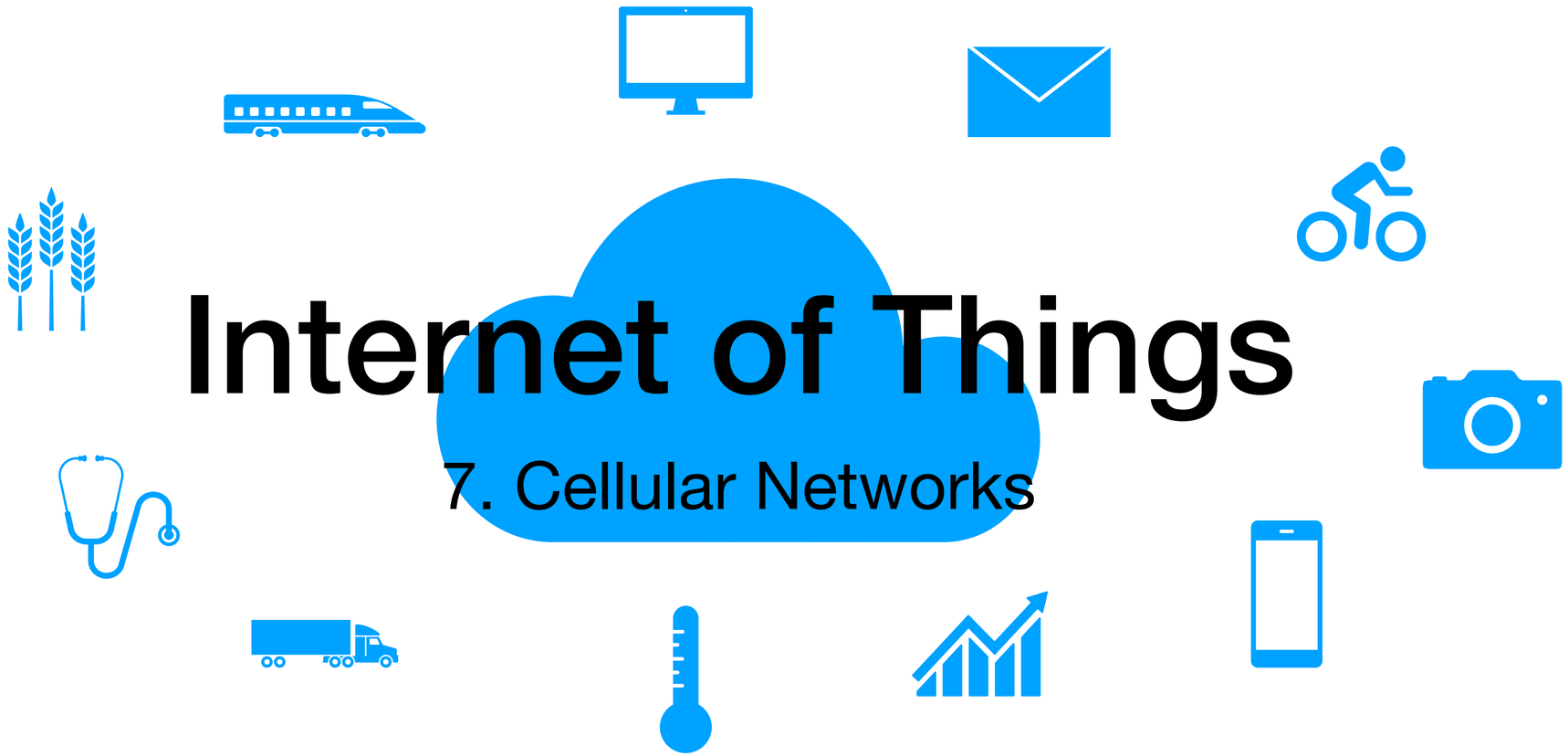


Internet of Things

7. Cellular Networks

M.Sc. Computer Science 2024-2025

Viviana Arrigoni

Before Cellular Networks

- Before the introduction of cellular networks, only landline telephone connections existed.

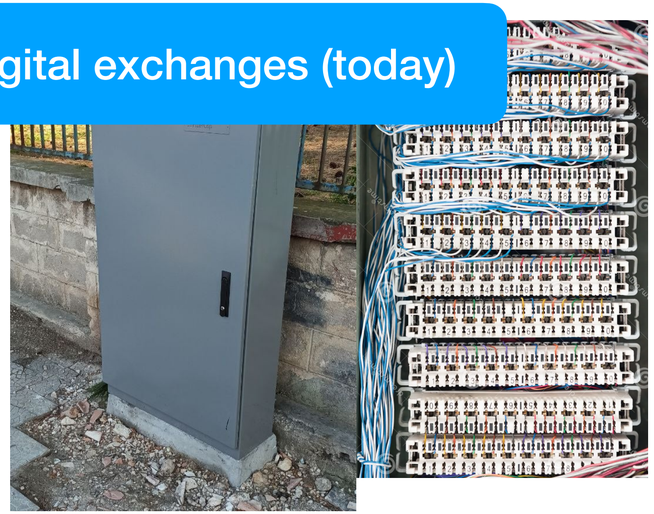
Manual telephone exchanges

Telephone operators late 1800s - early 1900s.
As you lifted the handset, you were connected to an operator at the exchange, who would plug your line into the line of the person you wanted to call using a switchboard.
You had to give to the operator the number or the name of the person you wanted to reach.

Automatic exchanges

Electromechanical automatic switching systems. You would dial a number and the switch would move mechanical contacts to connect your line to the destination.

Digital exchanges (today)



When you dial a number, digital signals are routed using digital switching systems

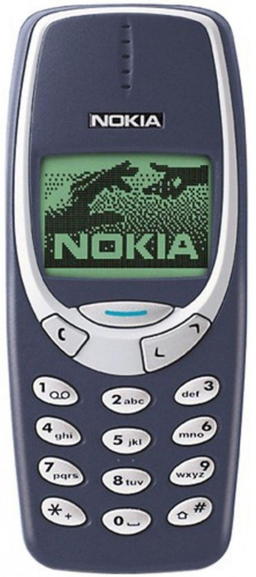
Only used for voice, i.e., only for **analog signals**

1G

- First Generation (1G) cellular networks were the first cellular networks, introduced in the 1979.
- Purely analog cellular systems.
  - No support for encryption, poor sound quality.
  - Very limited coverage and data rate. Very few people were using this technology in their every day life.

2G

- Beginning 1990s, second generation (2G) cellular networks superseded 1G.
- Introduced the concept of **digital modulation**: voice was converted into digital code, and then into analog (radio) signals.
- Based on the **GSM** standard (Global System for Mobile Communications), designed in Europe to establish a common standard for digital cellular voice communication.
- Did not support just voice calls, but also Short Messaging Service (SMS).



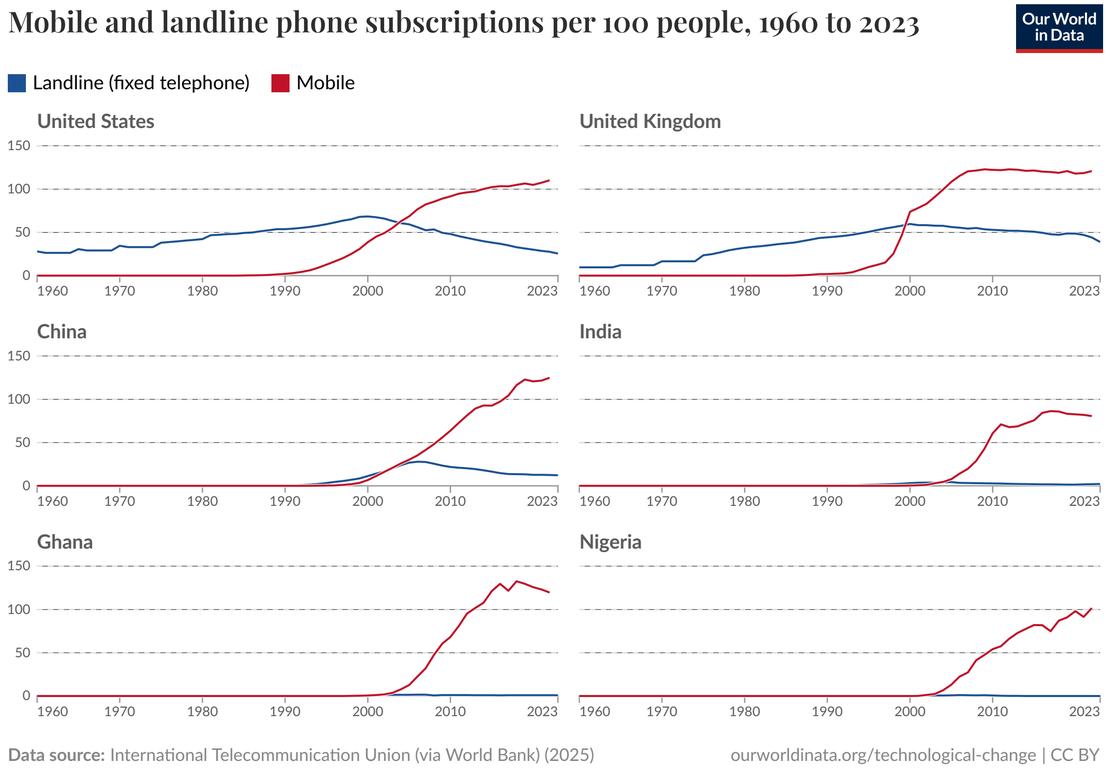
Nokia 33 30

Nokia 33 40

3G

- Born in 2000, represented a real revolution: 3G cellular data networks connected devices not only to the existing cellular voice network, but also to the public Internet!

- Increased data rate.



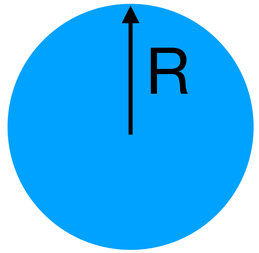
7.1 Cellular concept

Cellular Concept

- Landline telephones used high-powered base stations to cover large regions.
  - Very few transmitters per area unit, often used dedicated channels for each user, limiting scalability.
- **Cellular concept**: divide the area into many smaller “cells”, each covered by low-power transmitters and receivers, “Base Stations”, BS.
  - High capacity in a limited spectrum allocation
  - Each BS is allocated portion of the total number of channels available
  - Neighbouring BSs are assigned different groups of channels to minimise inferences

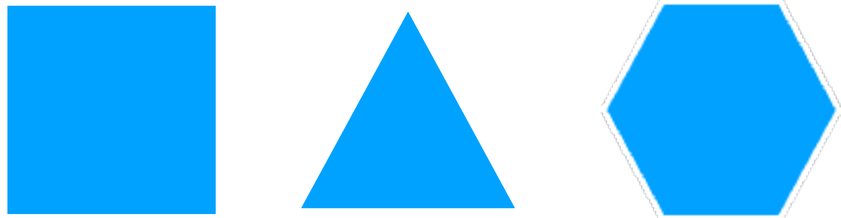
Cells (1)

- Cells are geographical areas covered by base stations.



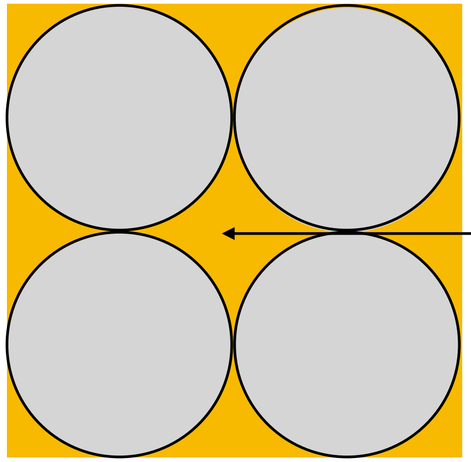
Ideal cell

Actual cell

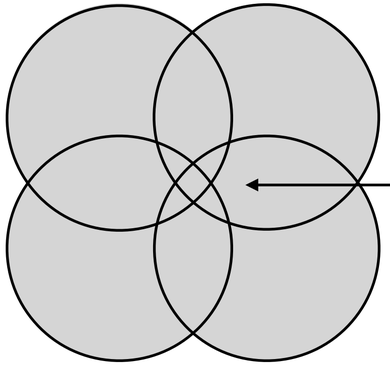


Different cell models

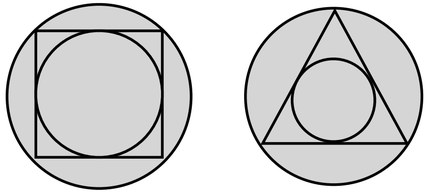
Tessellation

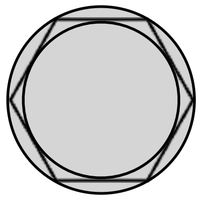


Uncovered areas



Overlapping areas (interferences may happen here)

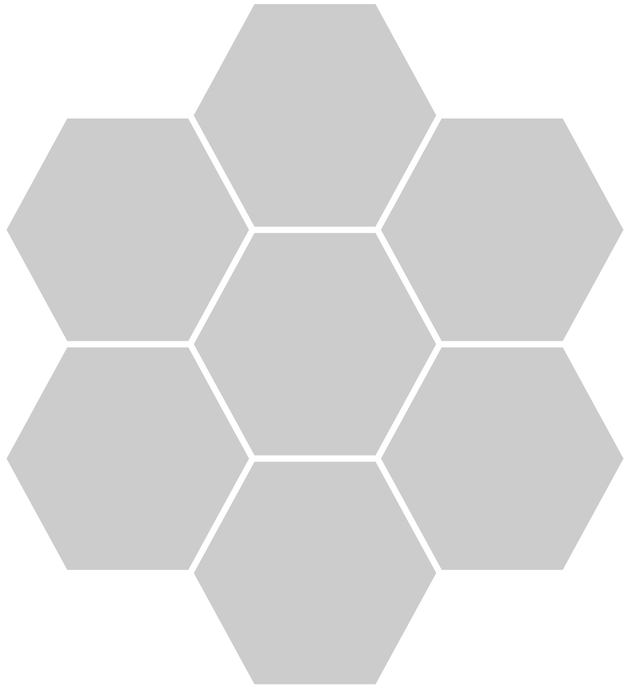




Hexagons approximate circles much better

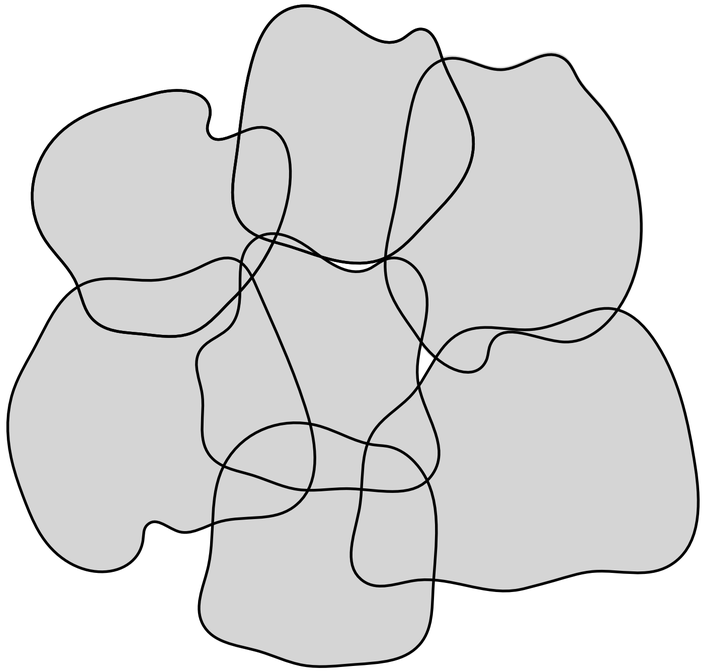
Cell (2)

- Honeycomb grid (i.e., representation of each cell as a hexagon) is the model typically used for for theoretical representation of area division in cellular networks.



Cell (2)

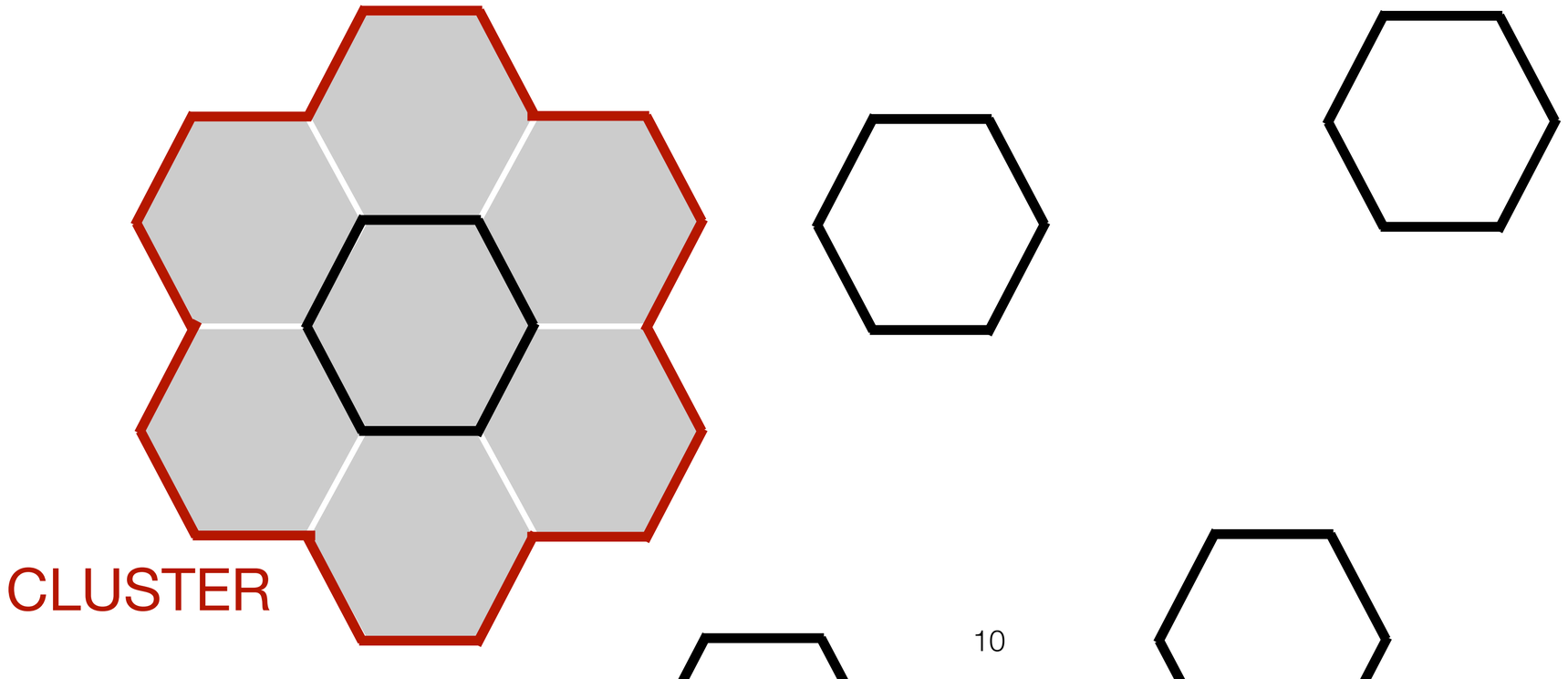
- Honeycomb grid (i.e., representation of each cell as a hexagon) is the model typically used for for theoretical representation of area division in cellular networks.
- In reality, the coverage area looks more like this:



Overlapping and uncovered areas are still there.
Still, honeycomb is the most used model and the one we will stick with

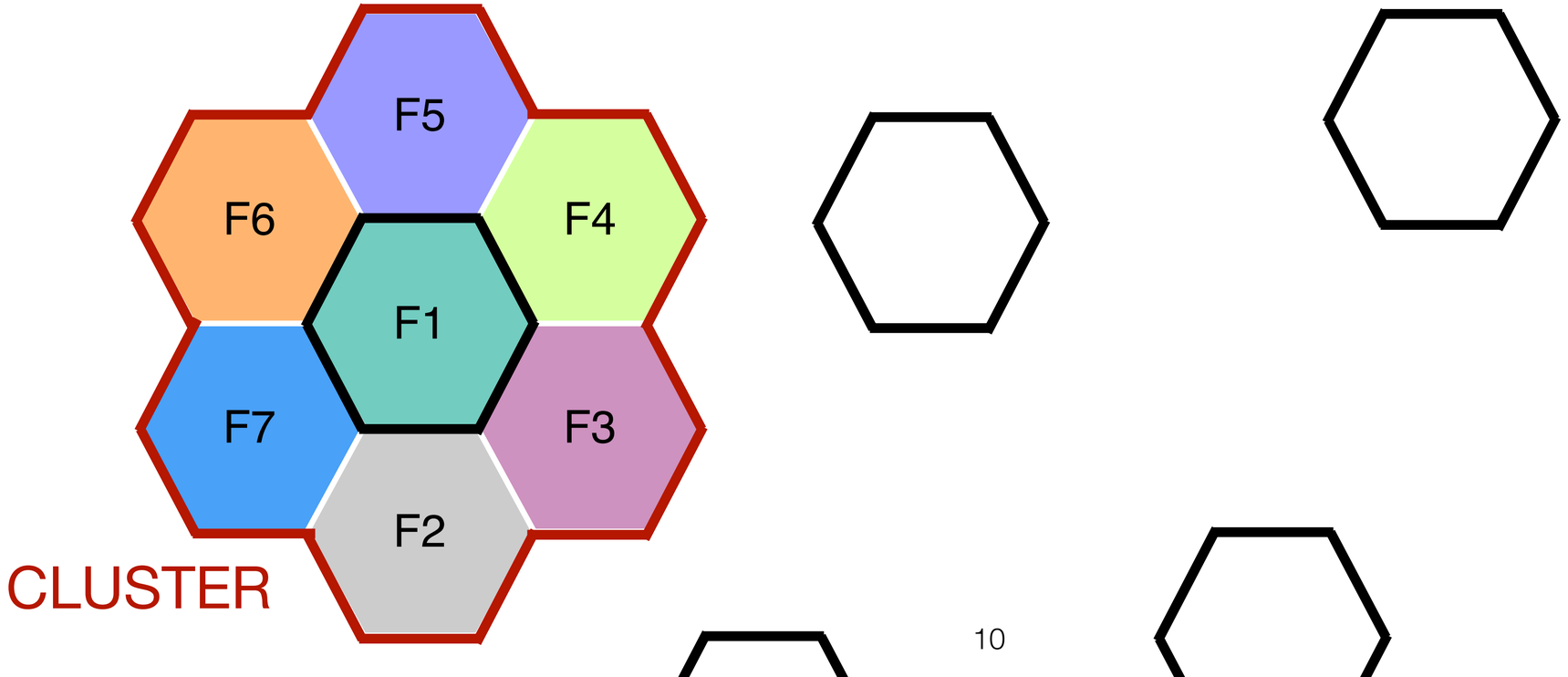
Frequency Reuse

- Frequency reuse or frequency planning consists in separating the frequency bands into sub-bands (i.e., different channels), and assign the same frequencies to different base stations (i.e., cells) that are distant enough.
  - Avoid collisions between neighbouring cells



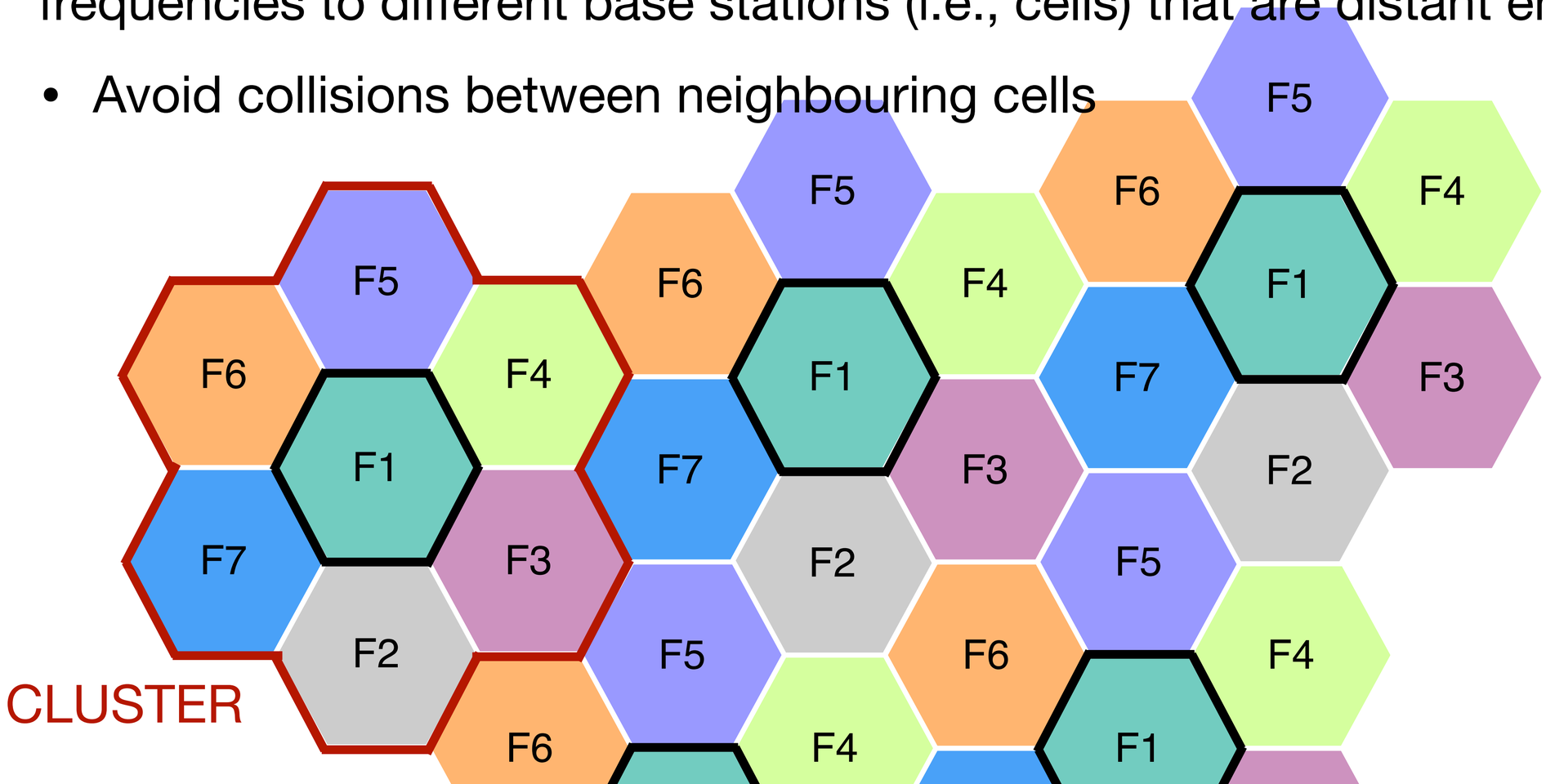
Frequency Reuse

- Frequency reuse or frequency planning consists in separating the frequency bands into sub-bands (i.e., different channels), and assign the same frequencies to different base stations (i.e., cells) that are distant enough.
  - Avoid collisions between neighbouring cells



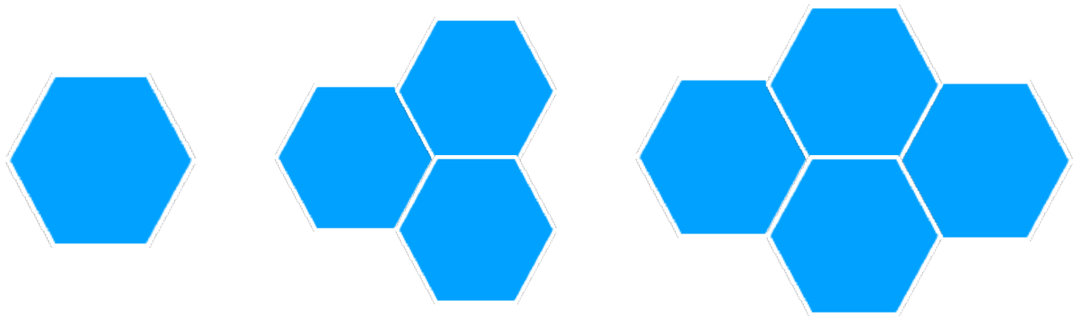
Frequency Reuse

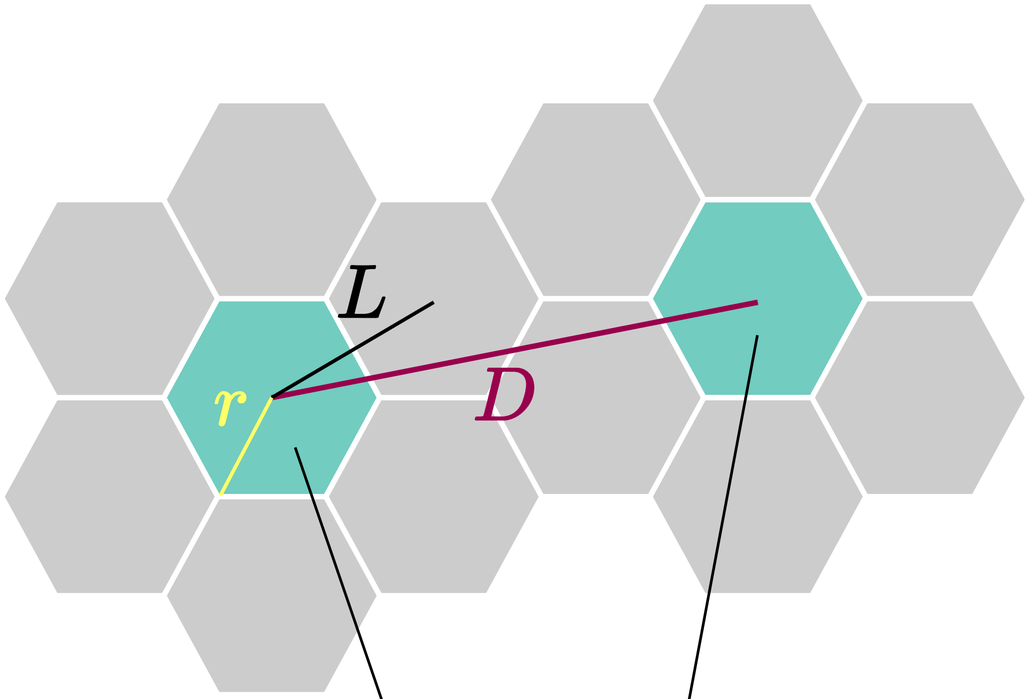
- Frequency reuse or frequency planning consists in separating the frequency bands into sub-bands (i.e., different channels), and assign the same frequencies to different base stations (i.e., cells) that are distant enough.
  - Avoid collisions between neighbouring cells



Cluster Sizes

- A cluster of cells is a group of N cells such that the resulting shape of the cluster is tesselable.
- Within each cluster, all cells are associated with different frequencies.
- A cluster of N cells can be built if $\exists i, j \in \mathbb{N}\, s\,.\,t\,.\, N = i^2 + ij + j^2$
- N is the **cluster size**.
- Possible values of N are 1,3,4,7,9,…





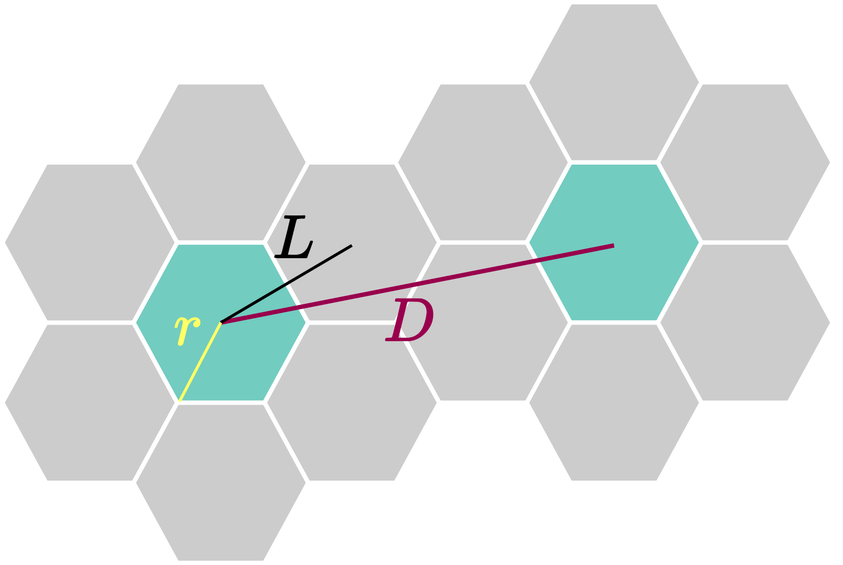
Co-cells/co-channels
(same frequency band)

- The **reuse distance** D is the minimum distance between two cells using the same frequency band.
- $D = \sqrt{3N}r$, where r is the radium of the hexagon and N is the cluster size (proof omitted).
- $q = \frac{D}{r} = \sqrt{3N}$ is called **reuse factor.**
- Low reuse factor (small N, large r) is best for rural areas or low-density networks.
  - less interference and capacity
- Large reuse factor (large N, small r) best for dense, urban area.
  - more interference and capacity

- Total number of available radio channels in a cluster: $S = kN$, where
  - k is the number of channels per cell, N is the cluster size.
- If the cluster is repeated m times in a area, then the total number of channels is $mS = mkN$

Cell Sectoring

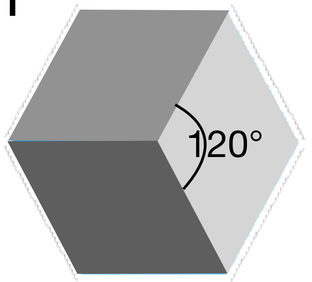
- If the reuse distance D is not big enough, then two co-channels can interfere with one another.



- One possible solution is placing directional antennas at each cell. They virtually divide the cell into **sectors**.

- In 3-cell sectoring, the frequency band of the cell is divided into 3 sub-bands. One directional antenna uses one such sub-bands, and directs signals towards its direction.

- The round angle is split into three angles of 120° each, dividing the cell into three sectors, one for each antenna.



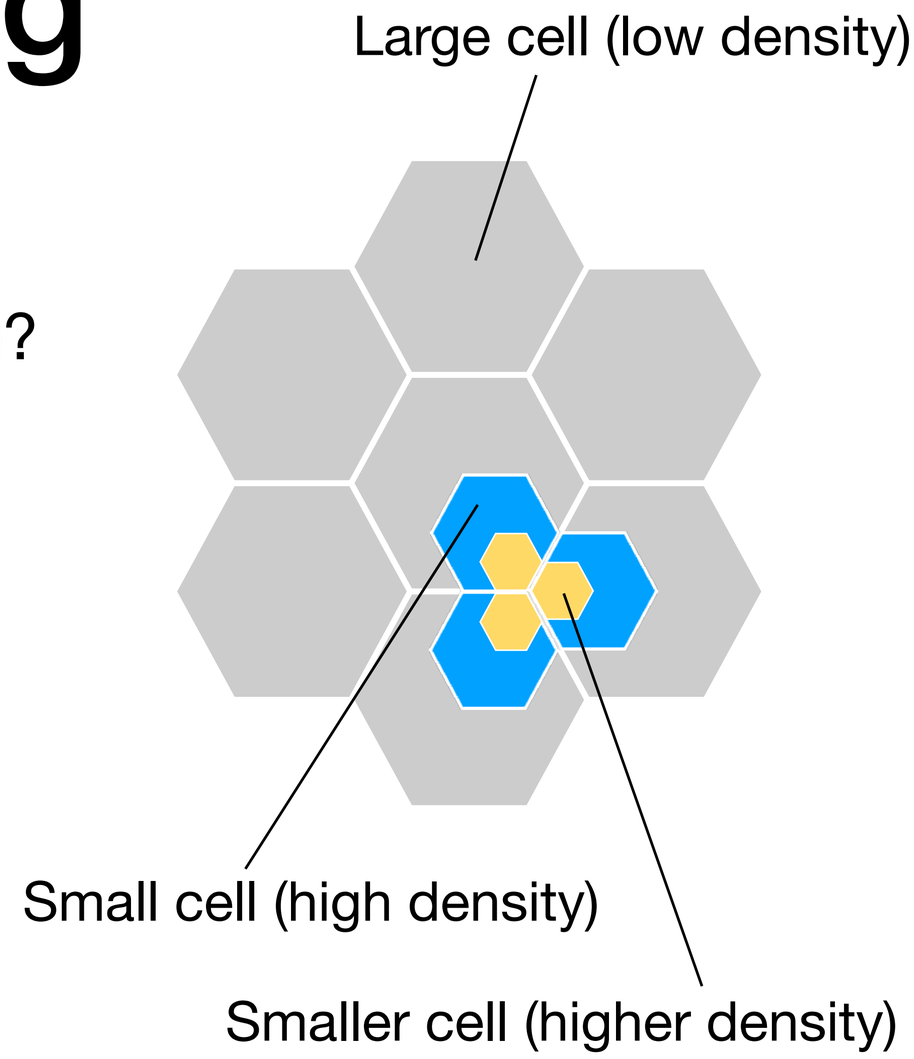
- Less interference between co-cells.
- Better isolation.
- More frequency reuse
- Lower power needs

Cell Splitting

- What do we do if the demand for more data rate increases in a region (e.g., an area gets more densely populated with the passing of the years)?

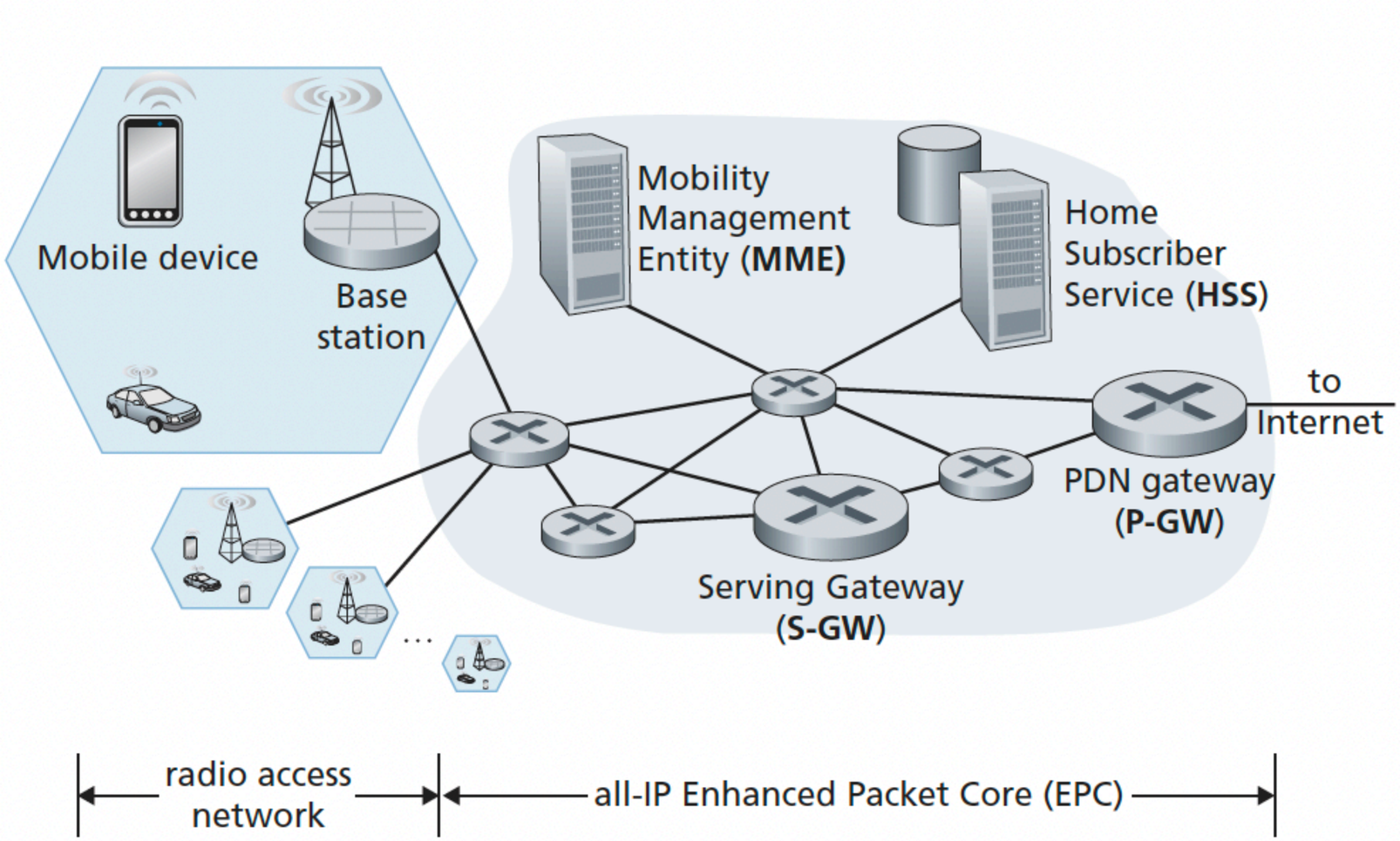
- Split existing cells by adding more base stations to provide more data rate.

Depending on traffic conditions, smaller antenna cells may be activated or deactivated for better resource usage.



7.2 4G LTE

Elements of the 4G LTE architecture



- Based on LTE (Long-term evolution) standard.
- Entirely IP-based, even for voice (VoIP/VoLTE).
- Orthogonal Frequency Division Multiple Access (OFDMA) and Multiple Input Multiple Output (MIMO).
- Higher data rates.
- IoT applications.
- LPWA-based licensed band technology.

Mobile Device

- Smartphones, tablets, laptops, or IoT devices that connect to a cellular network.
- Applications such as web browsers, map apps, voice and videoconference apps, mobile payment apps etc are run on mobile devices.
- Each mobile device is a network endpoint, with an IP address.
- Each mobile device also has a global unique 64-bit identifier called the **International Mobile Subscriber Identity** (**IMSI**), which is stored on its **SIM** (Subscriber Identity Module) card.
- The SIM card also stores information about the services that the subscriber is able to access. They depends on the “home network” or network operator of the SIM card.

Base Station

- The base station (BS) is a fixed station that covers an area. It consists of transmitter and receiver antennas mounted on a cell tower.

- A BS is responsible for managing the wireless radio resources and the mobile devices with its coverage area.

- Mobile device interact with a base station to attach to the carrier network (i.e., the internet or the telephone line), similarly to access points in WLANs.

- They provide the connection from the mobile devices to gateways, interact among themselves to **handle device mobility** among cells and **minimize interference between cells**. They are connected with one another through cables - no wireless.

Home Subscriber Server

- The Home Subscriber Server (HSS) is a database, storing information about the mobile devices for which the HSS’s network is their home network.

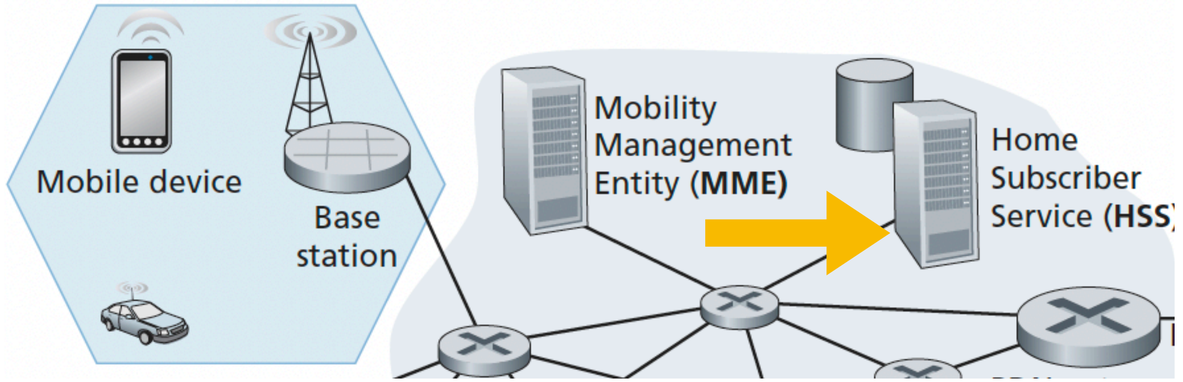
- It is used in conjunction with the Mobility Management Entity (MME) for device authentication.

Network Routers

- Serving Gateway (S-GW) and the Packet Data Network (P-GW) Gateway are two routers (often collocated in practice) that lie on the data path between the mobile device and the Internet.
- The Packet Data Network Gateway provides IP addresses to mobile devices.
  - To the outside world, the P-GW looks like any other gateway router.
- The Serving Gateway routes and forwards user data packets

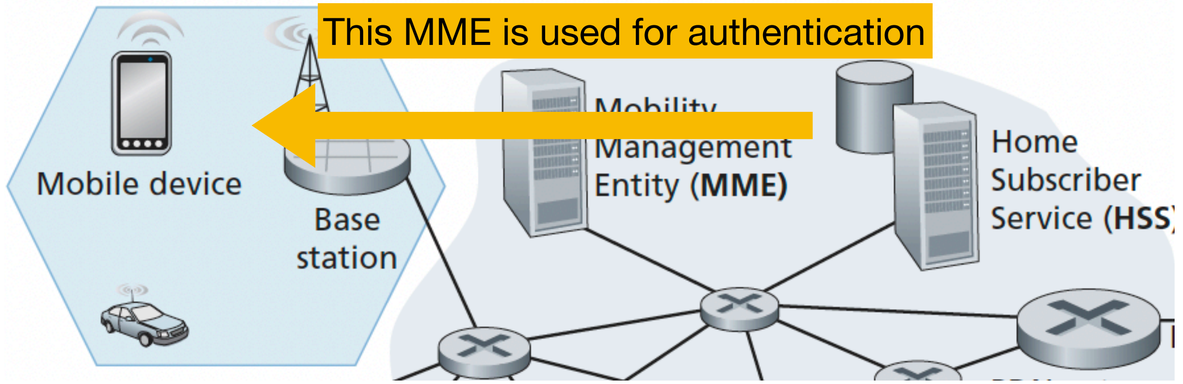
Mobility Management Entity (MME)

- The Mobility Management Entity (MME) serves to **authenticate** a device wanting to connect into its network.
  - After receiving an attach request from mobile device, the local MME contacts the home subscriber server in the mobile's home network.



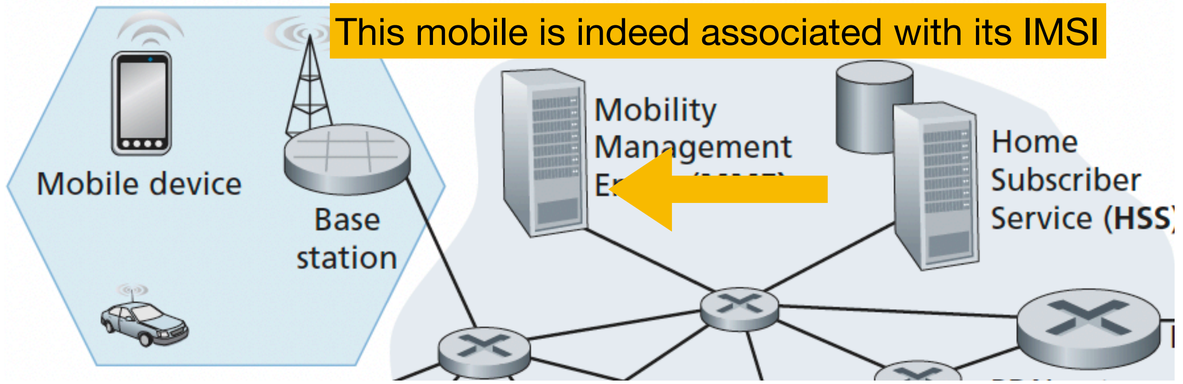
Mobility Management Entity (MME)

- The Mobility Management Entity (MME) serves to **authenticate** a device wanting to connect into its network.
  - After receiving an attach request from mobile device, the local MME contacts the home subscriber server in the mobile's home network.
    - The mobile device receives encrypted data confirming that the home HSS is performing authentication through this MME.



Mobility Management Entity (MME)

- The Mobility Management Entity (MME) serves to **authenticate** a device wanting to connect into its network.
  - After receiving an attach request from mobile device, the local MME contacts the home subscriber server in the mobile's home network.
    - The mobile device receives encrypted data confirming that the home HSS is performing authentication through this MME.
    - The MME gets confirmation that the mobile is indeed the one associated with the advertised IMSI.

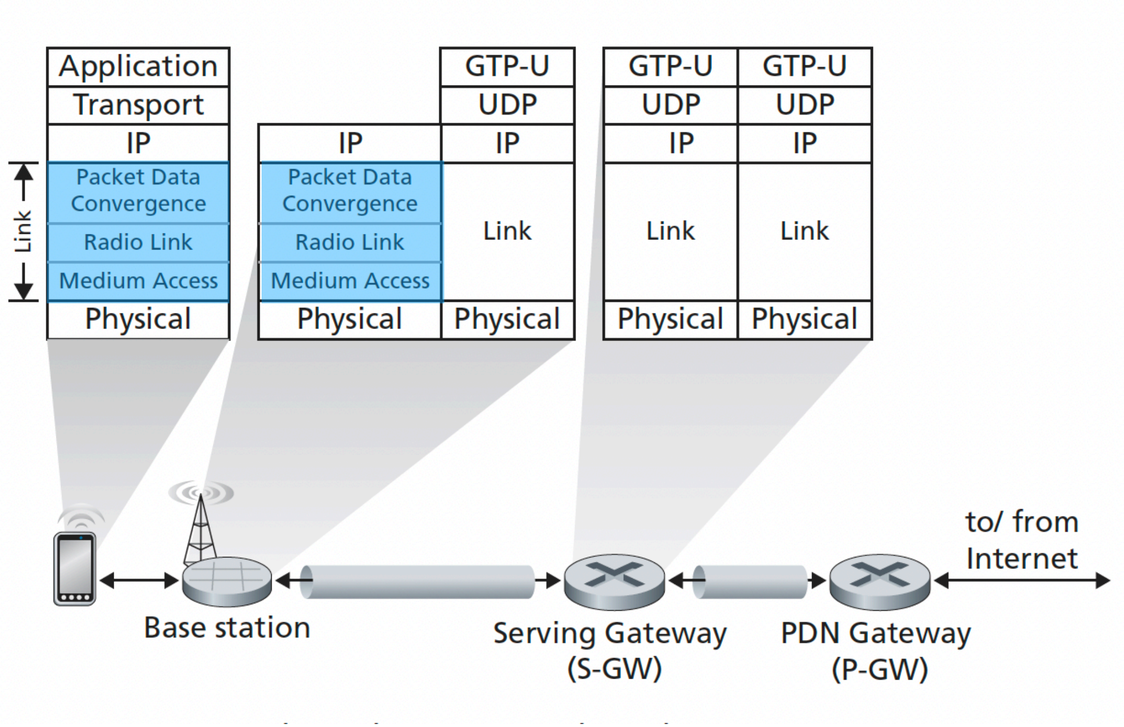


Mobility Management Entity (MME)

- The Mobility Management Entity (MME) serves to **authenticate** a device wanting to connect into its network.
  - After receiving an attach request from mobile device, the local MME contacts the home subscriber server in the mobile's home network.
    - The mobile device receives encrypted data confirming that the home HSS is performing authentication through this MME.
    - The MME gets confirmation that the mobile is indeed the one associated with the advertised IMSI.
- It sets up the **tunnels** on the data path from/to the device and the PDN gateway router.
- Maintains information about an active mobile device's cell location within the cellular network (**Cell Location tracking**).

LTE Protocol Stack

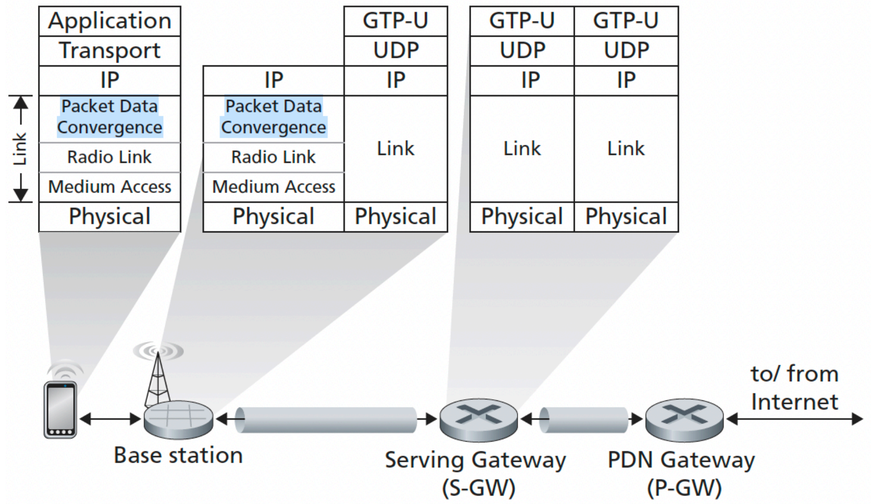
- 4G LTE architectures support the entire TCP/IP stack.
- Most of the user-plane protocol activity happens at the wireless radio link between the mobile device and the base station (**Device Link Layer**).



LTE Device Link Layer

The Device Link Layer is divided into three sublayers:

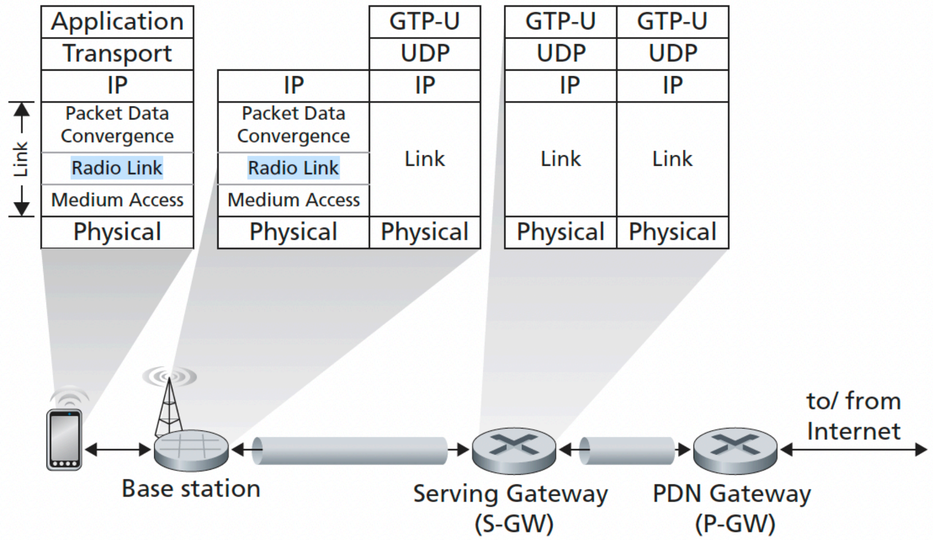
- **Packet Data Convergence sublayer.**
  - Sits just below the IP protocol.
  - The Packet Data Convergence Protocol (PDCP) performs:
    - IP header compression, in order to decrease the number of bits sent over the wireless link.
    - Encryption/Decryption of the IP datagram.



LTE Device Link Layer

The Device Link Layer is divided into three sublayers:

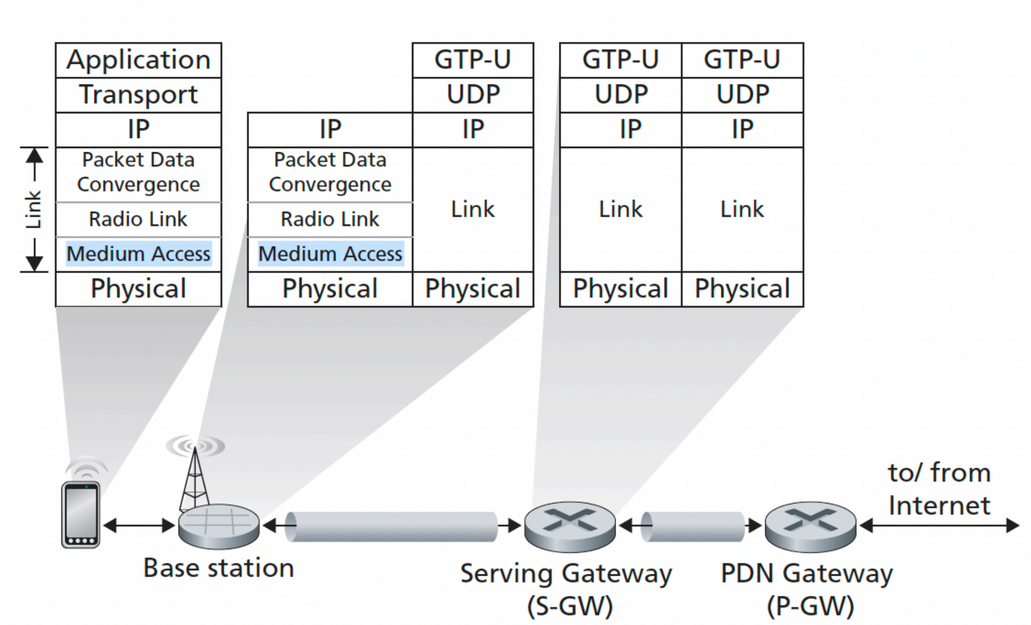
- **Radio Link Control sublayer.**
  The Radio Link Control Protocol (RLCP) performs:
  - Fragmenting and reassembly of IP datagrams that are too large to fit into the underlying link-layer frames.
  - Link-layer reliable data transfer.



LTE Device Link Layer

The Device Link Layer is divided into three sublayers:

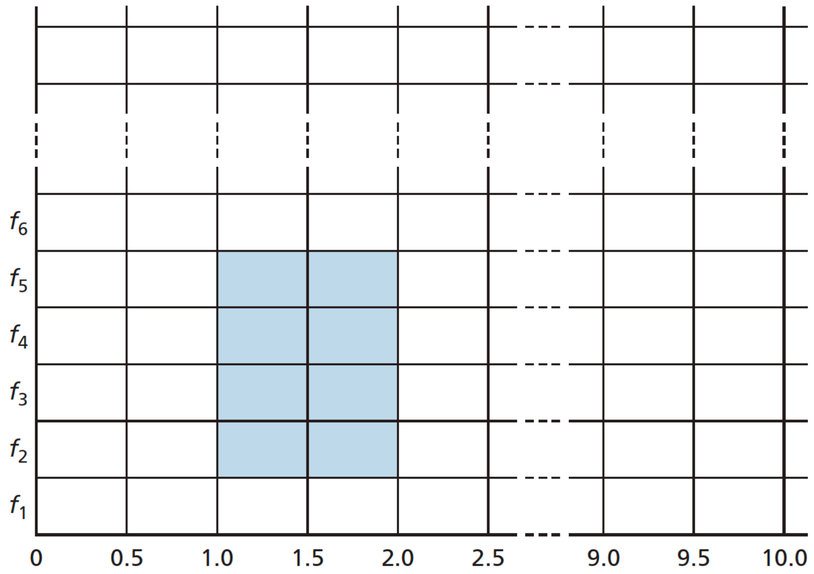
- **Medium Access Control (MAC).**
  The MAC layer performs:
  - Transmission scheduling (assignment of transmission slots)
  - Error detection/correction functions



LTE Radio Access Network

- LTE uses orthogonal frequency division multiplexing (OFDM) with TDM (0.5 ms slots).
- In LTE, each active mobile device is allocated one or more 0.5 ms time slots in one or more of the channel frequencies.
- Slot (re)allocation among mobile devices can be performed every millisecond.
- Different modulation schemes can also be used to change the transmission rate.
- The LTE standard does not define particular slot allocation strategies.
  -> This decision is determined by the scheduling algorithms provided by the LTE network operator.

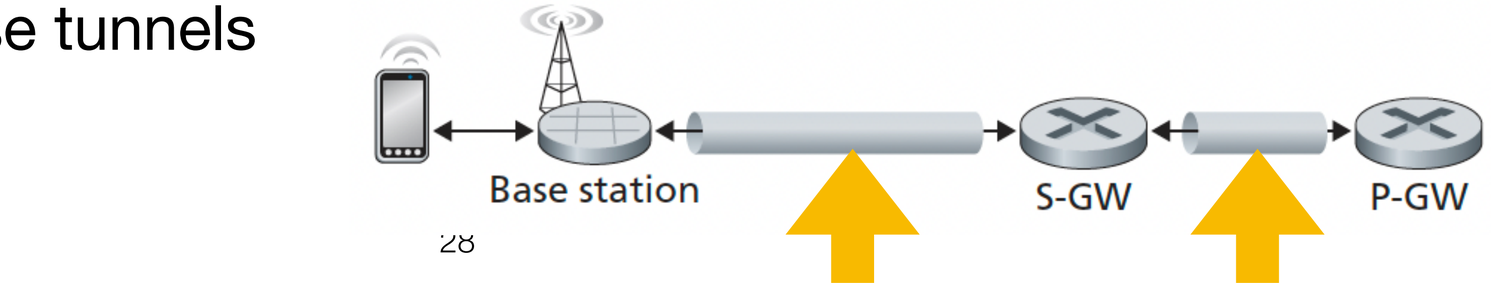
Twenty 0.5-ms slots organized into 10 ms frames at 4 frequency (eight-slot allocation)



Network Attachment

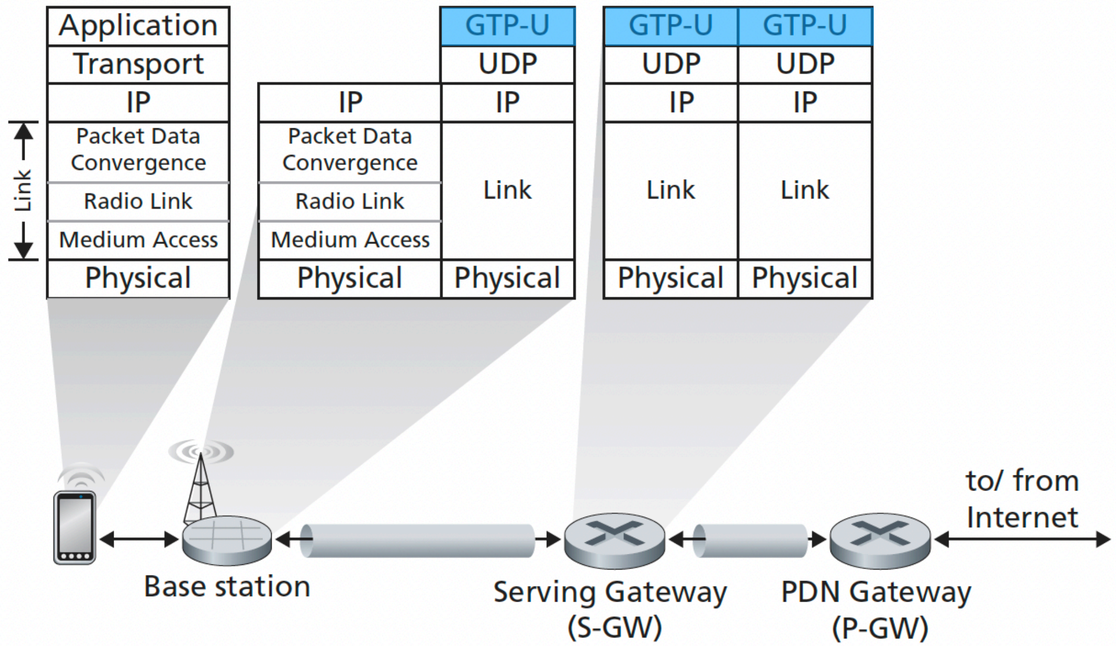
Network attachment is the process by which a mobile device attaches to the cellular network. It is divided into three phases:

- **Attachment to a Base Station.**
  - The mobile device initially searches all channels in all frequency bands and broadcasts signals every 5 ms and selects a base station to associate with (preferentially attaching to its home network if available).
- **Mutual Authentication.**
  - The base station contacts the local MME to perform mutual authentication.
- **Mobile-device-to-PDN-gateway Data Path Configuration.**
  - MME Creates these tunnels



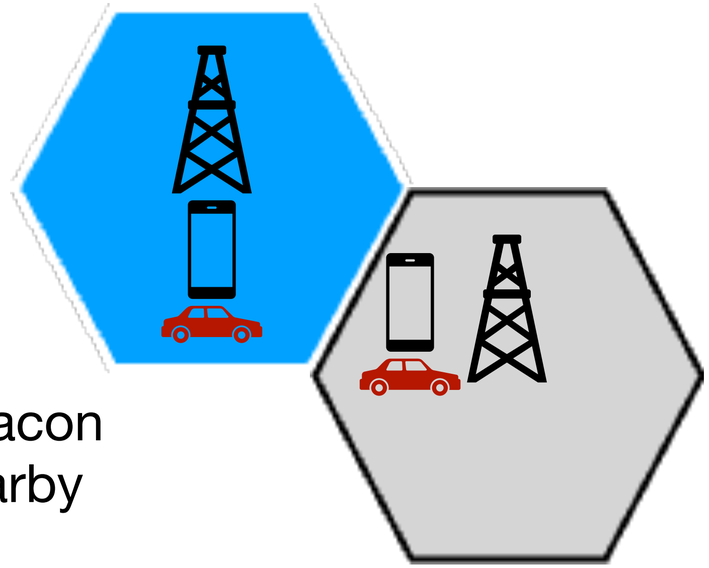
Tunnels

- Tunnelling is a communication technique to **encapsulates** the data packet sent by a host to another host.
- This technique enables secure access to network resources and services over the internet (e.g., connecting hosts in the same enterprise network deployed in two different areas of the Internet).
- Used for VPN and by IPv6 to route through IPv4 routers.
- In cellular networks, tunnelling protocols (e.g., GTP-U in 4G), are used to assign a **stable and unique IP address** to a cellular device as it **moves** through different areas covered by different base stations or even different network providers, allowing uninterrupted data flowing.



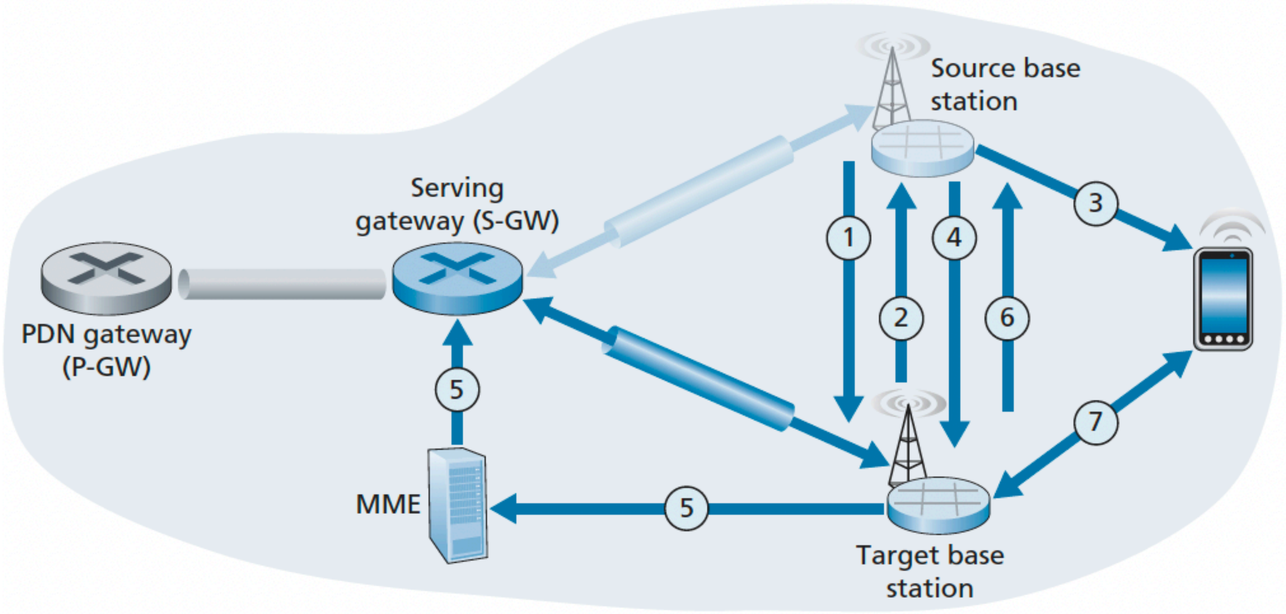
Handover

- A handover occurs when a mobile device changes its association from one base station to another.
- Reasons for handover to occur:
  - Severe signal degradation
  - Cell may have become over loaded, handling a large amount of traffic.
  - Mobility.



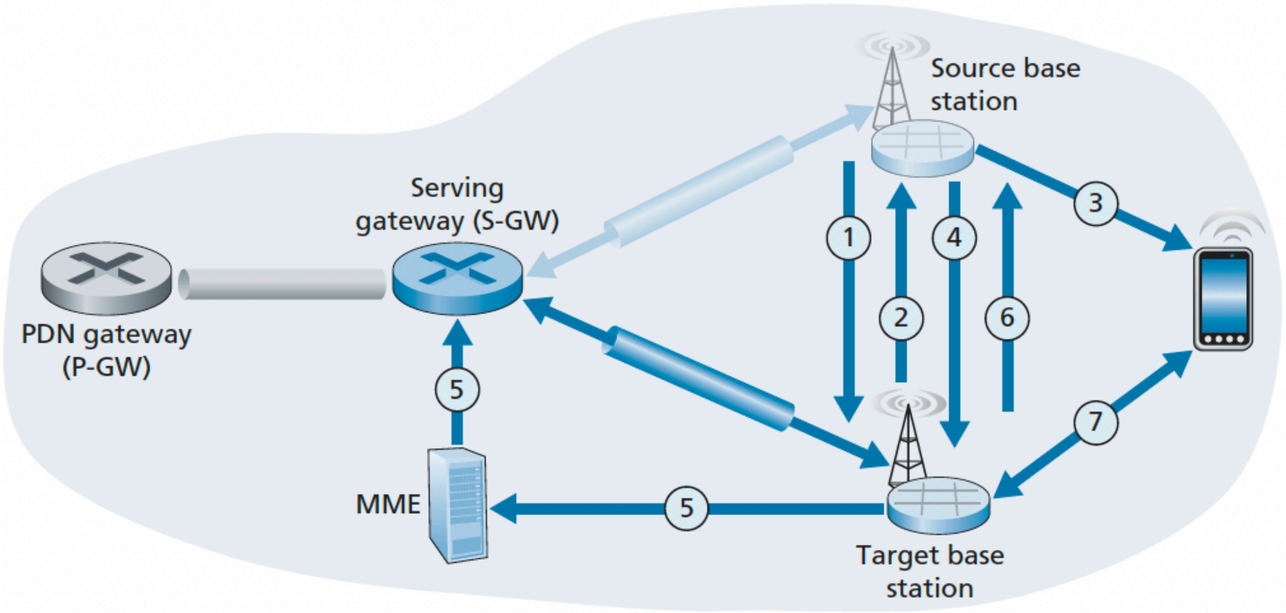
- A mobile device periodically measures characteristics of a beacon signal from its current base station as well as signals from nearby base stations that it can “hear.”
- These measurements are reported once or twice a second to the mobile device’s current (source) base station.
- Based on these measurements, the current loads of mobiles in nearby cells, and other factors, the source base station may choose to initiate a handover.

Handover



1. The current (source) base station selects the target base station, and sends a **Handover Request.**
2. The target base station checks whether it has the resources to support the mobile device and if so it preallocates them and acks the source BS.
3. The source base station receives the **Handover Request Acknowledgement** and informs the mobile device of the target base station's identity and channel access information.
4. The source base station stops forwarding datagrams to the mobile device and instead forwards any tunnelled datagrams it receives to the target base station.

Handover



5. The target base station informs the MME that it (the target base station) will be the new base station servicing the mobile device. The MME reconfigures the Serving-Gateway-to-base-station tunnel.
6. The target base station confirms to the source base station that the tunnel has been reconfigured.
7. The target base station can begin delivering datagrams to the mobile device.

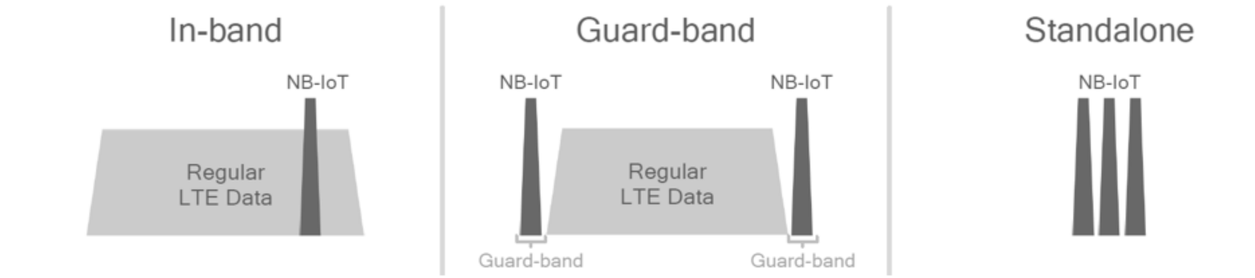
7.3 NB-IoT (overview)

NB-IoT

- NB-IoT (Narrowband IoT) is a technology that uses **cellular communication** for IoT purposes.
- It relies on **LTE infrastructures**, but uses narrow bands:
  - LTE devices and networks have 20 MHz bandwidth per channel and achieve high-speed data rates.
  - NB-IoT networks only use 180 kHz bandwidth (or 200 kHz max), that is the size an **LTE resource block (RB**) that is the smallest unit of resource that LTE can assign to a user for transmission.

NB-IoT

- Three deployment modes:
  - **In-band**: NB-IoT operates inside LTE carriers, using one of the physical resource blocks (PRBs) of the LTE channel.
  - **Guard-band**: NB-IoT signals deployed in the guard bands of the LTE channel (although LTE uses OFDM, LTE systems still include guard bands at the edges of the spectrum allocation).
  - **Standalone**: NB-IoT operates in dedicated spectrum, not shared with LTE.



Utilizing single resource block (180kHz) within an LTE carrier

Utilizing unused resource blocks within an LTE carrier guard-band

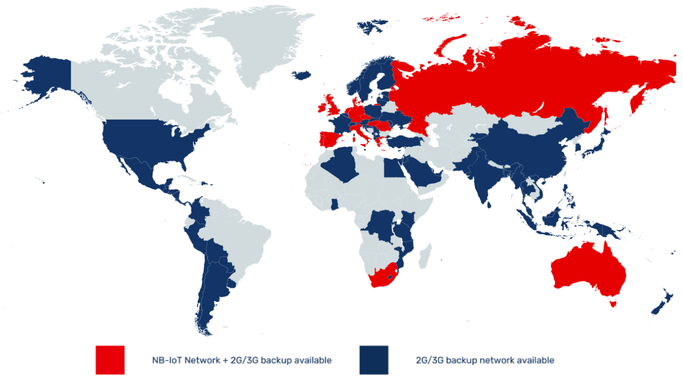
Utilizing stand-alone 200 kHz carrier

NB-IoT

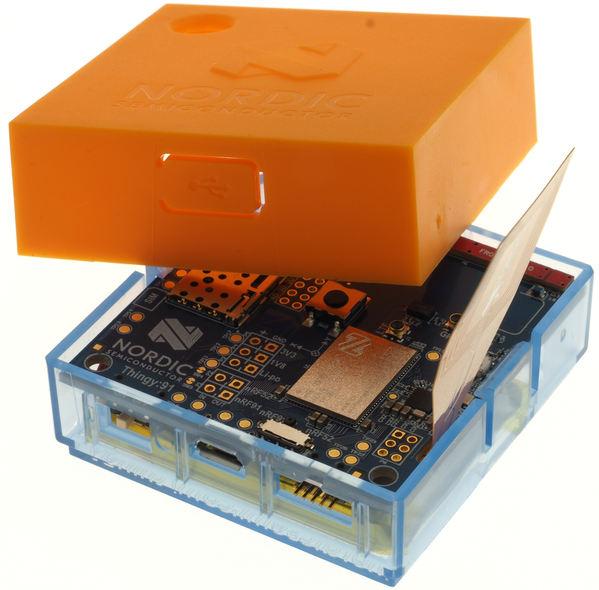
- NB-IoT has **better penetration** abilities than LTE and can reach deep indoor areas (basements etc) because it uses more power over a smaller bandwidth, making the signal much stronger per each frequency
- NB-IoT modules are cheaper than full LTE.
- Achieves massive number of devices, up to ~50,000 per cell.
- Support low data rate, perfect for IoT applications where nodes have to send on small data packets infrequently.
- Very efficient low power mode.

NB-IoT

- NB-IoT modules require special NB-IoT sim cards.
- Commercial mobile phones do have NB-IoT modules.
- Still has good coverage



NB-IoT module
for raspberry PI



Nordic Thingy:91

Bibliography

- Kurose, James F., and Keith W. Ross. "Computer networking: A top-down approach edition." Addision Wesley, eighth edition.

- Hanes, David, et al. IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things. Cisco Press, 2017.