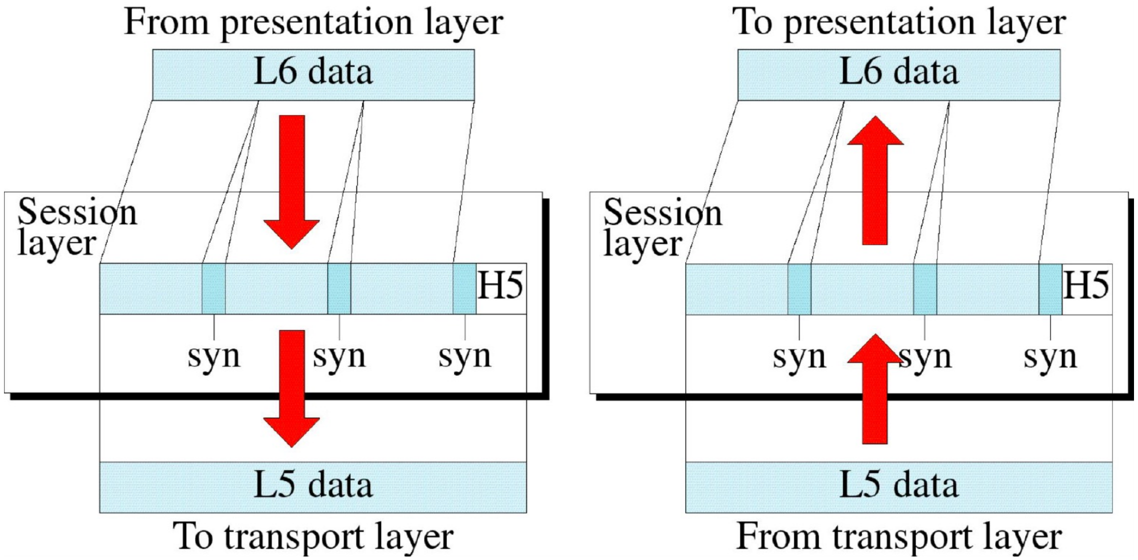
OSI Layers – Application and Presentation

- Each layer is a package of protocols
- Application layer
  - applications like web browsers and email clients
    - Use protocols in this layer: such as HTTP and SMTP
  - directly interacts with data from the user
- Presentation layer
  - receives data from application layer
  - responsible for preparing data for application layer
  - Main tasks



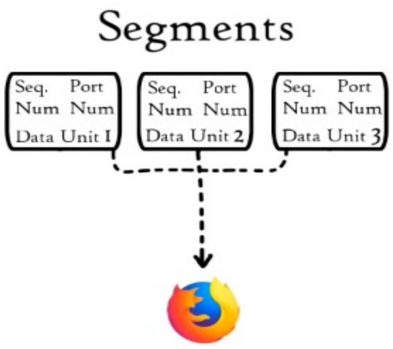
OSI Layers – Session

- Session layer
  - responsible for opening and closing communication between the two devices (time period=session)
  - **authentication** and **authorization**
  - **synchronizes** data transfer with checkpoints
  - ensures to **transfer all data**

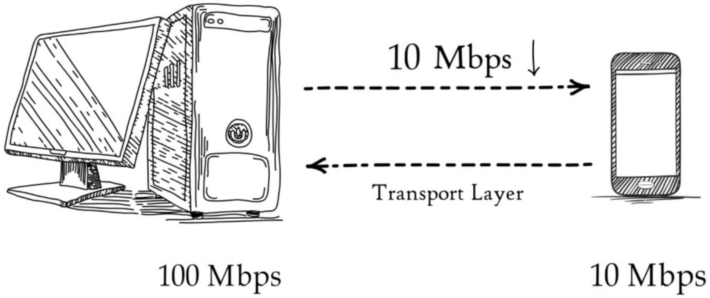


OSI Layers - Transport

- Responsible for
  - *Segmentation*: breaking data into chunks



  - *Flow control*: optimal speed of transmission
    - to ensure a sender with a fast connection doesn't overwhelm a receiver with a slow connection



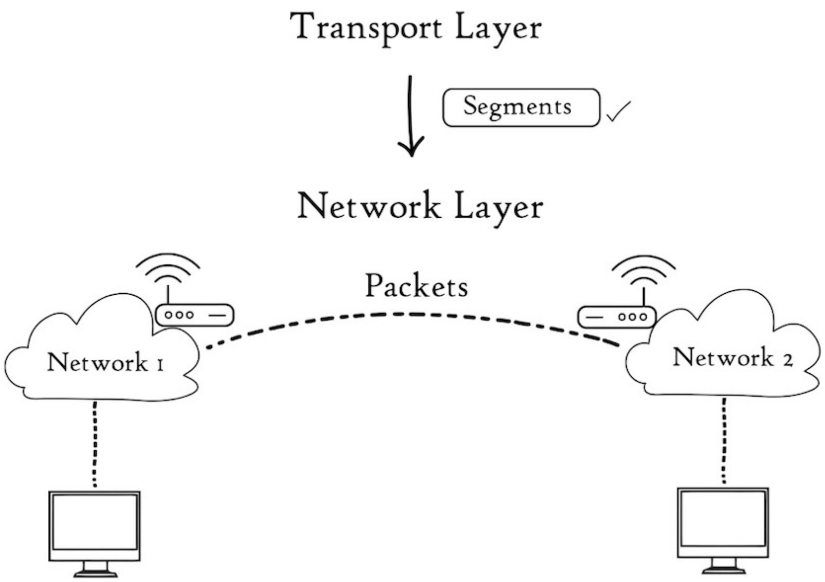
  - *Error control*: on the receiving end
    - ensuring the data received is complete
    - checksum: used to request a retransmission if not correct

- Main protocols
  - connection-oriented transmission (TCP): data ack
  - connectionless transmission (UDP): no ack
  - => UDP faster than TCP
  - UDP and TCP Examples?

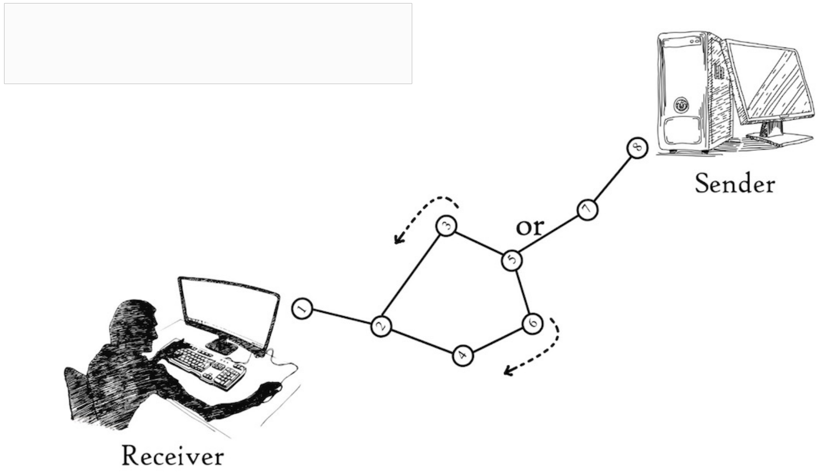
UDP

TCP

OSI Layers - Network

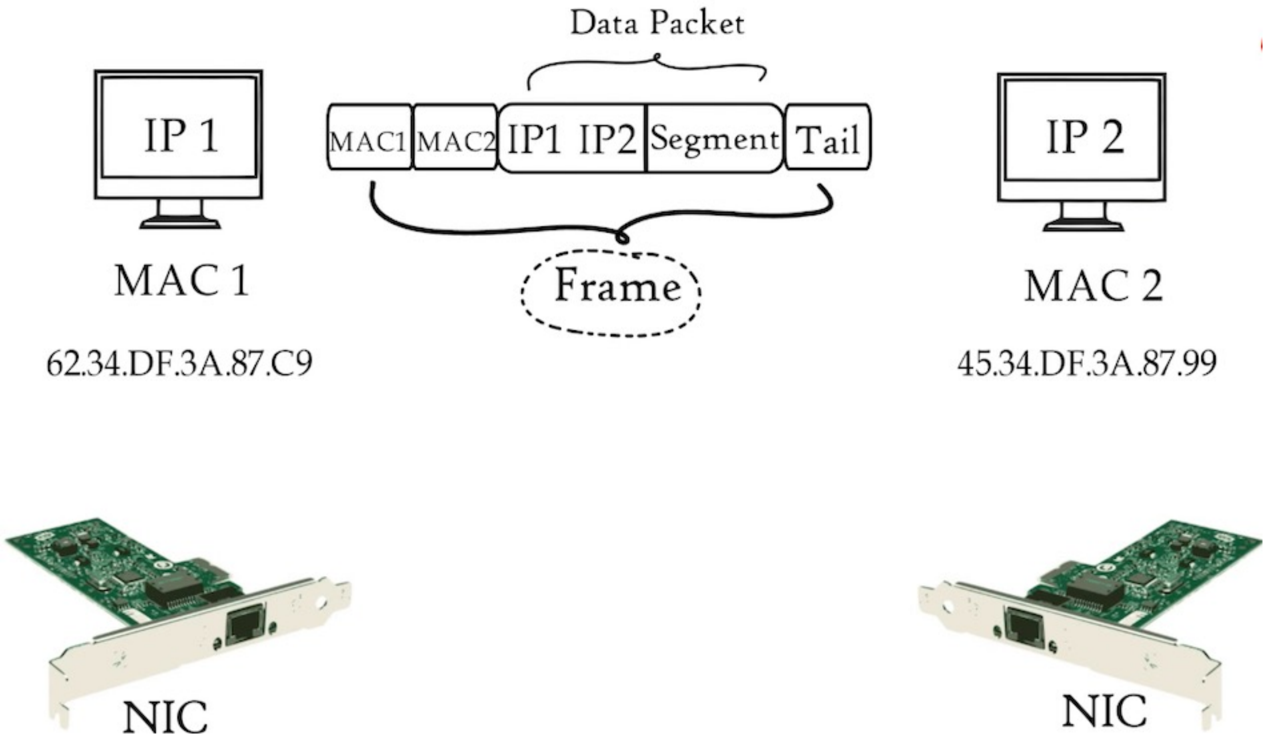


- Logical addreassing: IP
- Routing and path finding
  - moving data from source to destination



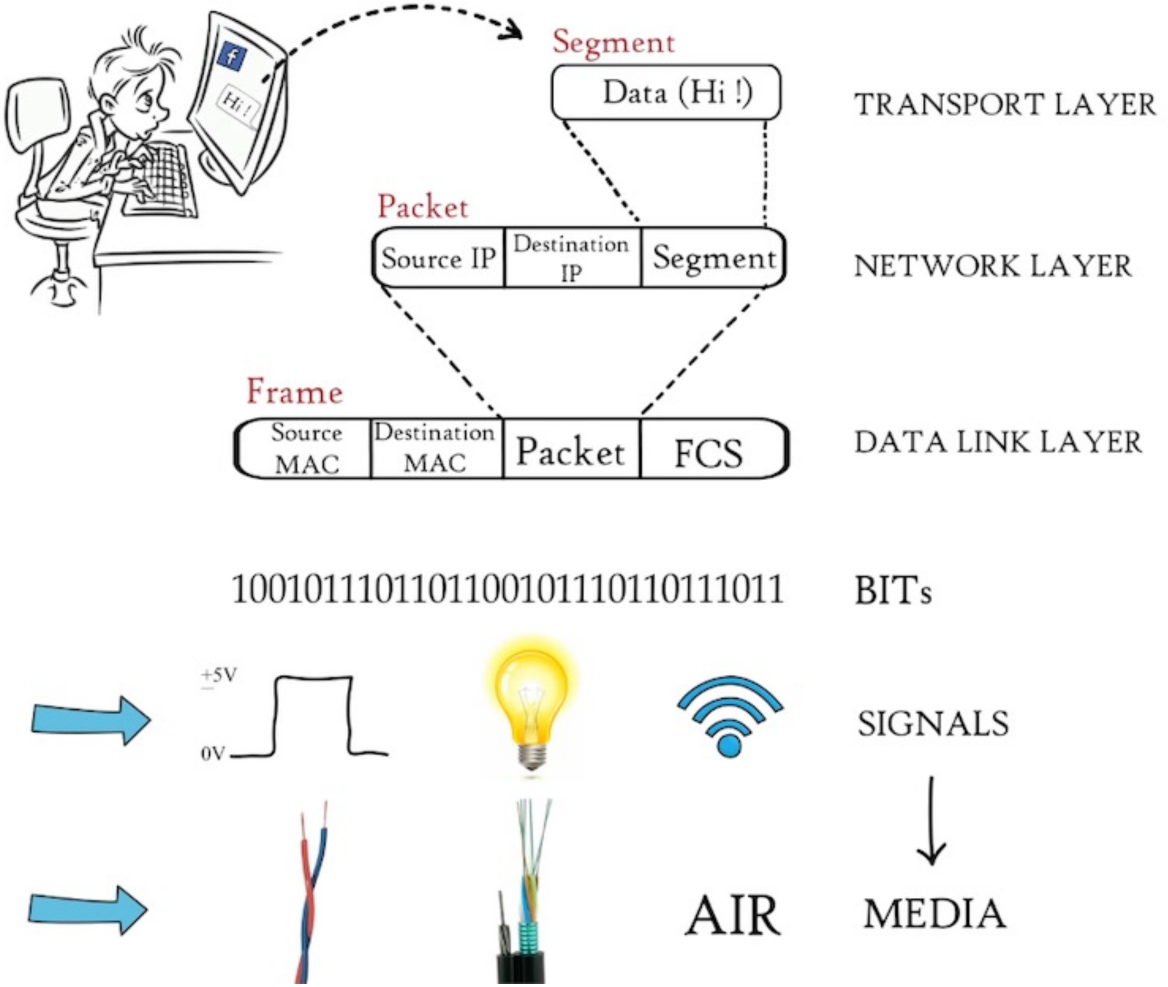
OSI Layers – Data Link

- takes packets from the network layer and breaks them into smaller pieces called frames.
- also responsible for flow control and error control in intra-network communication



OSI Layers – Pysical

- data is converted into a bit stream: a string of 1s and 0s



Summary

- Intorduction to computer entworks
- Computer networks classification
- Addressing in computer networks
  - IP, MAC and ports
- Network protocols
- Layring in computer networks
- OSI networking model