5.1. Introduction

LANs (Local Area Networks) allow connecting stations to a digital data network with fairly high data rates and inexpensive connection hardware, both in public and private sectors. Nowadays, practically every company has an Ethernet-type LAN, which is wired. Ethernet (IEEE 802.3 standard) is the most commonly used underlying protocol for wired LANs. However, these wired LANs are dependent on the physical and cabled infrastructure of the building, which poses a problem for users who need mobility within companies. Wireless LANs are particularly in demand in sectors like hospitals (patient file management), universities (heavily used LANs on campuses), airports, construction sites, factories (production management, inventory management, stock control). Indeed, all of these find wireless LANs to be particularly suitable solutions.

Wireless LANs are a good solution for applications such as:

- ✓ Extending wired LANs
- ✓ Locations those are difficult to cable (old buildings, museums, historic monuments...)
- ✓ Temporary setups (for periods of overload or special projects)
- ✓ Rapid deployment of networks
- ✓ Constantly changing environments
- ✓ Pre-installed LANs, ready-to-use, or needing to be scalable
- ✓ LAN access for mobile computer users
- ✓ Links through exterior antennas for quick replacement of leased lines
- ✓ Conferences...

5.2. Definition

A wireless network is a network in which at least two terminals (laptops, digital tablets, phones, etc.) can communicate without a wired connection (Figure 5.1).

Figure 5.1:Wireless Local Area Network

5.3. History

- Ethernet makes a comeback to radio waves.
- In 1998, the 802.11 standard is finalized.
- In 1999, first used by Apple under the name 'Airport.'
- Strong deployment since 2002.
  - ✓ Easy setup using transmission points.
  - ✓ Low cost.
    - » Easier and less expensive to install access points than to set up cables.
  - ✓ Linked to the rise in laptop computer usage.
- Towards the convergence of mobile computing and telephony.
  - ✓ Hotspots for Internet access.
- Issues
  - ✓ Interference
  - ✓ Security
    - » Anyone can listen to what is happening on the network.
    - » Encryption techniques (WEP, WAP, IpSec...)

5.4. Different hardware used

- WiFi card in a computer
  - ✓ Like a standard network card (Ethernet)
  - ✓ Operates
    - » in client mode (communicating with a WiFi access point)
    - » possibility in point-to-point mode (communicating with another WiFi card)
- Access point (or WiFi access point)
  - ✓ Similar to a switch: all packets go through the access point

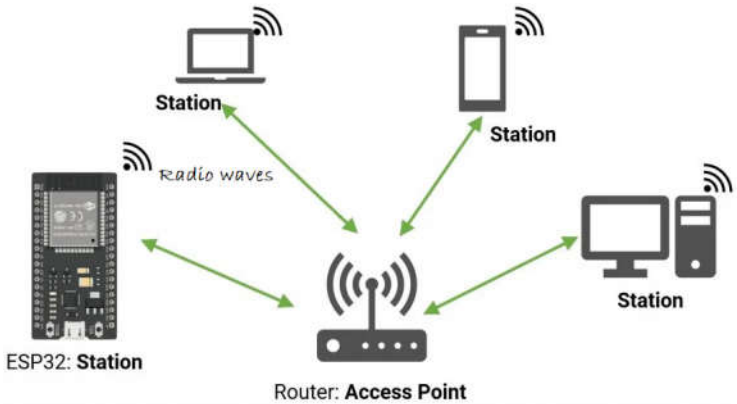


Figure 5.2: different hardware used in a WLAN

- A Wi-Fi access point can act as a bridge to another network
  - ✓ Such as a wired network (Ethernet) for example

5.5. WiFi Infrastructures

- Two possibilities:

  ✓ Classic '**infrastructure**' mode based on access points (WiFi switches)
  » Similar to cellular phones » Based on cells, with an access point located in the middle
  ✓ '**Ad Hoc**' mode: point-to-point mode (computer to computer)
  » Without access points (specific WiFi card configuration)

- Generally, omnidirectional antennas are used in 'infrastructure' mode
- However, directional antennas are possible for 'Ad Hoc' mode, especially for fixed point-to-point connections

5.5.1. Infrastructure Mode

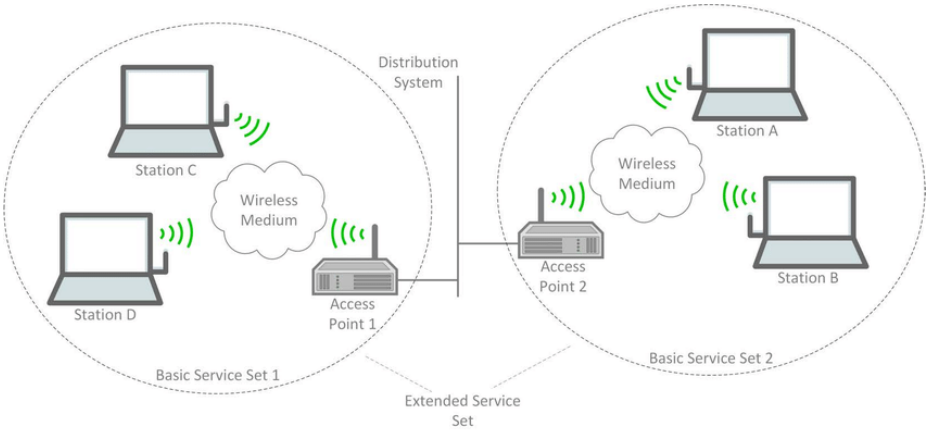


Figure 5.3: WiFi Infrastructure Mode

- BSS (Basic Service Set): basic service structure defined by an AP (Access Point)
- ESS (Extended Service Set): multiple access points serving the same WiFi network and connected by another network
- DS (Distribution System): connection network for access points
  ✓ Can be wired (e.g., Ethernet)
  ✓ Wireless: referred to as WDS (Wireless DS)

- ESSID (ESS Identifier) defines an ESS (32 characters in ASCII): network name
  ✓ This is the name that appears in the list of available WiFi networks

- ESSID is often abbreviated as SSID
- Overlapping cells use different frequency ranges
  ✓ 802.11b: 14 channels of 20 MHz each

- ✓ There should be at least 5 'different' channels of separation to avoid interference

- If cells overlap: possibility to change cells without losing the connection
- 'Roaming' service, also known as 'itinérance' in French
- Mechanism to implement this service: 'handover'
  - ✓ Standard 802.11f

5.5.2. Other WiFi Infrastructure (Ad Hoc mode)

- ✓ Ad Hoc Network
- ✓ User machines serve as routers among themselves (requires specific routing algorithms)
- ✓ Dynamic network infrastructure
- ✓ Referred to as IBSS: Independent Basic Service Set

Figure 5.4: WiFi Ad Hoc Mode

5.5.3. Other Uses of a WiFi Access Point

- Client Mode: The access point acts as a WiFi card
  - ✓ It can be connected via a wired network to a computer that does not have a WiFi card.

- Repeater Mode:
  - ✓ The access point must be 'connected' to a specific ESS (transmission and reception on the same frequency range)
  - ✓ The repeater retransmits frames it receives on the same frequency range
  - ✓ Consequently, there is a loss of performance due to additional collisions

- "WiFi Bridge" Mode
  - ✓ The goal is to have a wireless distribution network (WDS)
  - ✓ The WiFi access point acts as both a classic access point and a 'bridge' to another wireless network (connected to other access points)
  - ✓ Which channels are used?
  - ✓ Can WDS have the same ESS?"

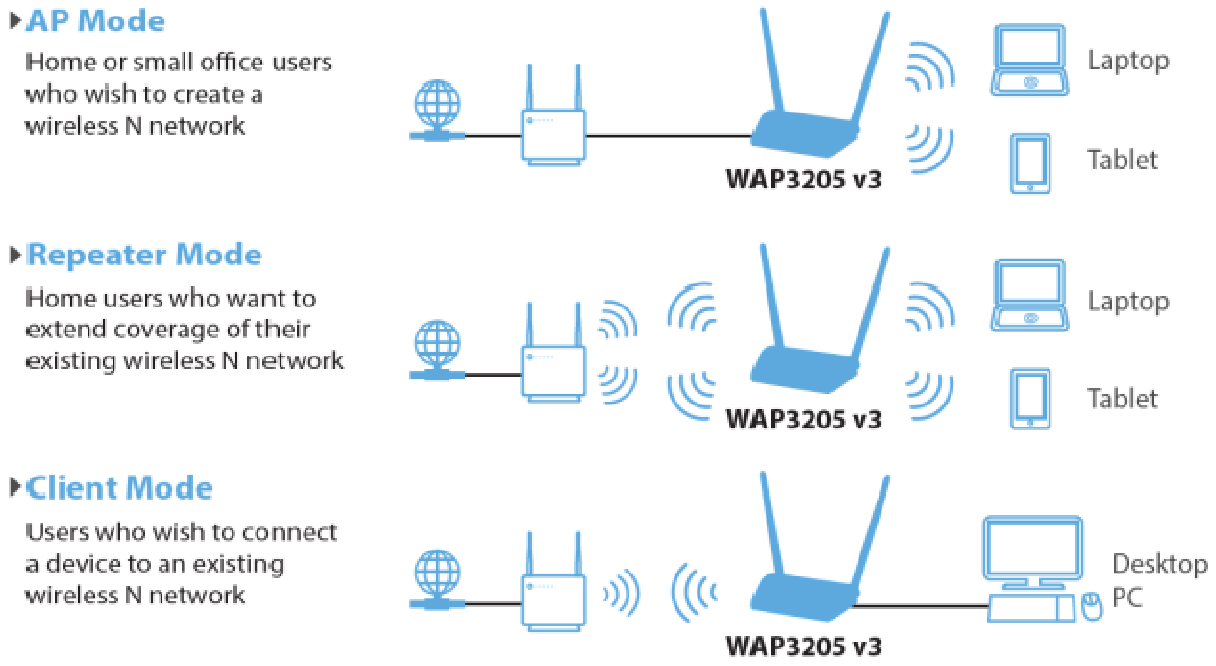


Figure 5.5: WiFi other modes

5.5. Protocol layers

- Couche LLC (IEEE 802.2)
  - ✓ Several possible functionalities within LLC

  » Type 1: Simple routing to upper protocols using LSAP (Source and destination Link Service Access Point)

  » Type 2: Connection, flow control, error recovery

  » Type 3: Datagram with acknowledgment
- For WiFi, Type 1 is used
- MAC common to all standards in the physical layer
- Physical: Various standards are found

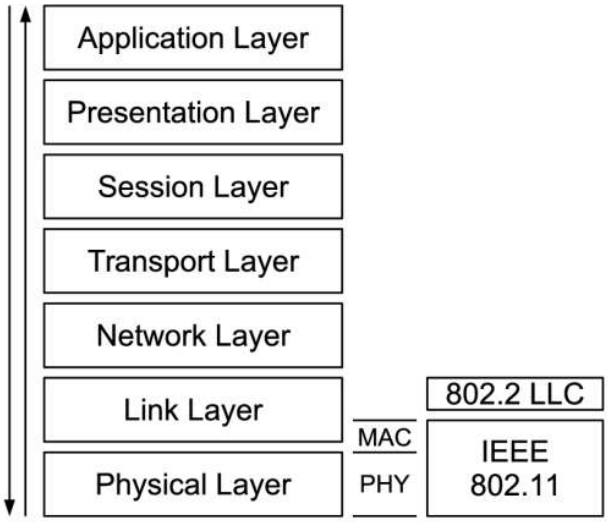


Figure 5.6: WiFi protocol layers

WiFi Standards (Physical)

- ✓ ISM Frequency Band (Industry Science and Medicine)
- ✓ No authorization required: 2.4 GHz - 2.4835 GHz

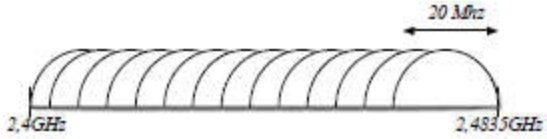
- ✓ Standards
- ✓ – 802.11 (1997) 1 Megabit/s, 2.4 Gigahertz band
- ✓ – 802.11b (1999) 11 Megabits/s, 2.4 Gigahertz band
- ✓ – 802.11a (1999) 6 to 54 Megabits/s, 5 Gigahertz band
- ✓ – 802.11g (since 2001) up to 54 Megabits/s, 2.4 Gigahertz band
- ✓ – 802.11n up to 540 Megabits/s (first cards in 2006, standard by 2008), 2.4 GHz and 5 GHz bands
- ✓ ….etc

The Physical Layer

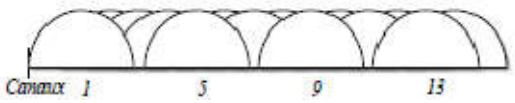
- Different technologies:
- ✓ DSSS Direct Sequence Spread Spectrum » 802.11b and g
- ✓ FHSS Frequency Hopping Spread Spectrum
- ✓ OFDM » 802.11a and g – Infrared

DSSS Direct Sequence Spread Spectrum

- ✓ 14 channels of 20 MHz between 2.4 and 2.4835 GHz (13 used in Europe)
- ✓ Use of one of the channels (user's choice)



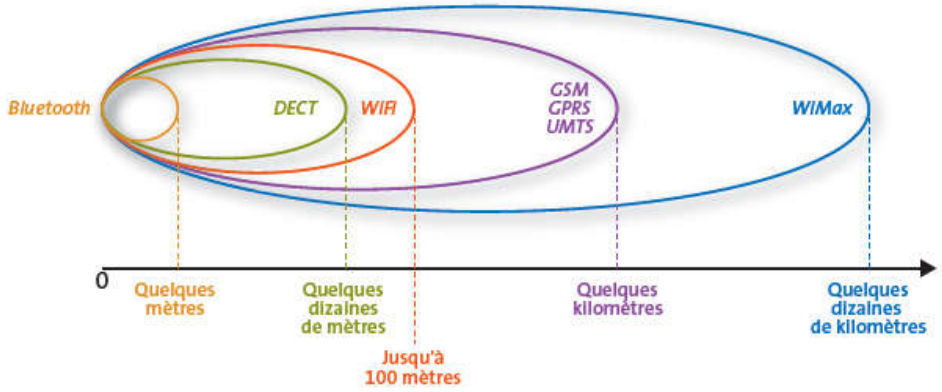
- ✓ Interference between 2 overlapping channels: a maximum of 4 non-overlapping channels simultaneously.



WI-FI Coverage

- Coverage depends on:
- ✓ Building structure and antenna placement
  » Concrete floors, plaster walls ...
- ✓ Interference with other radio networks in the same frequency ranges: Bluetooth, microwaves, other Wi-Fi networks
- Building F is equipped with one Wi-Fi access point per floor (limited at the end of each floor).

Standard Indoor Outdoor
802.11b 35m 100m
802.11g 25m 75m
802.11n 50m 125m



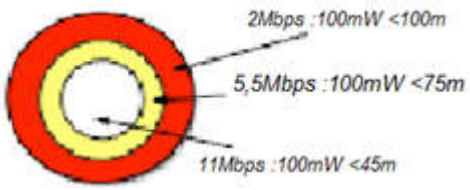
Wi-Fi Speed

The speed of Wi-Fi connections involves both theoretical and actual performance. The theoretical speed serves as a benchmark, but the actual speed is what matters in real-world usage. The physical speed is influenced by various factors, including distance. The system adjusts the speed automatically based on factors like obstacles and ambient noise that can lead to data loss. Additionally, there are extra bytes introduced due to the MAC protocol and the physical layer of communication. For instance, a theoretical speed of 11 Mbits may result in

an actual speed of 6.5 Megabits due to these considerations. Furthermore, the number of users sharing the connection impacts the actual speed. Collisions governed by the MAC protocol and the fair sharing of speed among users play roles here. The physical speed can also vary, as seen in obstacle-free environments where it can fluctuate.

- **For the final standard in 2008: 802.11n**

✓ Theoretical speed of 540 Mbit/s
✓ 100 Mbit/s at 90 m, maximum of 200 Mbit/s
✓ Compatibility with 802.11b and 802.11g



5.6. Wi-Fi Principle

Access to a Network

• Access Points (APs) periodically emit signaling packets known as beacon frames.
  ✓ This emission occurs every 0.1 seconds.
  ✓ Beacon frames contain information such as SSID, potential speed, and current loss rate.
• Devices equipped with Wi-Fi cards are able to interact with these beacon frames.
• When a device is configured for a specific network (in active mode):
  ✓ It sends out the desired SSID within a probe frame.
  ✓ An AP from the network may respond to this probe.
• Conversely, in passive mode:
  ✓ The device awaits signaling packets sent by APs.
• In cases where multiple APs are detected with the same SSID:
  ✓ The device selects an AP based on reception quality factors like speed and load.

The 802.11 MAC Layer

• Resembles a broadcast network like Ethernet
• Utilizes Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) for medium access control
• Involves addressing and framing of frames
• Utilizes CRC for error detection
• Supports fragmentation and reassembly
• Implements Quality of Service (QoS) • Includes mobility management
• Provides security features

Principle of Medium Access Protocol

• A station can determine if the network is busy.
  - ✓ Similar to Ethernet: CSMA (Carrier Sense Multiple Access)
    » Monitors the energy level of the radio frequency.
    » If the channel is detected as inactive for a specified duration known as DIFS (Distributed Inter Frame Space).

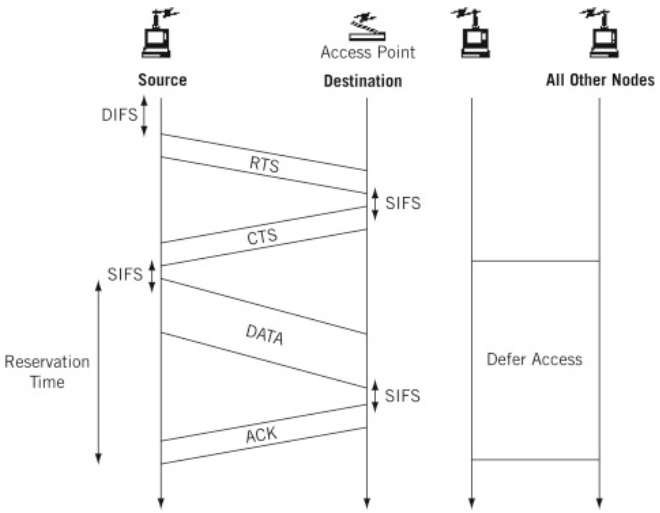
• Possibility of collision.
• Unlike Ethernet, it is unable to detect all collisions.
  - ✓ Hidden station issue (due to radio wave obstacles or distance)
    » A can 'see' B and C, but B and C cannot 'see' each other.

Protocol Principle

• CSMA/CA (Collision Avoidance): the goal is to try to prevent collisions.
• It's important to determine whether there has been a collision or not (whether the packet arrived successfully): acknowledgment mechanism.
• A frame received without collision is acknowledged (using a special packet) after a fixed duration called SIFS (Short Inter Frame Spacing).
  - ✓ Minimum duration required for switching from Reception to Transmission (~10 µs).

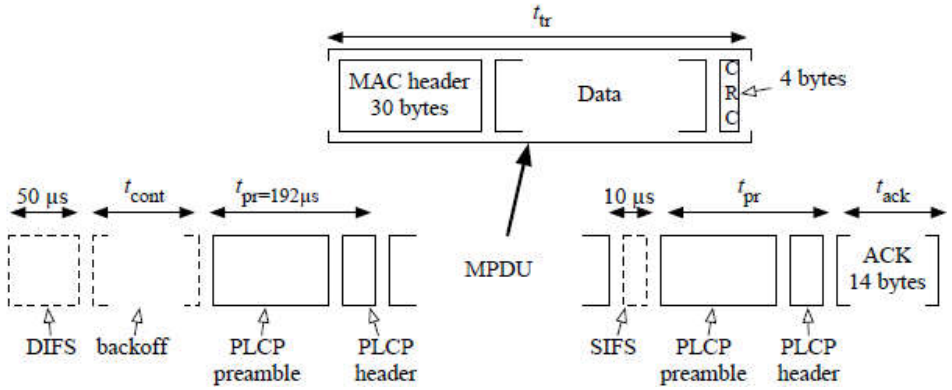
• In cases where the channel is detected as occupied,
  - ✓ We wait for it to become free.
  - ✓ Then we wait for the DIFS duration (50 µs).
  - ✓ DIFS > SIFS to allow collision-free ACK transmission.
  - ✓ Afterward, an additional random waiting period is initiated (known as backoff) within
    » 0 to CW * channel slot time (~20 µs).
  - ✓ Backoff = Random (0, CW) * Slot Time.
  - ✓ CW: Contention Window (initially set to 7).

• In the event of a collision (acknowledgment not received),
  - ✓ The interval for random backoff doubles after each new collision (similar to Ethernet).
  - ✓ Contention window after the i-th attempt: CWi = 2k + i - 1.



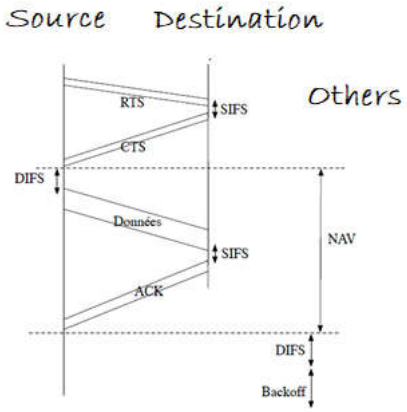
Efficiency

• Only one station transmits at 11 Megabits/s.
• Packets are 1500 bytes in size, which is 12 kbits; transmission time: 1 ms.
• Backoff: an average of 16 * 20 µs = 320 µs.
• Header + Ack = 48 bytes at 11 Mbit/s, approximately 40 µs.
• Effective throughput:
  ✓ 12 kbit / 1000 + 50 + 320 + 192 + 10 + 192 + 20 + 40 = 12000 / 1800 µs
  ✓ ~6.6 Megabits/s.



To Avoid Collisions

• A possible extension (optional)
  ✓ Resolves the hidden station problem
  ✓ Beneficial for transmitting large packets, even though it adds overhead to networks
• Before sending data, there is an exchange of special packets
  ✓ – RTS: Request To Send
    » The sender requests permission to transmit and specifies the transmission duration
  ✓ – CTS: Clear To Send
    » The receiver (access point) grants permission for transmission
    » All stations receive this packet (including hidden stations)
• Other transmitters receiving these CTS packets wait for the indicated duration (NAV Network Allocation Vector)
  ✓ If there is no collision on the RTS and CTS, it ensures that there will be no collision for the subsequent data packets.



Control Modes

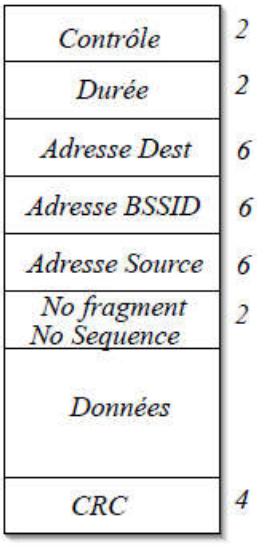
• Previous control mode: DCF (Distributed Control Function)
• Centralized control mode in the access point (PCF: Point Control Function)
  ✓ The AP manages transmissions and distributes transmission authorizations by sequentially polling the present stations (Pooling).
  ✓ Additional signaling packets.
  ✓ Collisions no longer occur.
  ✓ Possibility of managing quality of service: potential priority among stations.
• Both modes can coexist, thanks to inter-frame wait times.
  ✓ – The PCF mode waits for a shorter time between frames (PIFS < DIFS).

The 802.11 MAC Header

• Several types of frames.
• The header varies based on the type defined in the first two octets (frame control field).
  ✓ – Data frame
  ✓ – Access control frame: RTS, CTS, ACK...
  ✓ – Management frame: association, synchronization, authentication.

The 802.11 MAC Header - Data Frame

• Control: Determines, among other things, the frame type.
• Duration: Channel occupancy time
  » Calculated using the frame and its acknowledgment.
  » Used to calculate the NAV (Network Allocation Vector).
• Destination Ethernet Address, Cell AP Address, and Source Address.
• Fragment Number (4 bits): Enables fragmentation.
• Sequence Number (12 bits): Required for fragmentation and acknowledgment mechanism.
• Maximum data size 2312 bytes.



• CTS and ACK Frames

Contrôle	2
Durée	2
Adresse Dest	6
CRC	4

• RTS Frame

Contrôle	2
Durée	2
Adresse Dest	6
Adresse Source	6
CRC	4

Other Wireless Local Area Networks

Bluetooth

- ✓ Connecting digital devices: phones, cameras, printers, alarms, computers
- ✓ Range: 10 m to 100 m (depending on power)
- ✓ Frequency range of 2.4 GHz (interference with WiFi)
  - » Frequency hopping possible with each packet – Standards (802.15):
  - » Version 1 (1999): 1 Megabit/s speed
  - » Version 2.0 (2004): 3 Megabit/s speed

• UWB (Ultra Wide Band): 480 Megabits over short distances, standardized in 2007 but didn't gain wide adoption
• Bluetooth 3.0 adopted WiFi standard since 2009 (24 Megabit/s)

WIMAX

- ✓ Broadband Wireless or
- ✓ Standards 802.16 (from April 2002)
- ✓ Medium-range wireless network (1 to 15 km)
- ✓ Frequency range from 11 to 66 GHz
- ✓ Effective with few obstacles (antenna line of sight)
- ✓ In 2003 (802.16a): 10 Mbit/s over 20 km
- ✓ Alternative to ADSL for isolated areas
- ✓ In 2005: 802.16e: 30 Mbit/s up to 3.5 km allowing equipment mobility
- ✓ Heavily used in the USA, first commercial offering in 2010 in northern France departments
- ✓ Connected mode, QoS guarantees (unlike WiFi)
- ✓ 802.16m (2009) 1 Gbit/s stationary, 100 Mbit/s mobile: Standard that might be used for the 4th generation of the telephony network in Europe?"