ELEC-H410
REAL-TIME SYSTEMS

Chapter 12

Medium Allocation in broadcast network

Medium Allocation Control

CONTENTS

- **Introduction**
- IEEE 802.3 : CSMA/CD
- IEEE 802.11 : WiFi
- IEEE 802.5 : Token Ring
- IEEE 802.4 : Token Bus
- Conclusions

Sharing a medium

inherent to broadcast networks

- need for a **protocol** of **medium allocation**
  - only 1 transmitter at the same time
    - circulation of a token
    - the node which wants to transmit takes the token
    - transmission time is limited: chattering is prohibited
    - when transmission is finished, token is released
    - token can circulate or be distributed by a Master
  - simultaneous emissions
    - trivial case: never interrupt a current transmission => emission only if medium free
    - collision detection
    - anti-collision mechanism for future trials
- requires division of data in **frames**

When a medium is shared by several nodes likely to transmit, the problem of the conflict (collision) between 2 (or more) nodes transmitting simultaneously, must be absolutely considered.
This problem is called **MAC (Medium Allocation Control),** and gave its name to the sublayer #2a of the OSI model.

There are two main ways of allocating the medium:

- **prevent the simultaneous emissions** by authorizing only one transmitter, for example thanks to the circulation of a **token**. Only the owner of the token is allowed to talk. To avoid chattering (monopolizing the medium) a node is obliged to release the token after a maximum speaking time.

  Rem: the token can be implicit, for example in a master-slave system where the master node periodically questions the slaves

- **simultaneous emissions are authorized**; in this case:
  - trivial collisions are avoided: a node cannot transmit if the medium is already occupied
  - if the medium is free, it is impossible to prevent several transmitters from trying to speak at the same time; consequently, it is necessary to set up a **collision detection**, then a mechanism which tends to reduce the risk of collision for future attempts.

In all case the protocol requires that the information is divided into sucessive **frames of limited lenght.**

IEEE 802 Recommandations

very common standards

- define several network types
  - 802.3: CSMA/CD (≈Ethernet)
  - 802.11: Wireless (WiFi)
  - 802.4:Token Bus
  - 802.5:Token Ring
- Data Link Layer #2
  - common sublayer LLC (Logical Link Control)
  - several MAC sublayers depending on medium
- physical layer #1
  - several possibilities (see further)

LLC #2b	802.2			
MAC #2a	802.3	802.11	802.4	802.5
PHY #1				

The IEEE has published several standards called 802.x which correspond to layers #1 and #2 of the OSI model and provide several mechanisms of medium allocation associated to various physical layers.
The LLC is common.

LLC 802.2

the most widespread in the world

- provided services
  - type1 : unreliable (unconnected mode, no ACK)
  - type2 : reliable (connected mode and ACK)
  - type3 : unconnected mode with ACK
- types of primitives
  - connection, disconnection
  - transfer of data
  - reset after serious error
  - flow control

The common sublayer LLC is defined by 802.2, and it is by far the most widespread LLC layer in the world. This slide gives us a summary of the services it provides. Refer to the previous chapter on the basis of networks for the details on the OSI model and on the role of layer #2.

Medium Allocation Control

CONTENTS

Carrier Sense Multiple Access

prevent simultaneous emissions

- a node which wants to emit "listens"
  - **non-persistent CSMA**: if the carrier is present, waits a random time before listening again
  - **1-persistent CSMA**: listen permanently, when channel becomes free, wait a short time (Inter Frame Gap) before emitting
  - **p-persistant CSMA** listen permanently but
    - a time-slice T is defined
    - lottery drawing
      - probability of immediate emission: $p < 1$
      - probability of awaiting the next T: $q = 1 - p$
- remarks
  - does not prevent the collisions because of the propagation time (emissions are detected upon their arrival)
  - ineffective if long propagation time (satellites)

Standard 802.3 defines a mechanism of MAC on a copper physical medium (coaxial or twisted pairs). The first thing is to avoid the trivial collisions by waiting for a free medium before transmitting.
802.3 defines **CSMA: Carrier Sense Multiple Access**

"Multiple access" means that several nodes are likely to emit simultaneously on the shared medium.
The term "carrier" seems to indicate that the signal on the cable is modulated. Generally it is no the case, much LANs are in baseband. "**Carrier**" must thus be taken in a broader sense "**activity on the cable** indicating that a node is transmitting".

There are three manners of listening to detect the carrier:
- **non-persistent CSMA**: if the carrier is present, await a random time before listening again
- **1-persistent CSMA 1**: listen permanently; once the medium is free, wait a small delay before transmitting (it is the most frequent case)
- **p-persistent CSMA:** listen permanently, once the medium is free, start a probabilistic mechanism which created a probability
  - **p** to transmit immediately
  - **q=1-p** to wait during a delay T_{MAC}, fixed by the protocol; at the end of T_{MAC}, and if the cable is still free, the same probabilistic mechanism restarts

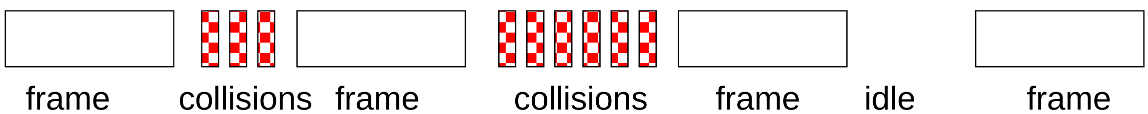
The carrier detection is an anti-collision condition which is necessary but unfortunately not sufficient, because of the propagation time on the cable. An absence of the carrier means
- either that nobody is emitting
- or that the message from the transmitter node has not yet arrived to the other node(s) wishing to transmit and which will thus decide in good faith that it(they) can get the medium.

A very long propagation time plays thus an unfavourable role in the detection of the carrier.

CSMA / CD

Carrier Sense Multiple Access / Collision Detection

- CSMA, then collision detection
- if collision occured
  - data are unusable
  - transmission is stopped **immediately** (just 32 bits of "jam") to save time and bandwidth
  - all nodes wait a random time
  - try to emit again



Since the collision cannot be avoided, it must be detected. Any transmitting node performs the collision detection during the whole duration of the transmission.

If the collision occurs, continuing the emission is useless since the data are scrambled and do not carry useful information any longer. To save the bandwidth of the cable and to be able to retry a transmission as soon as possible, the current frame is stopped quasi-immediately (in fact, a short "jam" sequence of 32 bits closes the frame)

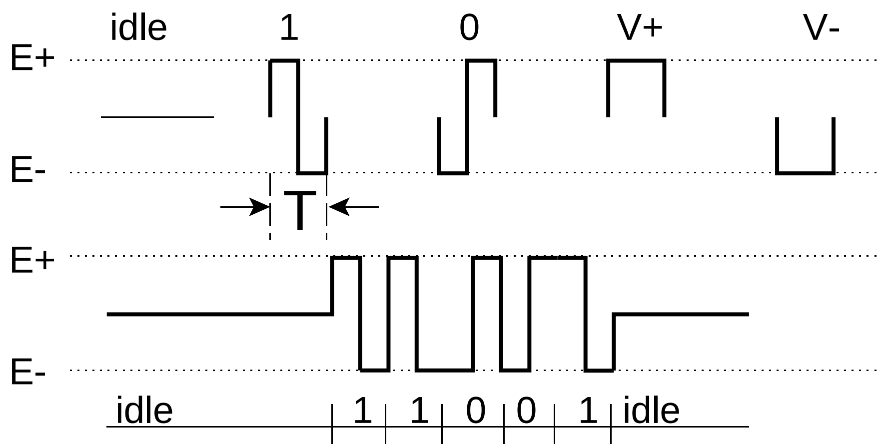
After the collision, the various concurrent transmitters will try to emit again. To decrease the risk of a new collision, a probabilistic mechanism is started, based on a random time before transmitting again.

The figure shows the analysis of the traffic on the cable with:
- some **idle time**: no node is trying to emit
- **normal frames** for which there no was collision
- **short frames**, sign of collision, with possibly several successive collisions before a node can emit a valid complete frame

Carrier sense

MANCHESTER coding

- baseband
- 2 normal states and 2 violations
- carrier = activity = edges at transmission frequency
- easy to code/decode



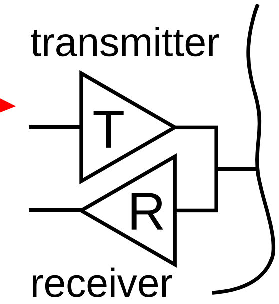
Many networks, including Ethernet, use Manchester coding, for which:
- each bit is separate in 2 half-bits called *moments*
- bit 1 is coded by a falling edge between the two half-bits
- bit 0 is coded by a rising edge between the two half-bits
- 2 transitionless bits called *violations*, also exist; they are used insides the frame delimiters to help differentiate them from the data

The Manchester code has got several advantages:
- the "carrier" is easy to detect by the activity of the signal, since an edge is always present at the middle of each bit
- its "self-clocking" i.e. it is easy for a receiver to identify the frequency of transmission and sample the incoming bits with a correct phase
- very simple hardware is required to code and decode

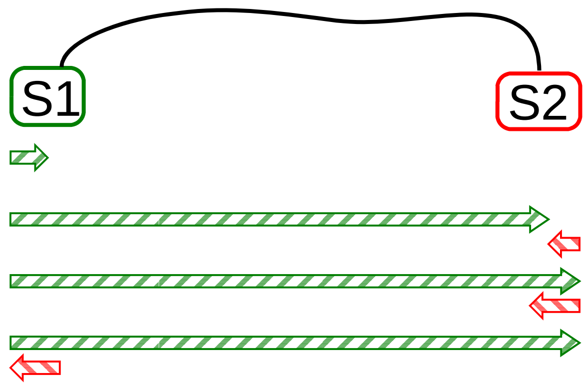
Collision detection

frames must be long enough

- mechanism
  - analog circuits ("transceivers")
  - transmitted bits are monitored by own receiver and compared to the original data
  - importance of MANCHESTER coding
- influence of the propagation time



critical delay = 2 .Tprop



t = 0	: S1 emits
t = Tprop - ϵ	: S2 emits
t = Tprop	: S2 detects collision
t = 2.Tprop - ϵ	: S1 detects collision

A node is connected to the cable by an analog interface called **transceiver**; this name is the contraction of *transmitter* (output amplifier) and *receiver* (input amplifier).

- the **carrier detection** consists in listening to the cable before transmitting
- the **collision detection** consists, for an emitter, in listening to the cable throughout all transmission to permanently compare the signal on the cable to what it should be (the emitter knows of course what it is emitting!); a difference is the symptom of a collision

It should be noticed that **collision detection is only feasible during the emission**. This will bring a significant constraint over the **minimum duration of emission**, as this figure shows.

The worst case occurs when the two transmitters S1 and S2, which are in competition for the cable, are located at the two ends. T_{prop} is the propagation time between S1 and S2.

- Let us suppose that S1 station starts to transmit at t=0; the frame is propagated towards S2
- at $t=T_{prop} - \xi$, the frame is about to reach S2; S2 does not detect the carrier yet and estimates it has the right to transmit
- at $t=T_{prop}$, the frame coming from S1 reaches S2, which detects the collision and stops immediately its frame;
- the jammed frame from S2 is propagated towards S1
- at $t=2T_{prop} - \xi$, **S1 will detect the collision provided it is still transmitting**

Therefore, any frame must last at least 2 propagation times.

Medium Allocation Control

CONTENTS

Ethernet

a particular case of IEEE 802.3

- caracteristics
  - 10 Mbit/s, 100 Mbits/s, 1Gbit/s)
  - CSMA/CD 1-persistant
  - MANCHESTER coding
  - $E_+ = 0.85V \quad E_- = -0.85V$
- media
  - coax 50Ω épais (thicklan or 10 BASE 5) (5=500m)
  - coax 50Ω fin (thinlan or 10 BASE 2) (2=200m)
  - twisted pair (10/100/1000 BASE T) (Twisted)
    - shielded (STP,FTP)
    - unshielded (UTP)
  - optical fibre

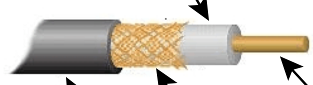
The famous Ethernet is named thus by reference to the *ether* which was supposed in the 19th century to be the support of electromagnetic waves. Ethernet was invented in the 70ies.

In fact, it is just a particular case of CSMA/CD, whose characteristics are given on this figure.

Several transmissions speeds and media are possible; currently, the most used is the unshielded twisted pair (UTP) at 100Mbit/s. (see further: Fast Ethernet)

Original Ethernet

CSMA/CD @ 10Mbit/s on a coaxial cable



- max propagation time
  - Lmax,segment = 500m
  - 4 repeaters max => Lmax = 2.5 km
  - c = 0.2 km / µs => $T_{prop,Cu}$ = 12,5µs
  - $T_{prop,repeater}$ < 1µs (qq bits)
  - $2T_{prop,total} = 2T_{prop,Cu} + 8T_{prop,repeater} < 33\mu s$
- min length for normal frame
  - 64 bytes
  - D=10 Mbit/s => normal frame ≥ 51.2µs
- Necessary Condition of detection is repected

$$\boxed{2\,T_{prop,Cu} + 8\,T_{rep} < 51.2\mu s}$$

- $T_{MAC} = 51.2\mu s$

Let us recall that the mechanism of CSMA/CD imposes a frame duration longer than twice the worst-case propagation time.

Let us see how this imposition is translated, for example in the original 10Mbit/s Ethernet:
- maximum length of the cable is of **500m** (to limit the attenuation); **4 repeaters** can be installed to lengthen the network and reach a total of **2,5 km**
- the minimum frame is fixed by the standard to 64 bytes=512 bits corresponding to a minimal duration of **51.2µs at 10Mbit/s**

The travel time in both directions is about 33µs and includes:
- the travel time in the cable, forwards and backwards (2x2.5km) in the cable: 25µs at 0,2km/µs
- crossing 2x4=8 times the repeaters => 8T_{rep} (delay of the repeaters < 1µs, the shift is just a few bits)

The minimal frame length of 512 bits, i.e. 51.2µs, is thus much larger than 33µs, which offers a good safety margin to ensure the collision detection.

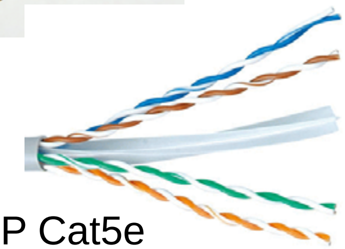
T_{MAC}=51.2µs is the unit of time in 10Mbit/s Ethernet and called " **MAC Time**".

Ethernet

CSMA/CD for Fast Ethernet

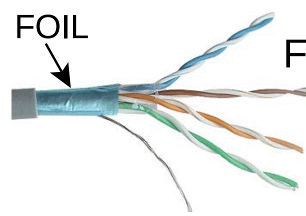
- 100 Mbit/s
  - min length of 64 bits is still used
  - T_{MAC}= 5.12µs
  - lenght reduced to 100m to ensure detection
  - only 1 (fast) repeater
- 1Gbit/s
  - 10m would be much too short => 100m
  - how to win a factor 10
    - other coding is required
      - bitrate = 5 x baudrate
    - 2 pairs in parallel in both directions
- Rem:
  - STP in industry (severe EMI problems)
  - FTP in buildings (could be mandatory)

UTP Cat5



UTP Cat5e

FOIL



FTP Cat5

At **100Mbit/s**, The minimum frame length of 512 bits still applies, hence the duration of the frame is 5.12µs; to ensure detection, the length of the cable has to be reduced to **100m and only 1 fast repeater** is authorized. The classical cable is called Unshielded Twisted Pairs (UTP Cat5) among which 2 pairs are used to ensure **full-duplex** transmission.

At **1Gbit/s**, it would be necessary to reduce the length to 10m, which is completely unrealistic. The same limit of 100m is kept, hence the frame length has to be kept also. Increasing the flow by a factor 10, while keeping collision detection relies on two different tricks:

- improve the modulation: the symbols are still sent à 100Mbaud/s (baud rate), but each symbol carries 5 bits of information and the bitrate is 500Mbit/s
- 2 pairs are used in each direction two double the flow

Better cables (UTP Cat5e) have to be used, a plastic twisted central cross is added to separate the pairs and reduce the parasitic capacitances and the crosstalk.

Rem: those unshielded UTP cables are cheap, but better cables exist if EMI (Electromagnetic interferences) have to be reduced (in emission and reception)

- in buildings **FTP** (Foiled Twisted Pairs) will probably become mandatory in the future; an aluminium foil is wrapped around the 4 twisted pairs
- in industry, the level of EMI is more severe (arc welding, electrophoresis, ...) and **STP** cable (Shielded Twisted Pairs) is frequently used. Each twisted pair is shielded individually. We shall see an example of STP in the chapter over the CAN fieldbus.

Consequently, it is better to use devices like switches and routers, which avoid the propagation of the collisions (see further).

Ethernet CSMA/CD

how to solve collision problem

- any station willing to emit awaits the absence of the carrier
- 2+ transmitting stations at the same time => collision
- emission is stopped (aborted frame is lost)
- each station waits randomly 0 or T before emitting again
- if 2nd collision => wait randomly 0,1,2 or 3T
- if i^{th} collision, wait $RAND(2^i - 1)T$ (max 1023T)
- => gradual reduction in the probability of collision
- => adaptation of the delay to the load of the network

- Ethernet gives only a probabilistic access to the medium
- no guarantee of access in a given time
- no improvement of the time of resolution if we increase the flow without reducing the length of the cable (to decrease T)

After the collision, the transmitters will naturally retry to emit. They will again enter in conflict if no measures are taken to avoid simultaneous emission. The algorithm implemented in Ethernet consists in reducing the probability of simultaneous re-emission by waiting a **random delay after a collision**. Each station draws a number between 0 and n and awaits n. T_{MAC} before emitting.

- after the 1^{st} collision: n=1
- after the 2^{nd} collision: n=3
- after the i^{th} collision: $n=2^i-1$

Exercise: show, on a simple example with only 2 nodes in competition, that the probability of collision is divided by 2 at each collision.

Ethernet provides thus a **probabilistic access** to the shared medium.

Compared to previous networks, Ethernet brought the advantage of not increasing unnecessarily the latency when the load of the network is weak; number N is adjusted automatically to the minimum required for one node to get the medium.

The latency to get the cable is a multiple of T_{MAC} which, for a given frame length, depends on the propagation time (i.e. on the length of the cable) but is independent of the bitrate. For this reason, increasing the bit rate is not a solution to accelerate the resolution of the collisions and to reduce the mean access time to the medium.

Efficiency of transmission

the bandwith of the cable cannot be fully used

- definitions
  - τ = frame duration
    = (bits/frame par trame) / bitrate
  - G = average number of **emitted** frames over τ
  - S = average number of **effectives** frames over τ
- ∃ simulation programs to estimate efficiency
  - realistic ➪ G < 1
  - collisions ➪ S < G <1
- efficiency
  - ➘ if number of nodes (load) ➚
  - ➚ frame length ➚ (delays collisions)

Let us introduce the concept or **efficiency** as the percentage of time corresponding to **valid frames** rated to the total transmission time.

Let us consider to simplify that we emit frames with a fixed length τ.

The average number G of frames over τ is thus ideally 1; actually, this is impossible because
- that would suppose that a station is always ready to emit
- the interframe delays have to be respected

We can define **S** as the average number of valid frames over τ; because of the collisions, some frames are lost, hence

$$S < G < 1$$

The efficiency is calculated by network simulators on the basis of statistical models of the traffic. We shall admit intuitively that the efficiency:

- falls with the load of the network (i.e. the number of stations wishing to transmit at the same time) because the percentage of collisions increases

- increases with the average length of the frames, because once a node has obtained the medium, the next collision cannot happen until the frame is finished.

802.3

composition of the frame

7	1	6	6	4	2	46-1500	4	>12
PRE	FSD	MAC DEST	MAC SRC	802.1Q	LD/ET	DATA	FCS	GAP

PRE = 01010101 (7 times)	preamble for synchro bit
FSD = 10101011	frame start delimiter
MAC DEST : 1111.....11111	broadcast (all)
1ugg..gg...xxxx	multicast (group gg..gg)
0ugg..gg..aaaa	unicast (node aaaaaa)
	u = 1 world address (7E13 !)
	u = 0 local addresses (isolated network)
802.1Q (optional)	VPN + QoS (8 priority levels)
LD = 46 .. 1500 or **1506+**	Length of DATA or **Ethertype**
DATA	Data from LLC or IP
FCS	Frame Check Sequence (CRC)
GAP	Inter Frame GAP

Let us examine more closely the structure of a frame (the numbers in the first line are in bytes):

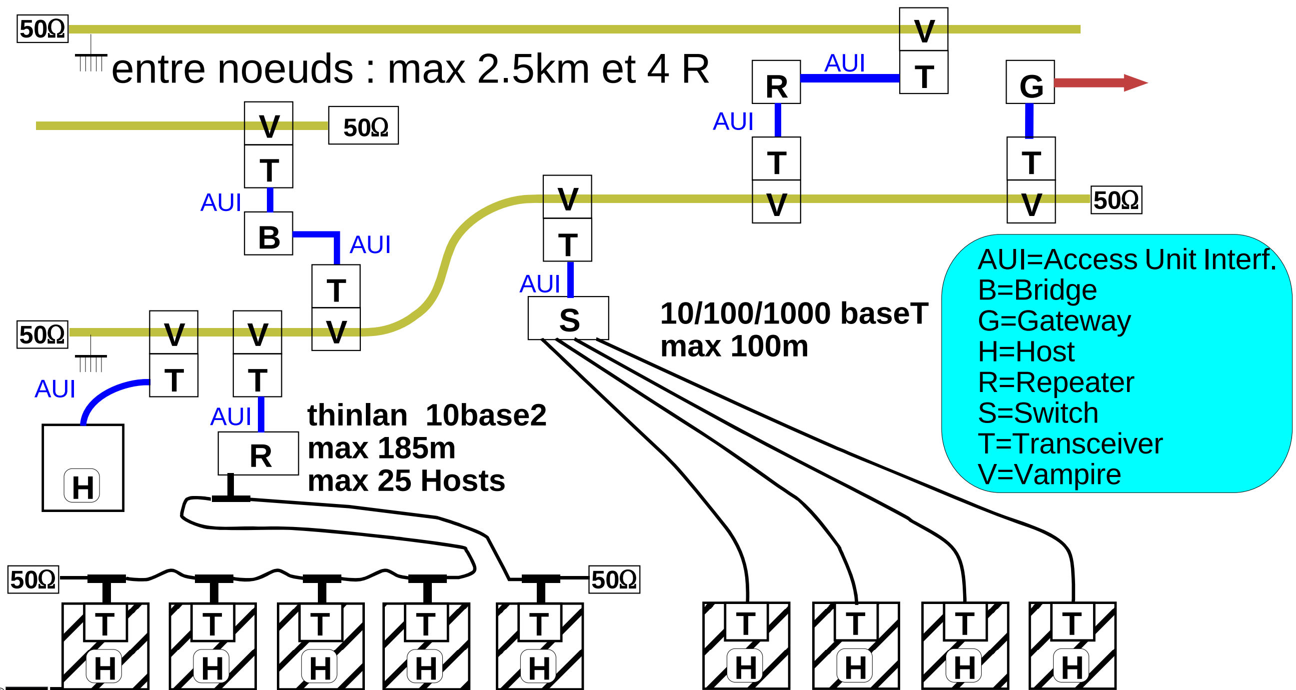
- a **preamble**, which is a regular succession of bits intended to synchronize the local clock of the receiver on the regular edges of the periodic preamble; a good synchronization is necessary to correctly sample the data
- a **frame start delimiter** announcing the beginning of useful information
- the **addresses** of the receiver and of the transmitter called **MAC addresses** in 48 bits; this address is (or should be) unique for each single network card produced in the world (the first 3 bytes indicate the manufacturer, the last 3 bytes a serial number); notice the possibility of emitting towards
  - all nodes "broadcast"
  - a group of nodes "multicast"
  - a single node "unicast"
- an optional field **802.1Q**, which has been standardized later to introduce
  - the concept of VPN (Virtual Private Network) a company is no more obliged to lease telecom lines to build its own network; a mechanism of authentication allows to use internet as a vector
  - 3 bits to deal with Quality of Service (QoS) and add a notion of priority which was a real lack in Ethernet; the **8 priority levels** are (Background, Best Effort, Excellent Effort, Critical Applications, Video<100ms latency, Voice<10 ms, Internetwork Control, Network Control)
- a field **LD**/**ET** announcing
  - **from 46 to 1500**: LD the length of the data; this is the strictest original 802.3 standard associated to LLC 802.2 as the upper layer. The minimum of 46 is imposed by the collision detection.
  - **≥1506**: it indicates the Ethertype, i.e. the type of protocol which is encapsulated in the data field (IPv4, IPv6, ARP, AppleTalk, Ethercat[1], Profinet[1], Sercos[1], PPPoE, Jumbo Frames,...). This is an older standard incorporated later in an extension of 802.3. Both frames are compatible on the same network. It is the most used frame when Ethernet is associated to TCP/IP; the upper layer is directly IP
- data (with a maximum of 1500 bytes) also called "payload" like in rockets; those data are the PDU coming from upper layer LLC(802.3) or IP(TCP/IP)
- a **frame check sequence** or CRC (Cyclic Redundancy Check) able to detect and correct errors in the frame, with a very low probability of declaring as valid a false frame.
- the **inter frame gap**, the cable should be "idle" for at least the duration of 12 bytes

[1] these are industrial networks based upon ethernet

Ethernet

cabling (historical)

10base5 thicklan ou backbone : max 500m , max 100 nodes



This figure shows a typical ethernet cabling when coax was the main standard.
Nowadays, the coax backbone is replaced by optical fibres in a star configuration, and 100Mbit/1Gbit Ethernet, use a star wiring (all cables are plugged in switches, like shown at the bottom right of this figure)

Ethernet

conclusions on wired 802.3 (1st generations)

- advantages
  - widespread and cheap standard
  - passive simple support
  - good performances
  - facility to add a node even under operation (live)
- disadvantages
  - η ➘ with the load
  - coax cable
    - shared medium: half-duplex, collisions
    - cabling constraints (length, curvature)
    - defects in wires are difficult to locate
- disadvantages for real time
  - not efficient for small frames (padding to 46 bytes at least)
  - probabilistic, hence **non-deterministic access**
  - concept of priority is optional (802.1Q)
  - => development of **special real-time networks**

Ethernet has become an extraordinary world-wide success; its advantages were prominent compared to its drawbacks.

For a long time, it has not be used in real-time industrial control, chiefly because

- the minimum lenght of the frame(64 bytes among which at least 46 for data) is a waste of bandwith when you have to transmit a single temperature in a 16-bits integer.

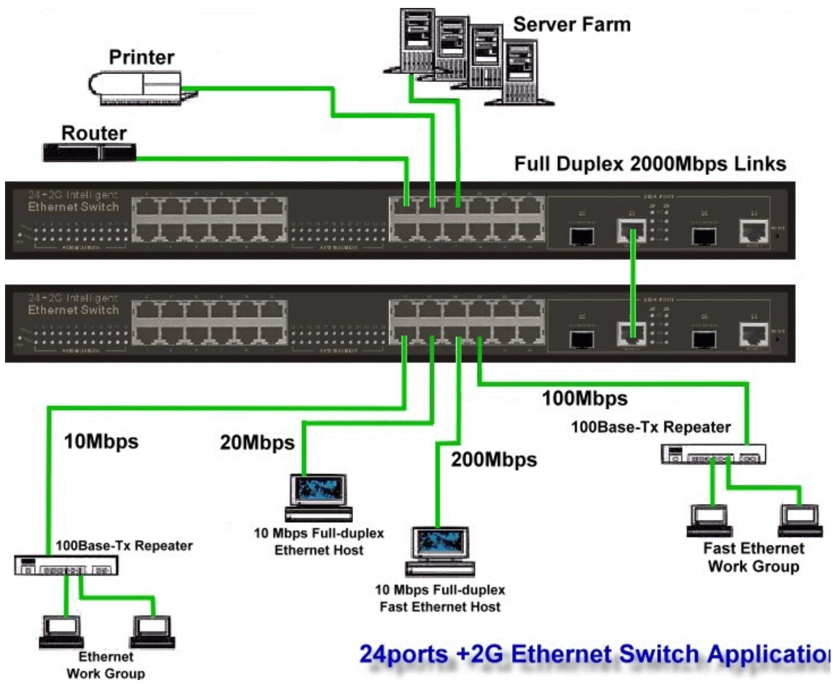
- a **probabilistic** access is just incompatible with the **determinism** required in real-time

For that reason, a lot of **real-time networks** have been invented.

Ethernet

Ethernet for real-time: Fast Switched Ethernet

- fast
  - low load
- 2 pairs
  - full-duplex
- switches
  - no collisions
  - just latency
  - full bandwith x n/2
  - several speeds



The actual trend is a large development of Ethernet in industry and the key of this evolution is the appearance of **Fast Ethernet** (100Mbit/s) and cheap **switches**.

Fast Ethernet brought decisive advantages:
- **100Mbit/s**
  - the shortest frame is only 5.12µs
  - the load for industrial traffic is a small percentage of the bandwidth and ethernet behaves very well when the load is low
- **twisted pair cabling** UTP/STP/FTP
  - fewer constraints (curvature is no more a problem)
  - 2 pairs, allowing **full-duplex**, which doubles the bandwidth
  - star topology with 1 node per cable, errors are very easy to fix

When Fast Ethernet became popular the centre of the star cabling was generally a **hub** (i.e. a repeater) which means that all cables of the star were subject to collision since all frames were repeated on all segments. Switches were very expensive.

The spectacular drop in the prices of **switches** was the final key
- the switch builds a table containing "which node on which input"
- a switch extracts the destination addresses in the frame to propagate it only to the cable of the receiver
- since each node has got its own cable to the switch, a **collision-less network** is obtained, hence, the access is no more probabilistic.
- if the destination cable is busy, the frame is buffered: the switch is seen by a real-time application as **latency**
- the **full bandwidth** is available **on simultaneous connections** between several transmitter-receiver pairs
- the information is more difficult to "sniff" because information is only propagated to one node
- the switch adapts automatically the speed of transmission to the speed of the nodes.

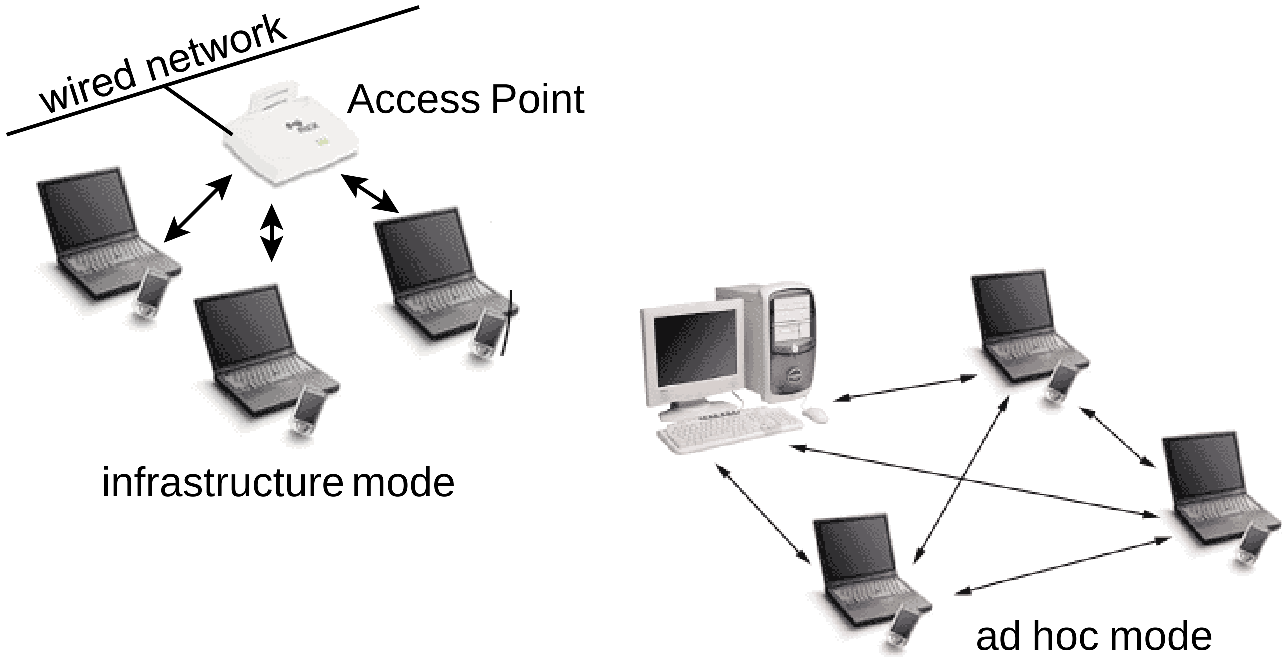
Medium Allocation Control

CONTENTS

- Introduction
- IEEE 802.3 : CSMA/CD
- **IEEE 802.11 : WiFi**
- IEEE 802.5 : Token Ring
- IEEE 802.4 : Token Bus
- Conclusions

802.11: WiFi

2 main modes



The 802.11 standard for wireless communications defines two modes:

In **infrastructure mode**, the wireless network consists at least of:
- an access point connected to a wired network. This access point is usually composed of a radio emitter/receiver, a wired network card and a "bridging" software
- a set of wireless nodes

This configuration is named BSS (Basic Service Set). An Extended Service Set (ESS) is a set of at least two BSS forming only one subnetwork.

The **ad hoc mode,** also called point-to-point, or Independent Basic Service (IBSS), represents simply a group of wireless 802.11 nodes which communicate directly with each other, without any access point to a wired network. This mode makes it possible to quickly and simply create a wireless network where
- no wired network is present
- the infrastructure mode is not required for the awaited services
- the access to a wired network is prohibited

802.11: Wifi

Lower layers

802.2 LLC			#2a
802.11 MAC			#2b
IR	FH	DS	#1

IR : Infrarouge

FH : *Frequency Hopping* < 2Mbit/s

DS : *Direct Sequence* < 11Mbit/s

$\left.\begin{matrix} \\ \end{matrix}\right\}$ ISM 2.4GHz

The 802.11 standard comes under the LLC (802.2) common to all the other 802 standards; it defines:

- a MAC layer specific to each wireless media used. The 48-bit MAC address structure is the same for all the other 802 LAN, which simplifies the bridge between wired and wireless networks

- 3 wireless physical layers are used :
  - 1 infra-red (IR)
  - 2 incompatible radio layers with spread-spectrum modulation
    - FH (*Frequency Hopping*) limited to 2Mbit/s
    - DS (*Direct Sequence)* for 11Mbit/s and above

The definition of these modulations is outside the scope of this course. Let us only mention that spreading the spectrum improves reliability, increases the flow and makes it possible to divide the spectrum between several stations without explicit co-operation and with a minimum of interferences.

The frequency band is the ISM (scientific and medical) at 2.4GHz, low power, low range (about 100m) and which does not require any licence.

Let us remark that in wired TCP/IP networks, the MAC layer#2a can be directly below the IP layer#3, bypassing the LLC #2b.

In 802.11 the IP protocol is encapsulated in the 802.2 frames of LLC, to benefit from the error management because the rate of error is much higher in wireless networks.

802.11: WiFi

wireless Collision Detection is impossible

- CD (Collision Detection)
  - based on transceiver to be able to emit and listen simultaneously
- radio is not copper: transceivers cannot be built
  - half-duplex => cannot receive while transmitting
  - full-duplex uses two different channels => cannot receive what you transmit

Collision detection (CD) is based on the **transceiver**: a node must be able to compare immediately via the receiver if the data on the medium is what he is currently transmitting. This is possible in wired networks, not in wireless ones, because the **concept of transceiver cannot be extended to radio**.

Indeed, using radio as a medium implies that you can never listen to what you transmit because

- either you work in half-duplex (the most common case) i.e. the communication channel is unique and the antenna cannot work simultaneously in transmission and reception

- or you work in full-duplex; in that case, two different channels are used for transmission and reception and you are not able to listen to what you transmit.

802.11

CSMA/CA Collision avoidance

- carrier detect and collision avoidance
  - transmitter node
    - listens to the carrier before emitting
    - if channel free (+Gap), waits a random delay
    - if channel still free: transmits
  - receiver node
    - if frame is correct, returns ACK frame
  - transmitter node
    - if ACK frame not detected => supposed collision and frame transmitted again with same random delay
- ACK is good for QoS
  - collisions + all other interferences
- efficiency is lower in wireless networks
  - half-duplex
  - ACK mechanism loads the network

Since the collision detection in unavailable, 802.11 uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):

- a station which wishes to emit starts by listening to the radio channel (Carrier Sense)

- if no activity is detected during a lapse of time equal to a defined GAP, the channel is free and the transmitter awaits a random time. If the channel is still free, transmission can start.

- if a correct frame is received, the receiver sends an acknowledgement frame (ACK); when the transmitter receives the ACK, the process is finished

- if ACK is not detected by the transmitting station (because the original frame was not correct or because the ACK itself was jammed), a collision is supposed and transmission process is restarted from the beginning after of another random time.

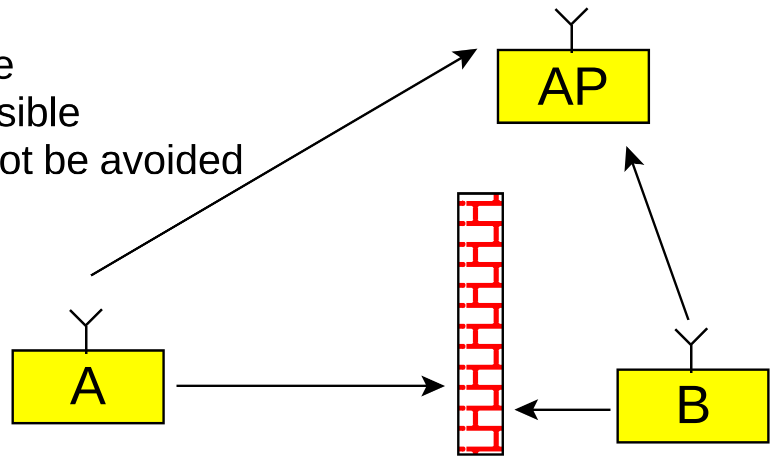
Notice that this ACK mechanism deals with collisions, but also with any other radio interferences (reflexions, diffractions, attenuations, EMI) and contributes to the quality of service (QoS)

However, it adds to 802.11 a load which did not exist in 802.3, so that a wireless LAN 802.11 will always have lower performances than an equivalent wired LAN.
Moreover, most modern wired LAN use two pairs of wires to work in full-duplex, whereas, WiFi is generally in half-duplex, meaning that the nominal bitrate is divided by a factor two.

802.11: WiFi

the "hidden node" problem jeopardizes CS and CA

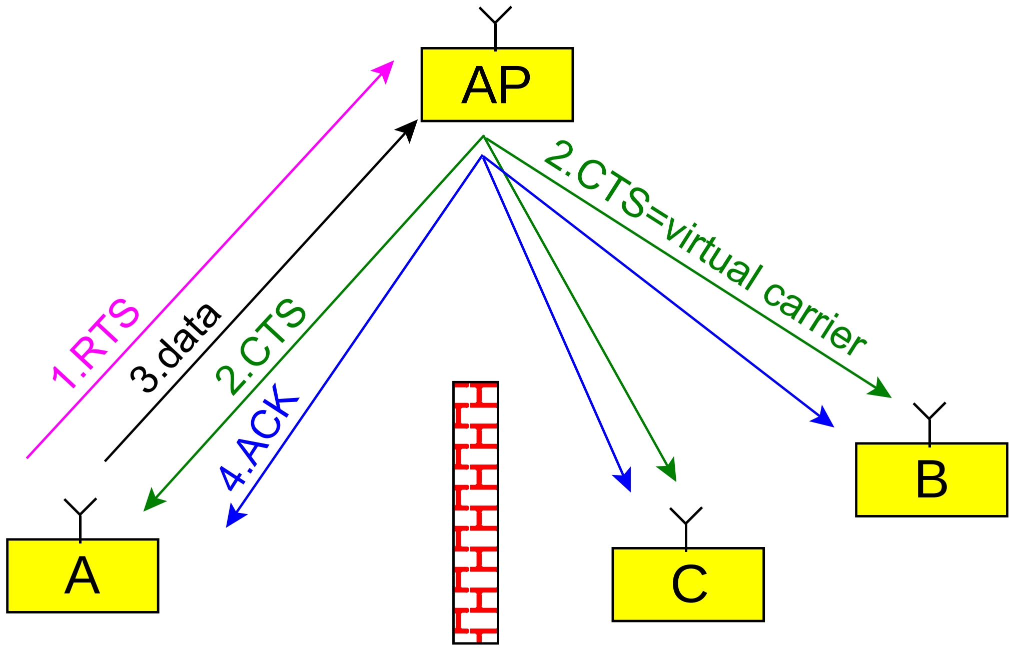
- A and B
  - both see the Access Point AP
  - do not see each other because
    - outside respective range of transmission
    - obstacle
- big problem
  - carrier sense impossible
  - a fortiori CA also impossible
  - collision at the AP cannot be avoided



A frequent problem is the **hidden node**. Carrier detection and Collision Avoidance can be impossible because two nodes cannot see each other and send simultaneously a frame to the Access Point.

802.11: Wifi

improved transmission: RTS/CTS



To solve the hidden node problem, 802.11 adds on the MAC layer an optional protocol: RTS/CTS (Request to Send/Clear to Send).

When this function is used,
- a transmitter node A begins by sending an RTS frame to the Access Point, which is the only one to have the visibility on the whole subnet. The RTS contains indications of data length and speed, so that an estimation of the transmission time can be made.
- When the channel is free, the AP will broadcast a CTS frame to all nodes like B and C. CTS is interpreted as a **virtual carrier** that will delay all tentative of transmission by the B and C nodes
- node A can transmit the data without collision
- the AP sends the ACK, which unlocks the subnet (there must be a timeout in case ACK is not sent, of course)

Owing to the fact that the protocol RTS/CTS increases the load of the network by blocking the channel temporarily, RTS/CTS is generally reserved for the largest data whose retransmission would consume too much bandwidth.

802.11: Wifi

improve robustness

- radio is prone to interferences
- 32-bit CRC
  - systematic error detection/correction
  - management of residual errors by LLC[1]
- fragmentation of data
  - useful if
    - heavy-loaded channel
    - much interferences
  - retransmission of large data => bandwidth lost
  - short data are less susceptible to be jammed

[1]by-passed in Ethernet/IP/TCP

The radio medium being prone to interferences, the 802.11 MAC layer offers two other characteristics contributing to improve its robustness

- a **32-bits CRC** and error management: this feature is generally bypassed in *wired* Ethernet/IP/TCP stack, because errors are rare and TCP is in charge of the robustness of the transmission

- the **fragmentation of the data**, particularly useful in very congested environments or when the interferences pose problems (large packets of data have more risks of corruption)

Medium Allocation Control

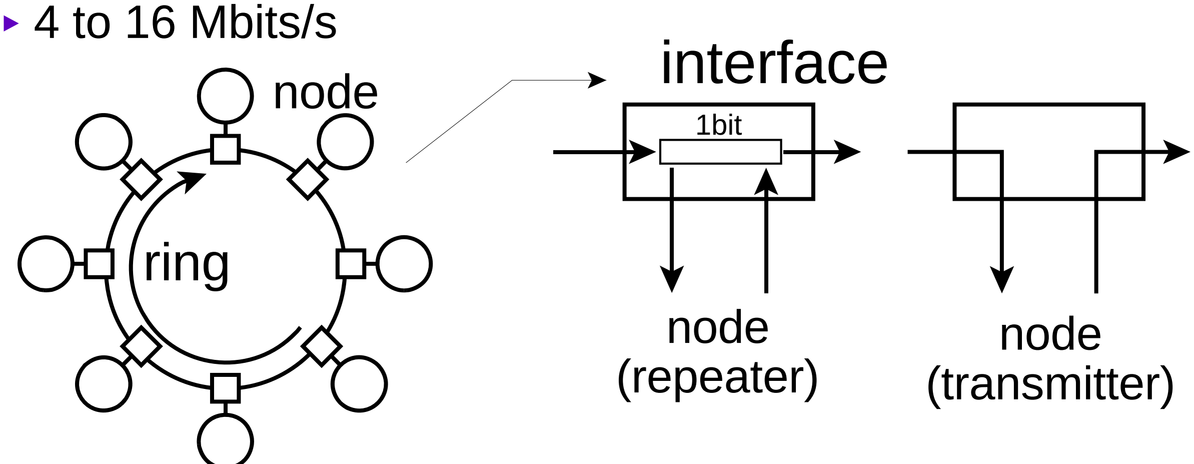
CONTENTS

- Introduction
- IEEE 802.3 : CSMA/CD
- IEEE 802.11 : WiFi
- **IEEE 802.5 : Token Ring**
- IEEE 802.4 : Token Bus
- Conclusions

Token Ring

structure

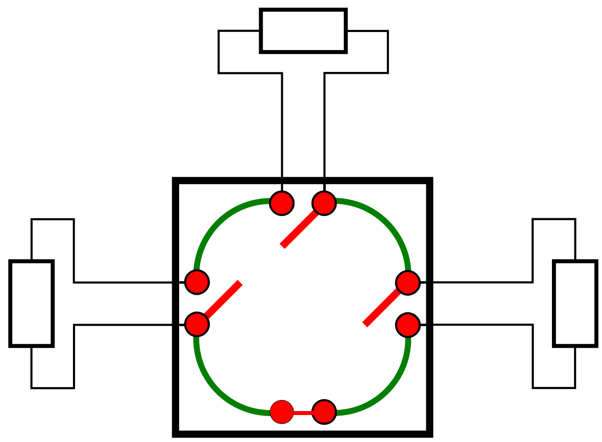
- succession of point-to -point links
- each node plays the role of repeater
- delay of 1 bit for tests and processing of frames
- fully digital
- 4 to 16 Mbits/s



Token Ring

Cabling

- twisted pairs, coax, fibre
- virtual star (connection box)
- extension: station replaced by box
- simple (de)connection
- 260 nodes max
- easy diagnosis
- sometimes difficult wiring



Token Ring

frame

1	1	1	2 ou 6	2 ou 6	n	4	1	1
SD	AC	FC	ADD DEST	ADD SRC	DATA	CTRL	ED	FS

SD	Start Delimiter
AC	Access Control
FC	Frame Control
DATA	any length
CTRL	CRC 32 bits
ED	End Delimiter
FS	Frame Status

TOKEN = SIMPLIFIED FRAME (3 bytes)

1	1	1
SD	AC	FC

Token Ring

Status / errors

1	1	1	2 ou 6	2 ou 6	n	4	1	1
SD	AC	FC	ADD DEST	ADR SRC	DATA	CTRL	**ED**	**FS**

- ED end delimiter
  - bit indicating CRC error (set by any repeater)
- FS Frame Status
  - 2 fields
    - A = address has been recognized
    - C = frame has been copied
  - the transmitter resets A=0 & C=0
  - the receiver sets A=1 & C=1 if frame copied without error
  - the transmitter reads FS ➜ 3 possibilities
    - A=0 & C=0: address invalid
    - A=1 & C=0: address OK, frame not copied
    - A=1 & C=1: address OK, frame copied

Token Ring

protocol (1)

- no traffic = the token circulates
- the node which wants to emit
  - waits until it sees the token passing
  - modifies 1 bit of the token which becomes a frame
  - starts to transmit this frame
- the node which recognizes its address
  - swallows the frame progressively
  - retransmits it with a delay of 1 bit
  - acknowledges at the end of the frame by FS and ED

Token Ring

protocol (2)

- the transmitter
  - receives the first re-transmitted bits and throws them
  - continues to transmit simultaneously
  - at the end of the frame, checks FS et ED
    - if not OK, retries
    - if OK
      - transmits to the next frame (!10 ms max for all)
      - releases the token when the transmission is finished

Token Ring

priority

1	1	1	2 ou 6	2 ou 6	n	4	1	1
SD	**AC**	FC	ADD DEST	ADD SRC	DATA	CTRL	ED	FS

- AC access control
  - 3 bits of priority ➜ level n
    - a station can emit only if it wants to transmit a frame whose level is > N
  - zone for reservation
    - a node can register the level of priority of its frame if no former reservation has been at a higher level
  - mechanism to avoid abusive rising of the level

Token Ring

occupation of the ring

- the cable contains few bits
  - B = 4 Mbit/s = 4 bit/µs
  - c = 200 m/µs
  - L = 800 m

  } 16 bits
- the 24-bits token turns permanently
- ⇒ need for a supplementarycmemory
  - 1 bit in each repeater
  - possible supplement provided by the **monitor** node

Token Ring

monitor

- role of the monitor
  - purge the invalid frames
  - regenerate the token
  - provide the complement of memory for the token
- creation of the monitor
  - the 1st station which sees the absence of monitor
    - launches a special frame "seek token"
    - if this frame returns intact
      - elects itself as the monitor
      - inject the token in the ring

Token Ring

conclusions

- advantages
  - varied supports, unlimited length
  - defects easy to locate
  - cheap
  - concept of priority
  - high efficiency
  - ∃ deterministic access time
- disadvantages
  - monitor = weak point
  - long latency at weak load
  - heavy wiring in much cases
  - problem if the ring opens
  - has lost the fight against Ethernet

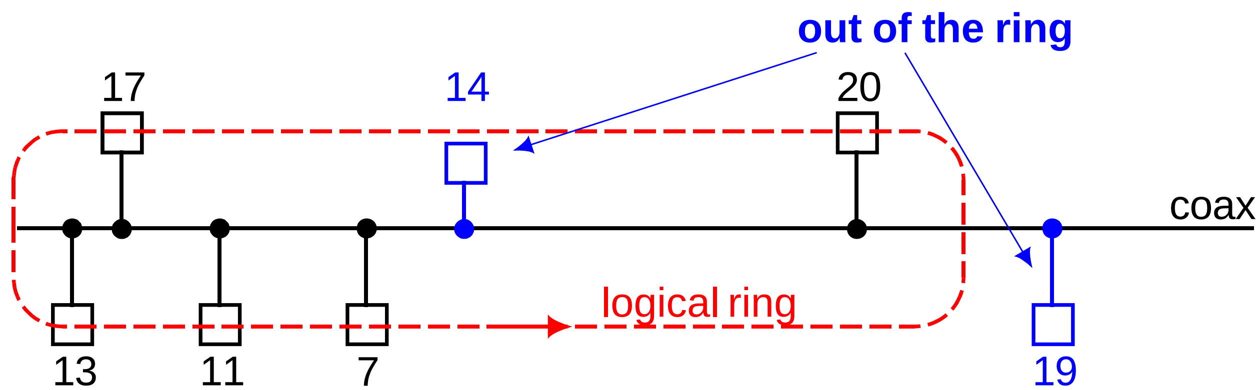
Medium Allocation Control

CONTENTS

Token Bus

principles

- goals: to reconcile the advantages
  - of token ring: determinism of the access
  - of Ethernet: broadcast on a bus
- implementation
  - logical ring traversed by descending node number



Token Bus

conclusions

- advantages
  - determinism
  - management of 4 levels of priority
  - guaranteed minimum flow
  - good efficiency for any frame length
  - connection/deconnection at the logical level
  - broadband multiplexable medium
- disadvantages
  - complex physical layer
  - complex protocol
  - latency at weak load
  - what happens if token lost in critical period?

Medium Allocation Control

CONTENTS

Conclusion

- enormous penetration of Ethernet
- industrial real-time buses
  - token bus: MAP, TOP (abandoned)
  - **ethernet** (fast switched)
  - other standards : **field busses**