Introduction to Local Area Networks

Fulvio Risso

Politecnico di Torino

A view from history (1)

- Wide Area Networks appeared first
  - ‘60s
  - A few mainframes; necessity to connect to them from remote
    - Partition their expensive cost between more entities
- Local Area Networks appeared later
  - End 70’s, beginning ‘80s
  - Minicomputers (and later PCs appeared)
  - Cost was fair enough so that was no longer the necessity to access a remote mainframe
    - Sharing resources between small workgroups (e.g., departments)

A view from history (2)

- At the beginning, WAN and LANs evolved independently
- Different protocols, engineered by different vendors for different purposes
  - Decnet, SNA, IP
  - Novell, Banyan Vineis, NetBeui
- Later we tried to connect LAN to to WANs
  - Progressive overlapping of functions/protocols
  - One winner: IP
    - Some overlaps still remain (e.g., addressing)

Why were LANs different from WANs? (1)

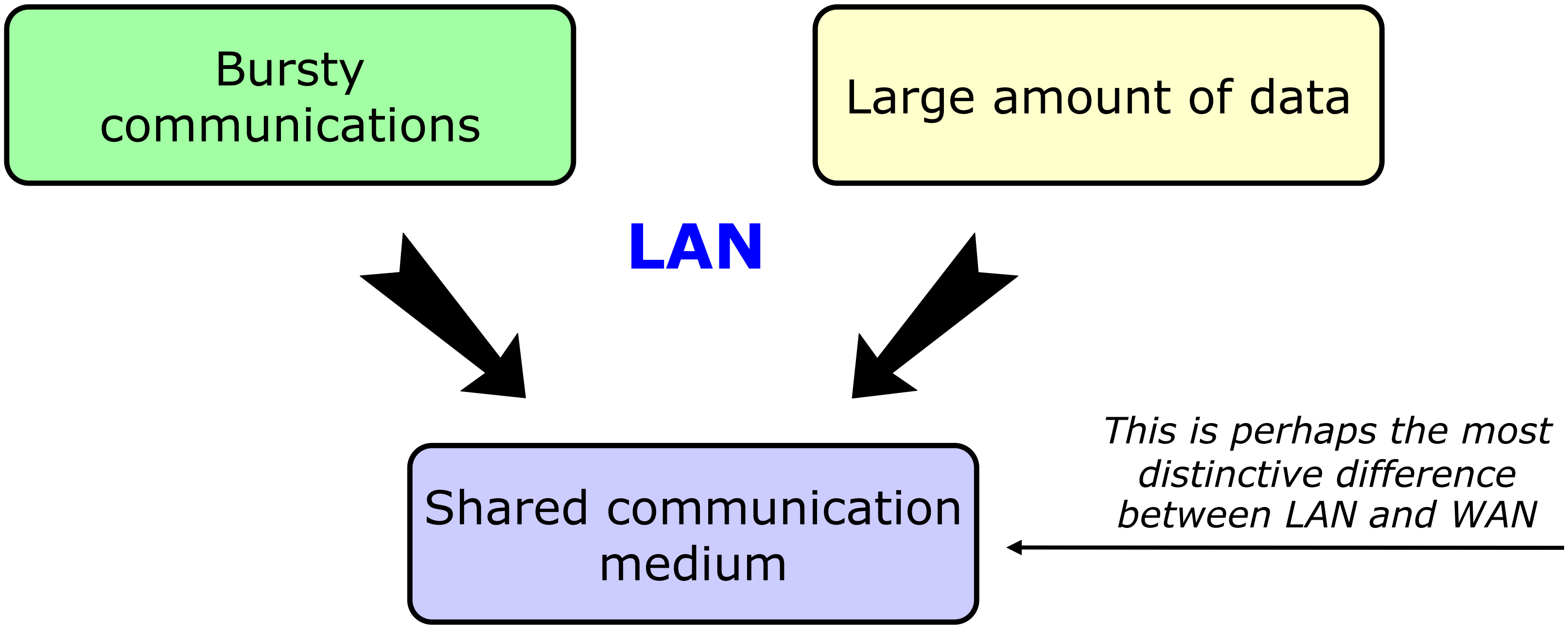
- Ownership of the physical medium
  - LAN: the network admin **owns** the cable
  - WAN: the network admin **leases** the cable
- Quality and speed of the communication medium
  - LAN: small distance, affordable communication, high speed
  - WAN: long distance, faulty cables, low speed
- Cost
  - LAN: reasonable cost, concentrated mainly when setting up the network
  - WAN: high cost, also in terms of operating costs
- Those differences triggered very different usage patterns on LANs and WANs

Why were LANs different from WANs? (2)

- Different usage pattern (at the beginning)
- LAN
  - Large amount of bandwidth, for short time
    - Data concentrated on small time intervals (*bursts*)
  - Data transmitted only locally
    - E.g., file and printer sharing
  - Short transfers not so expensive (e.g., advertisement/solicitation packets)
- WAN
  - Small amount of bandwidth, but for long time
    - E.g., phone call, telnet, email,
  - Smoother usage patterns (not bursty)

Why were LANs different from WANs? (3)

- Different usage patterns called for different engineering choices
  - Telephone switches that allowed several users to talk together
  - (vs) shared medium, in which only one entity can talk at a time



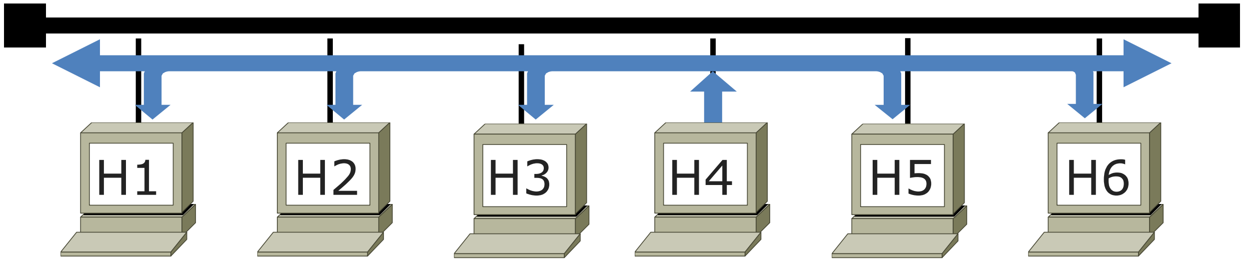
Shared communication medium: advantages

- Intermediate switching system not required
  - Cost
  - Higher speed (historic)
  - Flexibility (add/remove stations)
  - Reliability
    - No intermediate system, so no faults there

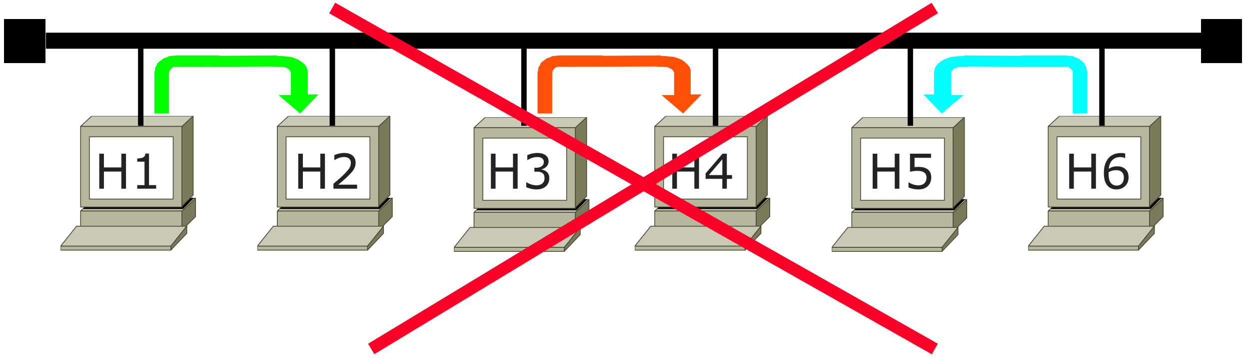
- Shared communication medium → broadcast communication
  - Easy broadcast/multicast
  - Simpler communication paradigm
    - Can use “solicitation” and ”advertisement”

Shared communication medium: problems

- Privacy

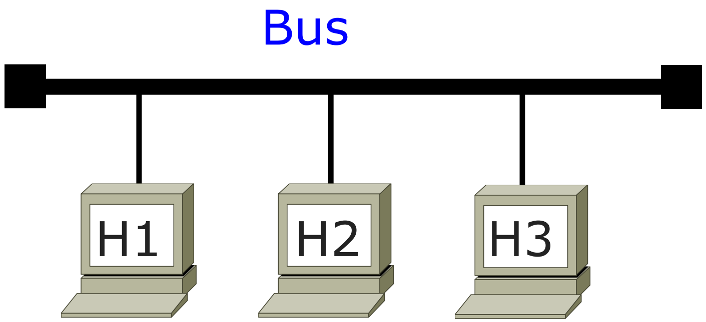


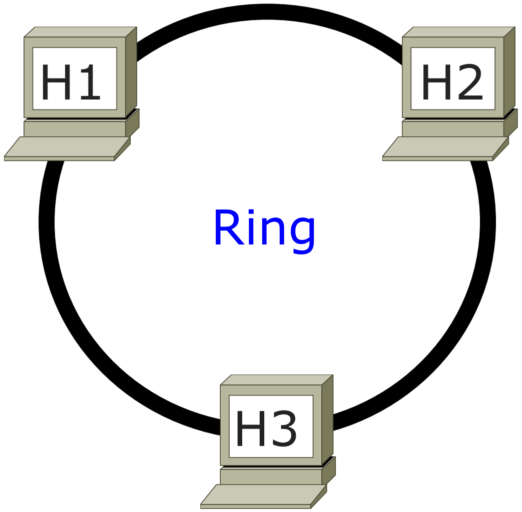
- One communication at a time



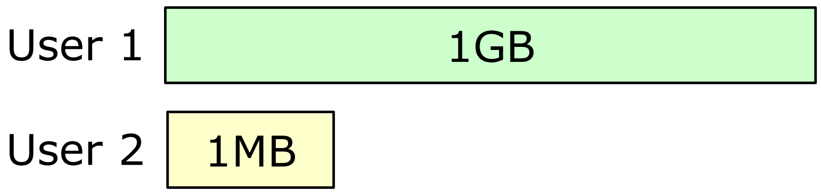
Implementing a shared communication medium

- Different possible implementations
  - Physical broadcast
    - Broadcast-based technologies (e.g. bus)
  - Logical broadcast
    - Point-to-point technologies (e.g. ring)
- Addressing required
  - (More retails later)

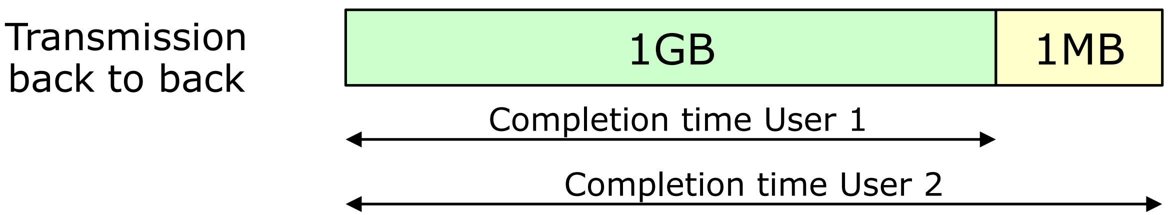




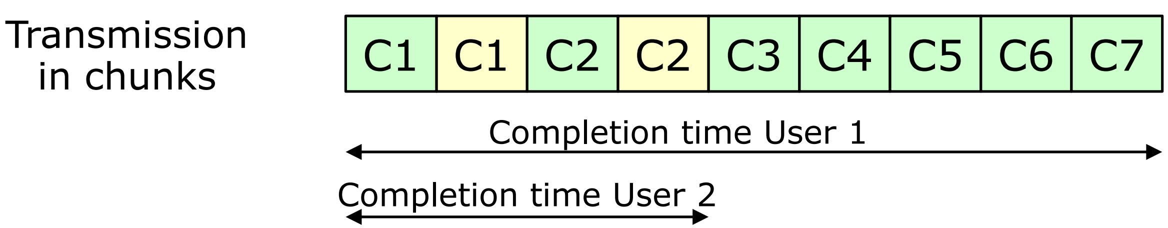
Handling multiple (long) data transfers (1)



Two users have to transfer some data on the network
User 1 begins the transmission first



User experience for User 2 can be rather disappointing



User experience for User 1 does not change that much, while it greatly improves for User 2

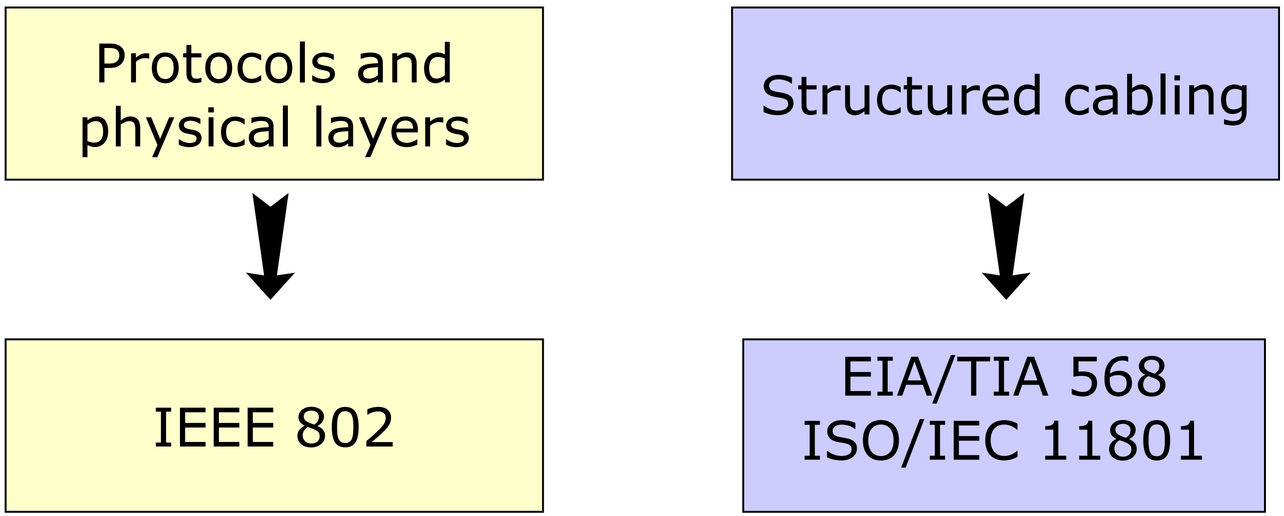
Handling multiple (long) data transfers (2)

- A shared communication medium cannot support multiple transmission at once
- This may hurt users when somebody else takes the ownership of the channel for too long
- Solution
  - Define a maximum transmission unit (i.e., *chunk*)
  - Split user-level data into multiple chunks of (max) that size
  - Release the channel after transmitting that amount of data
    - Offers to other stations the possibility to send data
  - If chunks are small enough, users have the perception of contemporary transmissions
    - Technically this is false, as only one entity can use the channel
    - E.g., 10Mbps network, 1000 bytes max: 0.8ms per chunk

LAN (Local Area Network)

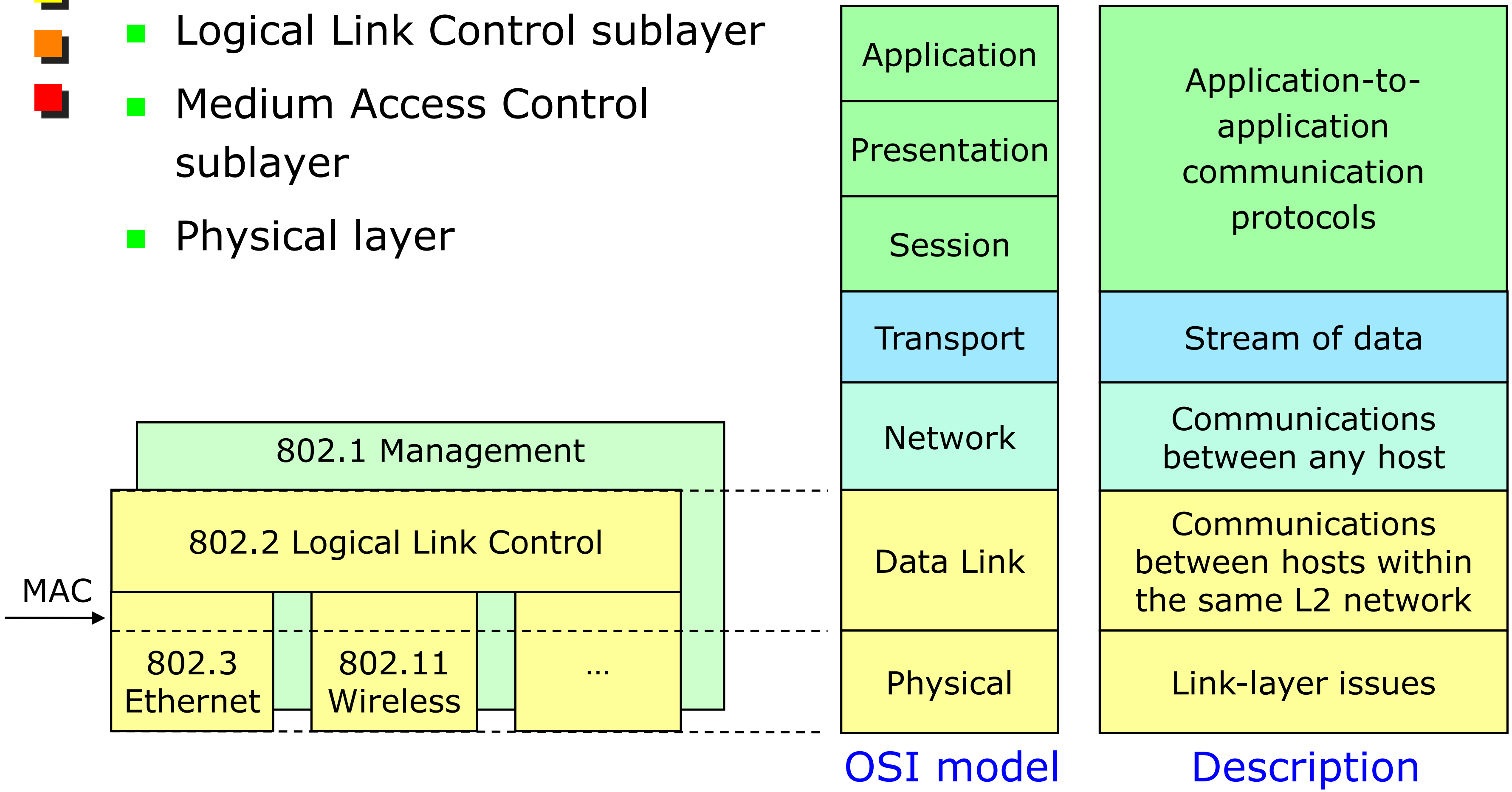
- Definition IEEE 802
  - Communication system through a shared media, which allows independent devices to communicate together within a limited area, using an high speed and reliable communication channel
- Keywords
  - Shared media
  - Independent devices (no *privileged* devices here)
  - Limited diameter (Km), on private area/campus (no *public soil* crossing)
  - High speed (> 100Mbps)
  - Reliable
- Standards IEEE (not ITU)
  - Delegated by ISO for layer 1 and 2

LAN important standards



LANs: IEEE and OSI models

- 802.1: Higher Layers and Management
- Logical Link Control sublayer
- Medium Access Control sublayer
- Physical layer



Most important problems on LANs

- The most important problems we have to solve on LANs are the following
  - Cabling
    - In order to guarantee interoperability
  - Medium access control
    - Specific for each technology
  - How to make a “shared communication medium”
  - Who is the sender/receiver of the frame
  - Which is the L3 protocol involved
  - Error control (FCS)
- Following slides will show how and in which component those problems are solved

Layer 1: Physical

- Transmission of binary sequences on the communication channel
  - Defines a way to send a stream of bytes
- Link: physical medium between two devices
  - At this level, we do not care if the link is point-to-point or broadcast
- Specification of
  - Voltage (for 0/1 symbols), type of modulation
  - Type, size, impedance of physical links
  - Connectors
- Domain of electrical/electronic engineering

Some physical layers

- Ethernet (IEEE 802.3)
- Token Ring (IEEE 802.5)
- WiFi (IEEE 802.11)
- FDDI (ISO 9314)
- Bluetooth (IEEE 802.15.1)
- ZigBee (IEEE 802.15.4)
- …

- Mostly no longer in use
- Warning: those specs include not only physical layer, but also the data-link layer

Layer 2: Data Link

- (Reliable) Transmission of frames on a single *logical* link
  - Interface from/to L3: set of frames
  - Interface from/to L1: stream of bytes
- Logical Link
  - Usually is a physical link
  - It can be a mixture of different physical links provided that the entire system is still a *shared communication medium*
  - Difference between *logical* and *physical* links will be more clear in the following
    - E.g., bridges

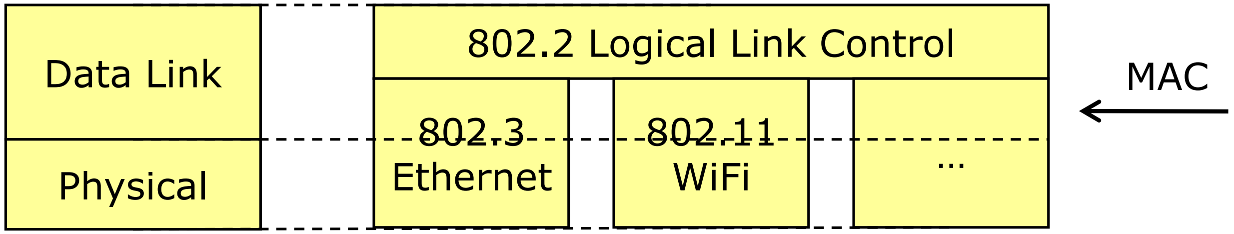
Data Link: main functions

- Error control (→ FCS)
- Error recovery (optional) through retransmission
- L3 protocol ID (→ “protocol type”)
- L2 addressing (→ MAC address)

- In order to achieve the above functionalities, the data-link layer is split in two portions
  - MAC
  - LLC

Data-Link Sublayers

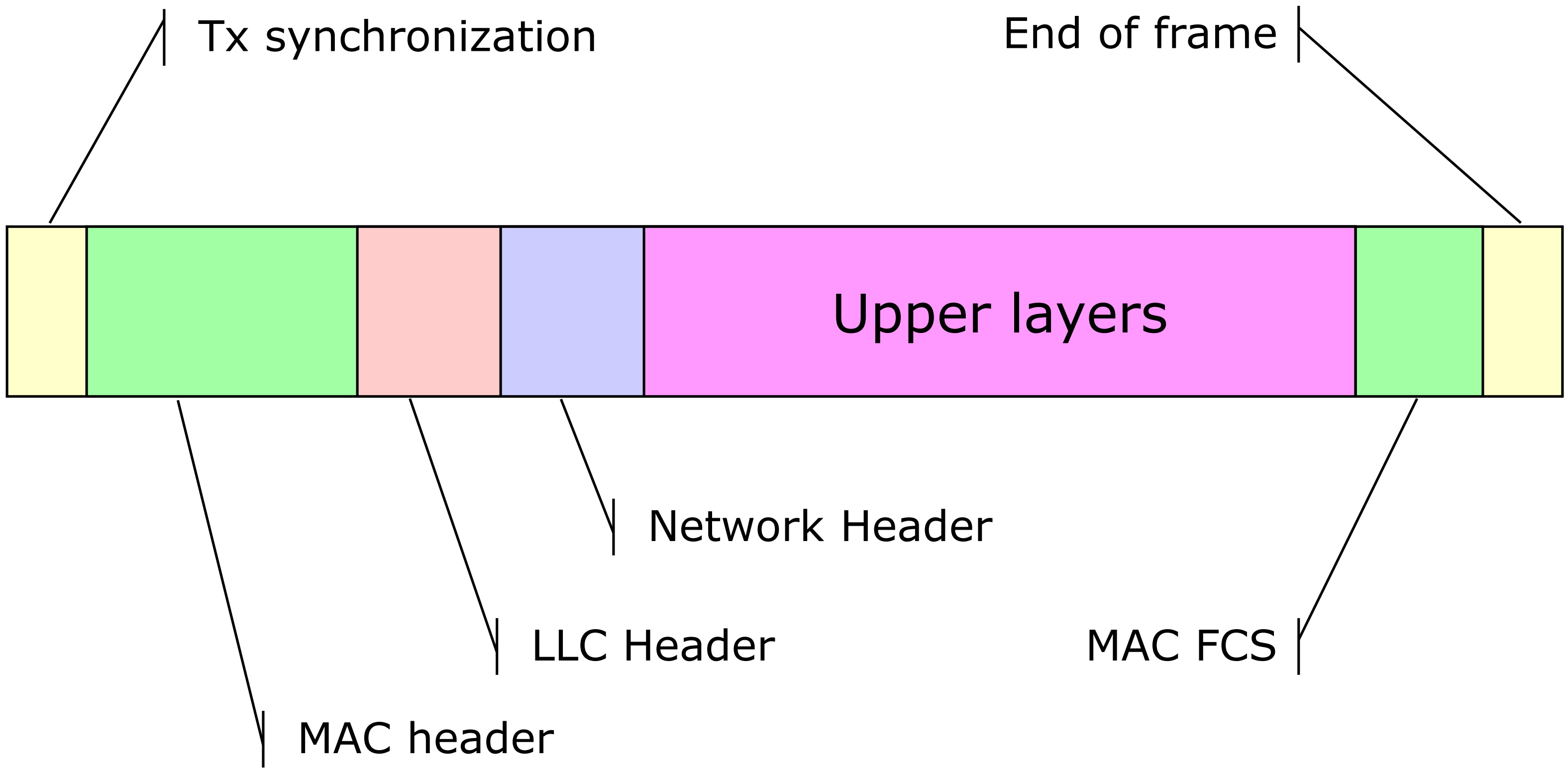
- LLC: Logical Link Control
  - Common in all LAN technologies
  - Defines the interface toward L3
  - Specified in IEEE 802.2
- MAC: Media Access Control
  - Specific for each technology
    - CSMA/CD, Token-based, etc.
  - Arbitrates the access to the physical medium
    - Other physical-related functions are in the Physical Layer



Data Link Sublayers: the MAC sublayer

- Implements the shared communication medium
  - Broadcast transmission either through a shared medium or through a proper emulation (e.g., ring)
  - Each station receives all the frames sent by all the other stations on the same link
- Problem to be solved:
  - Which station can take ownership of the channel?
  - Who is the sender/receiver of the frame
    - In principle, an LLC problem, but solved at MAC layer
- Supposes an “affordable” transmission
  - No error correction (at MAC level)
  - Connectionless (at MAC level)

A typical LAN frame

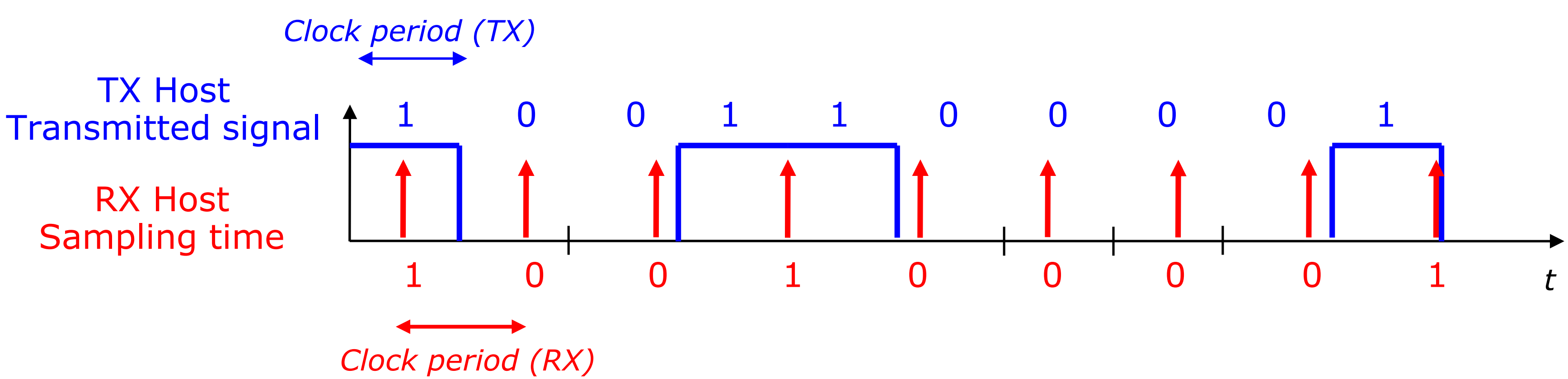


Note:

- "End of Frame" may not be present (e.g. in case another mechanism is available for defining the end of the frame)
- "frame" is the data at data-link level (e.g., no sync), "packet" is the data at L3

The reason for synchronization sequences

- Necessity to sync TX and RX clocks
  - Otherwise, data read is not correct
- Sync sequences at the beginning of the transmission
  - Needed when channel is kept idle during non-transmission time
- Often, self-synchronizing codes at the physical layer
  - E.g., Manchester is preferred to simpler coding (e.g., NRZ), although it consumes more bandwidth (in frequency)



MAC Header

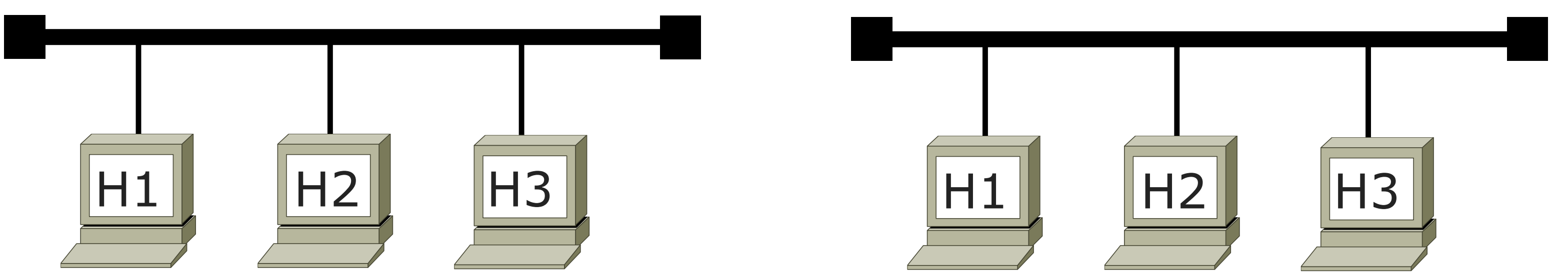
- Source/destination address
  - Unique ID
  - Destination address goes first
- Length of the LLC PDU
- LLC-PDU (LLC + network + … data)
- FCS (Frame Control Sequence): 32 bit CRC for integrity control (over the entire frame)

Destination address	Source address	Length	LLC PDU	FCS

MAC addresses: introduction

- Who is the sender/receiver of a frame?
- The address must be unique within the LAN (not in the world)
  - When H1 on the left receives a frame from an host named H2, there are no doubts about who is the sender of that frame
- In practice, this is not very convenient
  - Network manager has to keep track of the IDs already used on the LAN, and assign (manually?) unused IDs to new stations

Destination address	Source address	Length	LLC PDU	FCS



MAC addresses: structure

- A funny proposal: the serial number of an US dollar banknote
- Assigned by IEEE
  - 6 bytes (i.e. 48 bits)
  - Written as a set of 6 hex numbers
- 2 portions, 3 bytes each:
  - Vendor code or OUI (Organization Unique Identifier)
    - Can be stored in a database (e.g. network sniffer)
  - Progressive number, assigned by the manufacturer

000010000000000000101011001111000000011110011010

0	8	0	0	2	B	3	C	0	7	9	A

Vendor code (assigned by IEEE) NIC ID (assigned by the manufacturer)

08-00-2B-3C-07-9A

MAC addresses: some OUIs

Organization	Address Block
Cisco	00-00-0C
Broadcom	00-1C-23
IBM	08-00-5A
Sun	08-00-20

MAC addresses types

- Two orthogonal categories
  - Local vs. global identifier
  - Identifier of a single station vs. group-based identifier

- MAC address are not only for single stations
  - In fact, three types of addresses have been defined
    - Unicast (i.e., Individual)
    - Multicast (i.e., Group)
    - Broadcast (i.e., Group, FF-FF-FF-FF-FF-FF)

MAC addresses: multicast and broadcast

- Multicast/Broadcast addresses
  - Often used for solicitation/advertisement

- Solicitation
  - A station that has to perform a service discovery can send a multicast/broadcast packet
  - The station in charge of the service can answer to the question
- Advertisement
  - A station that provides a service can advertise its capabilities to all the other stations through a multicast / broadcast packet

MAC addresses: I/G and U/L

- First two bits transmitted on the channel
  - First bit: I/G (Individual/Group) (Individual = 0)
    - Individual= assigned to a single station
  - Second bit: U/L (Universal/Local) (Universal = 0)
    - Universal= univocally assigned (no duplication exists)
- Problems may happen due to byte ordering
  - 802.3: least significant bits of the first byte transmitted first
  - 802.5: most significant bits of the first byte transmitted first

0	2	0	0	2	B	3	C	0	7	9	A

0000 0010

802.3: this MAC address is Individual / Local (I, L)

802.5: this MAC address is Individual / Universal (I, U)

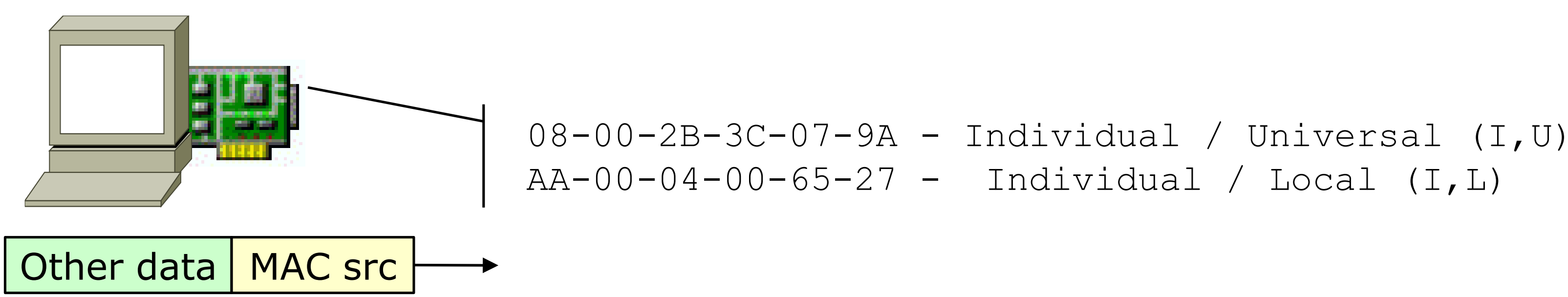
MAC addresses: examples

- Written in Canonical Order (i.e., network byte order)
  - Equivalent to the Native Order in 802.3
  - Bits are written from left to right in 802.5
    - E.g., bytes have to be re-arranged when reading data from the network and printing it on screen

Canonical order	Type	Native order (802.3)	Native order (802.5)
08-00-2B-2C-56-FE	Individual / Universal	08-00-2B-2C-56-FE	10-00-D4-3C-6A-7F
01-00-E5-7F-00-02	Group / Universal	01-00-E5-7F-00-02	80-00-7A-FE-00-40
AA-00-04-00-65-27	Individual / Local	AA-00-04-00-65-27	55-00-20-00-A6-E4
03-00-00-20-00-00	Group / Local	03-00-00-20-00-00	C0-00-00-04-00-00
FF-FF-FF-FF-FF-FF	Group / Local (broadcast)	FF-FF-FF-FF-FF-FF	FF-FF-FF-FF-FF-FF

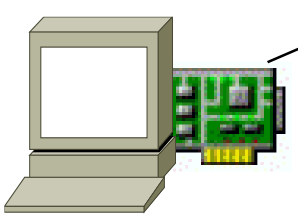
Source MAC addresses

- Source MAC address is always a unicast address
  - Often the MAC address of the Network Interface Card (NIC)
  - Other MAC addresses can be configured at run-time
- A NIC may have several MAC addresses dynamically configured on it
  - One "global" (always present), the other are "local" (dynamic)
- NIC cards have
  - A ROM that keep the global address
  - A special volatile memory to store all the other bindings



Destination MAC addresses

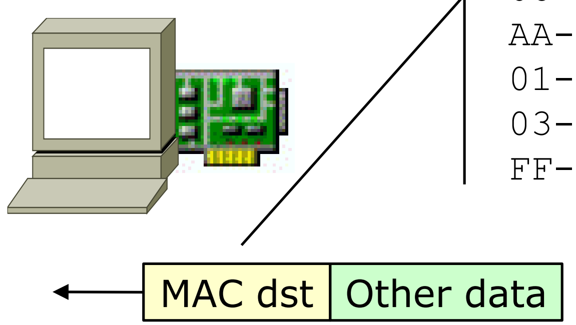
- Destination MAC address can be
  - Any of the unicast addresses configured on the NIC
  - Multicast, broadcast
- NICs may have several MAC addresses dynamically configured on them
  - Some always available
    - The individual/universal
    - The broadcast address (FF-FF-FF-FF-FF-FF)
  - Other configured on the flight (kept in a volatile RAM)



```
08-00-2B-3C-07-9A - Individual / Universal (I/U)
AA-00-04-00-65-27 - Individual / Local (I/L)
01-00-E5-7F-00-02 - Group / Universal (G/U)
03-00-00-20-00-00 - Group / Local (G/L)
FF-FF-FF-FF-FF-FF - Group / Local (G/L)
```

Receiving a MAC frame (1)

- When a packet is received by the NIC
  - It is forwarded to the upper-layer software (e.g. Operating System) only if the NIC has been configured to do so with that address




```
08-00-2B-3C-07-9A - Individual / Universal (I/U)
AA-00-04-00-65-27 - Individual / Local (I/L)
01-00-E5-7F-00-02 - Group / Universal (G/U)
03-00-00-20-00-00 - Group / Local (G/L)
FF-FF-FF-FF-FF-FF - Group / Local (G/L)
```

Receiving a MAC frame (2)

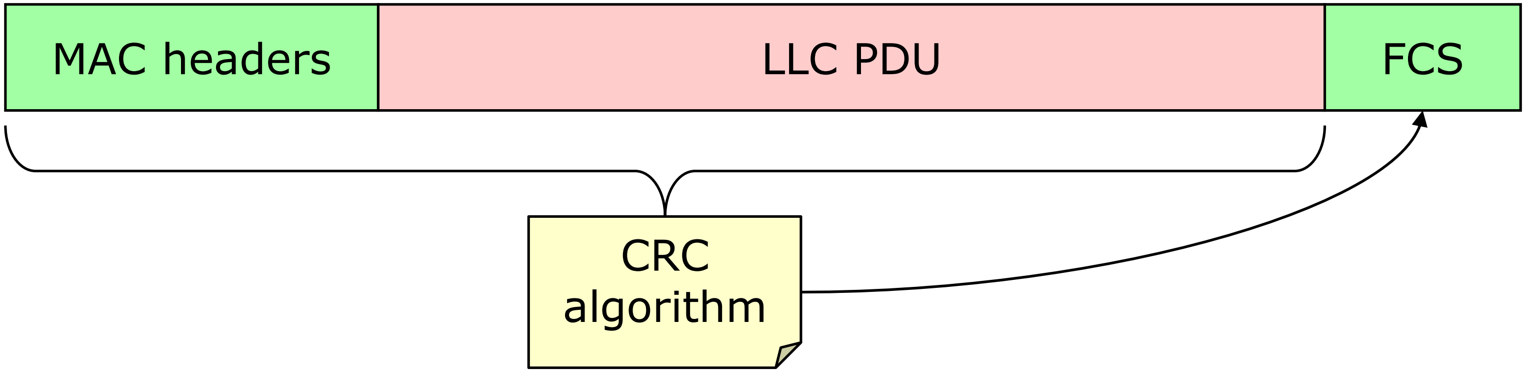
- In other words:
  - Broadcast: always forwarded to the OS
  - Unicast: only if the destination MAC address is equal to the HW MAC address or to another one present into the proper memory area
  - Multicast: if the MAC address is present into the proper memory area
- Important: all packets are received at the physical layer, while upper layers usually receive only a subset of them
  - Packets are usually filtered in hardware by the NIC

Receiving a MAC frame (3)

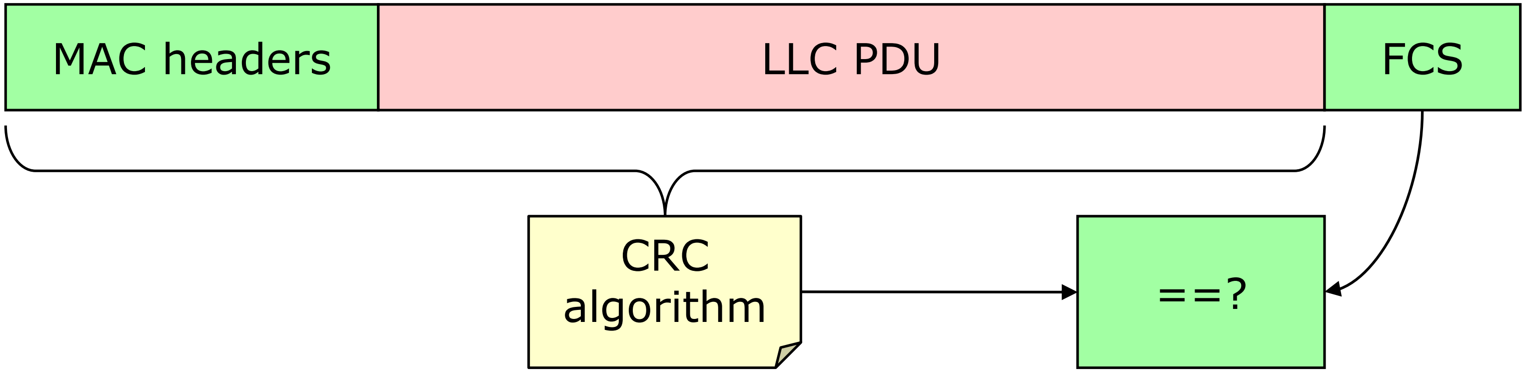
- Special case: NIC in "*promiscuous mode*"
  - The NIC-based filtering is disabled
  - All packets are forwarded to the OS
  - The OS has to decide if packets have to be kept or not
- Promiscuous mode almost useless on modern (switched) networks
  - It will more clear when "switched networks" will be introduced

Frame Control Sequence (1)

Frame sender



Frame receiver

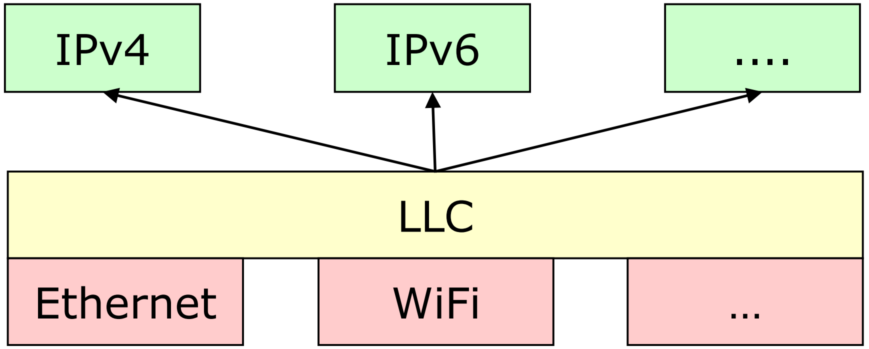


Frame Control Sequence (2)

- A frame with wrong FCS is discarded by the receiver
- No way to inform the sender that the transmission went wrong
  - MAC sublayer is connection-less
  - Very unlikely, though, given the “reliable” property of LANs
- Often due to collisions on Ethernet
  - Those frames are automatically retransmitted by the sender
- How to recover from a wrong frame?
  - Someone will do (e.g., TCP will detect a missing packet in the stream)

The LLC sublayer (1)

- MAC-independent
- In principle, just a L3 protocol demultiplexing is needed
  - This is what Ethernet DIX did
- What about if we need some additional functions?
  - This is what IEEE did
  - E.g., connection-oriented primitives?
  - But exactly, which primitives may be needed?
  - Uhm… let’s take some ideas from HDLC



The LLC sublayer (2)

- HDLC
  - Used to connect terminals to mainframes, back in the ’70
  - Defined by IBM for serial lines
  - Provided several features
    - Address terminals
    - Flow control
    - Connected services
- LLC derives from HDLC and provides two functions:
  - Defines three types of service
    - *Type 1:* Unacknowledged connectionless service
    - *Type 2:* Connection Oriented service
    - *Type 3:* Semireliable service
  - Defines addresses for L3 protocol demultiplexing

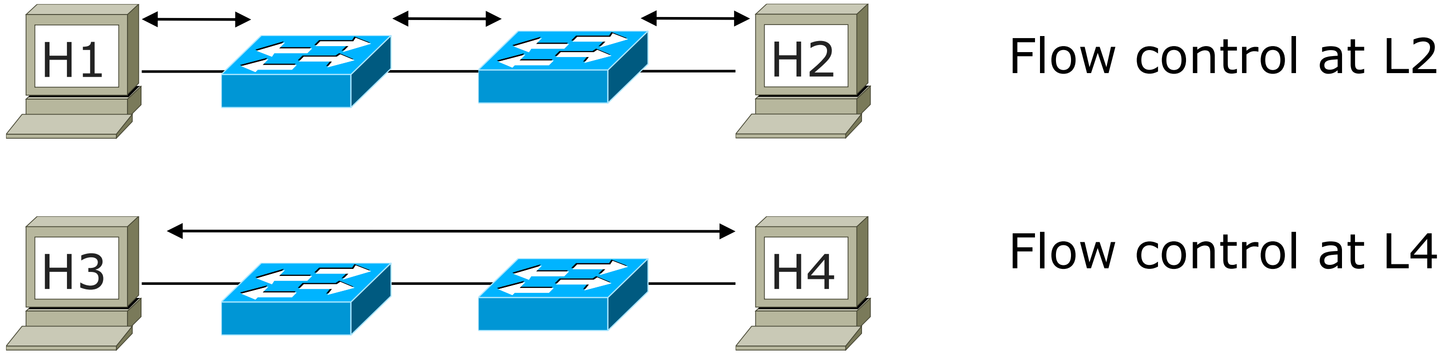
Is LLC useful in modern LANs? (1)

- First, LLC resulted in having several flaws
  - Small addresses, etc (presented later)

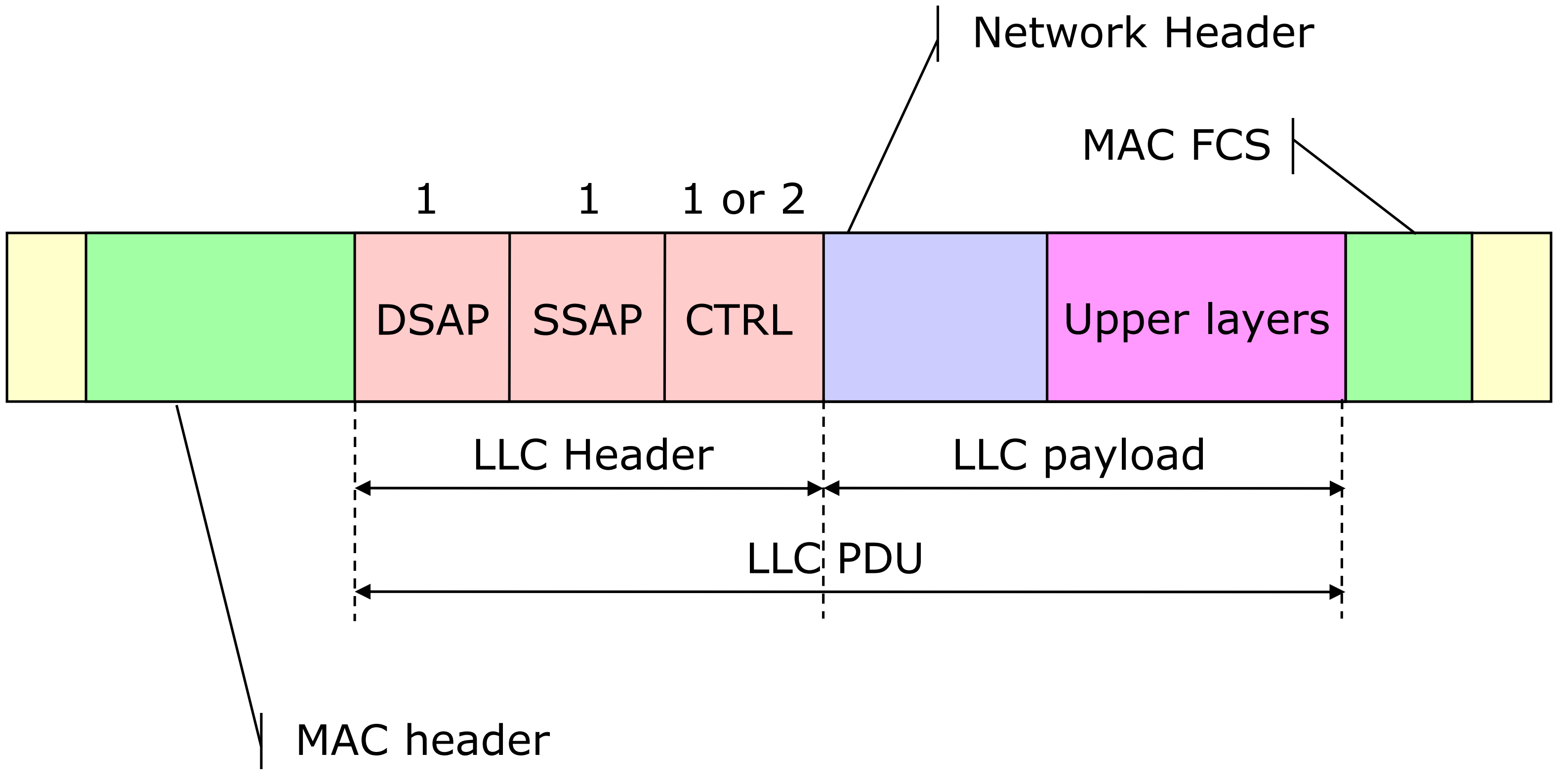
- Second, those features resulted useless in modern LANs
  - IEEE decided to integrate LLC in the LAN model, in order not to close the door to someone that would like to use some of these features in the future
  - But… original Ethernet designers were right when they choose not to provide advanced services at data-link layer

Is LLC useful in modern LANs? (2)

- In practice, sometimes LLC is even not present…
  - E.g., Ethernet DIX avoided LLC at all, although the IEEE version supports LLC (but nobody uses it)
- … and when is there, most of the features are disabled
  - E.g. WiFi
- No need for those features in current networks
  - E.g., flow control currently done at L4
  - Intermediate devices are simpler (hence faster and cheaper)



LLC PDU



Network Header
MAC FCS
1
1
1 or 2
DSAP
SSAP
CTRL
Upper layers
LLC Header
LLC payload
LLC PDU
MAC header

LLC Control

- Equal to the same field of HDLC
- Three types of formats for 3 types of LLC-PDUs
  - Information
  - Supervisor
  - Unnumbered
- Allows LLC to operate connectionless or connection-oriented
- Can be 1 o 2 bytes
  - 2 bytes only in connection-oriented mode, with extended numbering
- Not really used
  - Usually equal to 0x03 (Unnumbered Information)

LLC SAP

- Service Access Point (i.e. LLC addresses)
  - DSAP
    - 1 bit Individual / Group (Individual = 0)
    - 7 bits address
  - SSAP
    - 1 bit Command/Response (Command = 0)
    - 7 bits address (always Individual address)
- Some examples
  - 0xFE: ISO 8473
  - 0x42: IEEE 802.1D Spanning Tree
  - 0xAA: LLC SNAP
  - 0xFF: broadcast

Some problems of LLC SAPs

- Limited number of values
  - Only 128, but originally just 64
- SAP assigned by ISO
  - Only to protocols published by an internationally recognized standards organization
  - What about protocols defined by other bodies or pushed by some vendors?
    - Es: IP, NetBEUI, IPX
  - We need an additional framing (LLC SNAP)
- SSAP and DSAP: no reasons for having two fields
  - How can two different protocols A and B talk together?
- A departure from other existing (and successfully working) standards (e.g. Ethernet)

LLC SNAP PDU

- Subnetwork Access Protocol (SNAP)
  - For protocols that do not have a standard SAP
  - SSAP and DSAP equal to 0xAA
  - Additional header, 5-bytes long, called Protocol Identifier
    - OUI: organization that defined the protocol
    - Protocol Type: protocol identifier
  - If OUI == 00-00-00, protocol type is the value used in Ethernet DIX
    - 0x0800 → IP
    - 0x0806 → ARP

DSAP	SSAP	CTRL	Protocol Identifier		Payload
0xAA	0xAA	0x03	OUI e.g. 0x000000	Protocol Type 0x0800	
			3 bytes	2 bytes	

LLC and protocol demultiplexing (1)

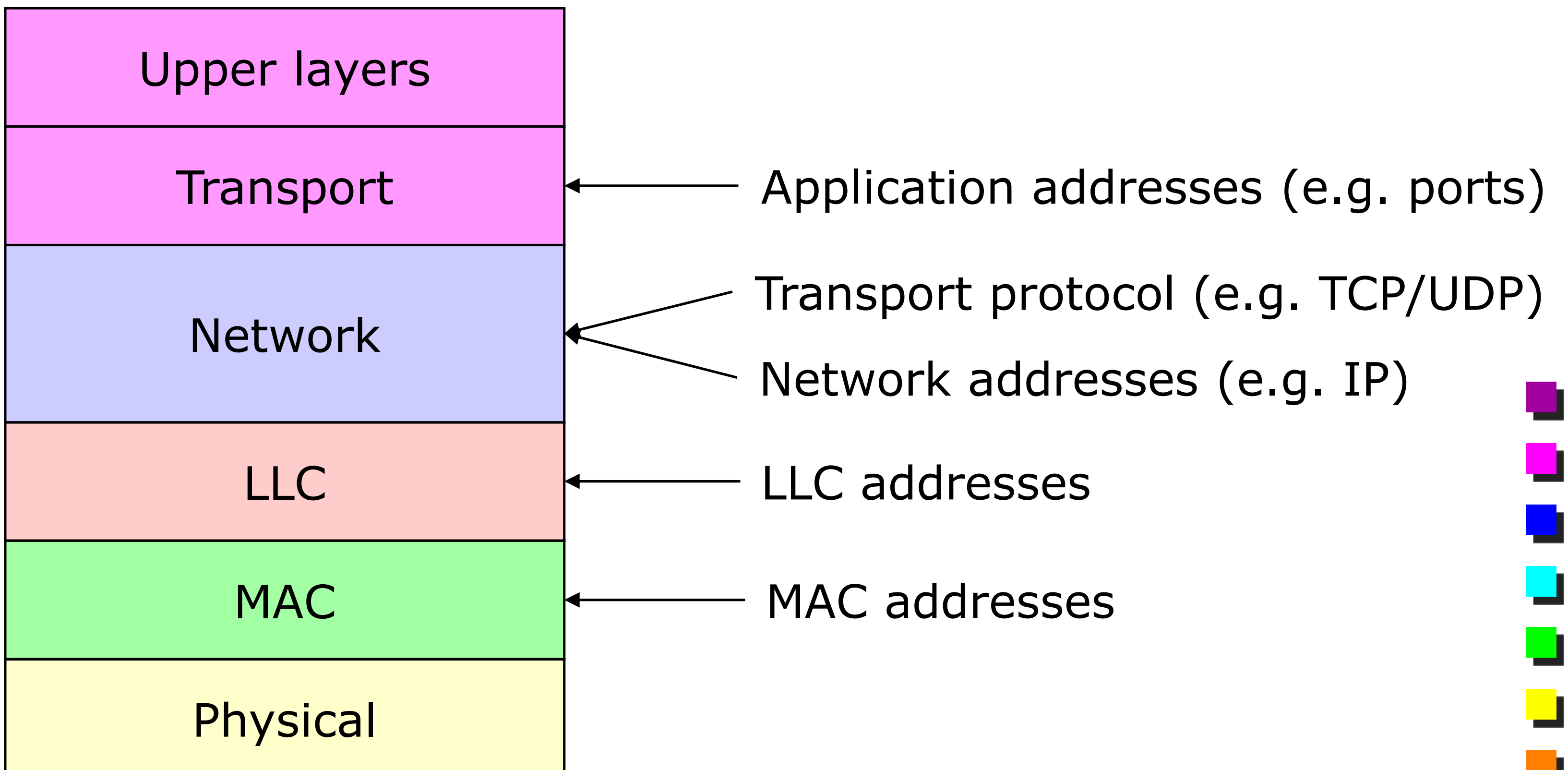
- All the LANs (e.g. 802.11 WiFi) use LLC
  - Most L3 protocols use LLC SNAP with OUI = 00-00-00
    - With LLC SNAP, 6 bytes are "useless" (AA-AA-03-00-00-00)
  - Only a few use LLC SAP
- Ethernet is an exception
  - Its specification is precedent to IEEE standards
  - The "protocol demultiplexing" function is included in the MAC frame
  - Most protocols working on the Ethernet keep the old format
  - Need for coexistence
- In theory, two hosts on the same Ethernet LAN, one using LLC and the other not, will have MTU problems
  - E.g. 1492 vs. 1500 bytes

LLC and protocol demultiplexing (2)

- LLC and IP
  - IEEE added a code for IP in LLC
    - SSAP/DSAP = 0x06
  - Never used
    - There is no SSAP/DSAP for ARP, so how I need to use LLC SNAP anyway

Addressing in nowadays networks

- Many different addresses, usually with different purposes
- Some overlapping between MAC and Network addresses



IEEE 802.1 (Higher Layers and Management)

- IEEE 802.1: general specification of the entire IEEE 802 project
- Includes several parts
  - 802.1 Part A: Overview and Architecture
  - 802.1 Part B: Addressing Internetworking and Network Management
  - 802.1 Part D: MAC Bridges

Conclusions

- LAN: network that spans across a limited area
  - Fast
  - Reliable
  - Cheap
- Guarantees the communication between two entities connected to the same physical link
- Includes
  - Physical specifications
  - Data-link
    - Medium Access Control sublayer
    - Logical Link Control sublayer