Computer Network I

Reti di Calcolatori I

Università di Napoli Federico II – Scuola Politecnica e delle Scienze di Base
Corso di Laurea in Informatica

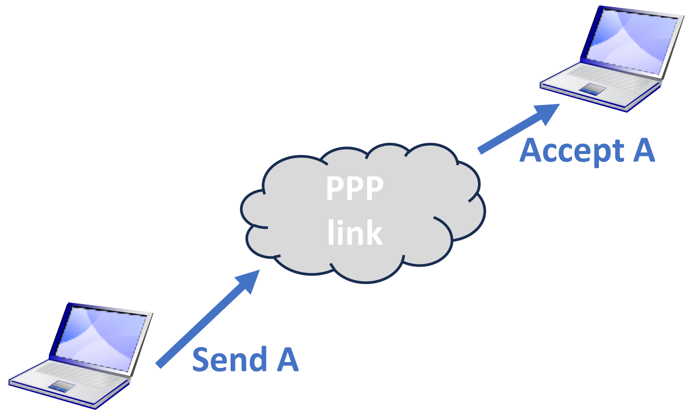
Riccardo Caccavale

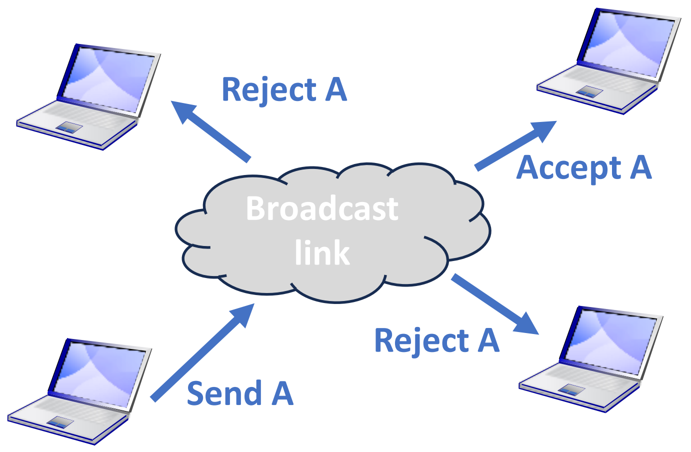
(riccardo.caccavale@unina.it)

Università degli Studi di Napoli Federico II

Link Layer
Link Types

- There are basically 2 types of links that can be managed:
  - **Point-to-point link**: consists of a **single sender** at one end and a **single receiver** at the other end. The **point-to-point protocol** (PPP) is one example of protocol managing such links.
    - E.g., direct ethernet link between 2 computers.
  - **Broadcast link**: multiple sending and receiving nodes all connected to **the same shared channel**. The term broadcast is used because when one node transmits a frame it is received by all nodes on the channel.
    - E.g., Ethernet bus, half-duplex Ethernet (rare, as most cables are todays full-duplex) or wireless LANs.



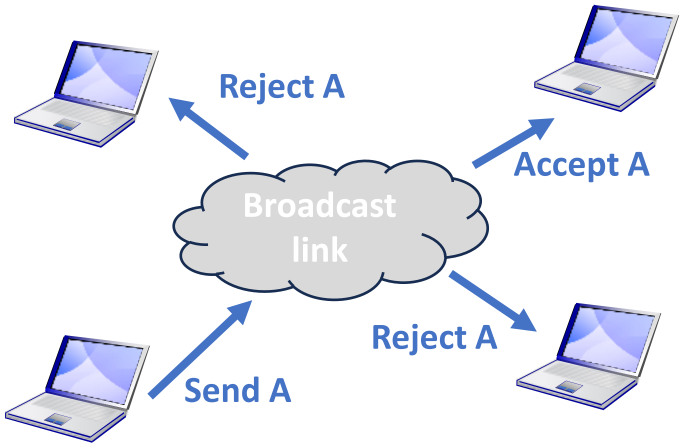


- The access to **broadcast links have to be coordinated** (multiple access problem) as multiple communication on a single link may interfere each other.

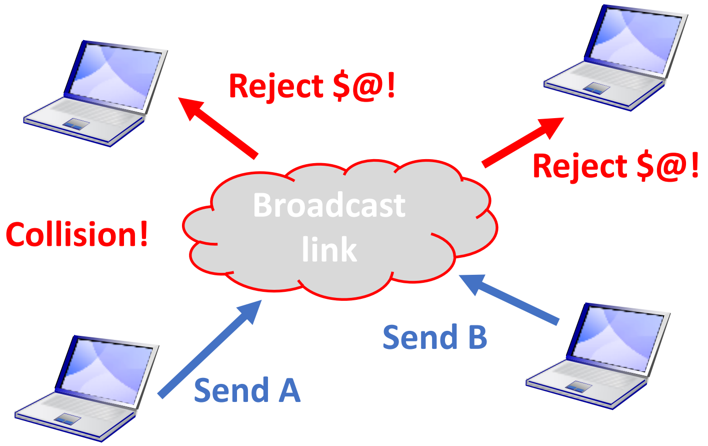
Link Layer

Collisions

- The main problem of broadcast link is the **collision**: if multiple nodes are simultaneously transmitting frames on the same channel, **all such frames overlap becoming incomprehensible**.



- These **collided frames are** then received by all nodes on the channel and **dismissed as errors** (no harm is done), but:
  - All **transmitted frames are lost**.
  - The **time-interval is wasted**, as the channel has been used to transmit useless data.

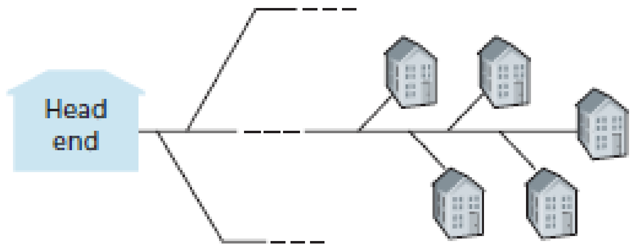


Link Layer
Multiple Access Protocol

- In computer networks **multiple access protocols** are used **to regulate transmissions via broadcast channels**, so that:
  - **Collisions are managed**.
  - Each node has a chance to transmit, so **nodes do not monopolize the link**.
  - Established **connections are not interrupted** (e.g., checking if link is busy).

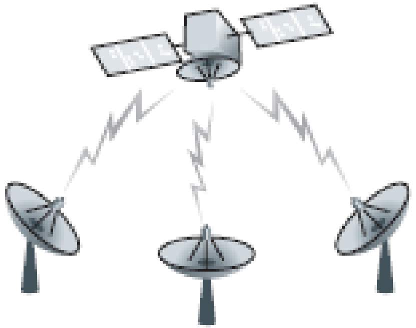
- Such protocols are needed for a variety of network settings, including both wired, wireless or satellite networks, **where hundreds or thousands of nodes can directly communicate over a broadcast channel**.

Shared wire
(for example, cable access network)



Shared wireless
(for example, WiFi)

Satellite



Link Layer
Multiple Access Protocol

- The primary role of a **multiple access protocol** is to somehow **avoid collisions** (there are dozens of protocols over different link-layer technologies). Main approaches are:
  - **Channel partitioning**: the bandwidth is partitioned for different nodes.
  - **Random access**: the nodes "gamble" for the access.
  - **Taking-turns**: the nodes waits for their turn.

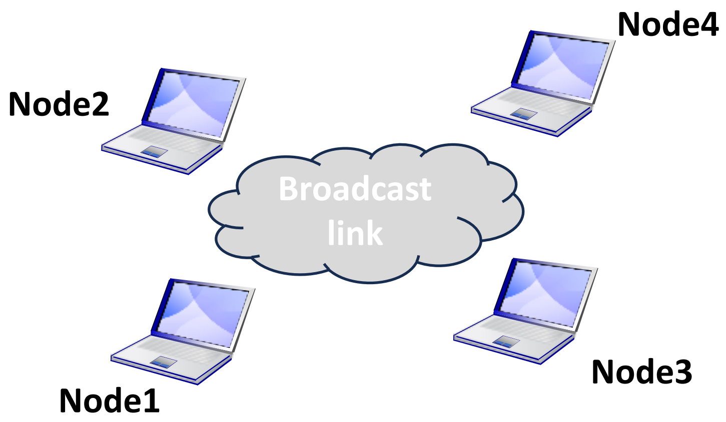
- **Desiderata**: a multiple access protocol for a **broadcast channel of rate *R* bps** should also provide the following characteristics:
  - To **maximize the usage of the channel**: if M nodes have data to send, each one should have, in average, a throughput of R/M bps (if M=1 then throughput should be R).
  - To be **decentralized**: a master node may be a single point of failure.
  - To be **simple and lightweight**: tons of frames are sent, there must be no overhead.

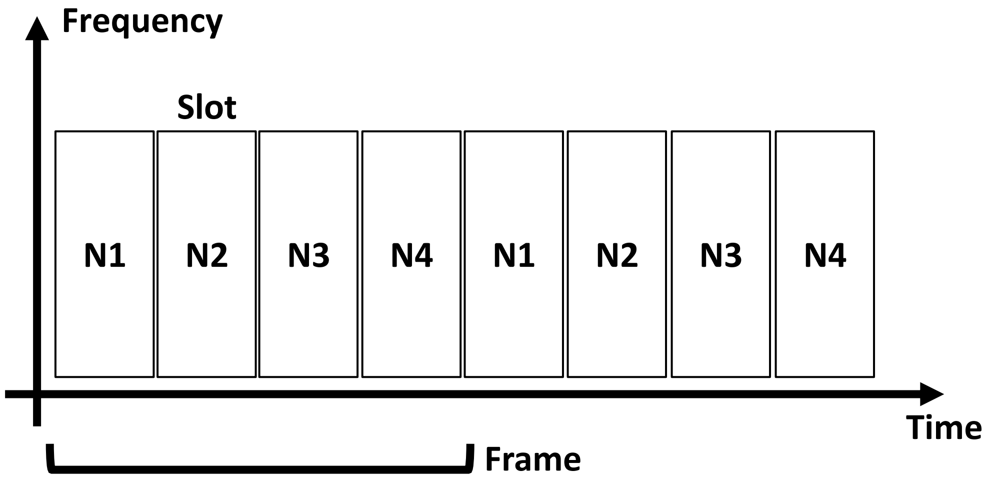
Link Layer
Channel Partitioning Protocols: TDMA

- **Time division multiple access** (TDMA): let's consider a channel with N nodes having transmission rate of *R* bps, **TDMA divides time into time frames** (steps) and further divides **each time frame into N time slots**.

- Each **time slot is assigned to one** of the N nodes. Whenever a node has a packet to send, it waits for the assigned time slot.

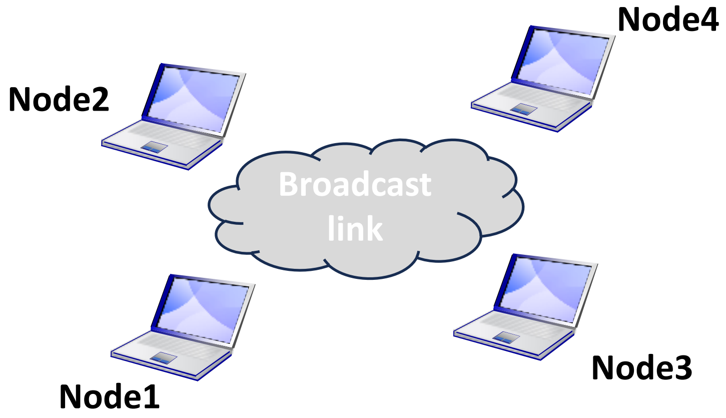
- Typically**, slot sizes are chosen so that a whole packet can be transmitted** during a slot time.



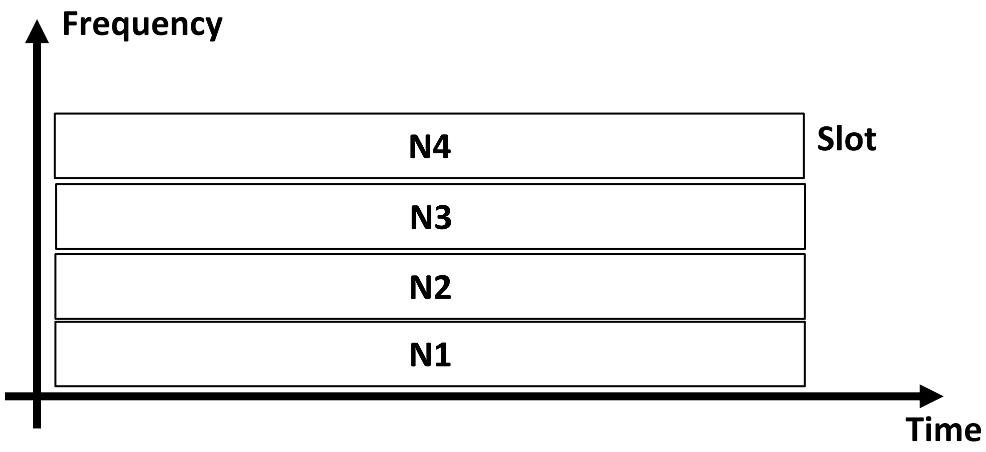


Link Layer
Channel Partitioning Protocols: FDMA

- **Frequency division multiple-access** (FDMA): divides the R bps channel into different frequencies (each with a bandwidth of R/N) and assigns each frequency to one of the N nodes.



- FDMA and TDMA shares pros and cons:
  - They **avoids collisions and divide the bandwidth fairly** among the N nodes.
  - A **node is limited to a bandwidth of R/N**, even when it is the only node with packets to send.

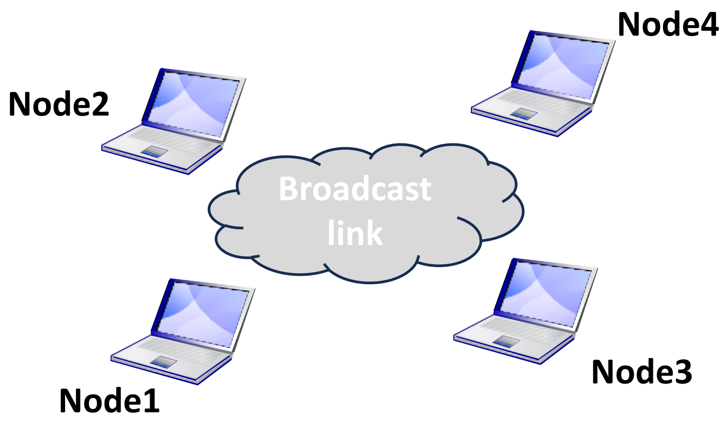


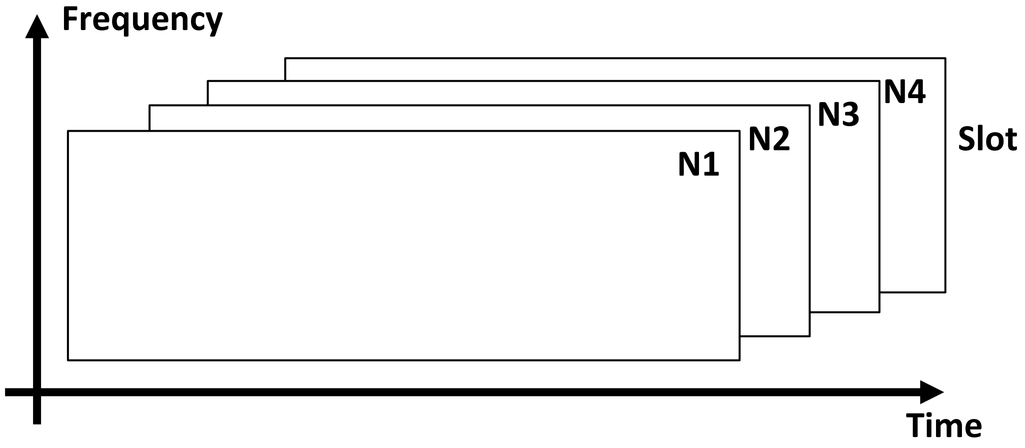
Link Layer
Channel Partitioning Protocols: CDMA

- **Code division multiple access** (CDMA): assigns a different code to each node which is used to encode/decode the data bits it sends.

- If the codes are chosen carefully, **CDMA networks allows different nodes to transmit simultaneously** without causing interference.

- CDMA works **mainly on wireless channels**; it has been used in military systems for some time (due to its anti-jamming properties) and **also in cellular telephony**.





Link Layer
Random Access Protocols

- In random access protocols, a **transmitting node always transmits at the full rate** of the channel (at *R* bps).

- If a **collision occurs** (i.e., at least 2 nodes are transmitting) all transmitting **nodes waits a random delay** before attempting again the retransmission.

- Since this **selection is performed independently**, it is possible for the 2 nodes to **choose a delay which is different enough** to allow one of the two contenders to sneak the message in.

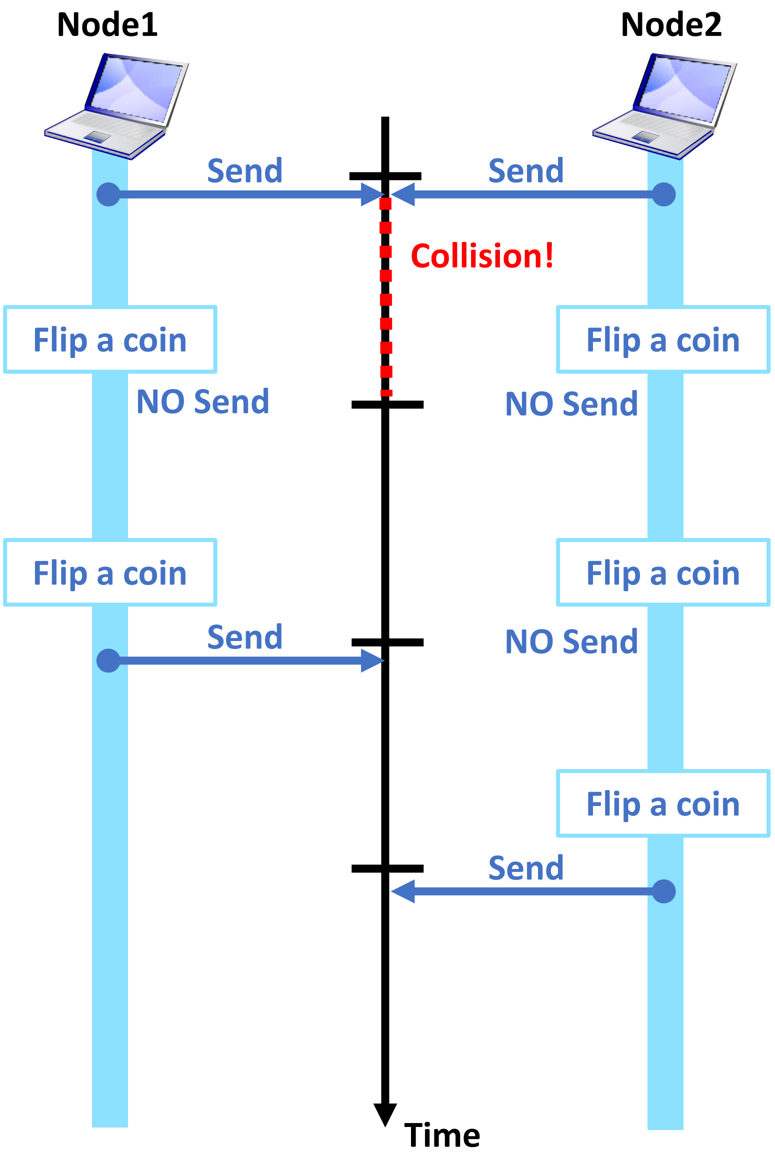
- If, otherwise, a **similar delay is chosen**, a new collision occurs, and **the process is iterated**.

Link Layer

Random Access Protocols: Slotted ALOHA

- The **slotted ALOHA protocol** works as follows:
  - The **time is divided into slots** (as in TDMA) where each slot is large enough to contain one frame.
  - The nodes are synchronized, so **each node transmit frames only at the beginnings of a slots**.
  - **If no collision** is detected within the slot, the **communication continues**.
  - Otherwise**, if a collision is detected** within a slot, **each colliding node have a probability *p ϵ [0,1]* of resending this frame** in each one of the following slots, until the frame is successfully sent.

- Features:
  - **If there is only one node, it will use the full rate** R of the channel (no collisions).
  - Is **decentralized** as nodes are totally independent from the others besides the synchronization.
  - Is **simple to implement** and to execute (random selection is quite fast).
  - Having **multiple consecutive collisions is unlikely**.



Link Layer

Random Access Protocols: CSMA

- One **weakness of ALOHA is that we may start transmission** (producing a collision) **even if the channel is already busy**. We understand it just through the effect of collisions.

- A solution is **to monitor the channel** and to attempt transmission only if the channel is idle.

- **Carrier sense multiple access** (CSMA) and **CSMA with collision detection** (CSMA/CD) protocols are based on 2 principles:
  - **Carrier sensing**: nodes **listen to the channel before transmitting**. If a frame from another node is currently being transmitted, it waits until no transmission is detected.
  - **Collision detection**: nodes **listens to the channel while it is transmitting**. If a collision is detected, it stops transmitting and waits a random amount of time before restarting.

- If all nodes perform carrier sensing, **why do collisions occur in the first place**?

Link Layer

Random Access Protocols: CSMA

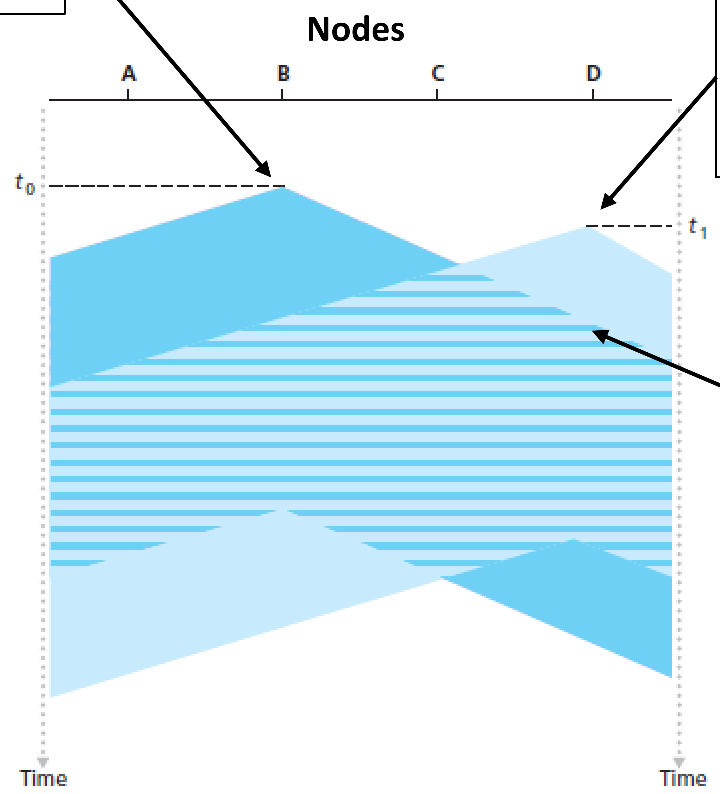
- Because of the **delay in the signal transmission**!

- Even if the propagation of signals in the channel is typically near the speed of light, **it takes time to reach all other nodes**. Therefore, a second node detect the transmission only after it has started.

- Because of this delay between transmission start and detection, **a node may consider as free a channel that is actually in use**, producing a collision.

Signal from B propagates in all directions

D has not yet received the signal and starts transmitting



D receives the signal, and understands the channel was busy

Link Layer

Random Access Protocols: CSMA

- The **pure CSMA** is very simple:
  1. **Check if the channel is busy**.
  2. **If channel is idle, send a frame**.
- **In CMSA collisions are not detected** but are still possible, we understand that a frame is lost just **because the ACK is not received**.

- The **CSMA/CD is more evolved** (currently **implemented on Ethernet**):
  1. **Check if the channel is busy.**
  2. **If channel is idle, send a frame**.
  3. **While transmitting, check for possible collisions.**
  4. **If collision is detected**, stop transmitting and **wait for a random period** $K \in \{0, \ldots, 2^n-1\}$ where ***n* is the number of detected collisions** on the current frame (**binary exponential backoff**).
- Since number of possible periods increases, **the probability to successfully send the frame increases with the number of collisions**.

Link Layer

Taking-turns

- **Polling protocol**: there is **one master node that selects in a round-robin way one node per time** allowed to transmit (up to the max throughput). This process is iterated every time transmission stops (e.g., Bluetooth).
  - There are **no collisions**.
  - There is a **polling delay** (time to select nodes).
  - The approach is **centralized**, there is a single-point-of-failure.

- **Token-passing protocol**: there is **no master node, nodes exchange a special frame called token**, if a node receive the token it is allowed to transmit, then the token is passed to another node.
  - There are **no collisions**.
  - The approach is **decentralized**.
  - There are **problems if some node forgets to release the token** (monopolizing the link).

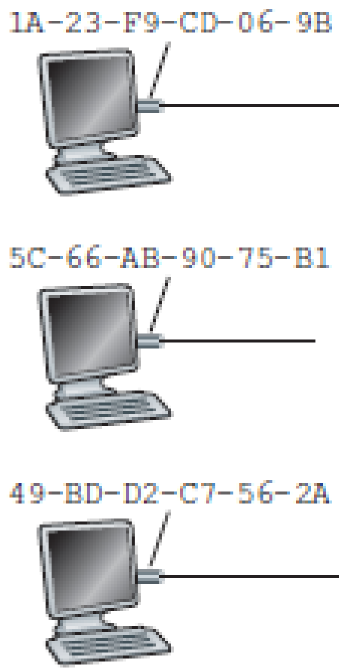
Link Layer
MAC Addresses

- At the link-layer, **devices are identified by MAC addresses**:
  - **Each network interface has a specific MAC address** (it was designed to be fixed but it can be changed).
  - **Each manufacturer has its own MAC.**

- The **MAC address** (or physical address) **is a link-layer address composed by 6 bytes** (2^48 possible addresses) often represented in hexadecimal notation:

  1A:23:F9:CD:06:9B or 1A-23-F9-CD-06-9B

- **MAC addresses are local** (while IPs are global):
  - All interfaces are associated to a MAC address, but this is only used inside a LAN.



Link Layer
MAC Addresses

- **In a LAN, 2 interfaces (A and B) communicate as follows:**
  - **A includes B's MAC address into the frame** and transmits it.
  - **B receives the frame and compares its own MAC with the destination MAC** of the frame.
  - **If the 2 MACs are equal, the frame is accepted**, otherwise the frame is rejected (the rest of the stack is not involved).

- There is also the possibility **to send broadcast messages** (that are accepted regardless of the MAC), for LANs that use 6-byte addresses (such as Ethernet and 802.11), **the broadcast address is a string of 48 consecutive 1s** (that is, FF-FF-FF-FF-FF-FF in hexadecimal notation).

- In a LAN it is quite possible (if not frequent) for an interface to receive frames directed to another interface, **the role of the MAC address is to filter out unintended frames** without disturbing the host.

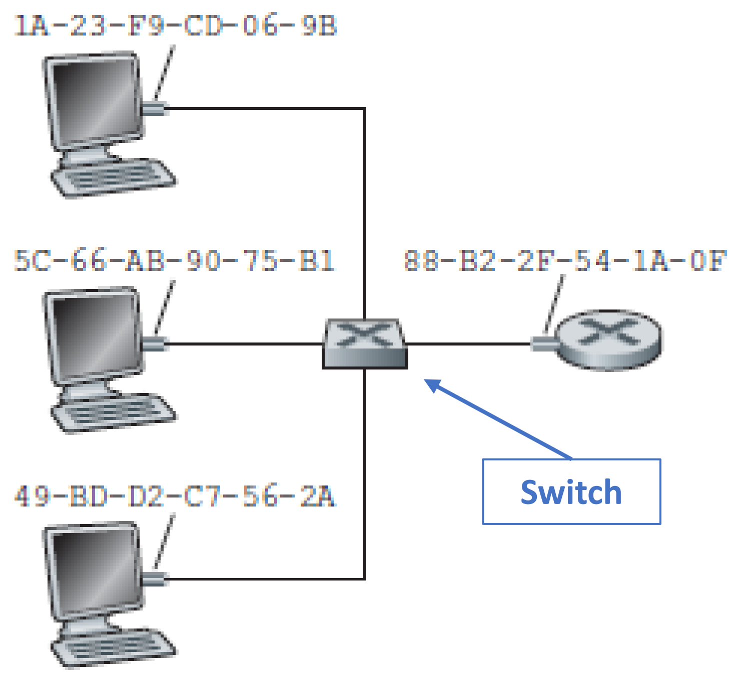
Link Layer

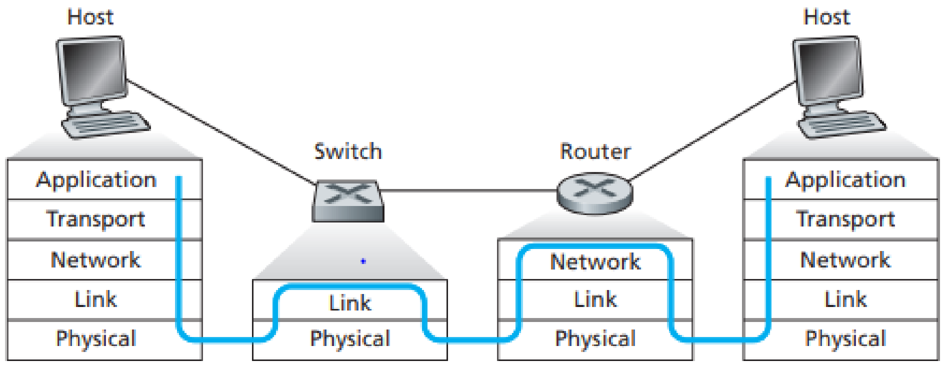
Switches

- **Switches are the link-layer equivalent of the routers**:
  - There is **no routing** algorithm implemented.
  - **Only MAC addresses are used**, the IP addresses are not considered.

- The role of the switch is to **receive incoming link-layer frames and forward them** onto outgoing links:
  - The **switch is transparent** to the hosts and routers in the subnet.
  - A switch also has **buffers on interfaces**.

- **Switches have forwarding tables** that associate MAC addresses to interfaces.
  - The **table is updated automatically and dynamically** (self-learning) as new devices are discovered.



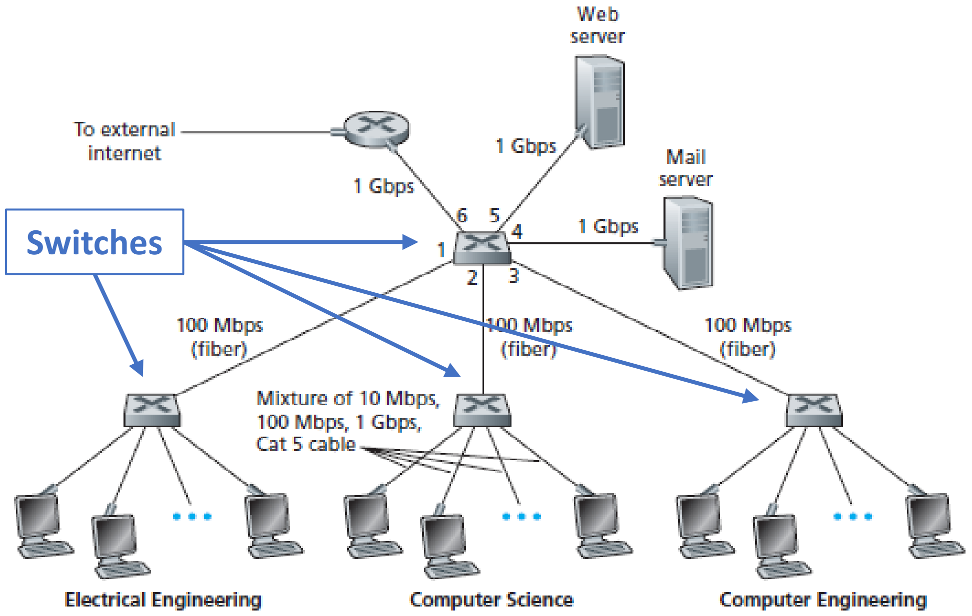


Link Layer
Switched LAN

- It is typical for **LANs to use one or more switches** connecting multiple local devices.

- Differently from routers, **switches are faster and plug-and-play**:
  - There is **no routing** algorithm involved.
  - **Only 2 layers** of the stack are considered.

- On the other hand, switched LANs are **limited in size** and must be **tree-structured**:
  - **MAC addresses are hard to group** (forwarding tables in switches may grow rapidly).
  - There is no routing, **loops are difficult to avoid**.



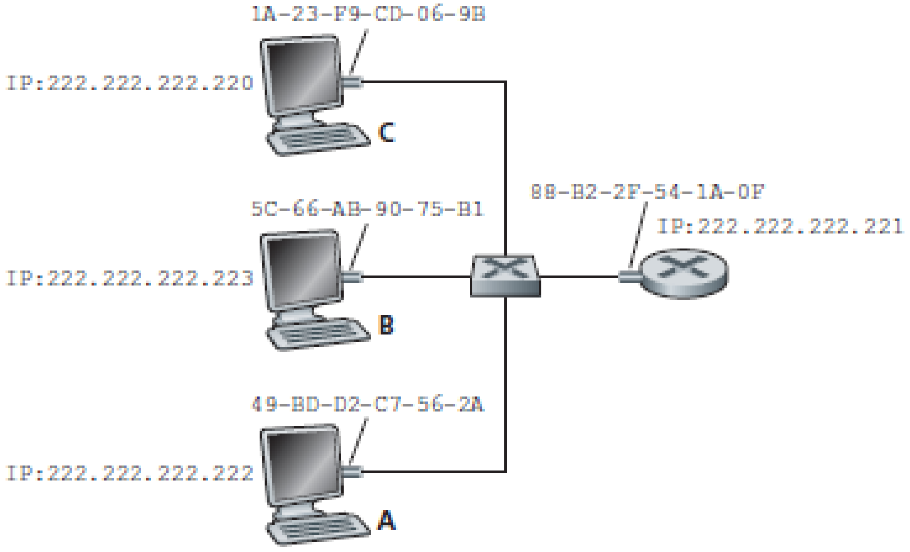
Link Layer
Address Resolution Protocol (ARP)

- Since upper-layer protocol works with IP addresses **we need to translate IP into MAC.**

- The **Address Resolution Protocol** (ARP) manages conversion between IP and MAC addresses.

- **Each interface is endowed with an ARP module having an ARP table** that associates each IP in the LAN to a MAC address **with a specific time to live** (TTL) value after which the entry is delated (typically 20 minutes).

- Since MAC addresses are local, also **ARP works only on local networks** (LANs).



IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

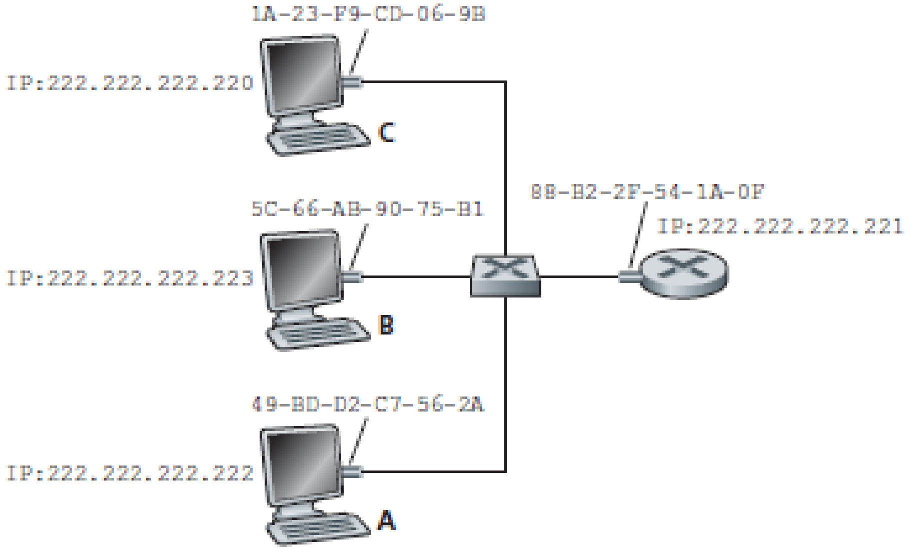
Link Layer

Address Resolution Protocol (ARP)

- Assume that **host C** (222.222.222.220) **wants to send messages to host A** (222.222.222.222). To do so, we need to know also the associated MAC.

- Before to send the message, if **A is not present into the table** an ARP packet is sent in **broadcast** to all devices of the network searching for the right IP.

- All nodes receive this packet but **only the searched IP** (222.222.222.222) **answers** with a direct message (not broadcast).



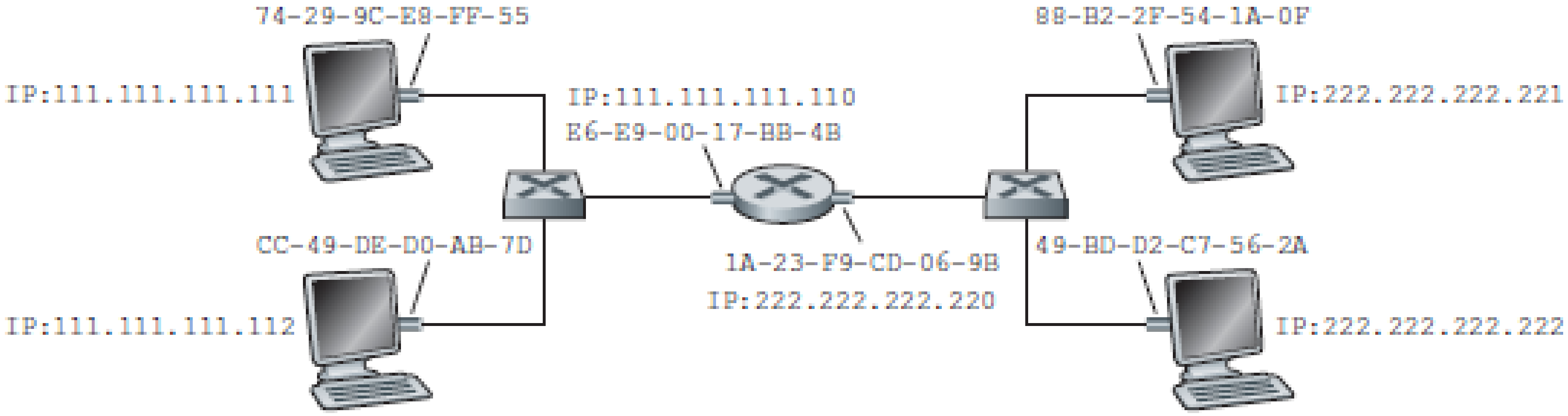
IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Link Layer
Address Resolution Protocol (ARP)

- What happens **if the IP is outside the network** (non-local)?

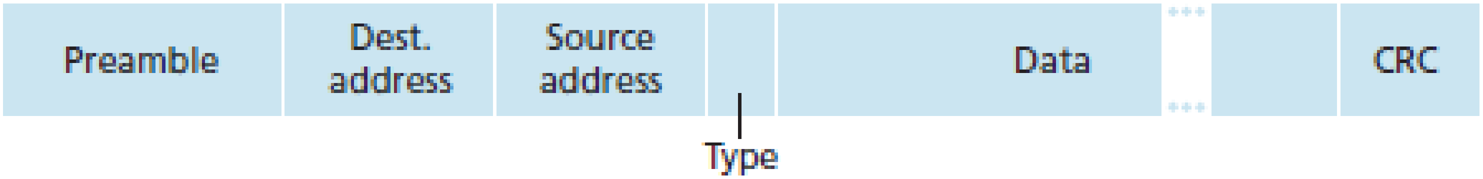
- The router connecting the 2 networks **must have at least 2 interfaces** (2 IP, MAC and ARP tables) each one inside the specific subnets.

- **Frames headed outside the subnet are sent to the first interface** of the router, moved to the second interface, **and headed toward the right host by using the second ARP table**.



Link Layer

Ethernet Frame



- **Ethernet** frame is composed by the following fields:
  - **Data field** (46 to 1500 bytes): **contains the IP datagram**. The maximum limit is given by the maximum transmission unit (MTU) of Ethernet, if datagram exceeds this size it is fragmented.
  - **Destination address** (6 bytes): contains **the MAC address of the destination** adapter.
  - **Source address** (6 bytes): contains the **MAC address of the source** adapter that transmits the frame onto the LAN.
  - **Type field** (2 bytes): specifies the **network-layer protocol** used for in this frame (there could be alternative to IP, for example, ARP packets have a specific type - 0x0806).
  - **CRC** (4 bytes): contains the **CRC number**.
  - **Preamble** (8 bytes): is a **“wake up” block of bits used to synchronize the clocks** of destination and source adapters.