Université Grenoble Alpes

1. Networks

http://www.gipsa-lab.grenoble-inp.fr/%7Ejean-marc.thiriet/miscit/miscit_en.html

MISCIT

jean-marc.thiriet@univ-grenoble-alpes.fr

Condensed CV

jean-marc.thiriet@univ-grenoble-alpes.fr

UGA Université Grenoble Alpes

Docteur (Ph.D.) Université Henri Poincaré Nancy 1: February 1993

* Associate Pr. Université Henri Poincaré Nancy 1 1993-2005
* Habilitation à Diriger des Recherches UHP-Nancy 1: December 2004
  DEPENDABILITY OF INTELLIGENT DISTRIBUTED CONTROL SYSTEMS
* Full Professor Univ. Grenoble Alpes since 2005
  Head of the GIPSA-Lab Research Lab (April 2011-December 2015)
  Research in the dependability of automation systems which integrates communication networks (Networked Control Systems) and cyber-security of cyber-physical systems (smart grids, drones)
  Teaching in networks, network security, signal processing, automatic control
  Education projects
  - Asean-Factori 4.0
  - SALEIE: Strategic ALignment of Electrical and Information Engineering in European Higher Education Institutions

From Industry 1.0 to Industry 4.0…

Industry 1.0 : mechanization, mechanical energy (water, steam), ex: agriculture , XIXth century

Industry 2.0 : mass production, electricity, ex: car factory ~from 1920s to 1970s

Industry 3.0 : automation (robots) => First PLCs (Programmable Logic Controllers) computer, ex: pharmacy, food, 1980

Industry 4.0 : Cyber-physical systems, communication (virtual tools: Cloud), ex: smart cities, Nowadays

And Industry 5.0…

Industry 5.0 :

Societal impact ***Technological evolution***

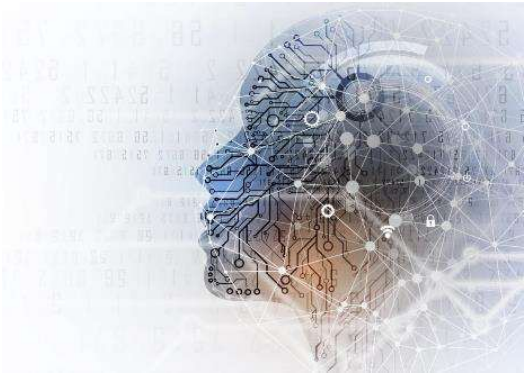
Resilience

Collaborative robotics

Human-centered…

Sustainability

Artificial intelligence



From Industry 1.0 to Industry 4.0…

Purposes: Production, minimal cost

- Production strategy => to product
- Maintenance strategy => to take care of the production tools
- Logistics and organization strategy => to organize production, transport and maintenance in the best way

Industry 4.0: some challenges

PARCE QUE CERTAINS SYSTÈMES SONT CRITIQUES
NOS SERVICES DATACENTER AFFICHENT 100% DE DISPONIBILITÉ DEPUIS 10 ANS

Certification ISO 27001 pour les services Datacenter, Cloud, hébergement, supervision NOC/SOC, administration, innovation, commercialisation

Certification Hébergeur de données de santé sur les 6 périmètres

Certification

Organisation

L'usine du futur devrait faire la part belle à la 5G plutôt qu'aux réseaux LPWAN. Ces derniers pourront servir cependant à l'optimisation des bâtiments.

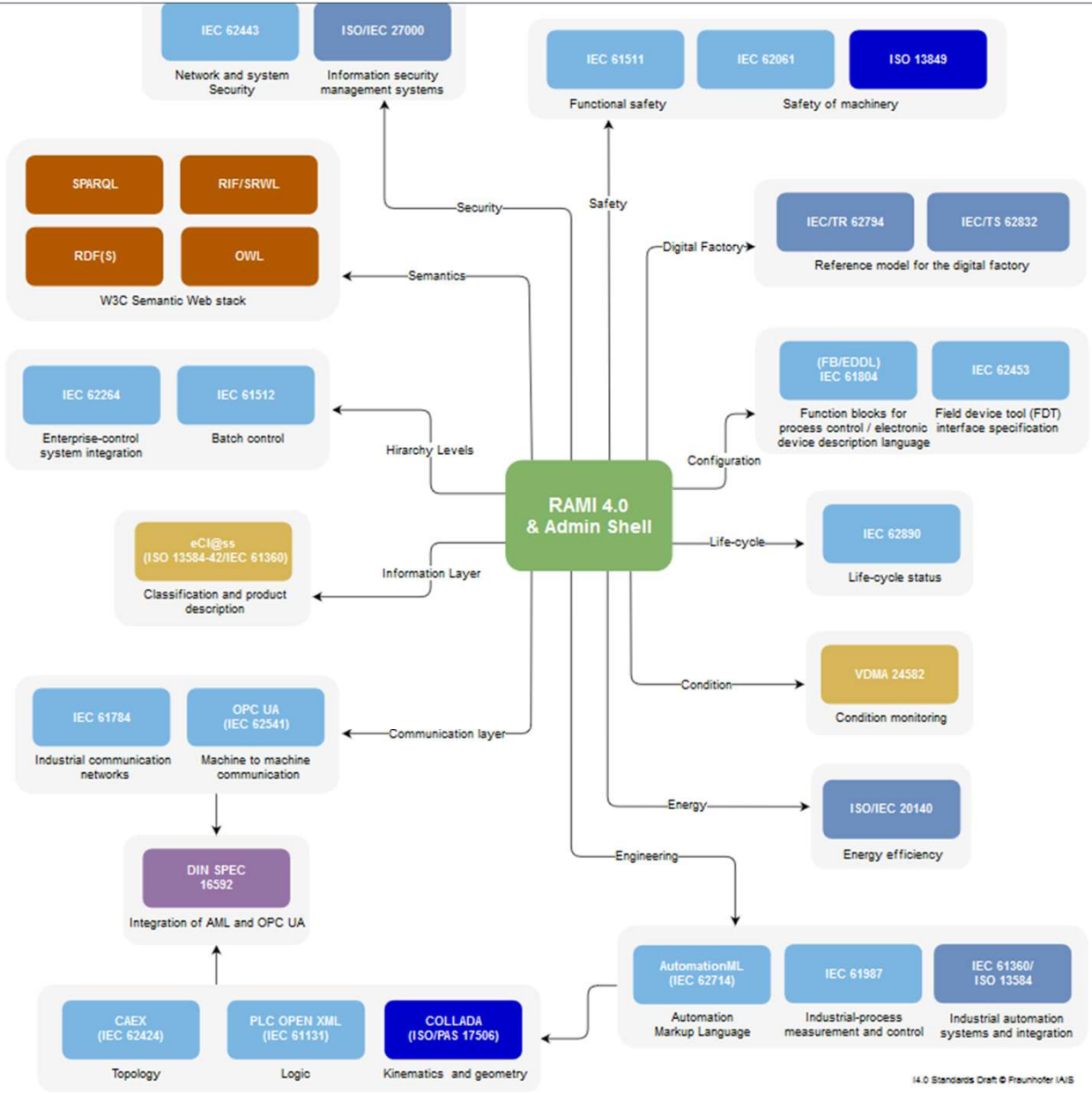
« New » networks: 5G

Certification

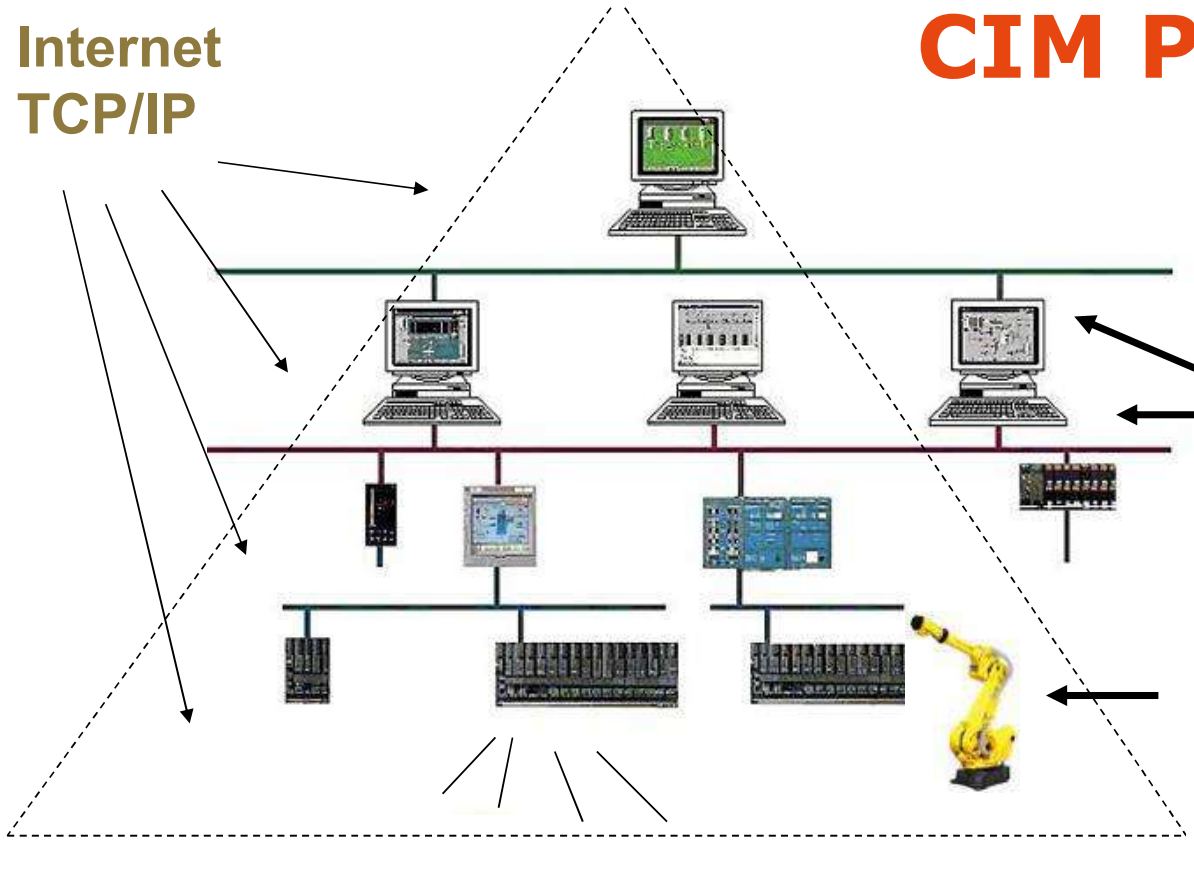
Standards…

State of the Art
Best practises
In security

Quality
Assurance
processes



CIM Pyramid



Computer-integrated manufacturing (**CIM**)
Describe the complete automation of manufacturing processes
Several network layers

Convergence between IT and cyber-physical systems

US Black-out, 2003

INFRASTRUCTURE

Industrial
Control
Systems (ICS)

Smart grids

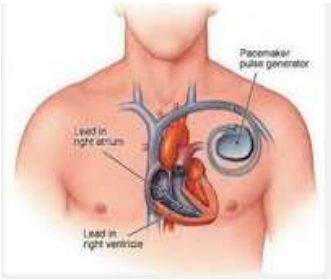
Cyber attack ukrainian power network, Dec. 2015

- Integrity of the information and communication infrastructure

→ Challenge: DEPENDABILITY (RAMS Reliability, Availability, Security & Safety, Maintainability)

EMBEDDED SYSTEMS

Drones
Autonomous vehicles
Connected objects



Maroochy shire, Stuxnet, CrashOverride

Context

Methodology, standards **Science** **Applications** **Societal**

1. Dependability : Confidence in the system to ensure its mission without risk (or with a risk management)
   - => Co-design approach (Network QoS ⇔ System QoC)
2. Functional safety: part of the overall safety that depends on a system or equipment operating correctly in response to its inputs [IEC 61508]
3. Cyber-security: Cyber security is the protection of systems, networks and data in cyberspace [www.itgovernance.co.uk, www.ssi.gouv.fr]
4. Networked Control Systems: Control System closed through a network
5. Complex systems, infrastructure, distributed systems
6. Embedded system, autonomous system, connected objects
7. ICS : Industrial Control Systems
8. IoT: Internet of Things, IIoT: Industrial Internet of Things
9. Cyber-physical systems (CPS): Marrying physicality and computation [persyval-lab.org]
10. Our interest: To analyse CPS from the point of view of the potential impact of the system in the physical world (dependability point of view) due to a cyber-attack (attack in the digital world) and define the ways to protect it

Course (master Miscit)

- Security and administration of networks
  - 18 hours : Course and exercises

- Labs
  - 15 hours « networks, security » (Mr Lubineau)

Networks

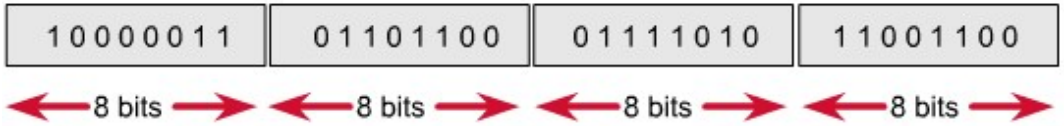
Some important aspects

- OSI model
- Physical layers
- Access control methods
- IP Addressing

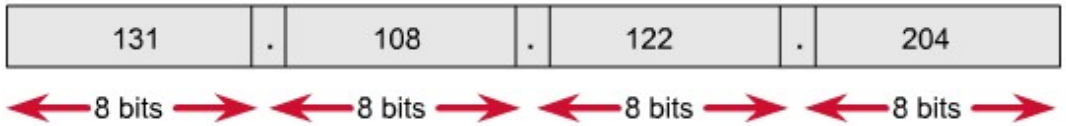
IP adressing V4

- Adresse Internet Protocole (Version 4) :
  - **32 bits address encoded (4 bytes)**
  - **Split in 2 complementary parts :**
  - Network reference number network()
  - Unit/machine host number (host)

  - **Division in 8 bit- (1 byte-) groups separated by points**

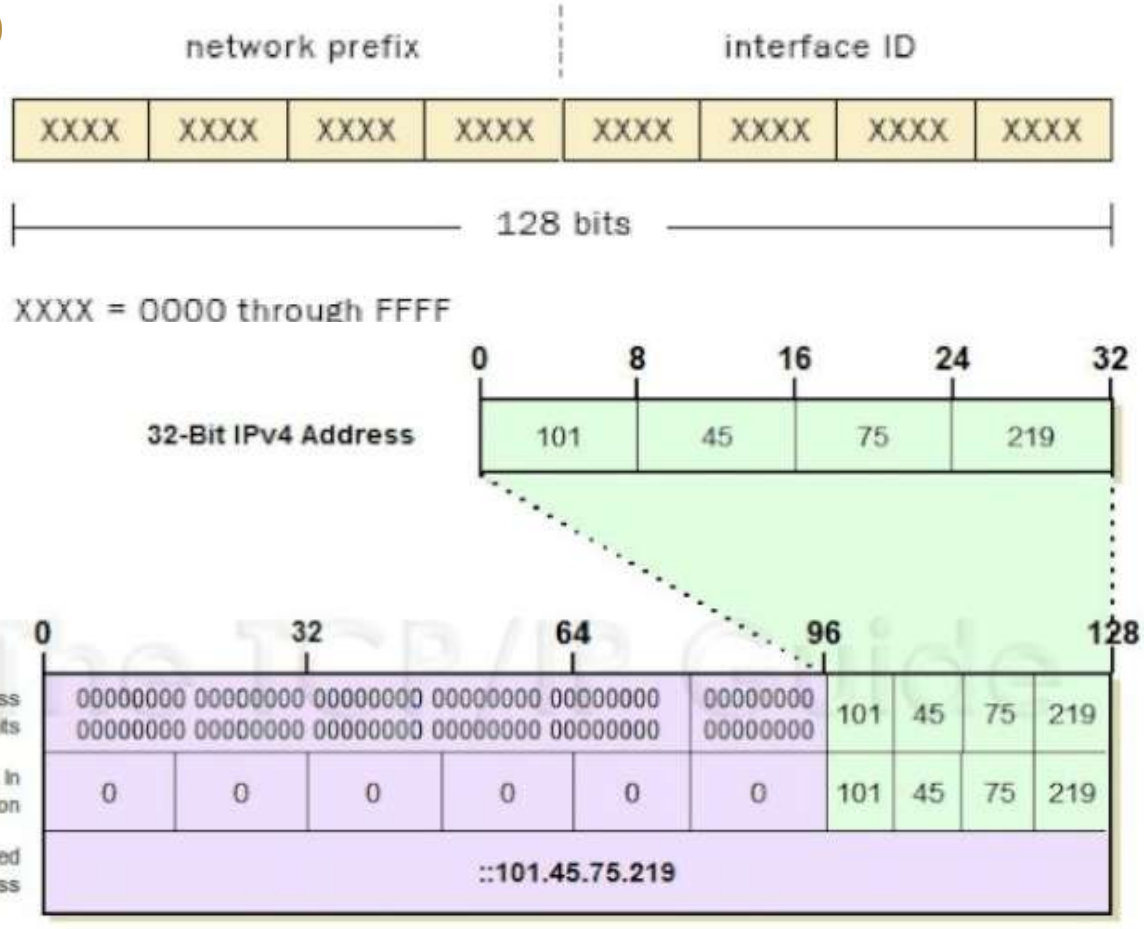


  - **For simplification, representation in a decimal form**

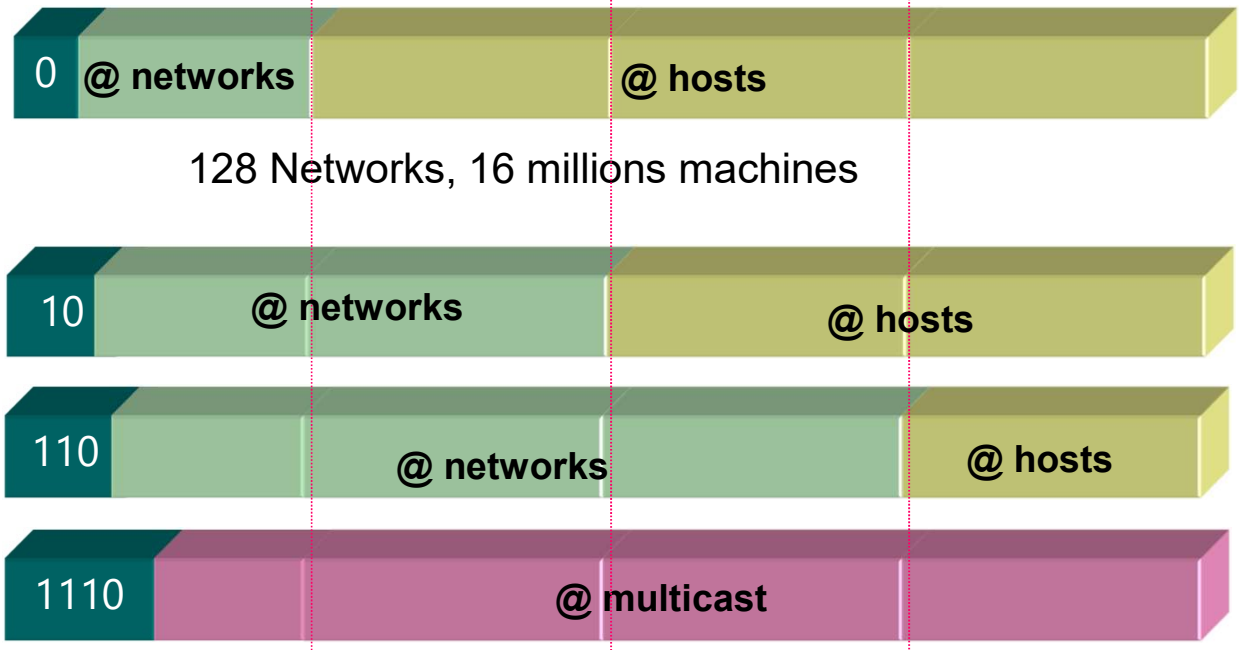


IP adressing V6

- New Adressing Internet Protocole (Version 6) :
  - **128 bits addressing encoded (16 bytes)**
  - **Split in 2 complementary parts :**
  - Network prefix network()
  - Interface ID Host number (host)



Internet Protocol adresses classes



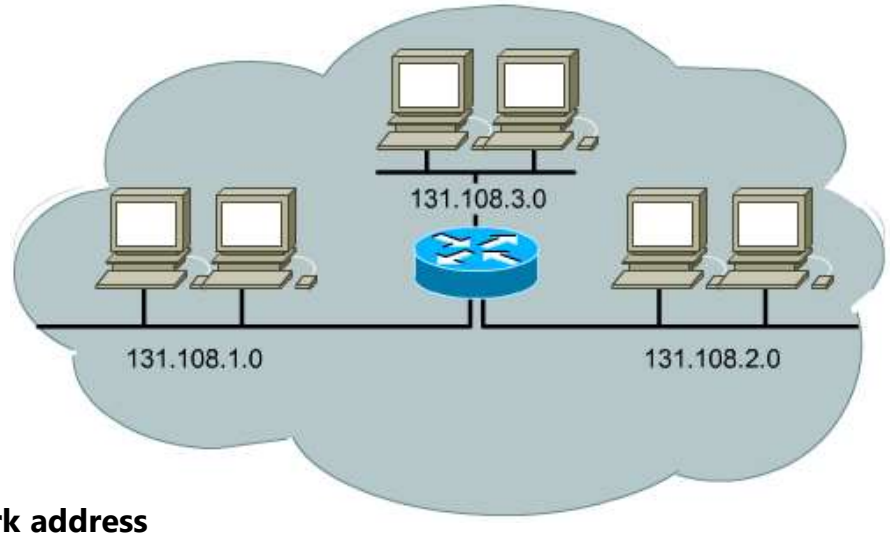
Dedicated adress: for example in classe A: 0.0.0.0

loopback adresse in class A: 127.0.0.0

Broadcast adress : class A: X.255.255.255

IP Subnets network examples

- Exemple:
  - **B class** with IP address : **131.108.0.0**, (B class is also define /16)
  - We want to split or local area network (LAN) in **3 subnets class network with the address :**
    - 131.108.1.0 /16 subnet 1
    - 131.108.2.0 /16 subnet 2
    - 131.108.3.0 /16 subnet 3



131 108 03 00

1000.0011 . 0110.1100 . 0000.0011. 0000.0000

Mask / 16

1111.1111 . 1111.1111 . 0000.0000. 0000.0000

Address & Mask / 16

1000.0011 . 0110.1100 . 0000.0000. 0000.0000 **Global network address**

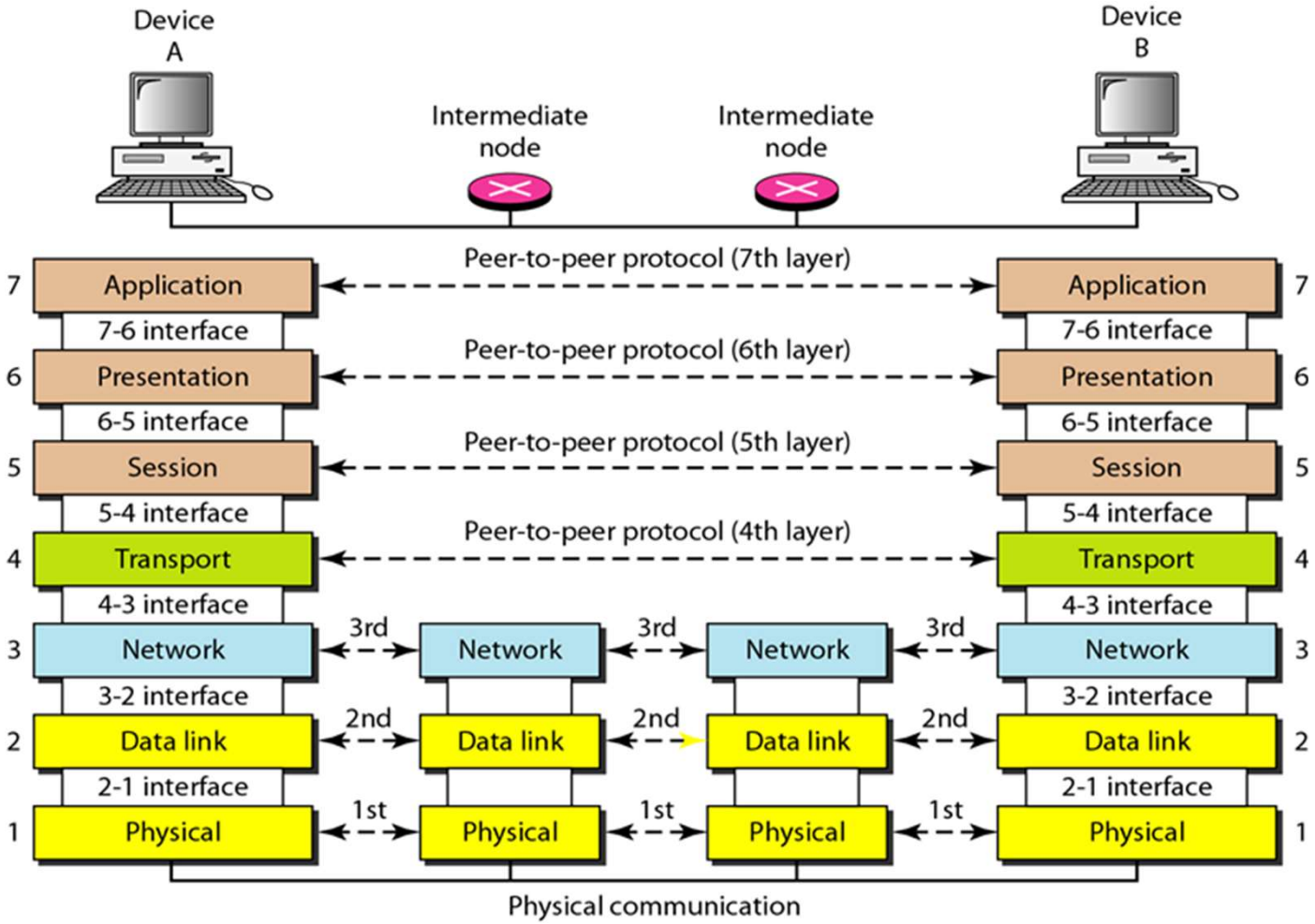
Hosts

1000.0011 . 0110.1100 . 0000.0000. 0000.0001 **1st host (machine)**
1000.0011 . 0110.1100 . 1111.1111. 1111.1110 **Last host (machine)**
1000.0011 . 0110.1100 . 1111.1111. 1111.1110 **Broadcast address (for all the host in the network)**

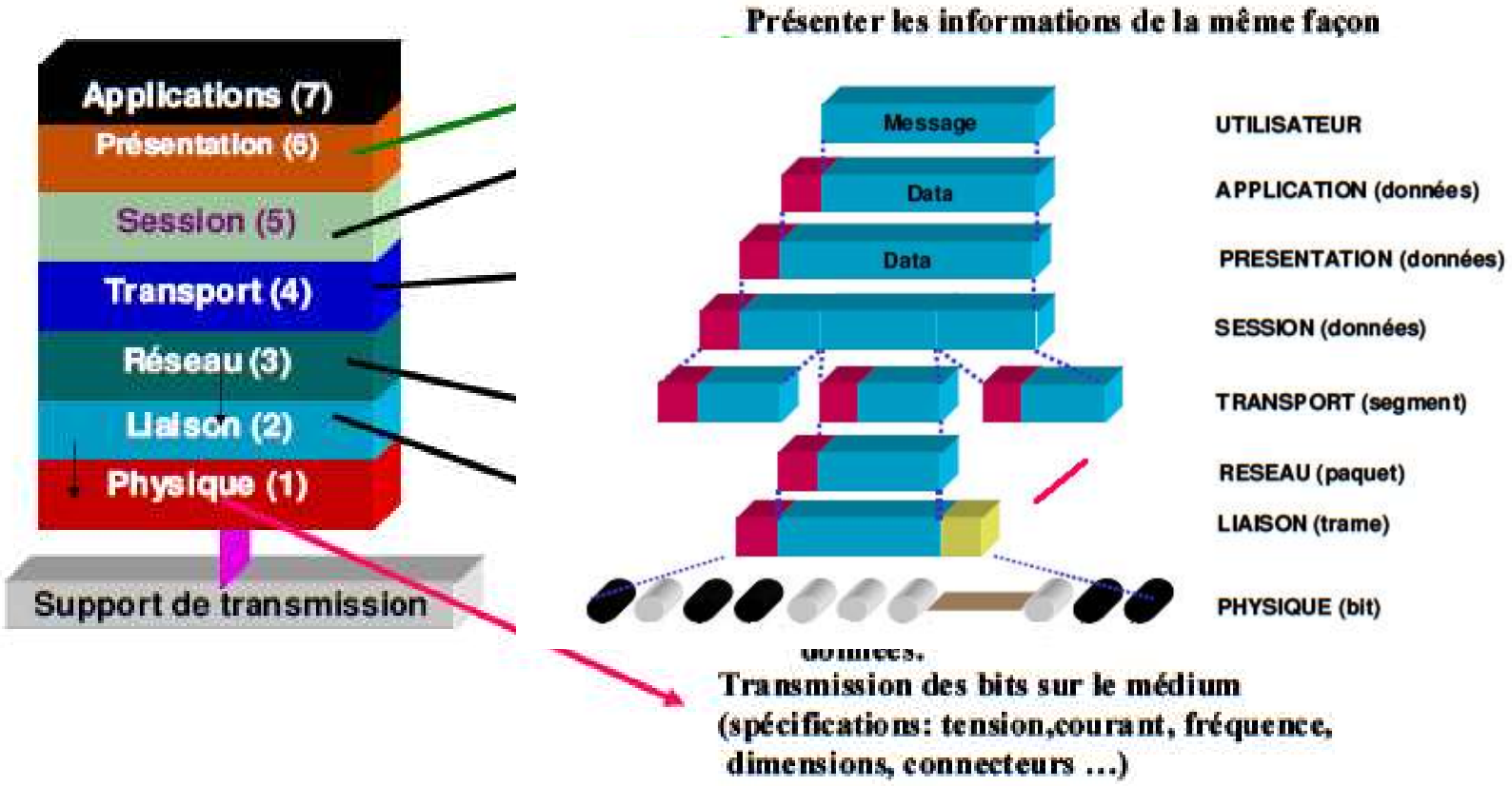
Private IP Addresses

- Internet Addresses (IPv4)
  - Theory, 2^{32} addresses (~4,3.10^9 addresses)
  - Practical
    - Public addresses: ~3,2.10^9
    - Reserved addresses: test…
    - Private addresses: reserved for the internal networks (non accessible from outside)
      - 10.0.0.0 to 10.255.255.255 (prefix 10/8)
      - 172.16.0.0 to 172.31.255.255 (prefix 172.16/12)
      - 192.168.0.0 to 192.168.255.255 (prefix 192.168/16)

OSI model


Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication

Modèle OSI (***O**pen **S**ystems **I**nterconnection / Interconnexion de Systèmes Ouverts) de l'ISO (International Organization for Standardization / Organisation internationale de normalisation)*

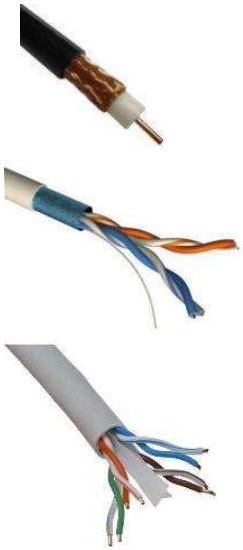


Physical layer

TIA :
Telecommunication Industry Association
previously
EIA : Electrical Industry Association

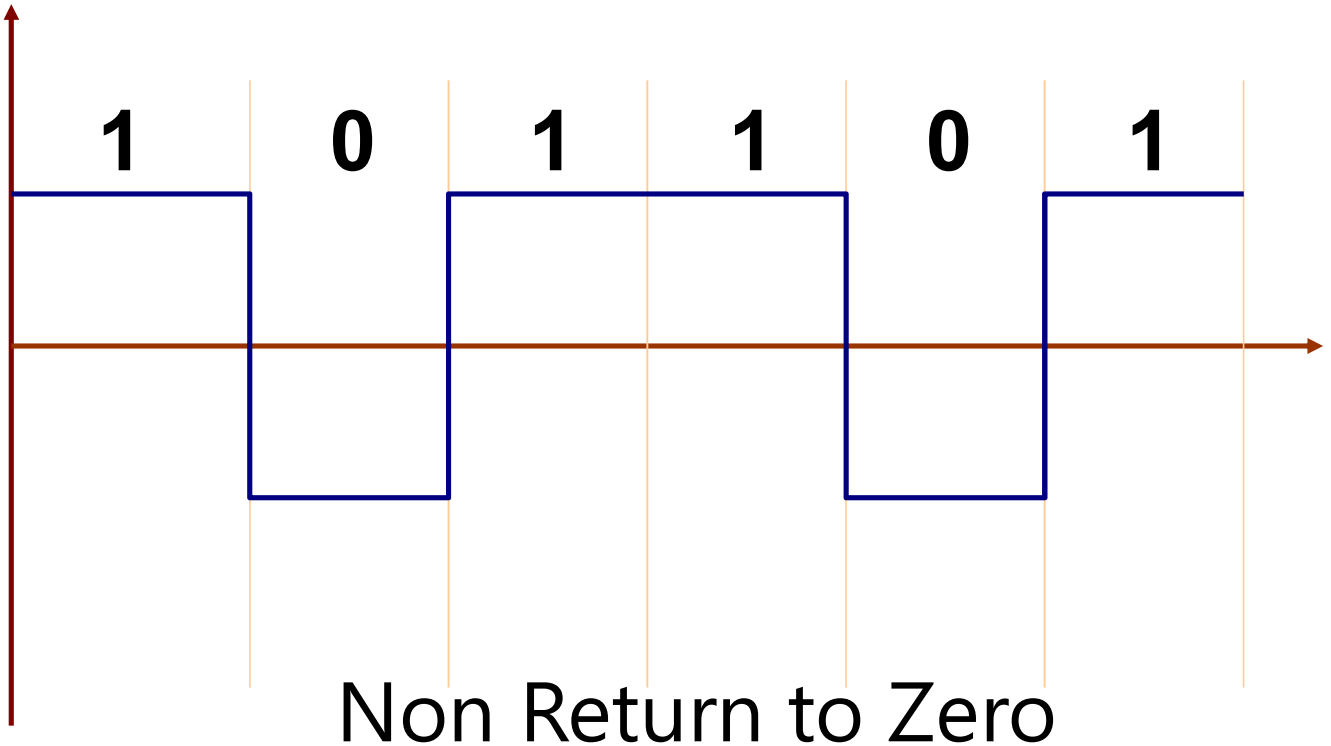
ITU-T :
International Telecommunicaiton Union
- Technical (normalization)
previously
CCITT :
Consultative Comity International Telephony Telegraphique

TIA/ EIA ITU-T / CCITT	RS232C V24/V28	RS422 V11/X27	RS485 V11/X27	TTY
Interface	Bipolar	Differential	Differential	Current Loop
Signal level	± 25 V max	± 5 V	± 5 V	0-20 mA
Sensibility	± 3 V	± 0,2 V	± 0,2 V	± 0,4 mA
Distance	10 to 15 m	1200 m	1200 m	1 to 2 km
Maximum throughput	19200 bds	10 Mbds	10 Mbds	19200 bds
Multipoint	Point to point	Point to multipoint	Point to multipoint	Point to multipoint
Nb. Transmitter	1	1	32	
Nb. Receivers	1	10	32	



+ Wireless

Baseband Physical layer: NRZ coding

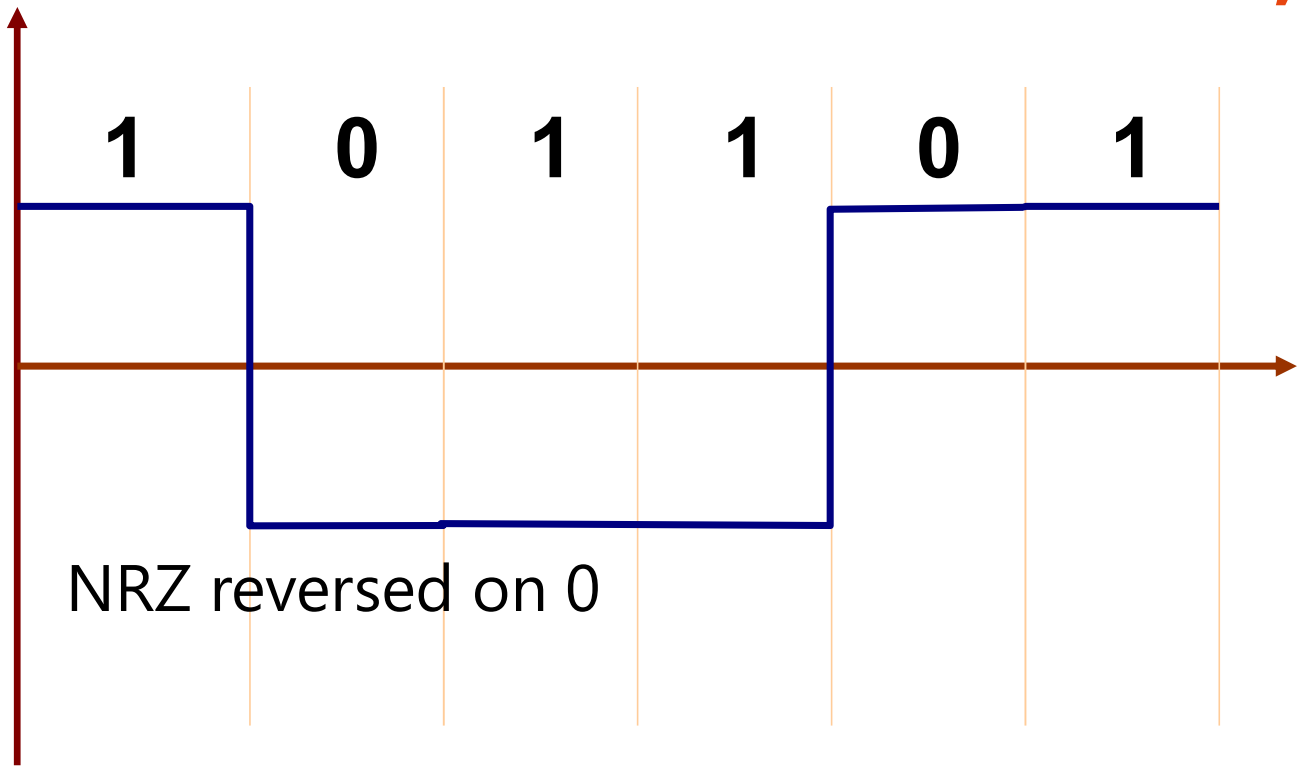


Non Return to Zero

Level 0 : voltage –V
Level 1 : voltage +V

- Synchronization problem at reception
Theoretical maximum rate is double the frequency used for the signal: 2 bits are transmitted per period

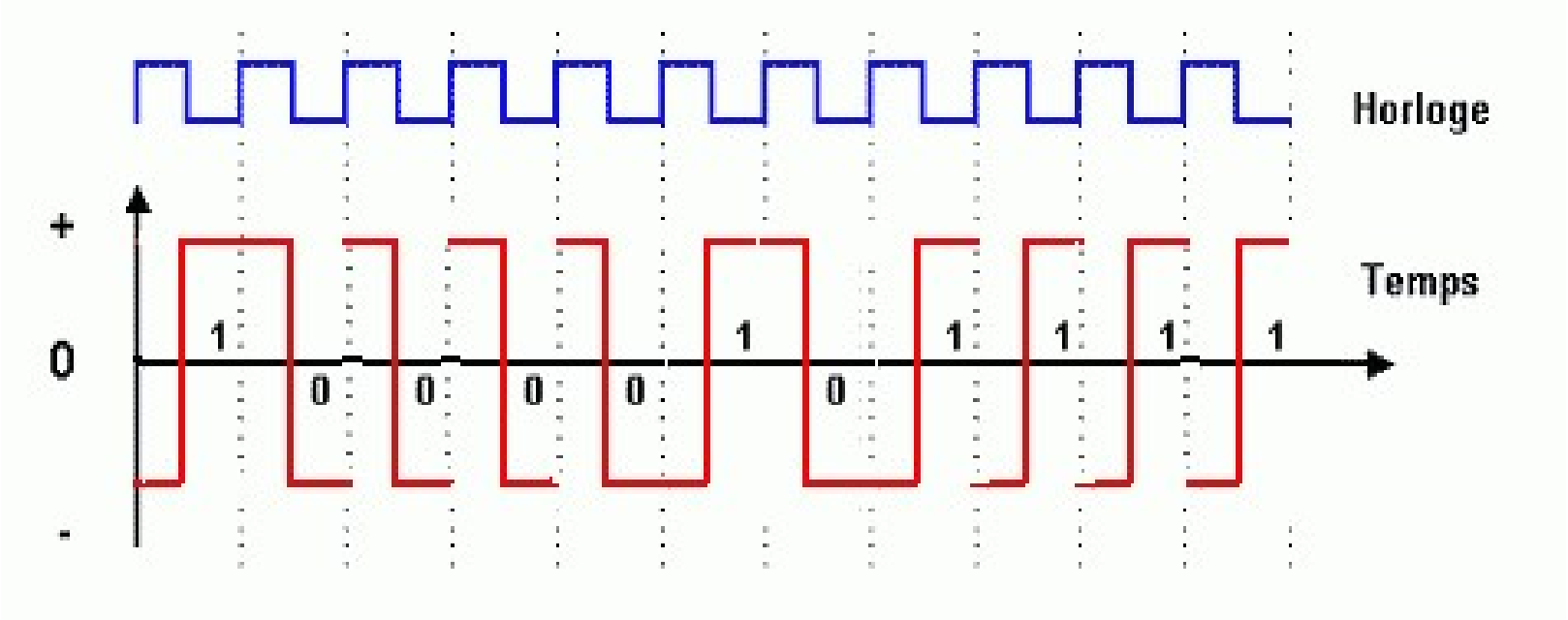
Baseband Physical layer: NRZ reversed on 0, 1



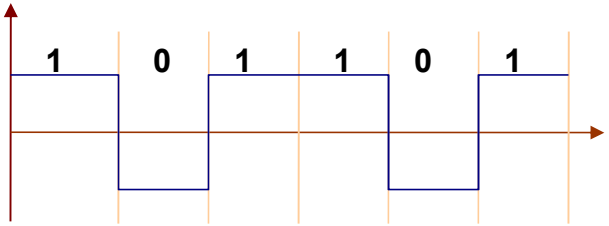
NRZ reversed on 1 : Fast Ethernet (100BaseFX, FDDI)

Baseband Physical layer: Manchester coding

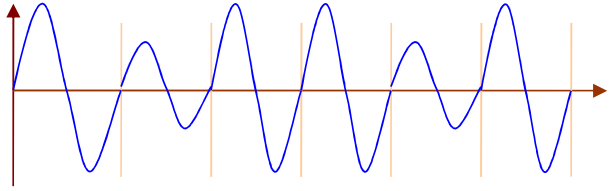
- One transition per binary element => synchronization
- Ascending front: 1, Descending front: 0
- Obtained by an XOR operation between the clock and the data
- Less sensitive to transmission errors
- Disadvantage: requires a bandwidth of 1 bit for 1 Hz (10 Mbits/s need 10 MHz)
- Ethernet 10Base5, 10Base2, 10BaseT, 10BaseFL



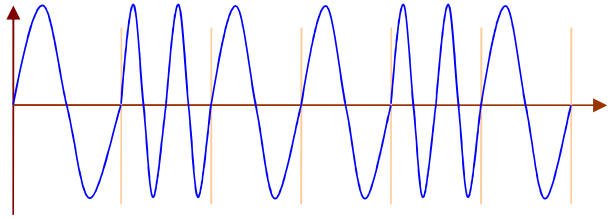
Physical layer
Examples of modulations



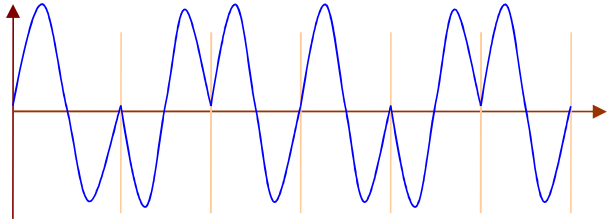
Information à transmettre



Modulation d'amplitude :
information véhiculée par l'amplitude
Ici : 0 ⇔ E sin $2\pi f_0 t$; 1 ⇔ 2E sin $2\pi f_0 t$



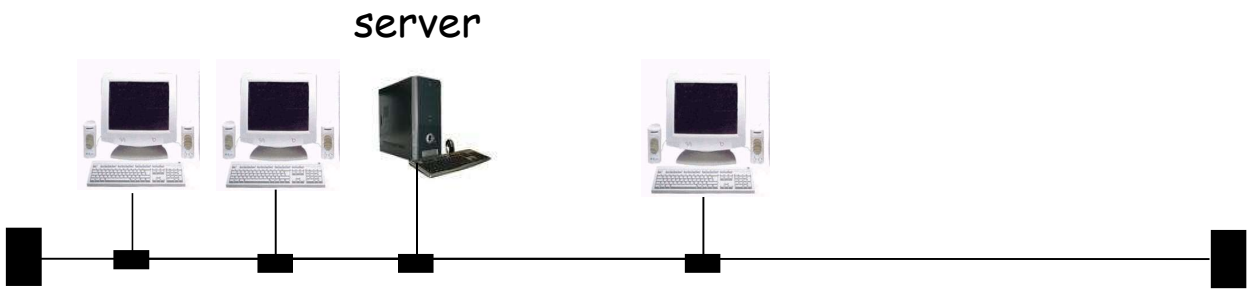
Modulation de fréquence :
information véhiculée par la fréquence
Ici : 0 ⇔ E sin $2\pi(2f_0)t$; 1 ⇔ E sin $2\pi f_0 t$



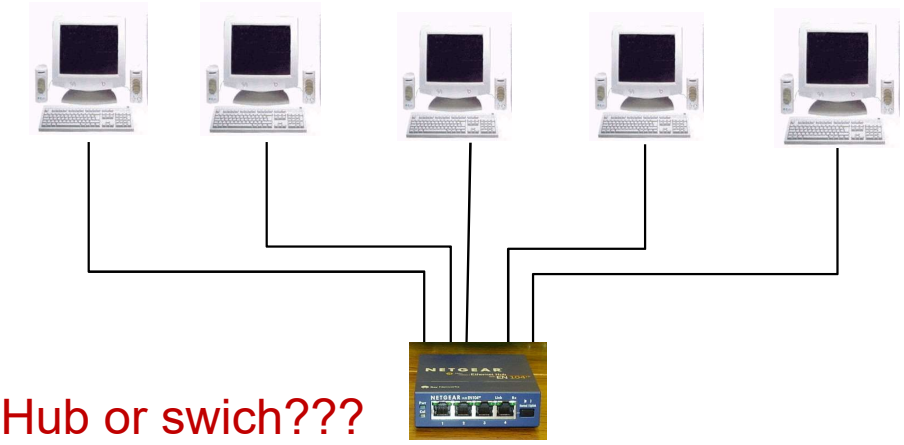
Modulation de phase :
information véhiculée par la phase
Ici : 0 ⇔ E sin $(2\pi f_0 t+\pi)$; 1 ⇔ E sin $2\pi f_0 t$

Topologies

BUS

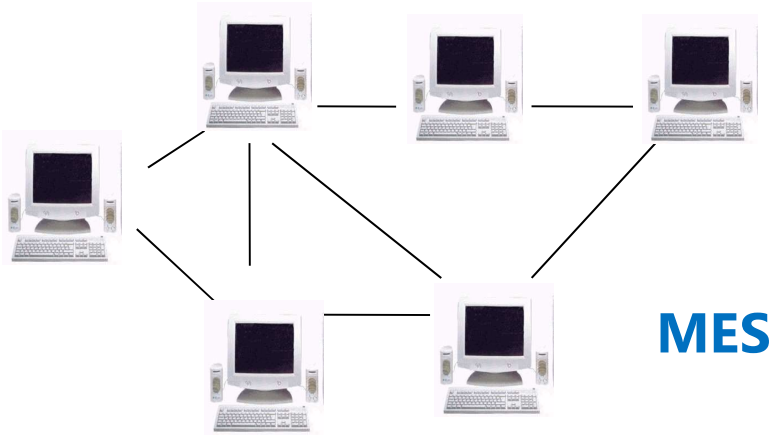


Physical vs Logical



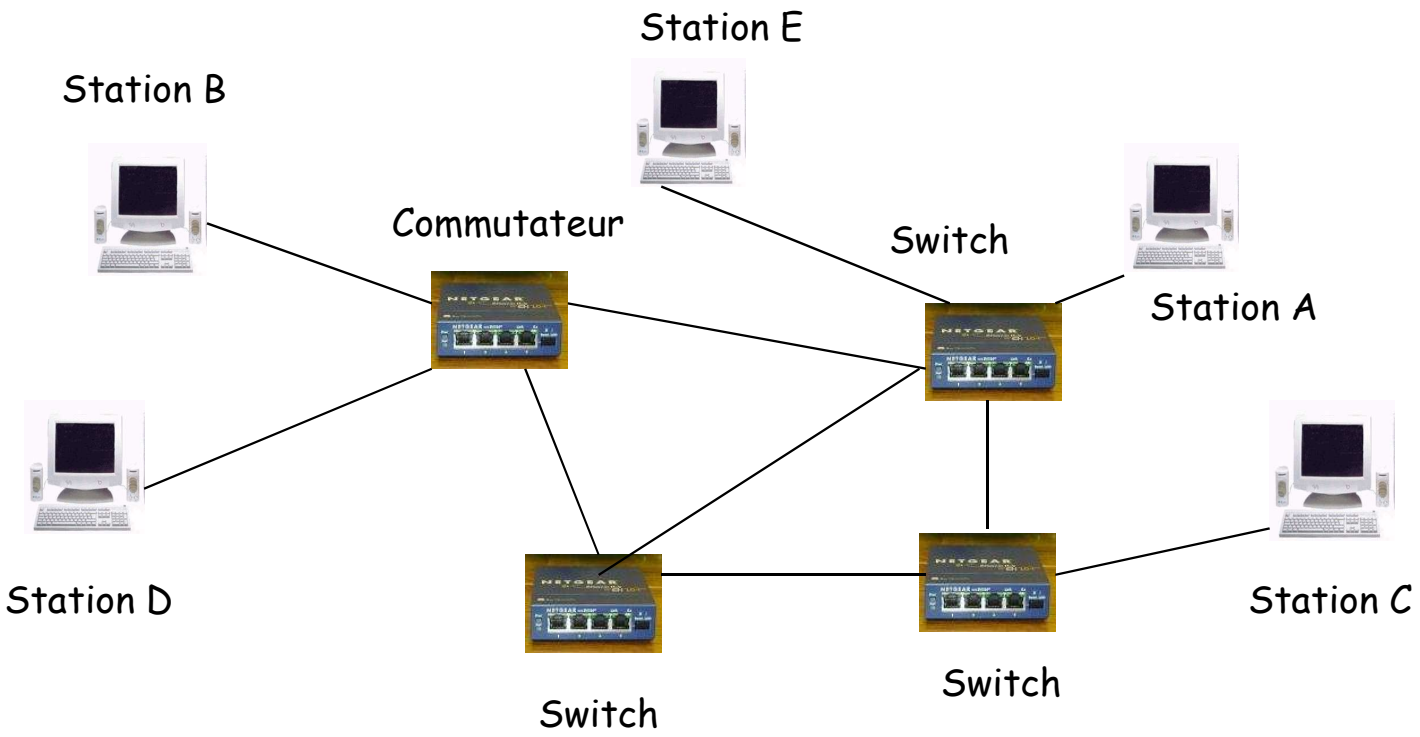
Hub or swich???

STAR



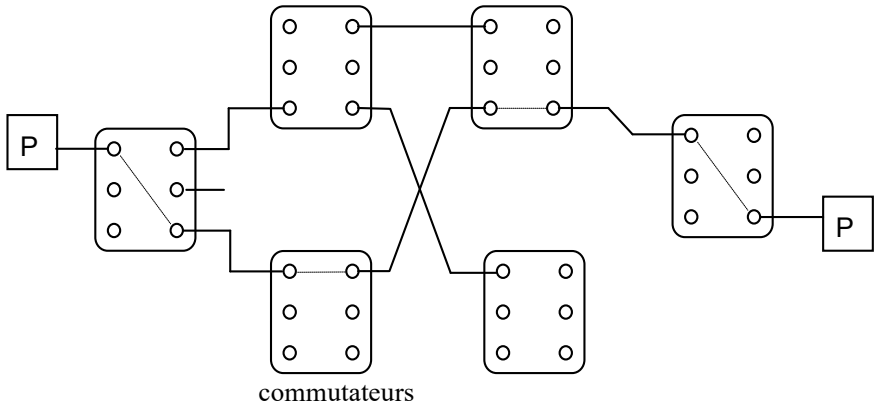
MESH

Switch network



Circuits swiching

- Data transmitted on a circuit, materialized by an electrical continuity, temporarily established between two stations
- Constant and short setup and switching time
- Free information format
- No storage of the communicated information in the network
- Low connection and activity rates



=> packet swiching

Access Control Methodologies

- Random access
  - Free access to the bus, as soon as the medium is free without prior authorization
  - Risk of collisions
- Principle: Competitive protocols
  - CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
    - transmission as soon as the channel is free
    - in case of collision:
      - 1. transmission of a jamming sequence
      - 2. after a delay: new attempt
      - 3. abandonment after too many failures
- CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)
  - Priority mechanism in case of simultaneous transmission

Stochastic vs Determinist

Access Control Methodologies

- Controlled access
  - Waiting for a right to communicate (avoid any conflict)
  - Centralized management: 1 station controlling the accesses
  - Decentralized management: pl. stations controlling the accesses
- Centralized access by "polling"
  - Each subscriber can poll in turn according to a predefined order.
  - Requires:
    - 1. an access controller
    - 2. a polling table
- Bus token method
  - Creation of a logical ring in which a token rotates
  - Right to communicate and access control held by the owner of the token
  - Possession of the token limited in time

Stochastic vs Determinist

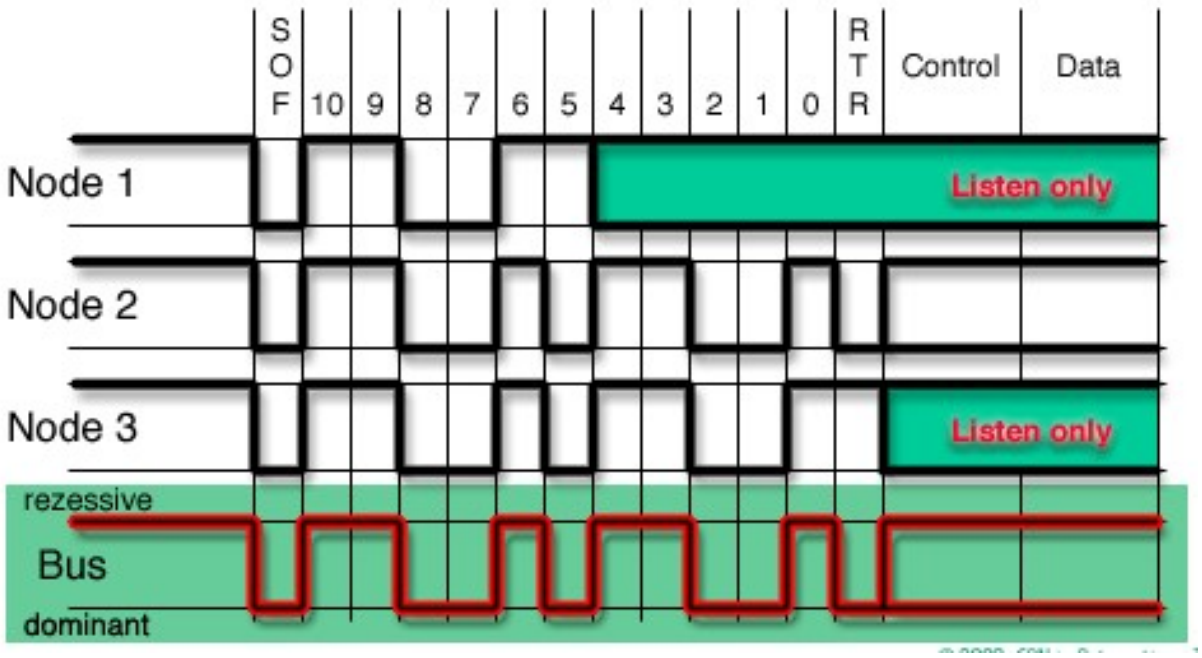
Example: Access mode: CSMA/AMP Arbitration by Message Priority

Ex. of Fieldbus networks

Scheduling of messages as a function of priorities

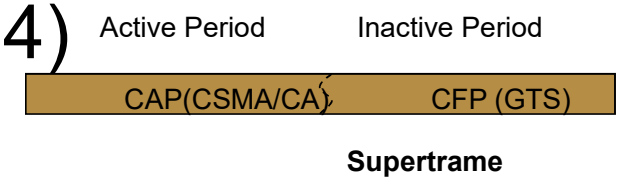
(ex : CAN network, Controller Area Network),

Partially determinist (configuration strategy)



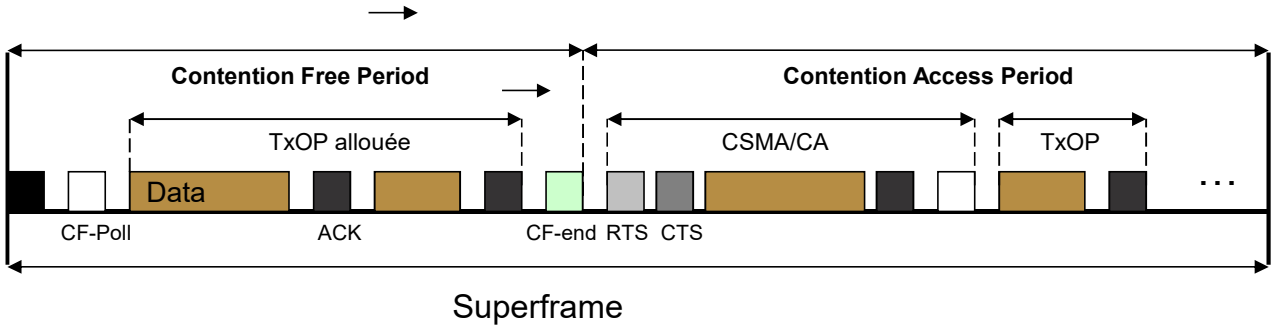
real time (critical time) Wireless network (if the physical layer works!)

- Zig-Bee (on 802.15.4)
  - Superframes :



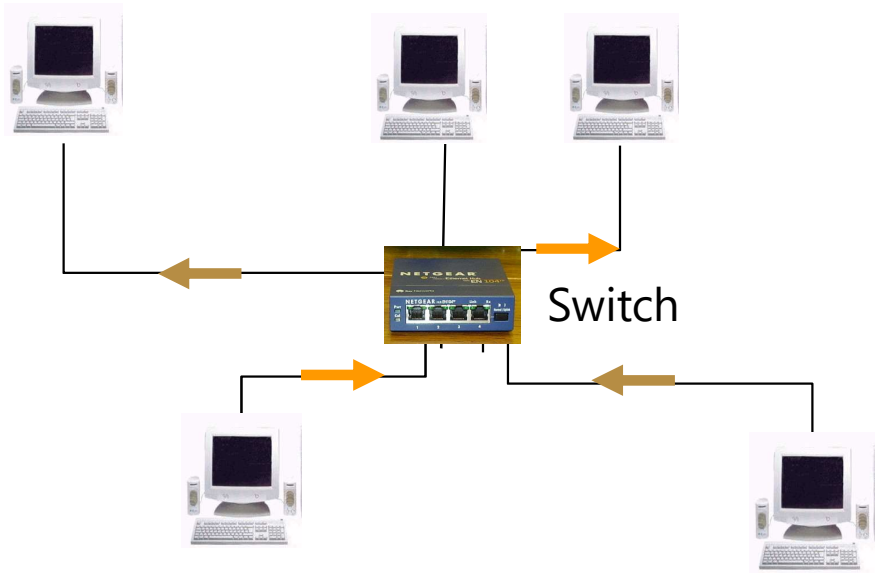
CAP (Contention Access Period) : all the nodes can transmit in a random way respecting the slot duration CSMA/CA
CFP (Contention Free Period) : Allow to garanty an access to a node during a certain amount of time (measured as a number of GTS slots)
GTS (Guaranteed Time slots) : Dedicated time slots (the coordinator can allocate one or several slots to a node, in particular for time garanties)

- Wi-Fi 802.11e



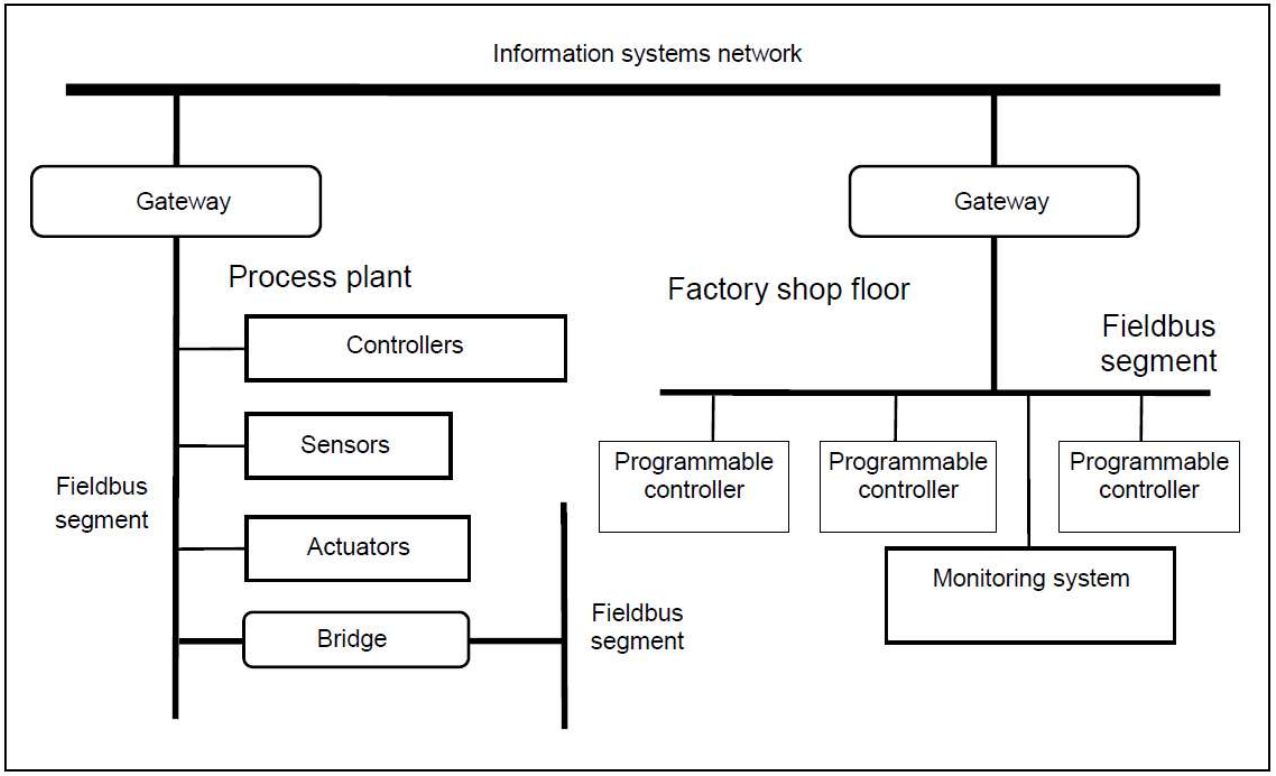
Switched Ethernet

- Ethernet = collisions
- Switches: delimitation of « free collisions » zones



Fieldbus specifications : IEC 61158/ 61784 series
Industrial communication networks

Industrial process measurement and control
Data communication networks
Multilayer applications



Protocols normalized by IEC 61138/ 61784

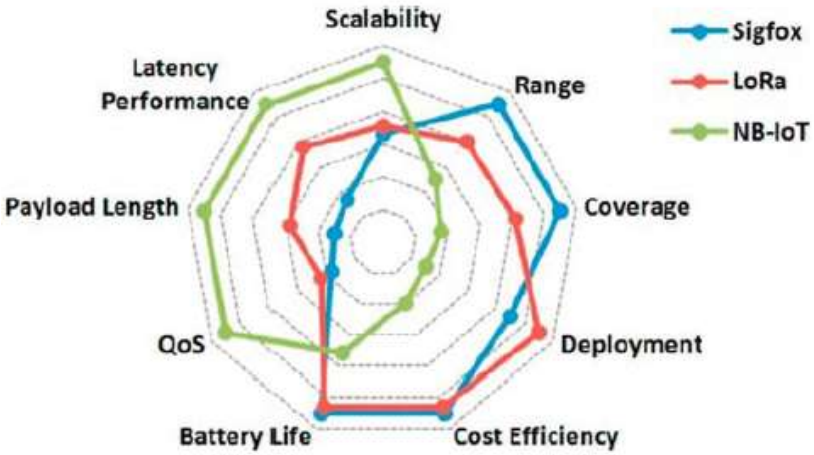
	Name	Vendor
1.	Fieldbus Foundation,	EU
2.	ControlNet, EtherNet/IP, DeviceNet	ODVA
3.	PROFIBUS, PROFInet	Siemens
4.	P-Net,	Danmark
5.	WordFIP	Alstom, Cegelec
6.	INTERBUS	Phoenix Contact
7.	Swiftnet (retired)	Boeing
8.	CC-Link	Mitsubishi
9.	HART	Hart
10.	Vnet/IP	Yokogawa
11.	Tcnet	Japon
12.	EtherCAT	EtherCAT group
13.	ETHERNET Powerlink	Open source
14.	EPA	Chine
15.	MODBUS-RTPS	Schneider
16.	SERCOS	Sercos
17.	RAPIEnet	Korea
18.	SafetyNET p	Pilz Gmbh

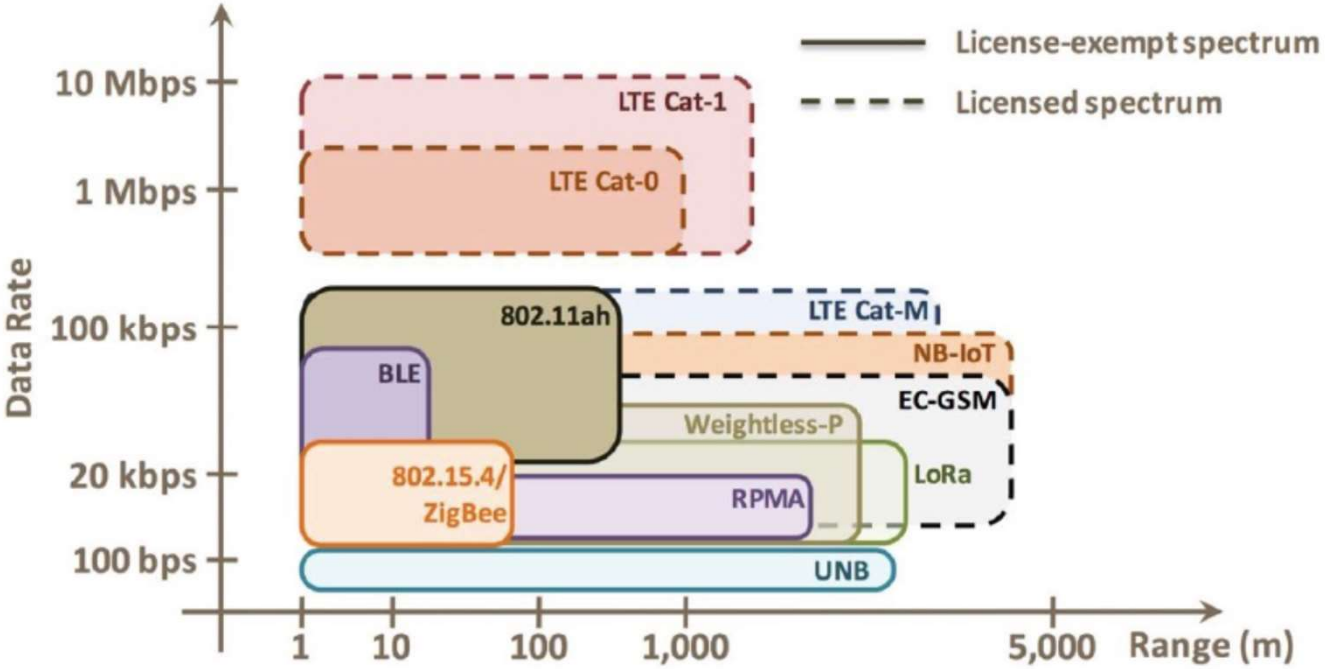
All these protocols are incompatible each other
IP gateway is the solution to transfer data

Wireless network

The main evaluation criteria for Low Power Wide Area Network - LWPAN:

- Range / Coverage
- Deployment / infrastructure cost
- Payload / Latency / Performance
- Consumption (battery life)
- Quality of service / Latency

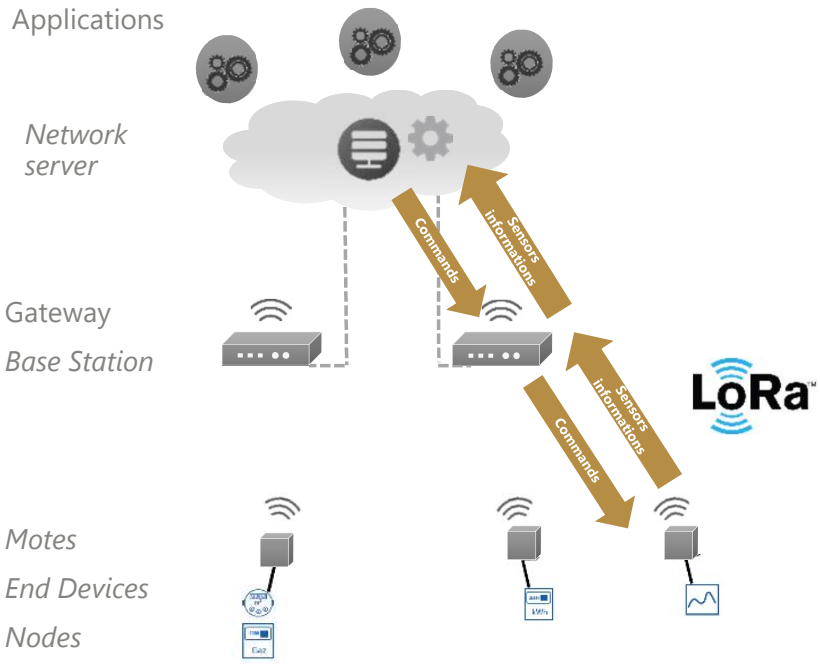




Source https://iotfactory.eu/

Wireless network: LoRa

Low Power Wide Area Network LWPAN : LoRa Long Range Wireless Network



Nom	DevEUI	OTA_AppKey	OTA_AppEUI
Temp extérieure	70:B3:D5:E7:5E:00:2F:07	45B36F05429E6B3D74AAAA2A12740***	70B3D5E75F600000
Contact porte	70:B3:D5:E7:5E:00:35:72	49A5495E312BBBB614CD354140341***	70B3D5E75F600000
Compteur Gaz	70:B3:D5:E7:5E:00:36:C4	718E1F2F315B0D933DCCC1F725D53***	70B3D5E75F600000
Temp Humidité RDC	70:B3:D5:E7:5E:00:37:F4	7EE54A7745E82D5AAAAE5E3A25B839***	70B3D5E75F600000
Anémomètre	70:B3:D5:E7:5E:00:41:93	23411FF30200BBBB560A226527713***	70B3D5E75F600000
Temp Etage 1	70:B3:D5:E7:5E:00:41:B3	1ED153B417E60DF35233CC1C716D4***	70B3D5E75F600000
Centrale de mesure	70:B3:D5:E7:5E:00:44:75	74730B42770D752AAAAD1BEA47D53***	70B3D5E75F600000

Severals gateways listening frequencies Motes messages

Only the gateway with the best signal sends messages to the network server

Sensors Motes

Actuators Motes

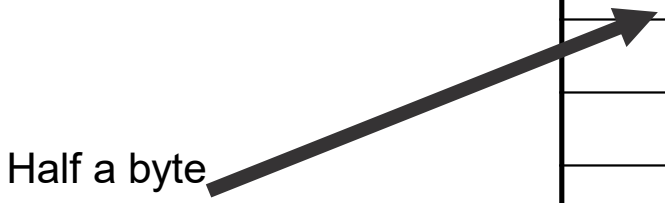
Fast Conversion decimal/binary/hexadecimal

- Decimal => binary
  - 125

• 2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
• 128	64	32	16	8	4	2	1
• 0 1	1	1	1	1	0	1	

Fast Conversion decimal/ binary/ hexadecimal

Base 2	Base 16	Base 10
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15



References

- Transmissions et réseaux, S. Lohier & D. Présent, Dunod, Paris, 2003.
- Cours de DUT RT et LPRO Grenoble, plusieurs auteurs
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Cours de Blaise Conrard, RLI, Université Lille 1
- Cours Eric Gnaedinger, Université de Lorraine
- Automates programmables industriels – W. Bolton – Dunod, 2015.
- Networking courses of Denis Genon-Catalot, Asean-Factori project, 2022.