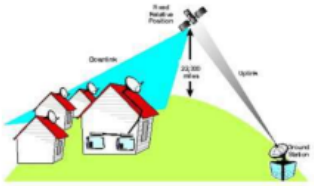
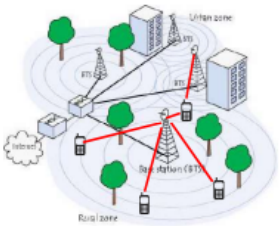
04 - Wireless infrastructure

04_Wireless_infrastructures.pdf

Introduction to wireless infrastructure

System overviews





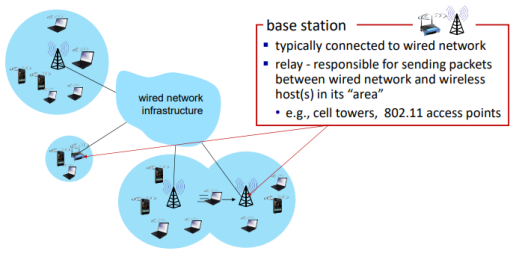
- **Satellite Systems**: Comprised of ground stations and satellites that relay signals. Satellites require "switching reference" as they move passively to maintain communication.
- **Cellular Networks**: Operate with terrestrial configurations, where base stations provide signals within cells, covering users in that area.
- **Wi-Fi**: Originally designed for local networks, later expanded to cover wider areas via IEEE standards.

Wireless technologies can be differentiated based on bitrate capacity and mobility support. For instance, 5G is designed to offer high data transmission rates, making it ideal for data-intensive applications. On the other hand, technologies like Bluetooth, Wi-Fi, and WLAN, while capable of supporting mobile users, were initially developed for fixed access and may not always provide optimal continuity for users on the move. Cellular networks, however, are specifically designed to support mobility, allowing smooth handoffs between cells and uninterrupted communication. In summary, the choice of wireless technology often depends on finding the right balance between bitrate capacity and mobility requirements, which are crucial factors for network performance and user experience.

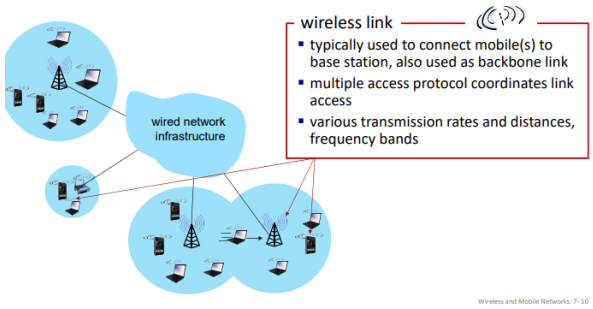
Wireless network

In a wireless network, the main elements include the base station and the wireless link, each with distinct characteristics and functions:

Base Station: This component is usually connected to a wired network, which can employ fiber optic cables for high-speed data transmission. Each base station covers a specific area, known as a cell, where it serves connected devices within that range.



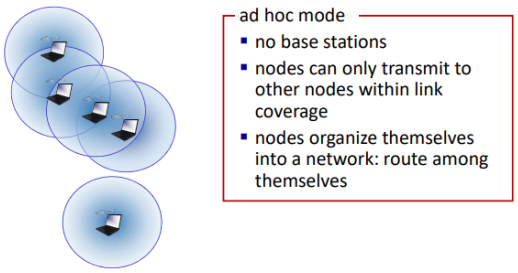
Wireless Link: Unlike wired connections, wireless links (e.g., those used by smartphones) differ significantly in terms of bandwidth, interference, and multiple access protocols.



ADSL and VDSL are point-to-point connections, meaning each user has a dedicated fiber link, thus avoiding multiple access issues. However, with Passive Optical Networks (PON), multiple users share the same link, which can lead to potential multiple access challenges.

This type of communication is known as infrastructure mode, where N users transmit their information through the network, always passing through a wireless network element. For example, if I send a message from my phone, it is first transmitted to the base station, which then forwards it to other users.

Ad hoc network



Ad hoc mode operates without any fixed infrastructure, allowing wireless links to be established directly between users. This approach offers advantages like reduced transmission time, bypassing the entire infrastructure, and the ability to form independent communities. However, it also has limitations, such as limited coverage area, inability to communicate with users outside the network, risk of network disconnection if a link fails, and security vulnerabilities.

In ad hoc mode, dynamic routing is required, so devices must handle functions like routing and addressing. A user may need to act as a relay node, maintaining the network, which adds complexity.

Ad hoc networks are commonly used in IoT applications, extreme environments, and vehicular ad hoc networks (between vehicles), enabling independent data exchange communities for security purposes. However, the complexity is higher because each device must support mobility, addressing, self-configuration, and routing within the network.

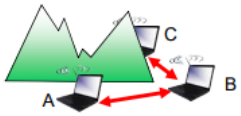
Wireless communication

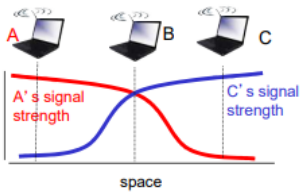
Introduction to wifi

Wireless communication differs significantly from wired communication in several key ways:

- **Decrease in Signal Strength**: Radio signals weaken as they travel through matter, a phenomenon known as path loss. The base station transmits at a certain power level, which decreases with distance as the signal reaches the receiver.
- **Interference from Other Sources**: Interference can be internal (occurring when multiple transmissions share the same frequency band at the same time) or external, caused by noise from surrounding environments. While internal interference can be managed, external interference often requires specific measures, such as using anechoic chambers to isolate signals.
- **Multipath Propagation**: Radio signals may reflect off objects, causing the receiver to receive the same signal at slightly different times. This effect can sometimes be harnessed to amplify the signal upon arrival.

At the receiving end, it's important to measure noise using the Signal-to-Noise Ratio (SNR), which serves as an indicator of transmission quality. Maintaining a known SNR level allows the network to monitor and control communication quality effectively.



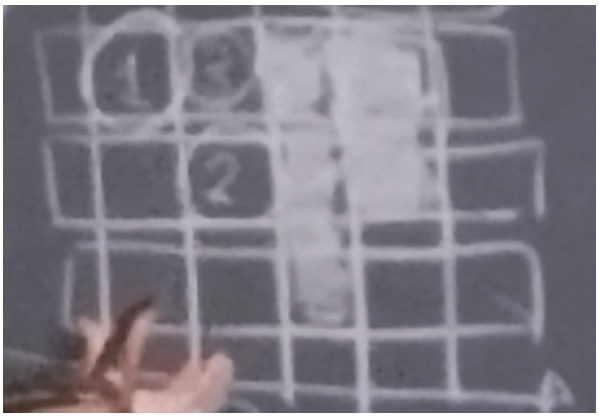


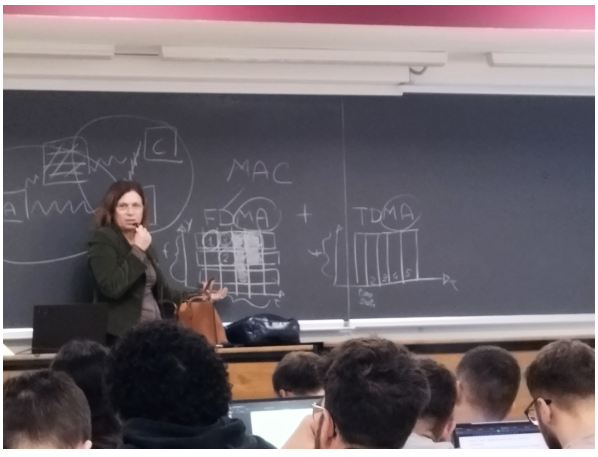
We have a terminal A, use a wireless link toward to terminal B (radio visibility), also a terminal C sendo something to C.

- **FDMA (Frequency Division Multiple Access)**: Multiple signals can be sent simultaneously, but each one uses a different frequency.
- **TDMA (Time Division Multiple Access)**: Each user has their own time slot to transmit.

Multiple access means that users collaborate to share media resources effectively.

We can combine **FDMA** and **TDMA** (result in CDMA), where users are identified by both their time slot and frequency. This allows greater flexibility and supports more users, but at the cost of reduced bandwidth and lower bit rates due to frequency splitting. However, we can allocate more time slots and frequencies to a single user to provide more resources (e.g., 1 time slot = 1 resource).

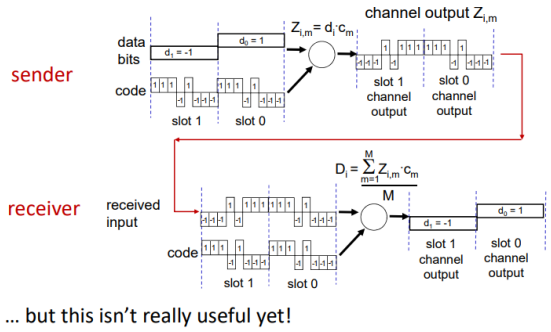


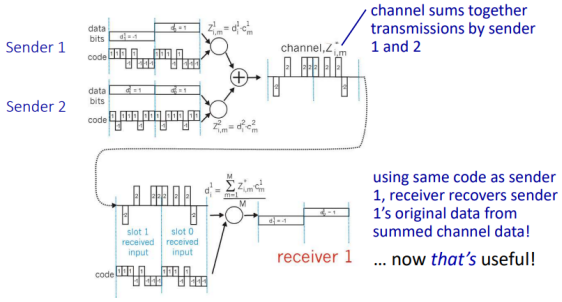


Code Division Multiple Access: CDMA

CDMA (Code Division Multiple Access) works differently. Here, users can transmit at the same frequency and time, but each transmission is distinguished by a unique code. The code is a specific bit sequence known to both the sender and the receiver.

Encoding and decoding add complexity. If the code has more bits than the original message, this requires the network to transmit at a higher speed, which demands more bandwidth. Since we're transmitting **M** bits, we must transmit **M** times faster, which increases the bandwidth usage.





The advantage of **CDMA** becomes clear when multiple users share the same frequency and time, but can still distinguish their communications thanks to the unique codes (this is known as **spread spectrum communication**).

There are license-free bands at 2.4 GHz and 5 GHz, allowing transmission without a license. Wi-Fi 4, 5, and 6 improved speeds and bit rates but still use these same frequencies.

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

- all use CSMA/CA for multiple access, and have base-station and ad-hoc network versions

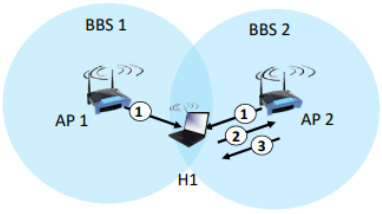
LAN architecture

we have

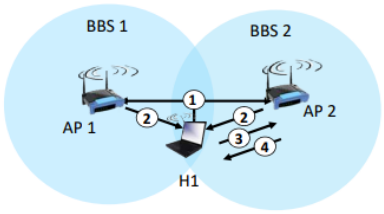
- **Access Point (AP):** A device that provides a wireless network connection to terminals (users) within a specific coverage area.
- **Terminals:** Users or devices connected to the AP.
- **Basic Service Set (BSS):** Also referred to as a "cell." It is the fundamental building block of a Wi-Fi network, representing the coverage area of one AP.

Wifi association process

When connecting to Wi-Fi, a terminal must associate itself with a specific AP within a BSS. The process includes detecting whether an AP is present and capable of establishing a connection. There are two scanning methods for this:



passive scanning:
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1



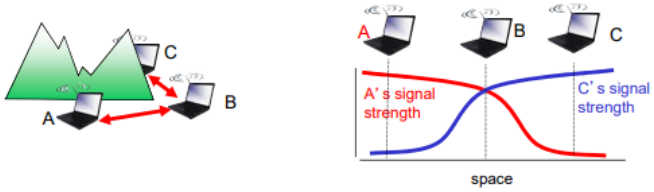
active scanning:
(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

- **passive scanning:** the AP continuously sends out a beacon, which is a message containing its information. When a user device captures this beacon, it sends an association request frame to the selected AP. The AP then responds with an association response frame, completing the connection.
- **active scanning:** the process is initiated by the wireless host (the user device). The host sends out a probe request frame to check if there are any APs in a certain area. The APs that are present respond with probe response frames. After receiving these responses, the host selects an AP, sends an association

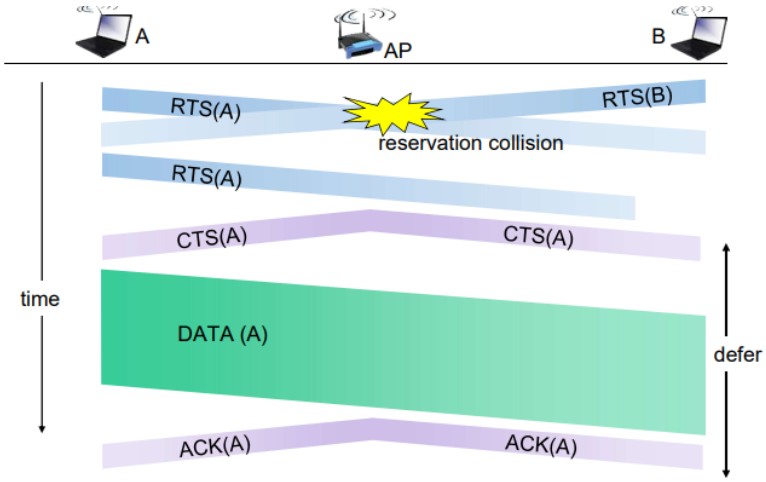
request frame, and the AP replies with an association response frame to establish the connection.

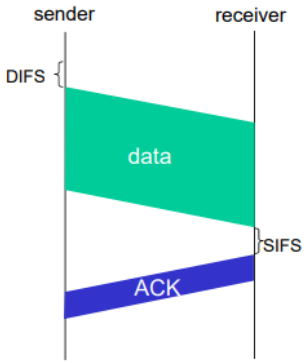
- When we turn on wifi, we automatically connect to AP because the system already already know the device (quick association), instead with Sapienza wifi we have to do the whole association procedure
- We can have some disatvantages with active scanning (minuto 50, riascolta)

Collision avoidance CSMA/CA protocol



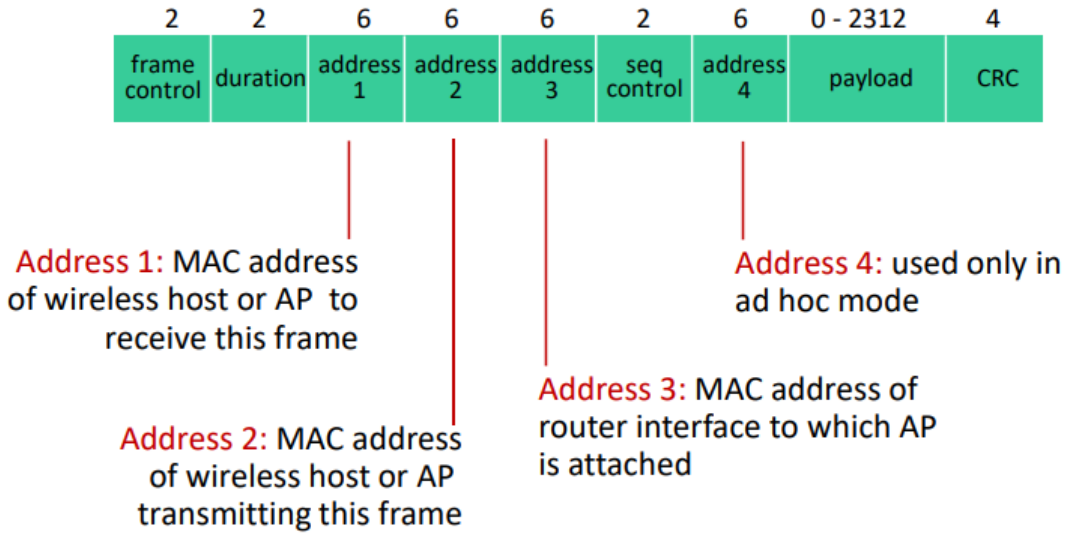
In this scenario we have two terminal communicating to B and thi can cause interference on B! To avoid collision we can use RTS-CTS exachange (Request To Send - Clear To Send exchange) or collision avoidance



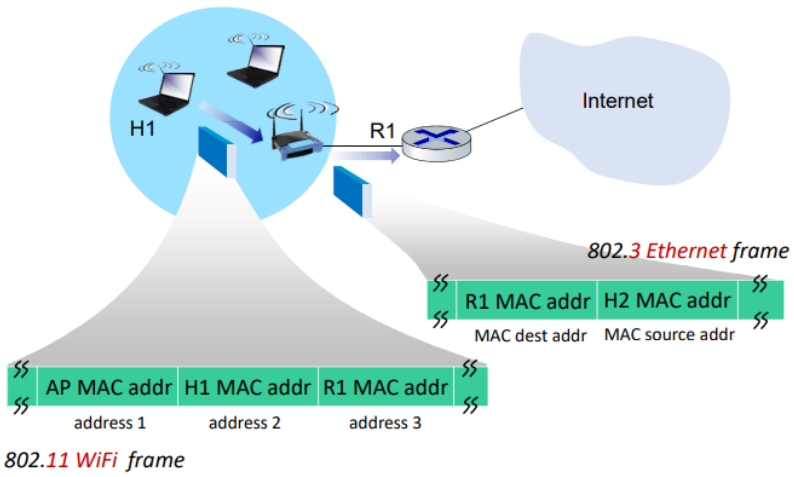


1. A and B are not aware of each other’s presence: before sending the actual message, they first send an RTS (Request to Send) message composed of a small amount of data. Before sending the RTS, they must wait for the medium to be idle for a period known as DIFS (Distributed Inter-Frame Space).
2. If a collision happens, there is no response from the central entity (in this case, the AP), and the hosts understand they had a collision. They will then schedule a new RTS after waiting for a random backoff time following DIFS to avoid immediate retransmission.
3. If the RTS is successful, the AP will respond with a CTS (Clear to Send) in broadcast, indicating to the correct receiver to transmit and instructing the others to wait because someone has been allowed to transmit. The CTS also includes the time the others need to wait. Notice that this solves the hidden terminal problem.
4. When the CTS arrives at the receiver, it will allow the transmission, and the channel will be fully occupied by user A.
5. When no more data is received for a certain period (backoff time called SIFS (Short Inter-Frame Space), the AP sends an ACK to acknowledge successful transmission.

Addressing



- **Frame Control**: Indicates the start of the frame and contains info on how to handle the frame.
- **Duration**: Time for which the channel will be occupied, time needed to read the frame. It is an important field.
- **CRC**: Frame integrity check using Cyclic Redundancy Check system.



When H1 needs to send a frame into the network, it has multiple addresses (since during association, the address of the Access Point (AP) is included). The **first**

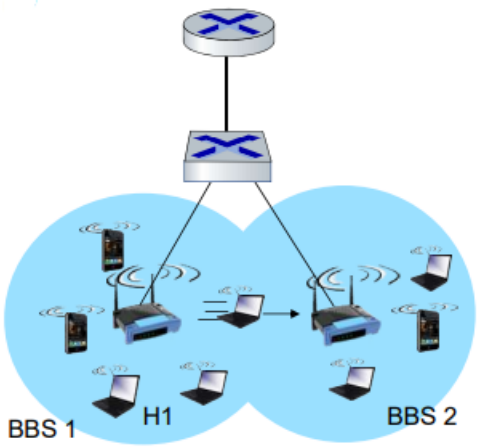
address is the receiver's address, so if there are multiple devices or APs, they know who the frame is intended for.

In Wi-Fi networks, three addresses are used (which requires more control information), while in internet communication, only two IP addresses are used.

Mobility with wifi

In this case, a device can change BSS (Basic Service Set) without needing to register again because it has already been registered to a certain server (which belongs to a specific subnet).

If I move to a different subnet, I need to register again.



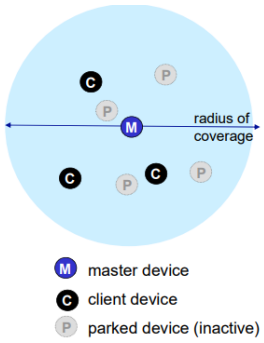
Some issue:

- **What is the data rate with an AP in older versions of Wi-Fi?** If I'm close to the AP, I have a high SNR. In the same area with the same AP, the SNR depends on the distance. In Wi-Fi, there are different bit rates because there is adaptation based on the SNR the device has.
- **Power management in APs**: APs have evolved in terms of power management.
- **When does an AP use power?** To transmit data to a device and when sensing the beacon.
- **When does an end-device use power?**

  To save power, the end-device should avoid scanning channels constantly. It can go to sleep when the device knows that someone else will transmit (as in RTS-CTS). During the defer period, devices that are not transmitting can go to sleep.

Bluetooth

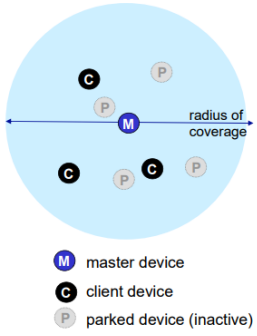
- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- 2.4-2.5 GHz ISM radio band, up to 3 Mbps
- master controller / clients devices:
  - master polls clients, grants requests for client transmissions



Bluetooth operates in the 2.4 - 2.5 GHz radio band, the same frequency range as Wi-Fi. It functions in an ad-hoc manner, but because it shares bandwidth with Wi-Fi, simultaneous communication can cause interference. To avoid this, Bluetooth uses a technique called **frequency hopping**, where it divides the bandwidth into subchannels and rapidly switches between different frequencies during transmission.

This frequency hopping can result in brief, frequent interferences with Wi-Fi, which perceives these as noise. For Bluetooth to work properly, the receiver must know the **hopping sequence** to identify and decode the transmitted signal.

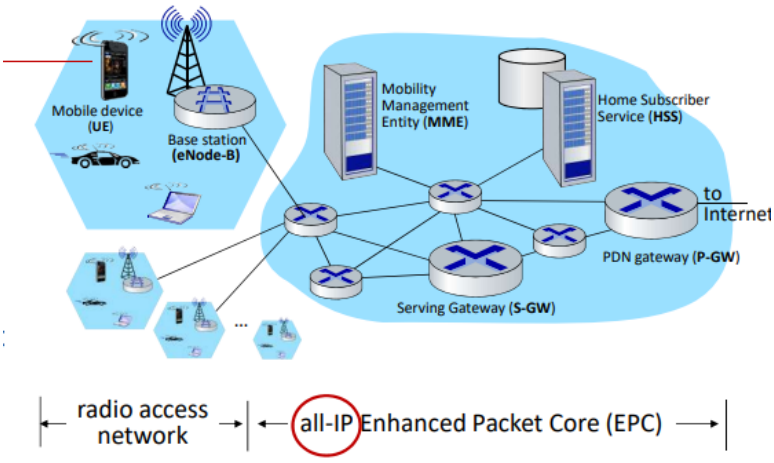
- TDM, 625 μsec sec. slot
- FDM: sender uses 79 frequency channels in known, pseudo-random order slot-to-slot (spread spectrum)
  - other devices/equipment not in piconet only interfere in some slots
- parked mode: clients can "go to sleep" (park) and later wakeup (to preserve battery)
- bootstrapping: nodes self-assemble (plug and play) into piconet



Wi-Fi and Bluetooth coexist in the same frequency band by using completely different methodologies:

- Wi-Fi uses the full bandwidth.
- Bluetooth divides the bandwidth into subchannels and uses frequency hopping.

Cellular networks



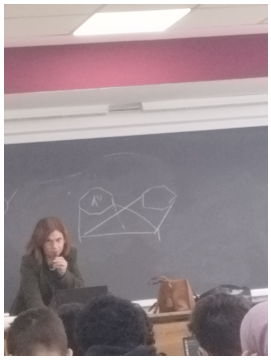
We have several new elements:

- **Concept of a cell**: Unlike wired networks, in cellular networks, a cell represents an area where transmission occurs. The shape and size of the cell are designed a priori based on the power of the base station, which can adjust the cell size to be smaller or larger depending on its configuration.
- **Base station**: A fixed station that facilitates wireless communication with mobile devices.
- **Mobile device**: The user's device that communicates with the base station.
- **Several servers and gateways**: Located in the core part of the network, they handle the infrastructure's management and connectivity.
- Nowadays, the core part of the network is entirely IP-based, meaning that all protocols run over IP. The only wireless part of the communication happens between the device and the base station.
- **Mobility management server**: This server is dedicated to managing user mobility. It allows a user to move from one cell to another while keeping the connection alive without interruption.
- **Home Subscriber Service (HSS)**: This server handles user authentication, manages traffic billing (tracking how much traffic the user consumes), and oversees user contracts (e.g., checking if the user has exceeded their data limit).

- **Gateways**: These routers physically interconnect the network infrastructure in an IP-based manner. They also convert wireless signals from mobile devices into formats compatible with wired infrastructure

The purpose of cellular networks is to cover large areas while optimizing the use of frequency bands. Cellular networks can reuse the same frequency in different cells without interference because the cells are physically separated. This allows for efficient frequency reuse.

We still have a wired part of the network where all protocols run over IP. Communication between mobile devices and base stations is wireless, but the core network remains wired.



Digital identity: In cellular networks, mobile devices are identified by the SIM card, which is a novel concept compared to other types of networks. Unlike a PC, which doesn't have a fixed digital identity, a mobile phone can be uniquely identified by its SIM card, allowing for user authentication.