ELEC-H410
REAL-TIME SYSTEMS

Chapter 11

Networks basics

Networks

CONTENTS

- **networks in industrial processes. Why ?**
- classification
- architecture

Networks in industrial processes

the revolution of cheap processors

- share tasks
  - sensors, actuators, controllers become "smart"
  - simpler tasks, easier development
- reliability of the data
  - digital transmissions better than analog
  - self-tests
  - filtering
- reduction in wiring
- abolish distances
  - office, workshop, factory, world are almost the same
  - SCADA via Internet => remote control
- transparency

Networks can be a real benefit for industrial applications:

- the remarkable performance/price ratio of microprocessors enables an important decentralisation of the tasks related to a process. **Sensors, actuators, controllers become digital and "smart"** , and a network is of course the natural way to interconnect them

- digital devices can **increase the quality** of the processes because they can do operations like self-tests, preprocessing of data, noise cancelling, and digital transmissions which allow powerful data checks

- a **significant reduction in wiring**: lot of industrial processes with analog point-to-point links require **thousands** of cables

- managing industrial processes is often called SCADA (Supervision, Control and Data Acquisition). With the help of networks, this control can be done locally in the workshop, but also remotely without (almost) any geographical barriers

- transparency: a machine that you access via the network must behave like a local machine. A traditional example is the creation of a file system through the network (Network File System): we can "mount" a portion of hard disk of a distant machine in our own tree structure as if it were physically present on our local disc.

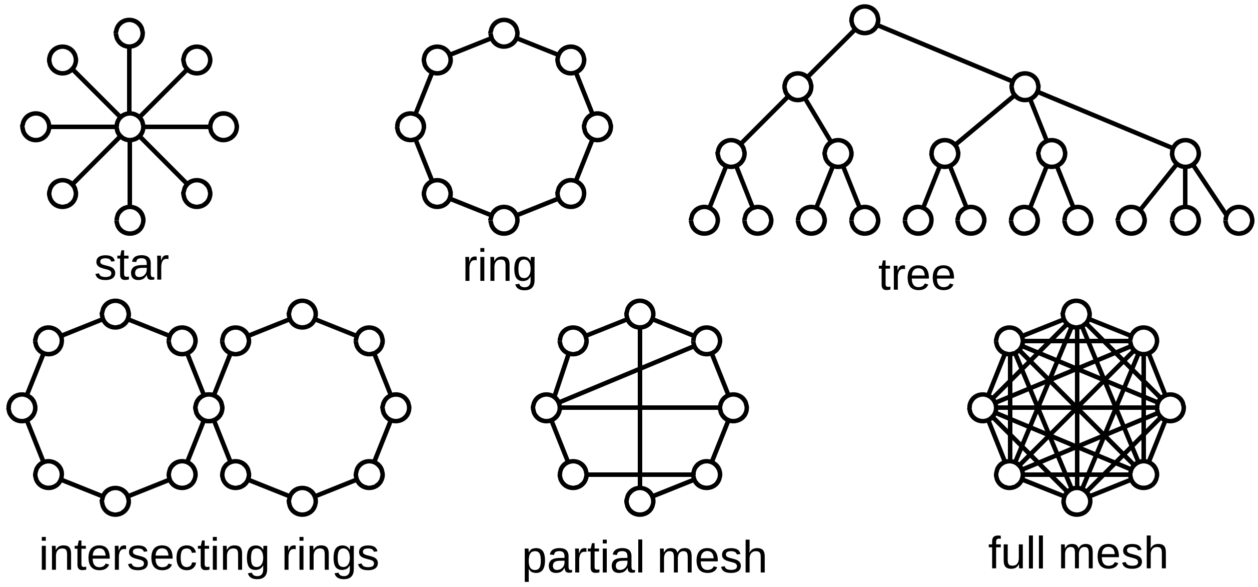
Networks

CONTENTS

- objectives
- **classification**
  - **on topologie**
  - **on distance**
  - **on hierarchy**
  - **with / without connection**
- architecture

Classification on topology: point-to-point

data follows a chain of successive emission-receptions



The first classification of the networks can be done on the **wiring topology** and on how a message is conveyed from one node to another.

In point-to-point networks, each node sees only one interlocutor on each network segment to which it is connected. Information must thus be forwarded by a chain of successive emissions/receptions. Transit nodes are not interested in the information and just propagate it in the proper direction.

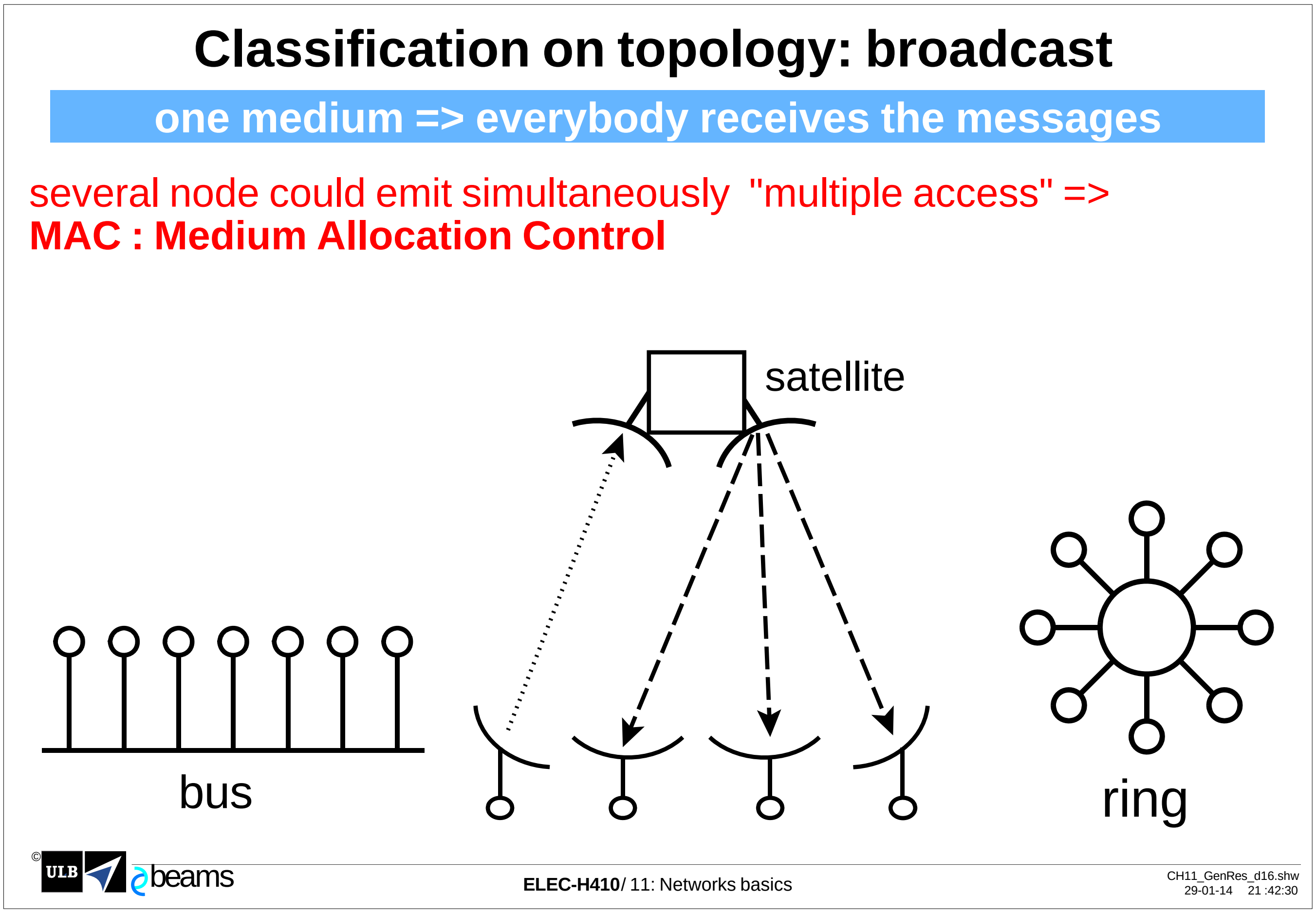
Several examples of point-to-point networks are visible on this figure:

- the **star**, whose single central node is the mandatory point of transit for all messages; the star is appropriate especially when all information must come to the central node (the control room for example) and when the various peripheral nodes exchange few messages between them

- the **ring** where each node has a connection on the left and on the right; the direction of messages can be unspecified or imposed. If the direction is unspecified, the opening of the ring does not prevent the traffic among all the nodes. Contrary to the star
  - all the nodes are hierarchically equivalent
  - the more nodes are interested by the current message, the higher is the efficiency, since each node as the opportunity to pick-up the message before forwarding it.

- the **tree** is a very hierarchical structure;
  - its advantage is generally to reduce the length of wire and to respect the hierarchy of buildings (building, level, rooms),
  - it is not efficient for important traffic between nodes of the same level. Two "brothers" must communicate through their "father", and two "cousins" by the "father", the "grandfather" and the "uncle"

One can also
- combine simple shapes, for example two rings having a common point
- add direct connections between nodes which exchange much traffic, this to lead to more or less meshed networks



Classification on topology: broadcast

one medium => everybody receives the messages

several node could emit simultaneously "multiple access" =>
MAC : Medium Allocation Control

In the **broadcast** networks, the information emitted by a node is directly accessible by all the other nodes almost at the same time (small are differences due to travel time).

The most common wiring structures are:

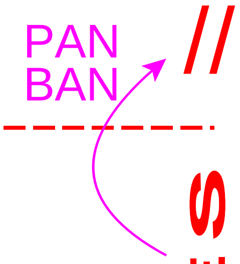
- the **bus**, generally of a pair of wire on which the various nodes are connected
- the **ring**, which can be seen as a closed bus
- **wireless** solutions based on radio or infrared waves, here illustrated by a satellite which "sprinkles" a certain number of ground stations.

Let us notice that, in the broadcast networks, the **difficulty of the multiple access** arises, i.e. of the possibility for several nodes to emitting simultaneously on the common medium what is called "collision". The information is jammed and useless. Therefore, it will be necessary to install **medium allocation control** mechanisms:
- to prevent emitting if the medium is already occupied
- to avoid the collisions and to detect them if they occur nevertheless

Classification on distance

xAN

- d < 1m : multiprocessor systems
  - within same computer



- 10 m < d < 1 km : local network (LAN)
  - room, building, campus
- 1km < d < 10 km : metropolitan network (MAN)
  - town
- 10 km < d < 100 km : wide-area network (WAN)
  - region
- 100 km < d < 10 000 km : network interconnection
  - no limit

SERIES

The way information is transmitted depends on the distance. The majority of elementary information comes from a processor whose word size is fixed by its data bus (8,16,32,64 bits).

Below one metre, it is possible to transmit all the bits of a word simultaneously; one wire per bit is needed (plus one return ground wire) and we speak about **parallel transmission**. A good example was the connection between hard disks and the mother board by flat cables.

When connections lengthen, the parallel transmission loses of its interest:
- the length of copper is multiplied by the number of bits
- the stray capacitance between wires is proportional to the length and can create interferences between bits carried by adjacent wires (crosstalk)
- the total stray capacitance (capacitance/unit length X length) between each signal and the ground causes a deformation of the signal; the transition times grows proportionally with length of the cable. If we want to preserve acceptable noise immunity, the bits should be lengthened, i.e. we have to reduce the transmission speed.

Beyond a few metres, we only find **serial transmissions**, in which the bits of the words are emitted successively.

Classically networks are classified as LAN (Local Area Networks) and WAN (Wide Area Network), depending on the distance. Serial transmissions have virtually no limit: we can communicate with space probes.

Let us notice that the current tendency is to use fast serial transmissions (up to several Gbit/s), even at very short distance (ex USB, FireWire, eSATA), as well as wireless transmissions (Bluetooth, ZigBee), to simplify or remove the connectors and the cables. Those short distance networks are called **PAN** (Personal Area Network). If their purpose is to collect information on our body (e.g. for health monitoring) the name **BAN** (Body Area Network) is also used.

Classification on distance

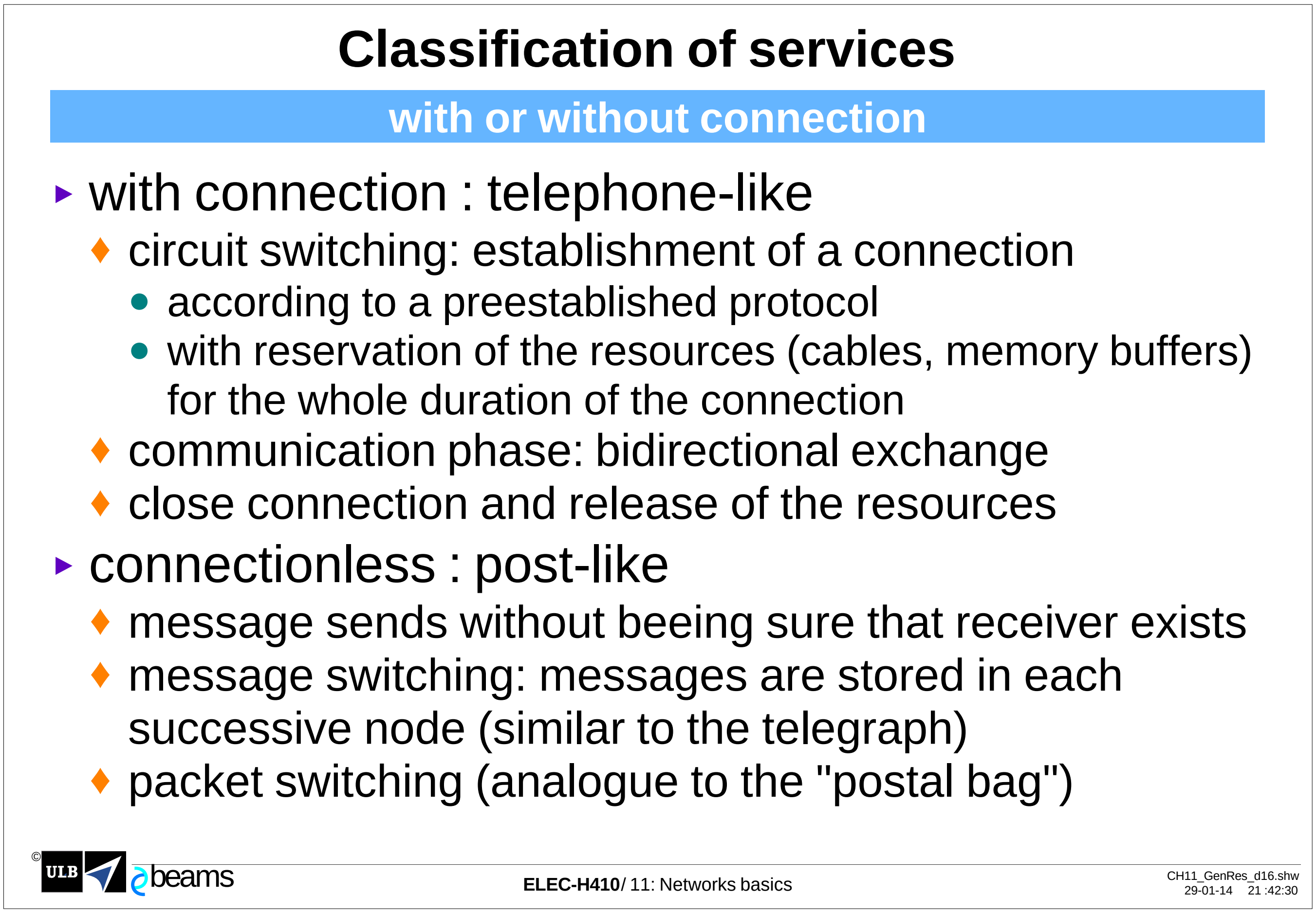
LAN - WAN

- Local Area Network
  - private medium
  - high bandwidth (100kbit/s to Gbit/s)
  - broadcast (multiple access)
  - low error rate => simpler protocols
- Wide Area Network
  - unlimited extension
  - medium : public telecom
  - bandwidth sometimes limited (old lines)
  - point-to-point
  - higher error rate

Classification on hierarchy

client-server or peer-to-peer

- clients-server
  - one or more machine(s), the server(s) provide(s) the resources (mass memory, databases)
  - the other machines (clients) exchange data with the server
- peer-to-peer
  - all the machines are equal
  - possible sharing of the various resources of all the machines (authorization required)



Classification of services

with or without connection

- with connection : telephone-like
  - circuit switching: establishment of a connection
    - according to a preestablished protocol
    - with reservation of the resources (cables, memory buffers) for the whole duration of the connection
  - communication phase: bidirectional exchange
  - close connection and release of the resources
- connectionless : post-like
  - message sends without beeing sure that receiver exists
  - message switching: messages are stored in each successive node (similar to the telegraph)
  - packet switching (analogue to the "postal bag")

Two modes of communication between can be used:

The mode called "**with connection**" functions in a way similar to our telephone calls:
- first a connection is established, with a definite protocol generally including
  - how the "address" of the correspondent is defined
  - how to seek if the correspondent is present
  - mutual identification of the 2 correspondents
  - the reservation of the resources (cables, memory buffers) throughout the whole communication
- then the phase of communication itself takes place: it is generally bidirectional, in full- or half-duplex
- finally, the communication is closed and the resources are released

In the mode "**without connection**" a message is sent at the address of the recipient without making sure that this one is able to receive it (nor even, without being sure of its existence).
- the message is "posted" in an entrance point ("gateway") of the network, whose task is to forward it to the destination, by choosing a road passing by other similar relay machines
- **message switching** occurs: the messages are stored in each successive node (similar to the telegraph)
- several messages sent between two nodes can be grouped in packets (similar to the "postal bag"): this is called **packet switching**.

Reliability of the transmission

connection and ACK => 3 levels of quality

- no connection / no acknoledgement (ACK)
- no connection / acknoledgement (ACK)
- reliable: connected with acknoledgement

service	example
with connection	
reliable msg transfer reliable transfer of data transfer without control of errors	pages of text measurements voice
no connection	
datagram transfer without ACK datagram transfer with ACK	e-mail e-mail + ACK

Working with or without connection influences obviously the reliability of the transmission. We can moreover add the concept of acknowledgement (ACK), in which the receiver of a message returns to the transmitter a short message indicating that data has been received and up to what point it is correct.

Four combinations are hence possible (with/without connection and with/without acknowledgement), among which only three are useful (ACK is always used in connected mode).

The only combination considered as **reliable** is the mode **with connection and ACK**.

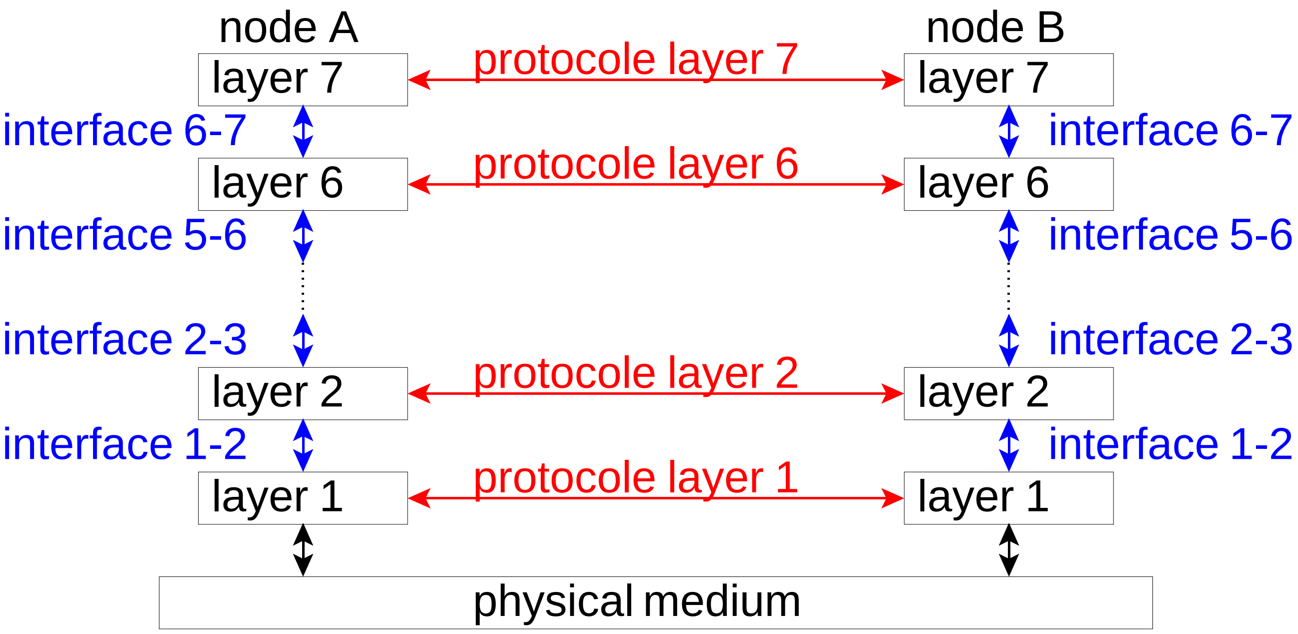
Networks

CONTENTS

- objectives
- classification
- **architecture**
  - **layers, protocols and interfaces**
  - OSI model
  - TCP/IP

Architecture (1)

layers + protocols + interfaces



When we speak about the architecture of a network, we refer to the software and the hardware tasks allowing to convey information from a node A to a node B and which includes **layers, interfaces and protocols.**

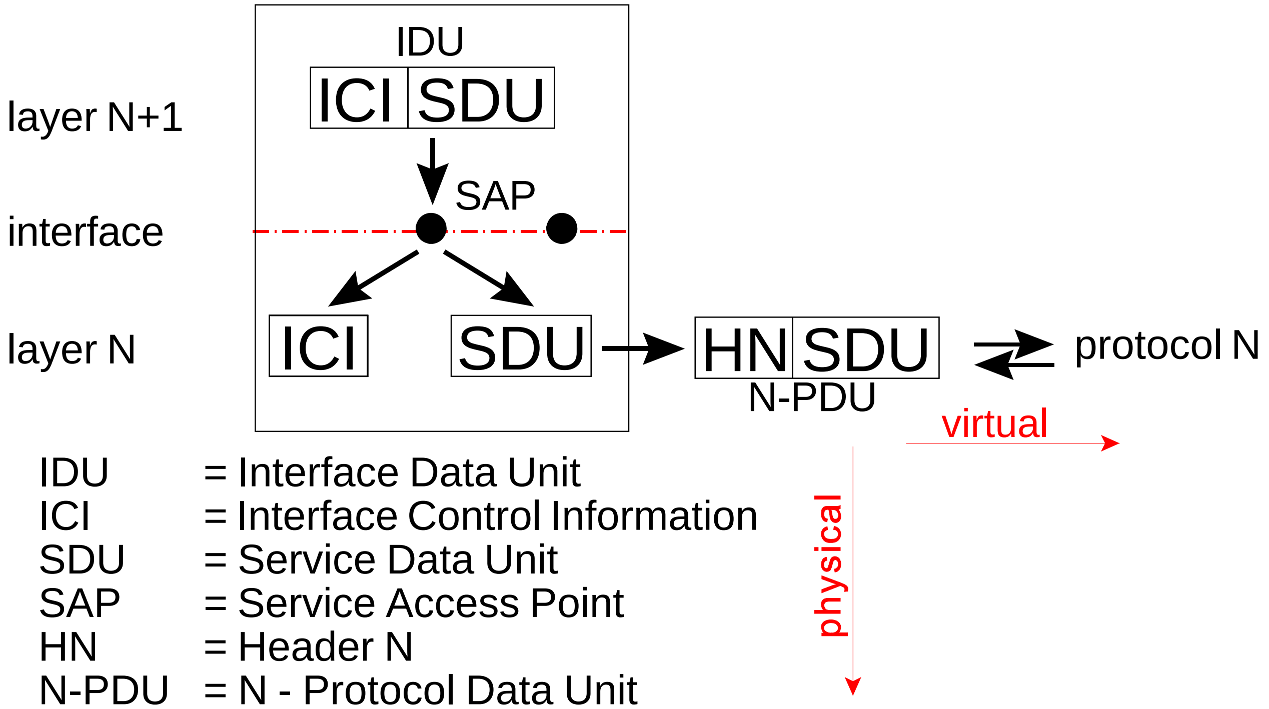
Along its way, the information coming from a program running on a node A passes by successive treatments, carried out by the layers 7,6,5,4,3,2,1 of A, then propagates on the physical medium, to reach a program running on node B through a whole stack of layers 1 to 7.

- each layer N offers services to the layer N+1, which subcontracts a precise part of work to it
- the interface between 2 layers defines services and their SAP (Service Access Points). Each SAP has got its own address
- each layer N follows a protocol N to establish a horizontal virtual logical communication with the "peer" layer. This protocol can be in connected mode or not according to the type of network and the layer. Layer N is unaware of how much layers precede it and follow it, it has only to know:
  - the services which can be asked by the N+1 layer
  - the N protocol
  - to which SAP of the N-1 layer it has to subcontract sending the information to peer N layer of the receiver

REM: the number of layers 7 comes from the OSI model which we will see hereafter

Interface mechanism

the service access point



IDU = Interface Data Unit
ICI = Interface Control Information
SDU = Service Data Unit
SAP = Service Access Point
HN = Header N
N-PDU = N - Protocol Data Unit

This figure gives the principle of the interface between the N+1 layer and N layer.

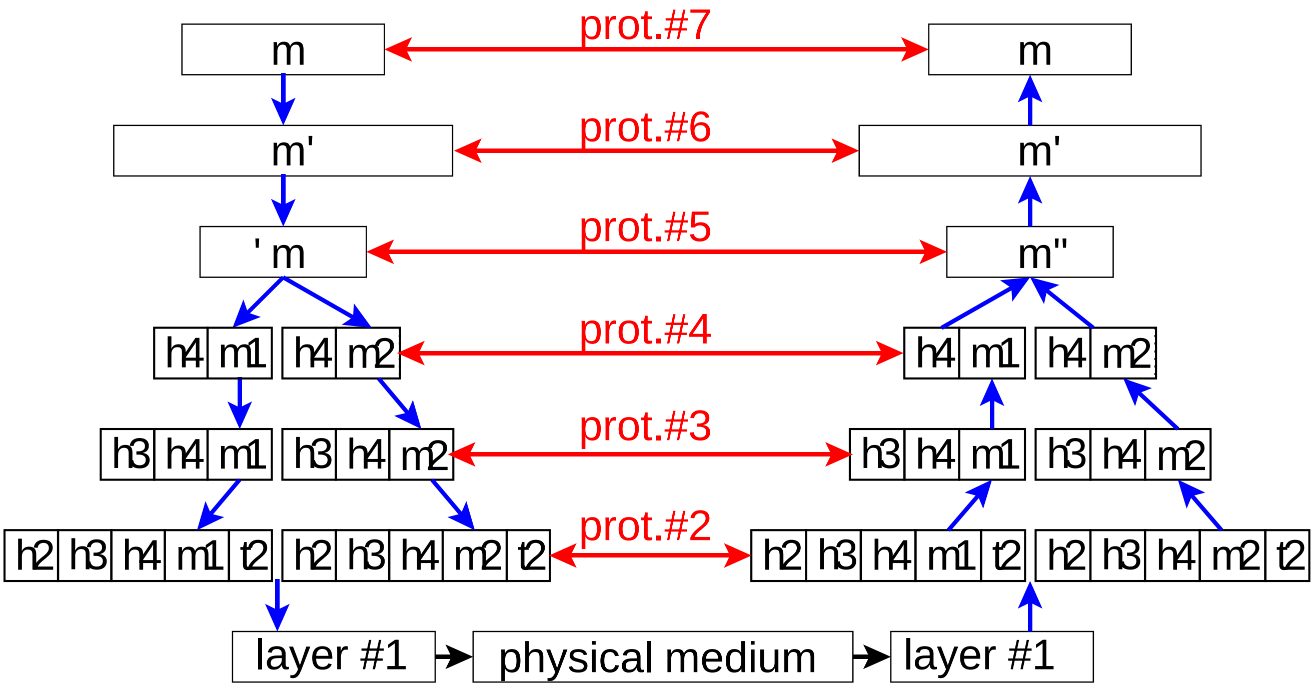
Data will to be forwarded to N+1 peer layer, by calling a service of layer N; these data are called SDU (Service Data Unit).

- the N+1 layer will prefix the data with an ICI (Information of Control of Interface) before calling the SAP of the interface towards layer N
- the SAP will separate ICI and SDU, will analyse the ICI to know which treatment is requested from layer N, and start this treatment.
- the protocol of layer N will prefix the SDU by a header HN, to form a package called N-PDU (Protocol Data Unit of level N) then send it towards layer N of the receiver. The figure shows the "horizontal" virtual departure of the N-PDU. Actually, the N-PDU will be dispatched by a physical "vertical" mechanism calling an SAP towards the N-1 layer. N-PDU will thus be encapsulated in the (N-1)-PDU.

Rem: to simplify, it was supposed here that layer N does not modify the contents of the data coming from N+1 and does not try to interpret them; protocol N relates only to header HN. It is not true for all layers (see next slide).

Physical vs logical data transfer

information evolves through the layers



prot.#7

m | m

prot.#6

m' | m'

prot.#5

' m | m''

prot.#4

h4 m1 | h4 m2 | h4 m1 | h4 m2

prot.#3

h3 h4 m1 | h3 h4 m2 | h3 h4 m1 | h3 h4 m2

prot.#2

h2 h3 h4 m1 t2 | h2 h3 h4 m2 t2 | h2 h3 h4 m1 t2 | h2 h3 h4 m2 t2

layer #1 | physical medium | layer #1

On this figure, we see the transfer of the data through the successive layers and their progressive transformation, until the physical transfer in layer #1.

Let us consider a message m coming from an application; it will undergo, for example, a transformation of the data (compression, encoding) in uppers layers (#7, #6, #5).

The lower layers (#4, #3, #2) do not modidy anymore the data, on the other hand they can split them and add a header (H_i) and possibly a termination (T_i) corresponding to the protocol of level i.
Headers and terminations are withdrawn by the peer layer in reception as part of the protocol.

We see that the treatment generates an increased quantity of information to be transmitted by the physical layer, since the original data has been supplemented by the data of all the successive protocols (*overhead*).
The real useful flow of information is thus lower than the flow of data on the physical medium.

Choice of the layers

arbitraty choice

- one layer =
  - an additional level of abstraction
  - well defined functions
  - obeys a protocol
- choose the borders to minimize flows at interfaces
- arbitrary number
  - not enough layers = too many fonctions/layer
  - too many layers = heavy structure, slow-down, reduction in the effective throughput

Networks

CONTENTS

- objectives
- classification
- **architecture**
  - layers, protocols and interfaces
  - **OSI model**
  - TCP/IP

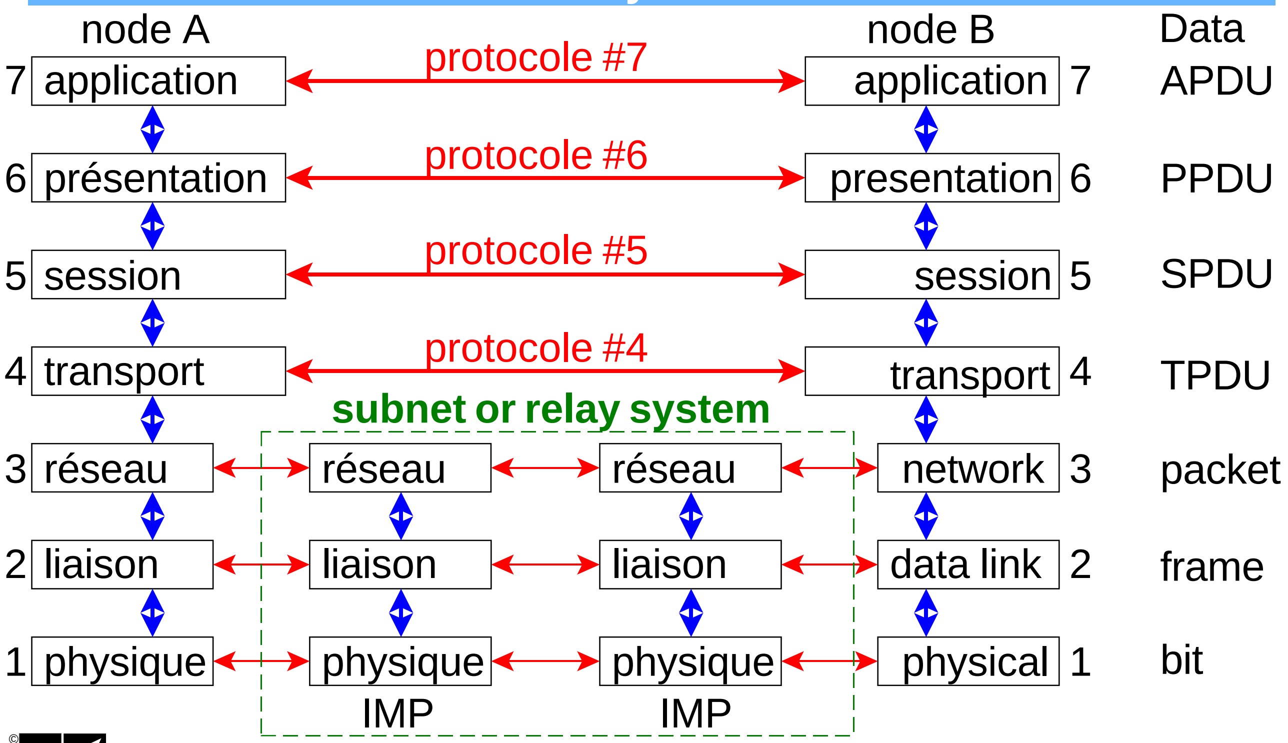
OSI

introduction

- **O**pen **S**ystems **I**nterconnection
  - non-proprietary
  - heterogeneous interconnections
- normalized: ISO 1984
- reference model:
  - specify the functions of the layers, but not explicitly the services and the protocols of each layer
  - ∃ standards for each layer in addition to the model
  - a lot of organizations are responsible for standardization

OSI

the 7-layer model



	node A			node B		Data
7	application	protocole #7		application	7	APDU
6	présentation	protocole #6		presentation	6	PPDU
5	session	protocole #5		session	5	SPDU
4	transport	protocole #4		transport	4	TPDU
		subnet or relay system				
3	réseau	réseau	réseau	network	3	packet
2	liaison	liaison	liaison	data link	2	frame
1	physique	physique	physique	physical	1	bit
		IMP	IMP			

© ULB beams

ELEC-H410/ 11: Networks basics

CH11_GenRes_d16.shw
29-01-14 21 :42:30

OSI model defines 7 layers, whose French and English names are indicated on this figure.

We clearly distinguish 2 types of layers:

- **lower layers** (#1,#2,#3), charged **to relay** the information through possibly several
  - successive physical media
  - machines of interconnection, called IMP (Interface Machine Processor). Those machines generally belong to the big telecom operators;

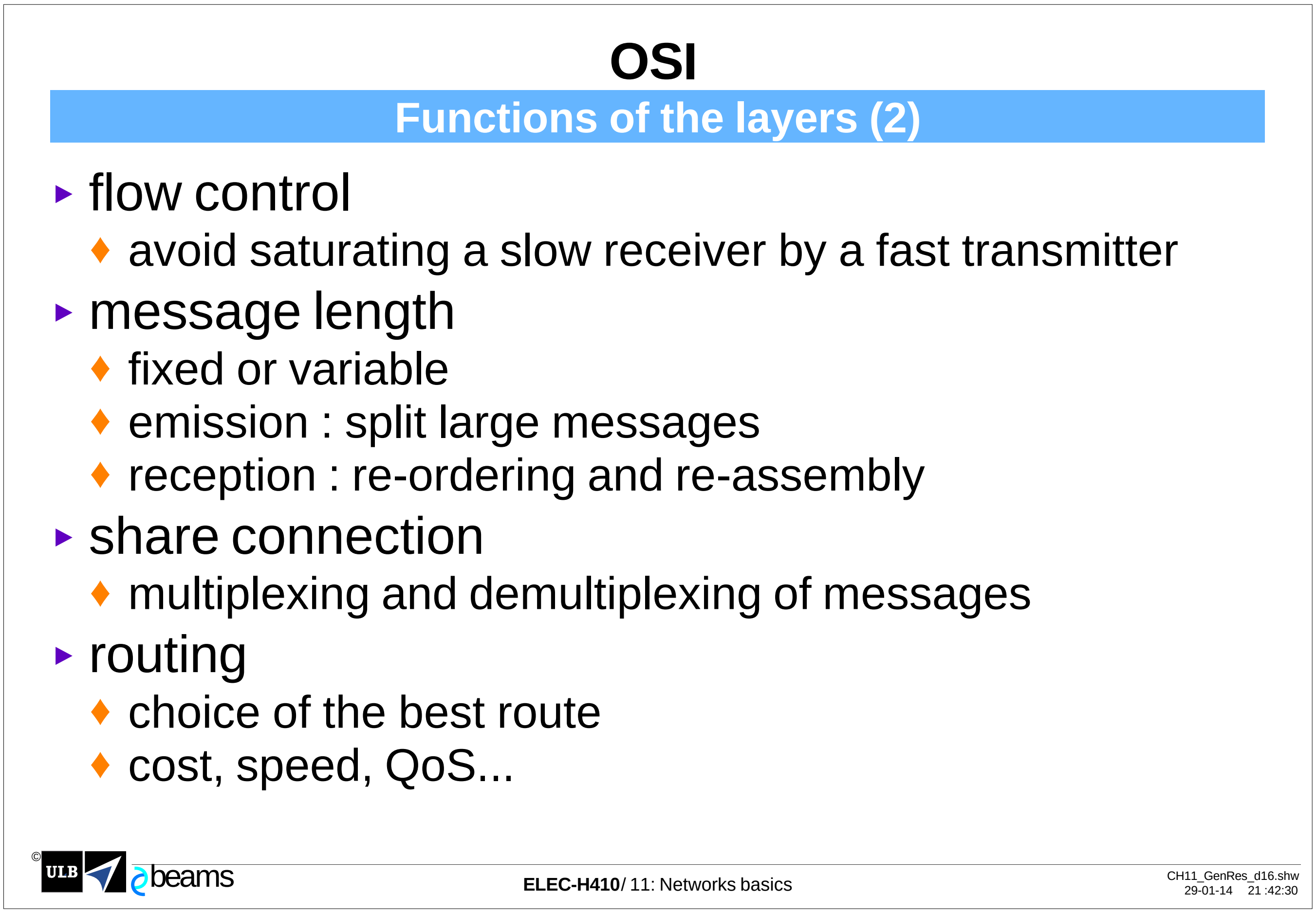
- **upper layers** (#4,#5,#6,#7), for which the protocol proceeds directly between two final nodes A and B of the transmission.

The name of the information (Data Unit) transmitted to each level of the model is also indicated on the right on the figure.

OSI

Functions of the layers (1)

- mechanism of identification emitter/receiver
  - at the level of each layer
- direction of the data
  - *simplex* : one-way
  - *half-duplex* : bidirectional alternate (like walkie-talkie)
  - *full-duplex* : bidirectional
- error control
  - no physical support is perfect
  - detection and correction of errors by the receiver



OSI

Functions of the layers (2)

- flow control
  - avoid saturating a slow receiver by a fast transmitter
- message length
  - fixed or variable
  - emission : split large messages
  - reception : re-ordering and re-assembly
- share connection
  - multiplexing and demultiplexing of messages
- routing
  - choice of the best route
  - cost, speed, QoS...

- if the flow that the receiver can accept is systematically or temporarily lower than the flow coming from the transmitter, at least one of the layers must be in charge of slowing down the transmitter

- the length of messages must be managed. The protocols always define elementary messages, whose length can be fixed or variable, but there is always a limit to this length. In the most frequent case, the quantity of information to be transmitted (a file for example) is larger than the maximum length. One of the layers must thus cut the data into chunks which have to be reassembled at the reception. It will possibly be necessary to sort the received chunks which could arrive out of order at the receiver
  - either because they have travelled on different paths
  - or because there has been a retransmission due to an error

- conversely, a connection can be shared between several applications: it is then necessary to ensure the multiplexing in emission and the demultiplexing in reception

- to relay the information from A to B, several roads are generally possible; it is then necessary to choose the best one according to various criteria (cost, speed, quality of service, ...)

Physical layer [#1]

- one or more physical supports
  - copper: coaxial cable or twisted pairs
  - optical fibres
  - wireless: infrared / radio
- for each support
  - connectors and physical connection (hot plug ?)
  - duration of a bit or a symbol (baudrate)
  - bit level transmission
    - definition of the logical states 0 et 1
      - current, voltage, levels, edges, or modulation
    - differential transmission or not
    - high fanout buffers
  - simplex / half-duplex / full-duplex
  - initialization and termination of the connection

Data link layer [#2]

- MAC sub-layer (Medium Access Control)
  - manage access conflicts to the medium (multi-master networks)
  - fundamental in broadcast networks
- LLC sub-layer (Logical Link Control)
  - improve the reliability of transmission
    - data are split in **frames**
      - header + data + detection/correction codes + footer
    - ACK of received frames
    - possible retransmission if error
    - destruction of double frames
    - optional: coding, encryption, compression
  - flow control
    - avoid the clogging of the slowest receiver
    - avoid the monopolization of the medium ("chattering")

The #2 layer is called **data link layer**. It is a paramount layer which is always present, even in the most simplified broadcast networks.

It comprises a sublayer called **MAC (Medium Access Control)**, which depends on the medium used and is charged with determining which node can emit; it is a vital function in broadcast multimaster networks.

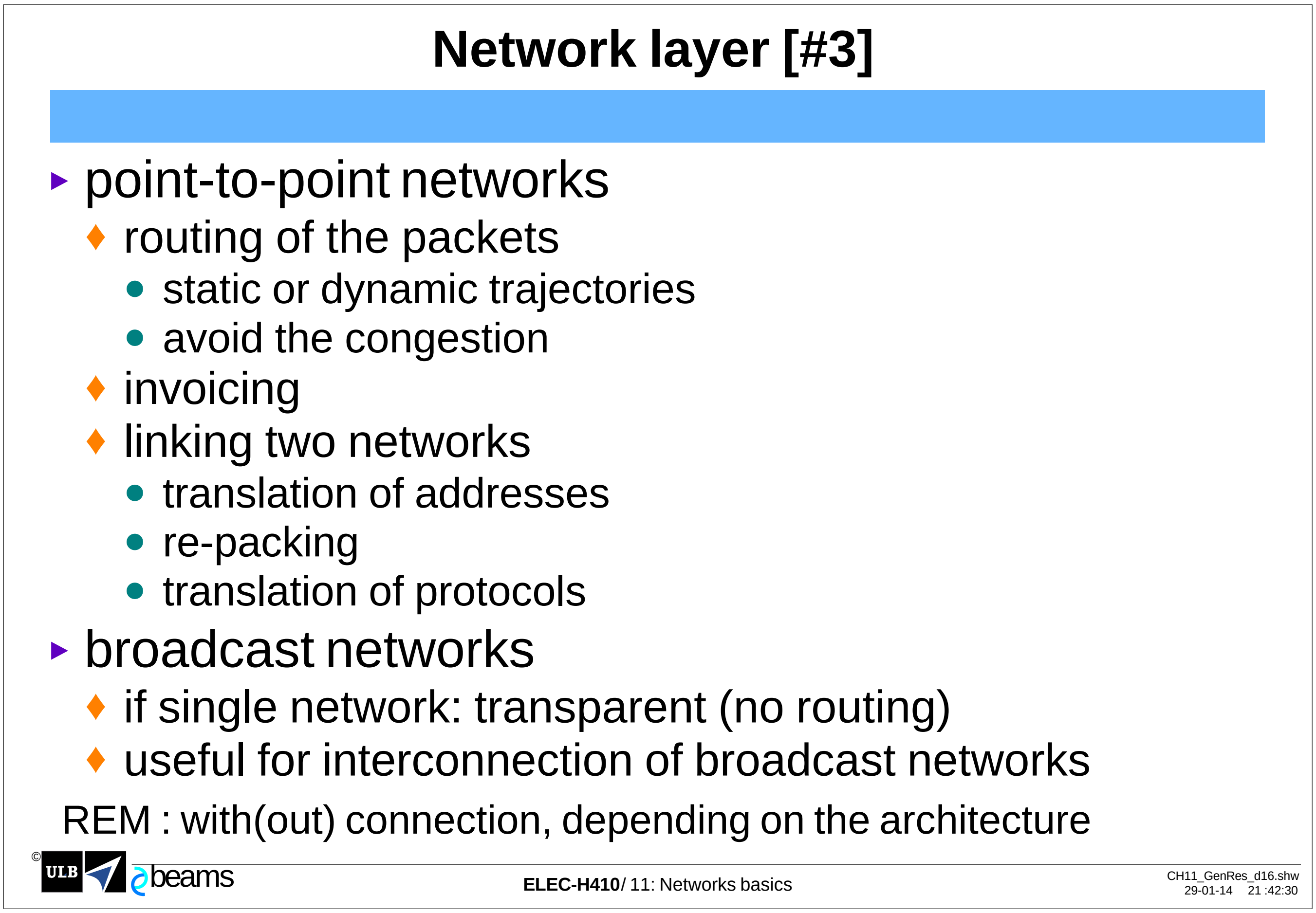
The second sublayer, just above the MAC is called LLC (Logical Link Control). LLC is independent of the medium, its main responsibility is to ensure the reliability of the transmission, in particular by error detection and correction codes (see next lesson). Since these codes are not applicable to a continuous flood of data, but to blocks of finite length, LLC must thus cut out the data in **frames** made of:

- a start delimiter
- a block of data resulting from cutting of the data provided by layer #3
- a CRC (Cyclic Redundancy Check): integer number calculated as the remainder of the division of the storage block by a polynomial (equivalent with the check code which finishes your bank account number)
- an end delimiter

When receiving, the #2 layer will recompute the CRC and compare it to the value written in the frame by the LLC of the emitter. A positive acknowledgement ACK will be returned to the emitter if there were no errors or if the number of false bits was sufficiently low for the receiver to make the correction. If the frame cannot be corrected, a negative acknowledgement NACK is returned. The protocol generally specifies that the emitter will retransmit until an ACK is received, with a maximum number of attempts. It can happen that an ACK is lost, in which case the receiver will get two correct frames and will have to eliminate one of them.

LLC is also in charge of
- the regulation of the flow to avoid the clogging of the slowest receiver
- to ensure that a transmitting node does not monopolize the medium ("chattering").

In option, LLC can take care of an encrypting or compressing the data.



Network layer [#3]

- point-to-point networks
  - routing of the packets
    - static or dynamic trajectories
    - avoid the congestion
  - invoicing
  - linking two networks
    - translation of addresses
    - re-packing
    - translation of protocols
- broadcast networks
  - if single network: transparent (no routing)
  - useful for interconnection of broadcast networks

REM : with(out) connection, depending on the architecture

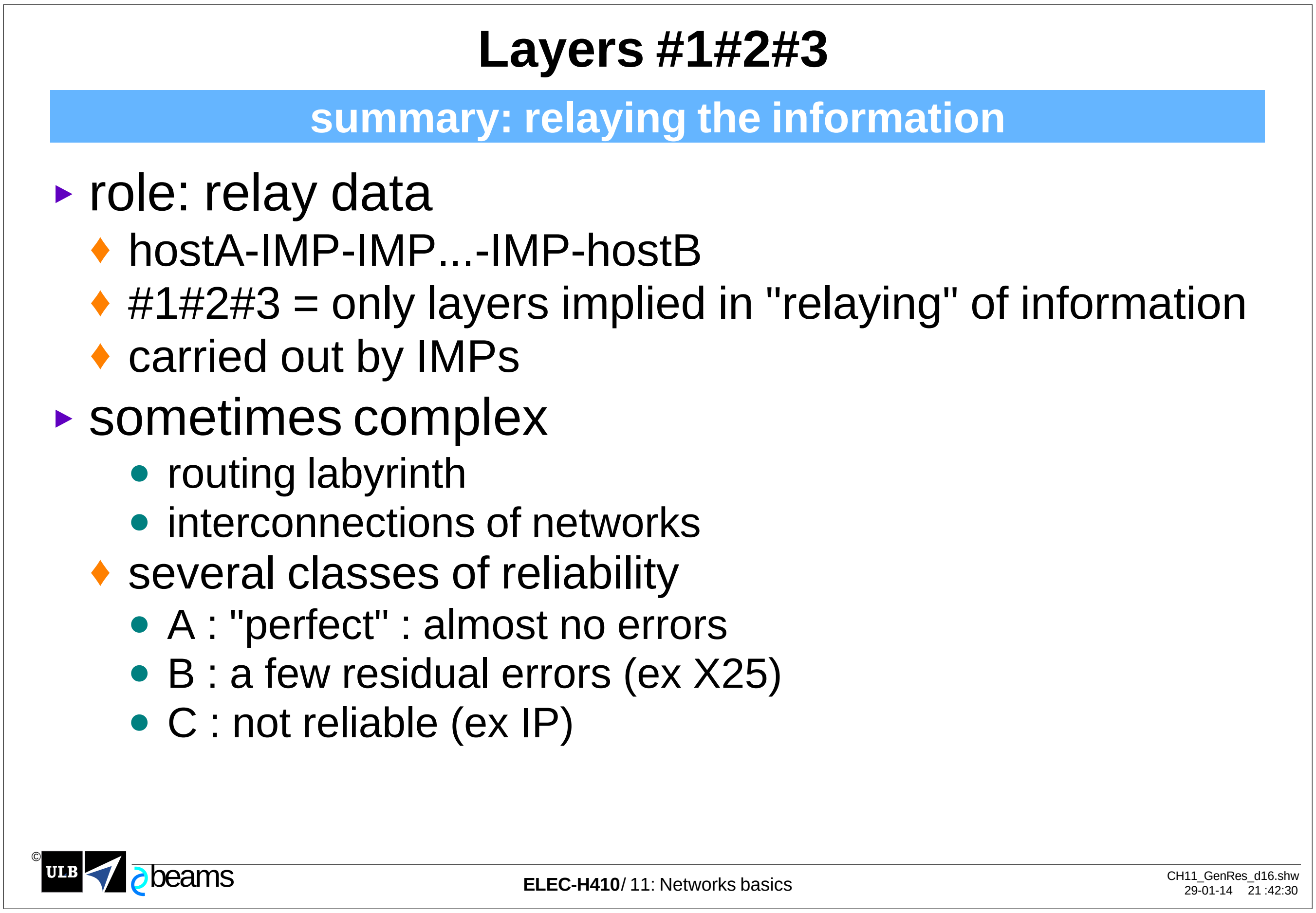
The layer #3 is called **"network layer"** and its role differs in point-to-point or broadcast networks.

In point-to-point networks, the network layer is essential and in charge of:

- routing the packets, with algorithms of search for static or dynamic trajectories to avoid the congestion of the network
- invoicing, obviously related to the path, which will generally pass through several operators
- passing from one network to another: if networks are different, the layer #3 can have to make:
  - a translation of addresses
  - the opening of the packets and repacketing
  - a translation of protocol

For broadcast networks:

- if the network is unique and isolated, the layer #3 can be empty because there is no routing (since all the nodes are on the same medium); it is the case of many industrial local area networks (for example the network of train)
- the #3 layer is active to interconnect broadcast networks



Layers #1#2#3

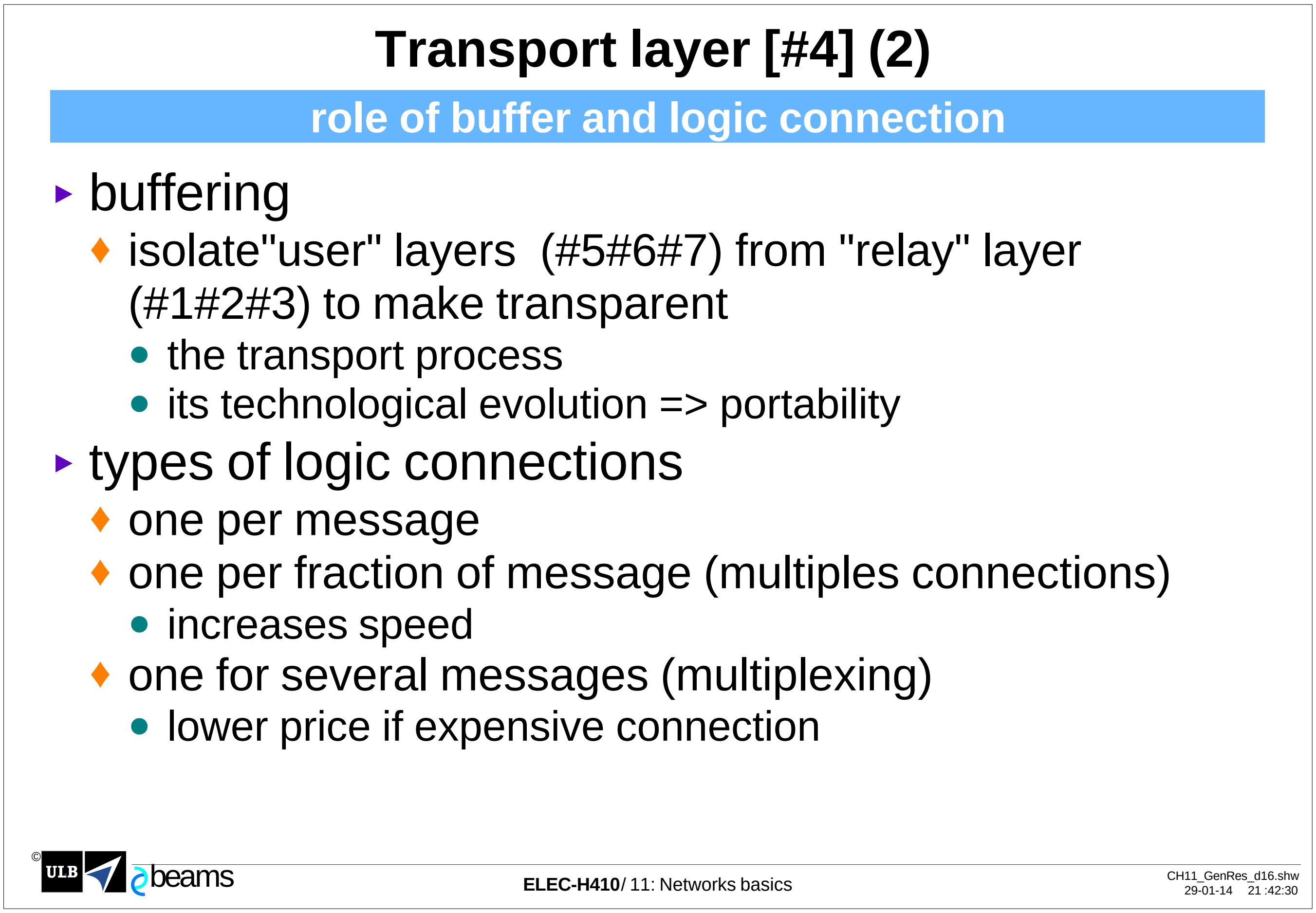
summary: relaying the information

- role: relay data
  - hostA-IMP-IMP...-IMP-hostB
  - #1#2#3 = only layers implied in "relaying" of information
  - carried out by IMPs
- sometimes complex
    - routing labyrinth
    - interconnections of networks
  - several classes of reliability
    - A : "perfect" : almost no errors
    - B : a few residual errors (ex X25)
    - C : not reliable (ex IP)

Transport layer [#4] (1)

1st layer with a direct protocol A<=>B

- essential role: effective and reliable transport
  - 5 classes
    - TP0 : almost empty (for reliable #1#2#3 type A)
    - TP1 : minimal corrections (for #1#2#3 type B)
    - TP2 : TP0 + multiplexing (for #1#2#3 type A)
    - TP3 : TP1 + TP2 (for #1#2#3 type B)
    - TP4 : reliable connected mode (for #1#2#3 type C) similar to layer #2
      - establishment of connection
      - split data in packets
      - error management
      - flow control



Transport layer [#4] (2)

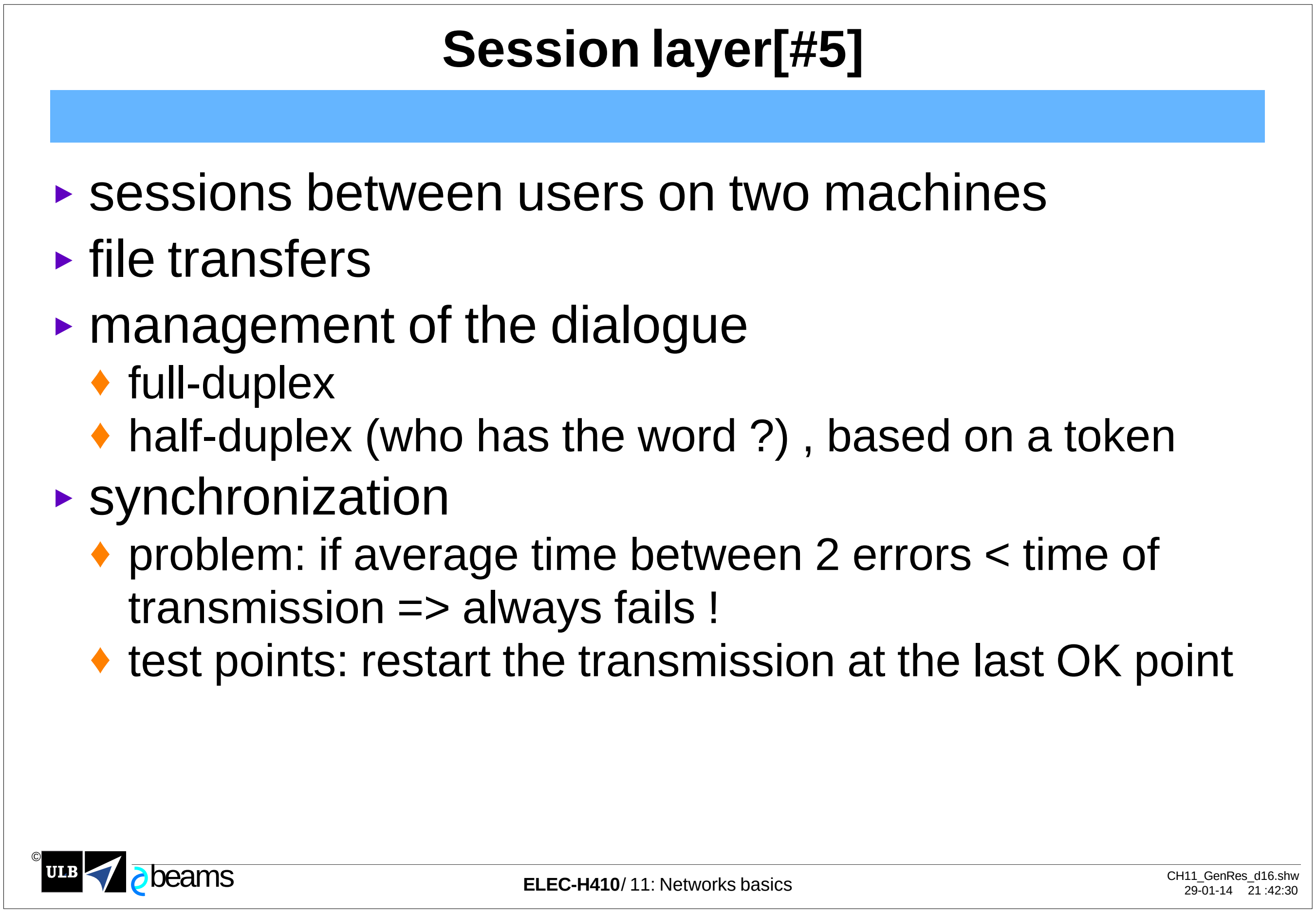
role of buffer and logic connection

- buffering
  - isolate"user" layers (#5#6#7) from "relay" layer (#1#2#3) to make transparent
    - the transport process
    - its technological evolution => portability
- types of logic connections
  - one per message
  - one per fraction of message (multiples connections)
    - increases speed
  - one for several messages (multiplexing)
    - lower price if expensive connection

In the missions of the layer #4 we still finds a role of **buffer** to isolate the "relay" layers #1#2#3 from the "user oriented" layers #5#6#7, for which the operation of transport must be transparent. The purpose is also to avoid a modification of the upper layers (#5#6#7) if the technological development changes the lower layers (#1#2#3). In this case, only layer #4 layer ust be adapted.

In the protocol between the two hosts A and B, we can plan to manage **several types of logical connections** when several messages have to be transmitted:

- simplest is to establish a connection by message
- to increase the speed, messages can be split into chunks which will be sent by several connection in parallel
- on the opposite, if the connection is expensive, we can multiplex several messages on same connection



Session layer[#5]

- sessions between users on two machines
- file transfers
- management of the dialogue
  - full-duplex
  - half-duplex (who has the word ?) , based on a token
- synchronization
  - problem: if average time between 2 errors < time of transmission => always fails !
  - test points: restart the transmission at the last OK point

The layer #5 **"session"** deals with

- establishing the session between users on two machines
- file transfers
- managing the **dialogue** between the 2 hosts, if the mode is "half duplex", a **token** is used to define which node can emit
- managing the **synchronization** in the transfer, in particular when large quantities of significant information pass through a medium suffering from a high error rate.
  Let us suppose that the average time between 2 errors is lower than the transmission time of a file; if we always restarts the transmission at the beginning, there is a significant risk that the file is never transmitted.
  The layer #5 is then charged to introduce **test points**, so that the transmission is only restarted at the last correct test point.

Presentation layer [#6]

the translator - interpreter

- [#1 à #5] : reliable transmission of bits
  - no role on the transmitted data
- [#6] : ensures the transparency in the syntax of information
  - encoding of the characters
    - ASCII
    - EBCDIC
    - UNICODE
  - format of the numbers (little/big endian, ...)
  - structures of the data
  - compression (if not done by #2)
  - encryption (if required and not done by #2)

Application layer [#7]

provides services to your applications

- file transfers
  - management of names
  - management of the file delimitors
- messaging
  - fundamental in the industrial applications
  - data exchange between sensors, regulators and actuators
- e-mail, remote login, ...
- small µC: you call functions of a library
- larger systems: you call the OS
  - which call the services
  - contains the drivers for networking hardware

Finally the layer #7 or **"application layer "** contains the functions and various services listed on this figure; your applications will call those functions when they require the services of the network.

That can be done,
- either by calling directly in your program functions from a library (it is the case in many small embedded systems)
- either by calling the operating system which contains the standard network protocols and the drivers of the network card.

Interconnection of networks

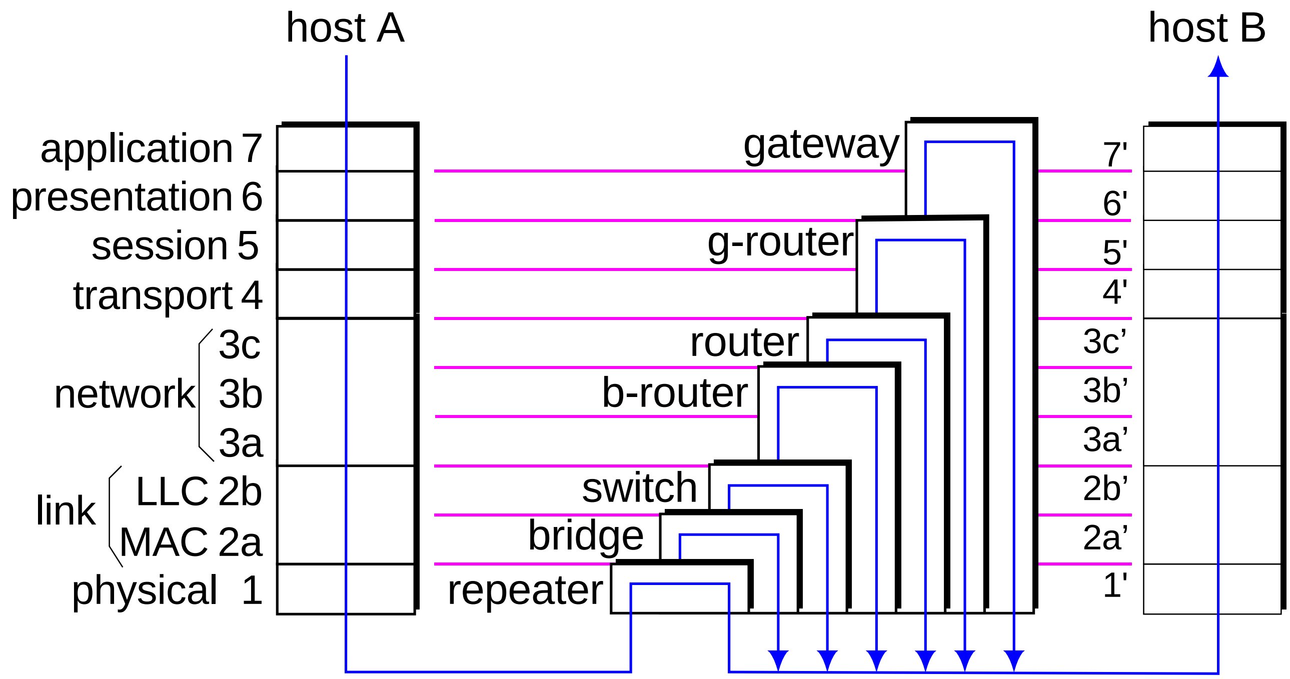
OSI was not foreseen for many small nodes

- interconnection neglected in first standard
  - layer #3 had to be split into 3a,3b,3c
    - #3c : *internet sublayer* : true interconnexion and routing between sub-networks
    - #3b : *subnet enhancement sublayer* : harmonization so that #3c layer identical for all the sub-networks
    - #3a : *subnet access sublayer* : protocol #3 for the sub-network
  - OSI designed to interconnect a few number of very large networks (main telecom operators)
  - OSI not designed to interconnect a large number of local area networks
- various types of relays exist, depending on the layer of interconnexion

.

Interconnection of networks

the device depends of the number of layers involved



host A

host B

application 7

presentation 6

session 5

transport 4

network 3c 3b 3a

link LLC 2b MAC 2a

physical 1

gateway

g-router

router

b-router

switch

bridge

repeater

7'

6'

5'

4'

3c'

3b'

3a'

2b'

2a'

1'

The interconnection of networks will require relay machines in which the number of layers depends on several factors:

- when the interconnection must be intelligent (for example, routing requires to go up to layer #3)
- to translate the different protocols when the interconnected networks do not use the same architectures

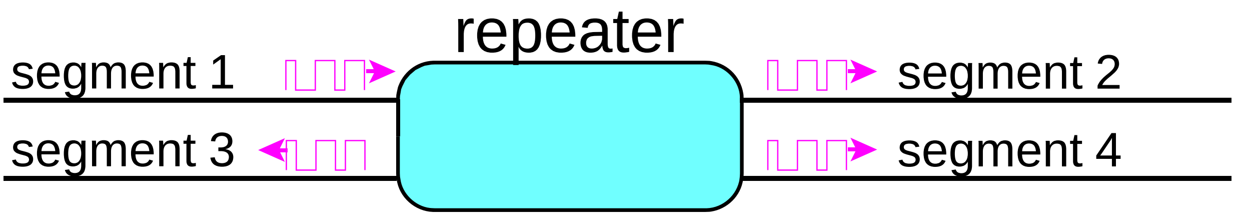
The name of the relay machine depends on the layer at which the interconnection is done (i.e. on the number of layers that have to be processed, starting from layer #1).

The following slides will specify these variants.

Interconnection of networks

repeater or hub: layer#1

- interconnection of segments working on same electrical standard to make a single network
- simple bidirectional analog amplifier
- filtering:
  - disconnect of a faulty (electrically) segment
  - no filtering of the frames: repeats false frames and collisions



The length of the segments of a network is limited (in particular to limit the attenuation of the signal). The repeater is simply a means of lengthening the network by restoring (i.e. amplifying) the electric level of the bits on the cable.

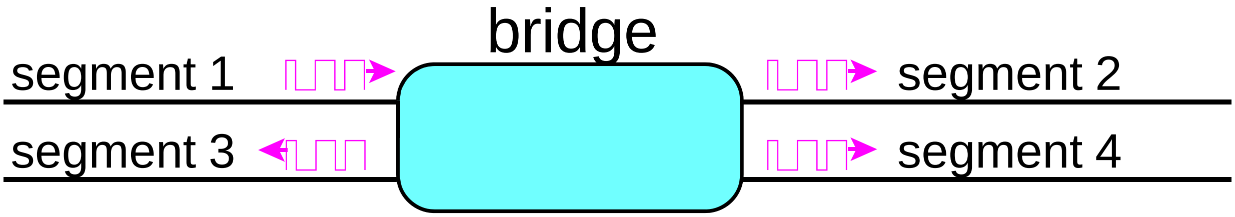
The figure presents here a 4-port repeater. Any frame arriving at any port is repeated (with a slight delay) on the 3 others ports

There is no validation of the frame, and no kind of filtering of the traffic. The only limitation carried out by the repeater is to isolate a segment which is electrically faulty (short-circuit, absence of termination), so that it does not disturb the other ones.

Interconnection of networks

bridge: layers#1+2a

- interconnection of networks with same LLC #2b
- filtering: see repeater plus
  - analyze the MAC addresses (transmitter + receiver) of the frames
  - builds a table of addresses in each segments
    - internal traffic of a segment not repeated on other ones
    - outgoing traffic of a segment repeated on all the others
    - can block the traffic to/from a given node on the basis of its MAC address

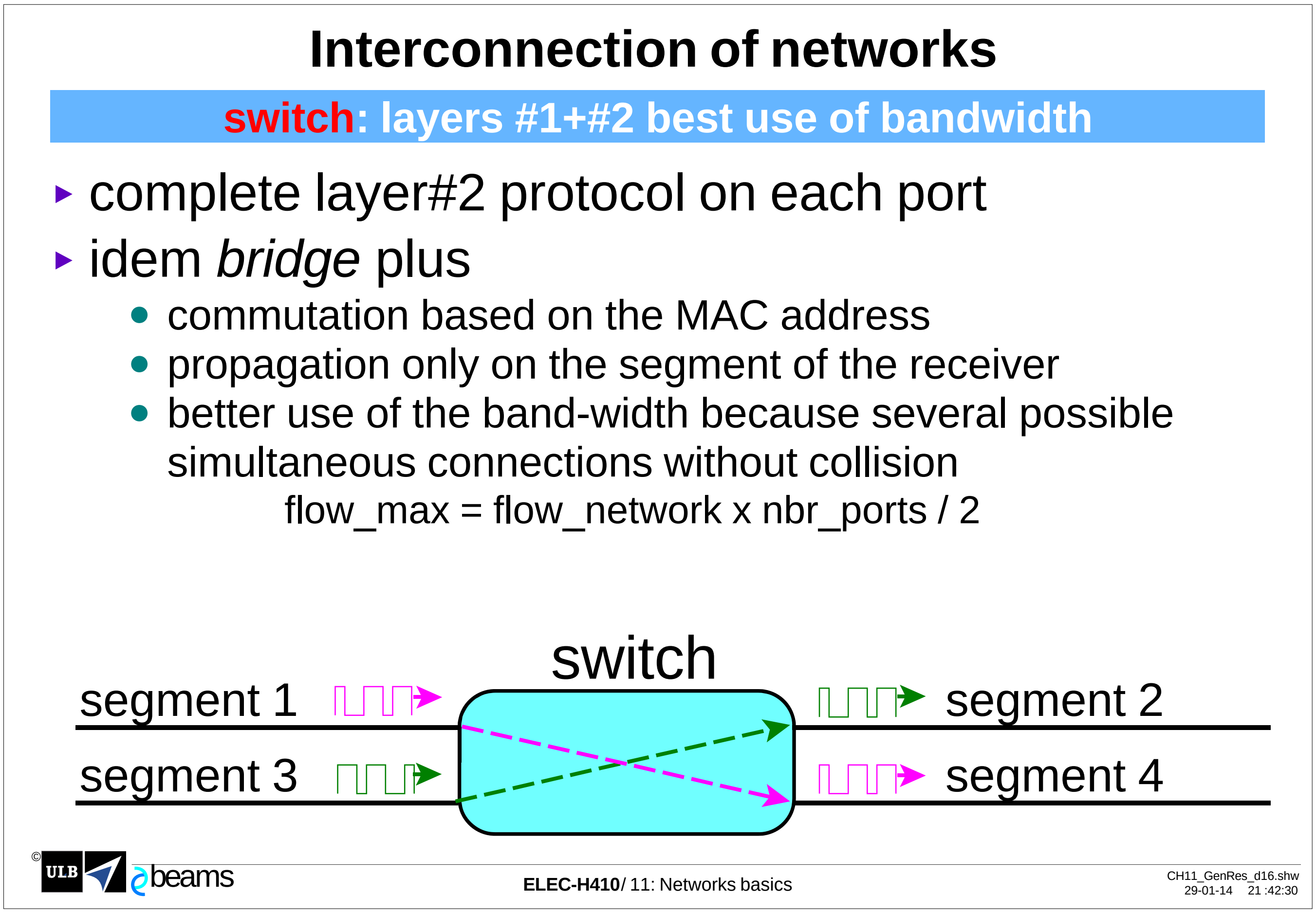


The **bridge** fulfills the same function as the repeater, but is more "intelligent". Indeed, it analyses the frames up to layer #2 to know the MAC addresses of the transmitter and of the receiver. The bridge builds tables a table of the MAC addresses of the machines which are on each segment (by using a dynamic mechanism which we will not study here).

The bridge is then able to:

- **reduce** the number of **collisions**: if frames are exchanged between 2 nodes of the same segment, the bridge does not repeat those frames on the other segmenst, where no node is concerned.
- to **filter** the traffic by preventing the reception(emission) of a frame on the basis of the MAC address of the transmitter(receiver)

A frame which crosses the bridge is repeated on all ports.



Interconnection of networks

switch: layers #1+#2 best use of bandwidth

- complete layer#2 protocol on each port
- idem *bridge* plus
  - commutation based on the MAC address
  - propagation only on the segment of the receiver
  - better use of the band-width because several possible simultaneous connections without collision

    flow_max = flow_network x nbr_ports / 2

switch
segment 1
segment 2
segment 3
segment 4

The **switch**, adds an additional function to the bridge: instead of repeating a crossing frame on all ports, it **repeats it only on the destination segment**.

The switch can be seen like a matrix of interconnection allowing to connect
- any port with any other one in the case of a communication from a transmitter towards only one receiver (*unicast*)
- any port with any group of other ports in the case of a communication from a transmitter towards several receivers (*multicast*)
- any port with all the others in the case of a communication from a transmitter to the whole network (*broadcast*)

The bandwidth of the cables is better used since the total flow that can cross the switch in the best case (all ports connected per pairs) is

flow_network x nbr_ports/2

The need for treating a higher flow leads to a higher price for the switch than for the bridge or the repeater. Since the popularisation of fast ethernet, the **switch has become the most popular relay machine**, with an excellent price/performance ratio.

Interconnection of networks

layers #3 +

- router
  - layer#3 split in 3a,3b,3c
  - pass from a sub-network to another with same 3c
  - translation of addresses
  - routing
- gateway
  - strongly heterogeneous interconnection
- b-router
  - *bridge* + some routing functions
- g-router
  - router + some gateway functions

One of the most significant relays is the **router**. This name clearly indicates that a router has to be installed if packets have to be routed
- to choose between several paths in a mesh network
- to pass from a subnetwork to another one.

In a completely heterogeneous connection, it is necessary to equip a machine with 2 different network card and to make the translation by a program running above the seven layers; in this case, the relay machine is called a ***gateway***.

REM: a confusion can arise with the concept gateway of IP which is the machine of a sub-network which gives access to the rest of the IP world (see further).

OSI

conclusions

- merits of OSI
  - clear separation in 3 groups
    - upper layers "application-oriented" (#5#6#7)
    - transport (#4)
    - lower layers carrying the information (#1#2#3)
  - possibility of defining software helped by hardware (peripherals and coprocessors) dedicated to each layer
- all the networks refer to OSI model
- all the networks are not in conformity with OSI model (cf TCP/IP, field busses)

Réseaux : plan

CONTENTS

- définition
- objectifs
- classification
- **architecture**
  - couches, protocoles et interfaces
  - modèle OSI
  - **TCP/IP**

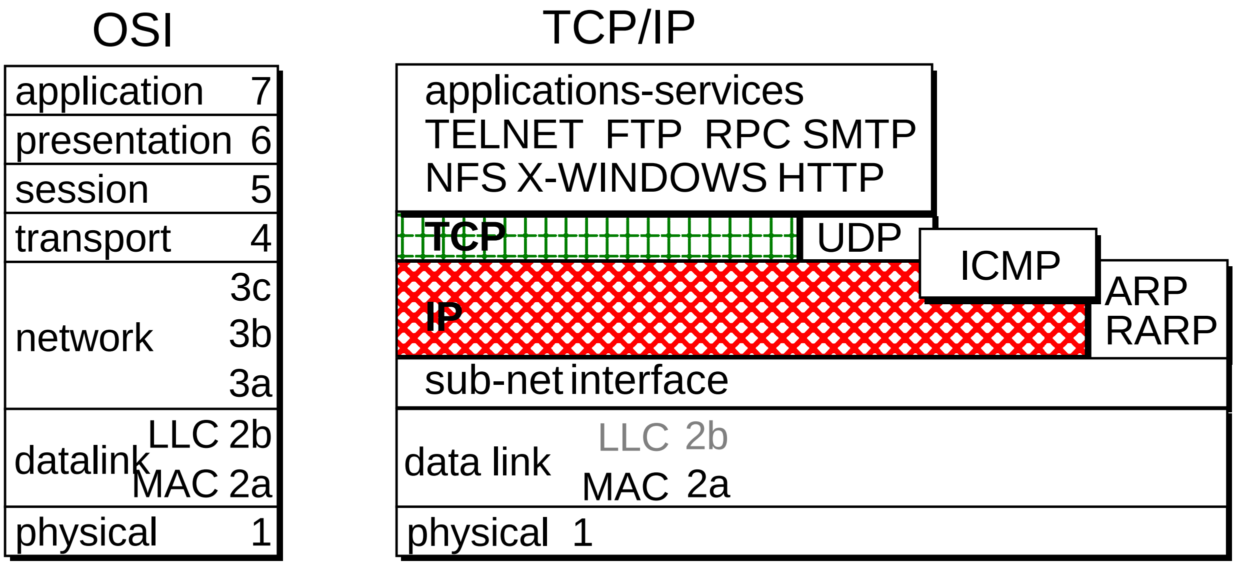
TCP/IP

introduction

- history
  - ARPA : ministry of defence USA 1969
  - reliable interconnection of computers so that the destruction of a node cannot prevent the system to work => creation of TCP/IP protocols
  - interconnection of universities and public organisms especially in the UNIX world; birth of INTERNET
  - extraordinary development
- forces
  - de facto standard
  - designed from the beginning to interconnect many networks, contrary to OSI
- TCP/IP and OSI
  - TCP/IP is NOT OSI (came 10 years earlier)

TCP/IP

TCP/IP vs OSI



OSI

application 7
presentation 6
session 5
transport 4
network 3c 3b 3a
datalink LLC 2b MAC 2a
physical 1

TCP/IP

applications-services
TELNET FTP RPC SMTP
NFS X-WINDOWS HTTP
TCP
UDP
ICMP
IP
ARP
RARP
sub-net interface
data link LLC 2b MAC 2a
physical 1

This figure shows us how to put in parallel (approximately) the stacks of OSI and of TCP/IP.

We suppose here that the layers #1 and #2 are identical (for example Ethernet).

The IP layer is at the "network" level, while TCP deals with "transport".

There is only one layer on top of TCP, which includes different services offered to the applications and gathers the various functions of the OSI layers #5, #6 and #7.

REM : the LLC layer is greyed because in the very popular case TCP/IP over Ethernet, the IP layer dialogs directly with the Ethernet MAC layer.

TCP/IP

IP (Internet Protocol) just post datagrams

- purpose : interconnection of networks
- principles are different from OSI
  - **single virtual worldwide network**
  - any node has a single IP address 32 bits (v4)

    $2^{32} = 4.10^{9}$ nodes
- send a message = **post a datagram** to the receiver's IP address
  - if receiver $\in$ same sub-network: direct transfer
  - if receiver $\in$ other sub-network: datagramme is posted on the *gateway* (=bridge,routeur or gateway)
- unconnected service => **IP is not reliable**

The basis of Internet is the IP (Internet Protocol) layer, which is responsible for the interconnection. The philosophy is to create a **single worldwide network** in which each machine has got its own **single address** (the IP address).

Consequently, sending data to a receiver is done in a "postal" mode: the **emitter "posts" a datagram** carrying the address of the receiver by broadcasting it on the network cable, or wireless.

- if the receiver is on the same subnetwork as the transmitter, it will recognize its address and receive the message immediately
- otherwise, one of the machine of the subnetwork, the " **gateway**" plays the role of P.0. box, and will search for a route to the receiver through several routers.

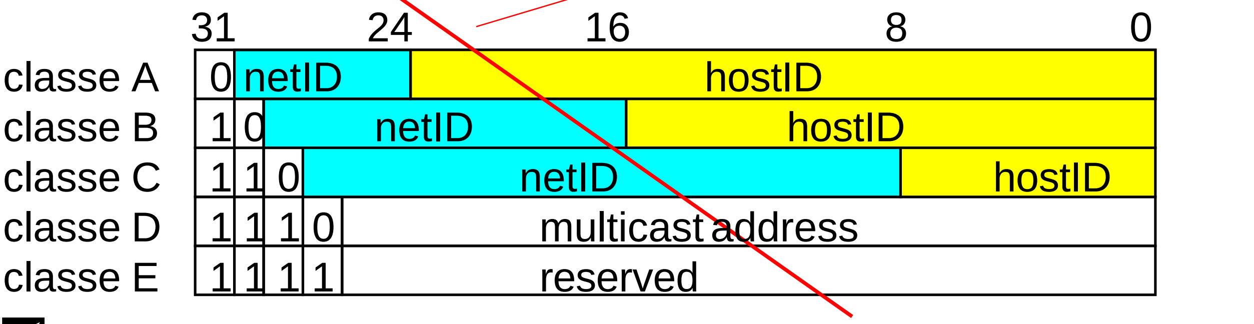
This philosophy has got a drawback: posting is done in **unconnected** mode, and thus considered as **unreliable**.

TCP/IP

IP addresses

- allotted by Internet Advisory Board
- structured to facilitate the routing
- 3 classes + multicast + reserved (->1990)
  - A : 128 networks of 16 M hosts
  - B : 16 K networks of 64 K hosts
  - C : 2M networks of 256 hosts

addr 192.168.000.035
mask 255.255.255.000



31 24 16 8 0

classe A 0 netID hostID

classe B 1 0 netID hostID

classe C 1 1 0 netID hostID

classe D 1 1 1 0 multicast address

classe E 1 1 1 1 reserved

The most common IPv4 address consists in 32 bits, divided into 4 bytes separated by dots and expressed in decimal form.
The address range is thus from 0.0.0.0 to 255.255.255.255

Until the middle of the years 1990, several classes of addresses existed, defining subnetworks of different sizes. The most significant bits of the address defined the class (size) of the subnetwork, and the least significant bits defined the address of the node within its subnetwork. This technique has been abandoned because it contributed to wasting addresses.

Today, the address is completed by a mask whose "1" bits define the portion of the address that all members of the subnet have in common. In the example of the figure:

- address 192.168.001.035 (it is in fact a particular address indicating a private network)
- mask 255.255.255.000 means that all the addresses 192.168.000.xxx belong to the same subnet.

TCP/IP

IP adresses : 32 bits are no more enough

- saturation due to explosion of nodes (2011)
- solution
  - recuperation of too much liberally allocated addresses
  - resort to special intelligent routers: a whole sub-network occupies one world IP address (NAT: Network Address Translation)
  - IPv6
    - 128 bit address = 3.4 10^{38} nodes = 6.6 10^{23} nodes/m²
    - currently only 1% of the nodes

There is no doubt that the designers of IP in 1969, when they foresaw 32bits (i.e. 4 billions of nodes) did not think that it would have ever been saturated, which finally happened in 2011.

The shortage was delayed by increasing the intelligence of the routers: a mechanism called NAT (Network Address Translation) allows to create a whole subnetwork under only one address IP.

A new version (IPv6) has been available since 2000 and uses 128 address bits. Both versions of IP coexist but are incompatible and the penetration of IPv6 was only 1% in 2010.

128 are more than sufficient: they corresponds to $2^{128} = 3.4\text{x}10^{38}$ i.e. $6.6\text{x}10^{23}$/m² on earth.

TCP/IP

how to associate MAC address to IP address

- addressing problem
  - IP: logical address in a single virtual network
  - layer #2: each node has got a unique **physical MAC address**
- ARP : Address Resolution Protocol
  - a host who wants to know a physical address broadcasts an ARP packet containing the IP address
  - the node which recognized its IP address answers by an ARP packet containing its MAC address
  - IP<=> MAC tables are build progressively
- RARP : Reverse ARP
  - a host unable to memorize its own IP address sends to its gateway a RARP packet containing its MAC address
  - the gateway answers by allotting an IP address

Without going into the details, it should be noticed that a TCP/IP node has got two addresses:

- the IP address in 32 bits, managed by IP (layer #3)
- the MAC address in 48 bits, managed by the layer #2

The latter is clearly the one which is the true address allowing that a frame arrives physically at the receiver because it is registered in the network adapter, which is completely independent of the protocol of layer #3.

There must be a mechanism to associate the unique IP address of the node in Internet to the unique MAC address of the network adapter. Two protocols called ARP or RARP can be used.

TCP/IP

TCP : Transmission Control Protocol

- similar to OSI#4 in TP4 mode
  - IP not reliable, not connected
  - TCP ensures a **reliable** and **connected** network service
    - full-duplex
    - error control: spilt into packets with sequential numbering and acknoledgement
    - flow control: when receiver sends ACK it indicates the size of the data it will accept for the next transaction
- ∃ also non-connected #4 sevices
  - UDP : User Datagram Protocol, for multimedia and real-time applications
  - ICMP : Internet Control Message Protocol: for errors and status messages

TCP ("Transmission Control Protocol ") is on top of IP. It plays a role similar to that of a layer #4 OSI in mode TP4, i.e. it is charged to compensate for the lacks of IP, which is not reliable due to its unconnected principle.

TCP ensures a **bidirectional reliable network service in connected mode, with control of error and of flow**

TCP is not the only possible layer on top of IP, we also find:

- **UDP** (*User Datagram Protocol*) works in unconnected mode and allows by its simplicity a more significant flow for less critical applications like multimedia file transfer. Is is also used for real-time application, because, in case of transmission errors, the retry mechanism of TCP is not deterministic
- **ICMP** (*Internet Control Message Protocol*) ensures the passage of management data of the network (errors and status messages)

TCP/IP

application services

- same role as OSI#5#6#7
- several standard applications:
  - file transfer
    - FTP : File Transfer Protcol
    - HTTP : Hyper Text Transfer Protocol
  - distributed file system
    - NFS : Network File System (via UDP)
  - e-mail
    - SMTP : Simple Mail Transfer Protocol
  - virtual terminal
    - TELNET

TCP/IP

Conclusions

- the oldest standard
- most widespread
- not supplanted by OSI, contrary to certain forecasts end of the '80ies
- in constant expansion in the industry

OSI, TCP/IP

originally not well adapted to real time

- some drawbacks and lacks
  - many layers = heavy model
  - no notions of timestamp
  - no determinism in the transfer time
  - no management of priority
- first solutions: birth of more efficient networks
  - fulfill the most possible functions in hardware
  - add time management
  - reduce the number of layers
    - **#1 essential**
    - **#2 responsible for medium allocation and reliability**
    - ~~#3~~ broadcast+single network=>no routing=>transparent
    - ~~#4~~ useless if reliable #2
    - ~~#5#6~~ not essential
    - **#7 essential** (interface to application)

Conclusions

- the world of the networks is divided in
  - OSI: declining
  - TCP/IP : local area networks and their worldwide interconnection (Internet) or within enterprise networks (Intranet)
    - strong pressure of the users for
      - generalize its use
      - generalize usage of the tools like the browsers
        - databases
        - SCADA : Supervision Control And Data Acquisition
  - others : specialized networks (ex field busses)