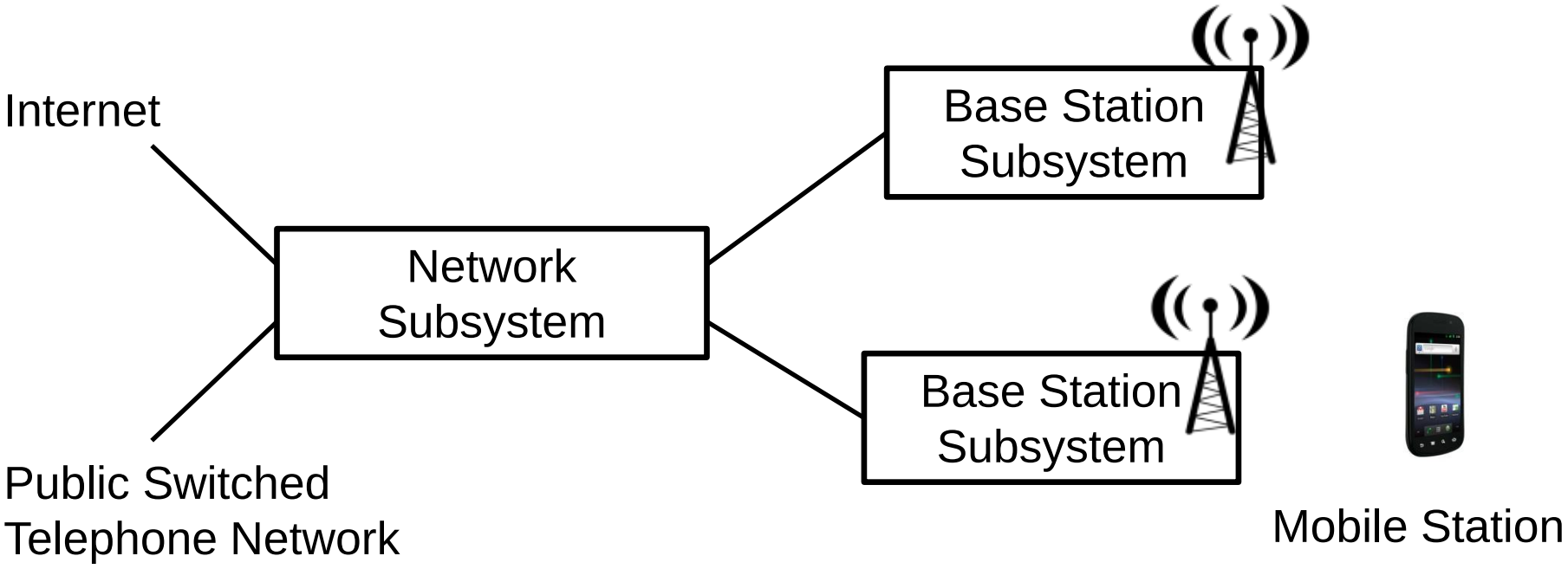
GSM

Generations

- 1G = analog mobile phone networks (C-Netz,…)
- 2G = GSM
- 2.5G = GPRS
- 2.75G = EDGE
- 3G = UMTS, CDMA2000
- 3.5G = HSPA
- 3.75G = HSPA+
- 4G = LTE, WiMAX
- 5G = in progress

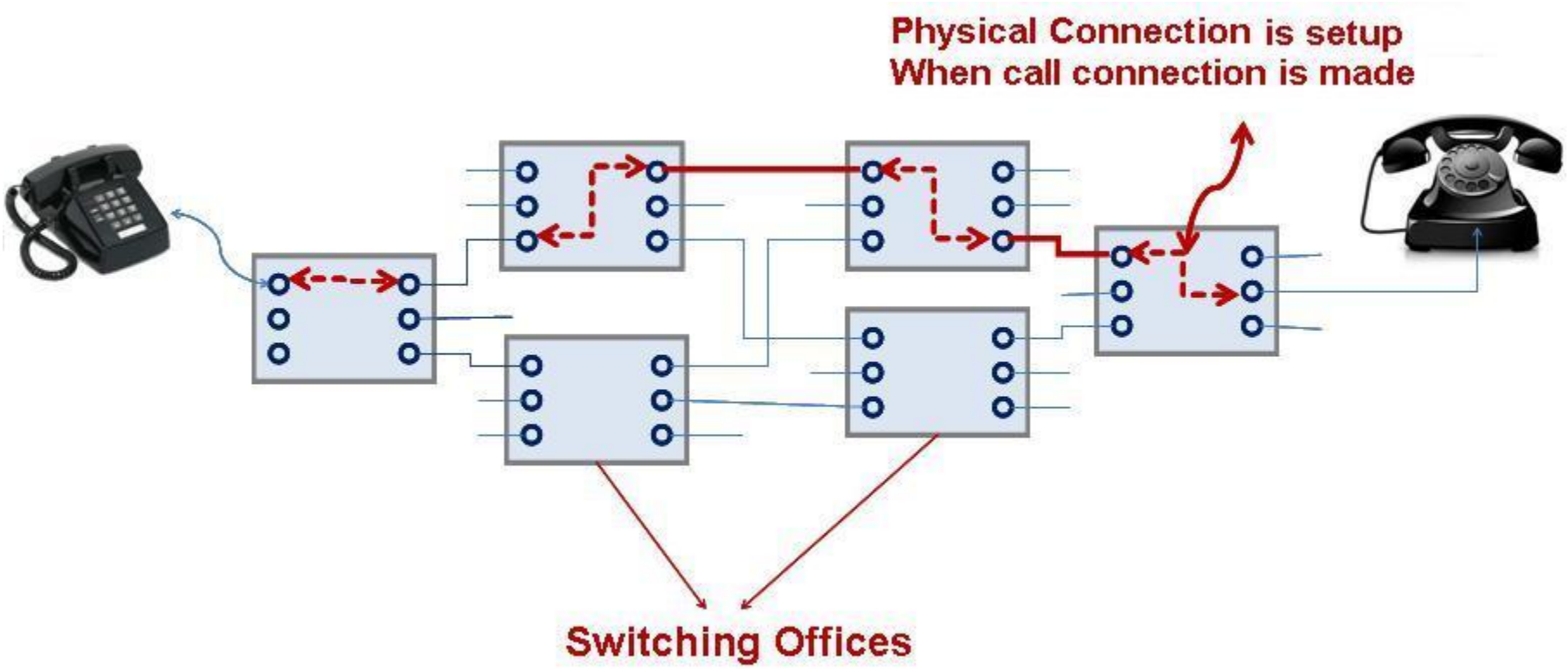
GSM

- GSM = Global System for Mobile Communications (originally: Groupe Spécial Mobile)
- 2nd generation cellular radio network
- Uses SDMA, TDMA and FDMA



Fixed-line phone networks

- Short history lesson: Fixed-line phone networks were originally circuit-switched



Source: computernetworkingsimplified.com

Signaling in fixed-line networks

- How was the connection set up (and teared) down?

  → Signaling protocol
- First signaling protocols were *in-band:* Signaling uses the same channel as the voice and data
  1. Human operator
  2. Pulse dialing
  3. Tone dialing

- SS5 (Signaling System No. 5): set of protocols for in-band signaling
- Advantage on in-band signaling: very easy to implement
- Disadvantage: Fraud. End user can hack the signaling by creating the right pulse or tone sequences

Out-of-band signaling

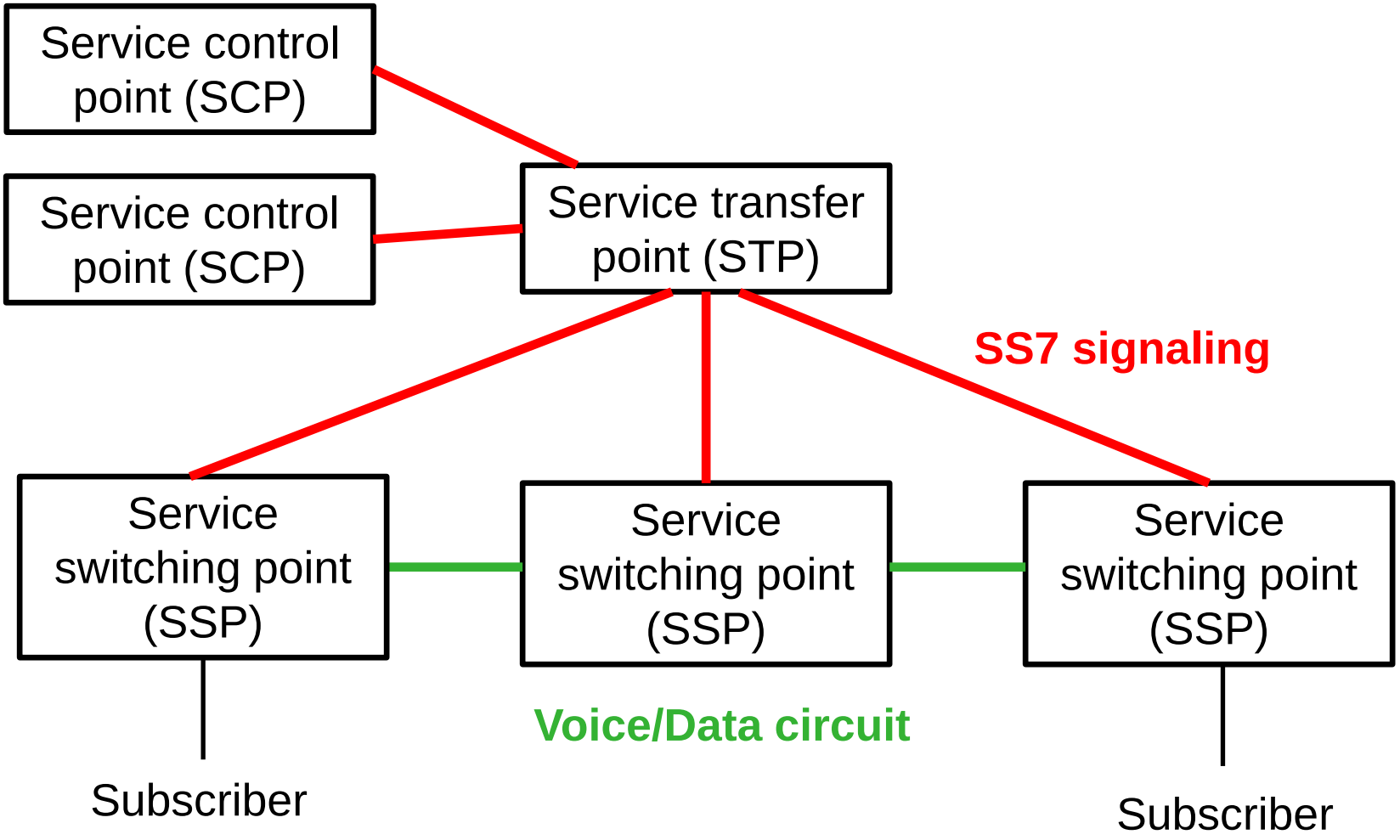
- Because of the disadvantage of SS5, SS6 was introduced in early 1970s
  - *Out-of-band* signaling: Separate digital channel for signaling, ~2.4kbit/s
  - Analog channels for voice (and later: data)
- Replaced by the more flexible and powerful SS7 in late 1970s

- SS7 is today the most popular signaling protocol for national and international phone networks

SS7 protocol stack

- SS7 is a packet-switched protocol
  - Messages for call setup and tear down
  - Also used for other kind of management information (billing, SMS,…)
- Protocol stack similar to IP
  - MTP-1 (Message Transfer Part 1): Physical layer
  - MTP-2: data link layer, defines packets
  - MTP-3: packet routing, packets have source and destination address called “point codes”

SS7 network architecture

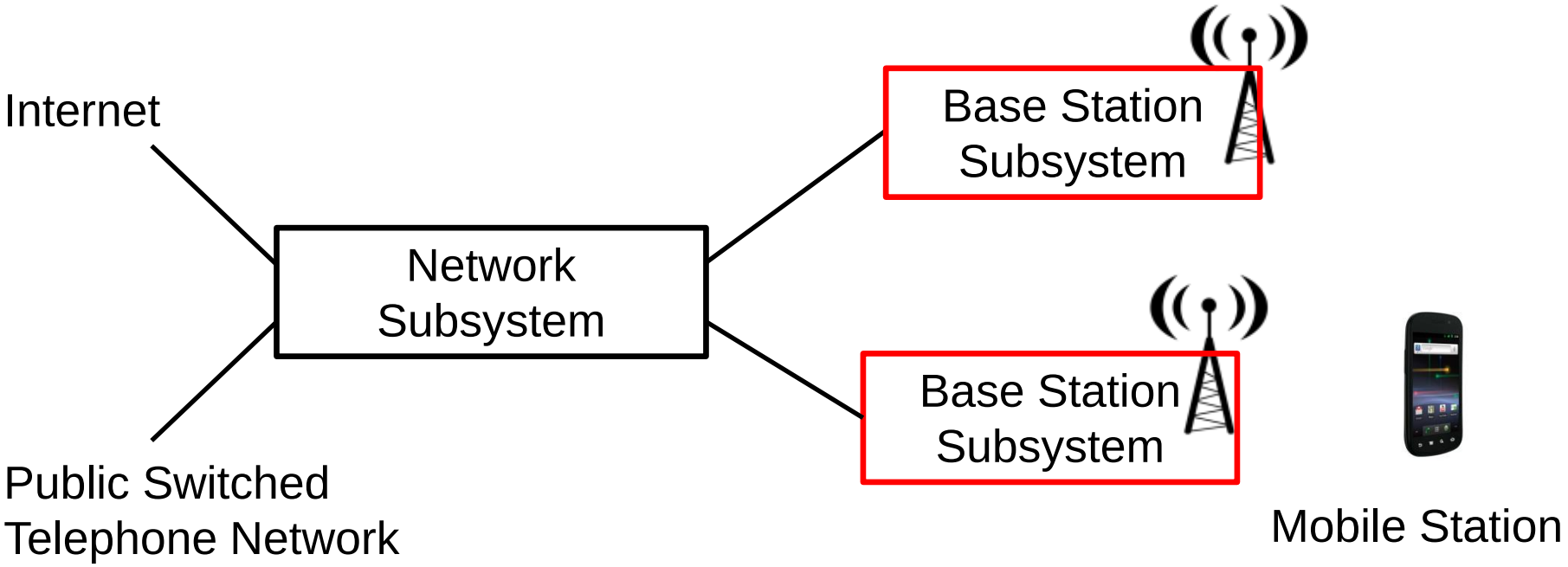


SSP = switching centers for voice and data connections
STP = router for signaling messages
SCP = run software and store information for connection management

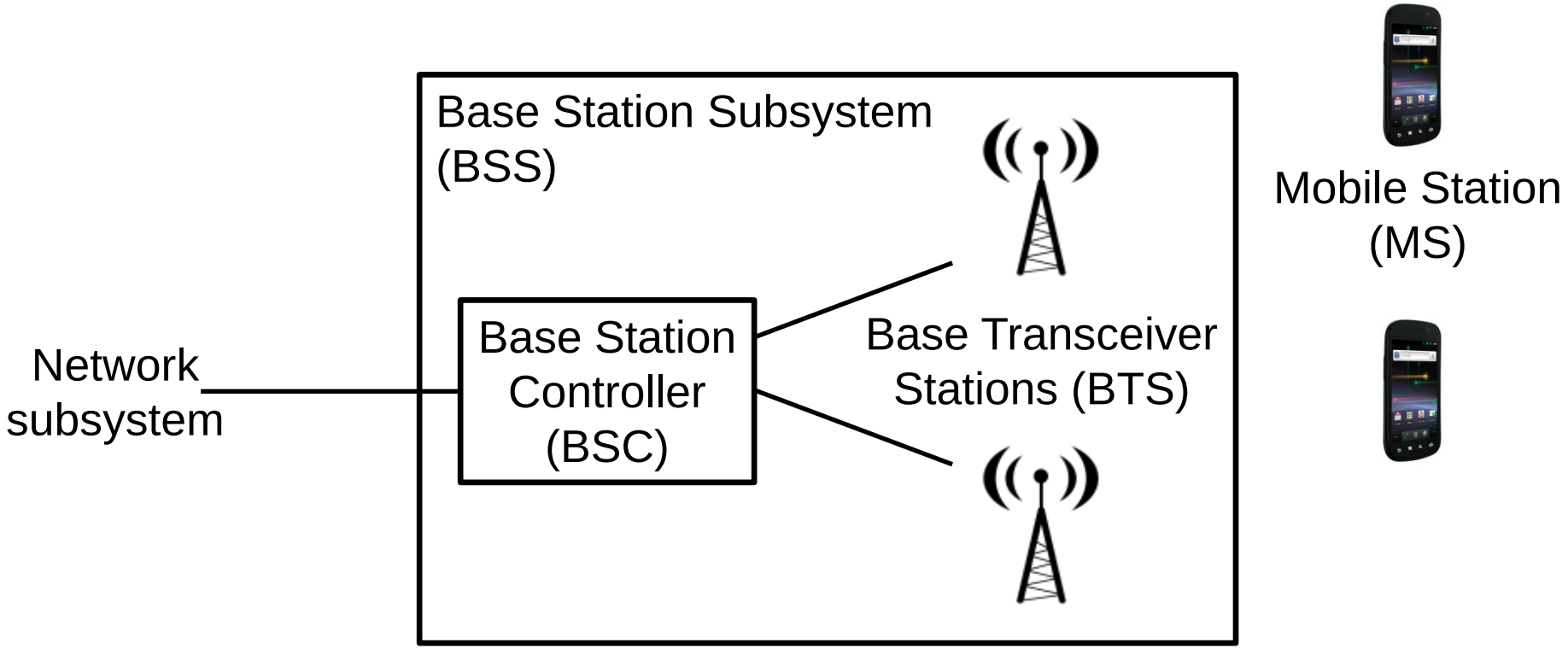
Beyond MTP

- MTP-1 to MTP-3 only define basic signaling functionality
- Other protocols run on higher layers, for example protocols for core network management, protocols for mobile call management, etc.
- SS7 nowadays runs over IP:
  - MTP-1 replaced by Ethernet
  - MTP-2 and MTP-3 replaced by
    - IP
    - SCTP (IP protocol, instead of UDP and TCP)
      - SCTP is a reliable transport protocol like TCP. Differences to TCP: message streams instead of byte streams, multi-streaming, multi-homing, connection bundling into single “associations”
    - M3UA (adaptation layer on top of SCTP to simulate MTP-3 functionality for higher layers)

GSM network


Internet
Network Subsystem
Public Switched Telephone Network
Base Station Subsystem
Base Station Subsystem
Mobile Station

Base Station Subsystem



- BSS contains all necessary components for the radio communication
- The network subsystem was developed to run with the existing telephone network (with new SS7 protocols), but the BSS had to be developed from scratch since existing mobile networks were analog

Frequency band

- GSM-900:
  - 124 downlink carrier frequencies from 935.2 MHz to 960 MHz (base station -> mobile station)
  - 124 uplink carrier frequencies from 890.2 MHz to 915 MHz (mobile station -> base station)
  - Each channel 200kHz bandwidth
  - 2 Watt transmission power in handset
- GSM-1800: 374 channels 1710-1880 MHz

- For cost reasons, a GSM mobile station operates on only *one* frequency at a time: It can either receive on a downlink frequency or transmit on an uplink frequency at a time.

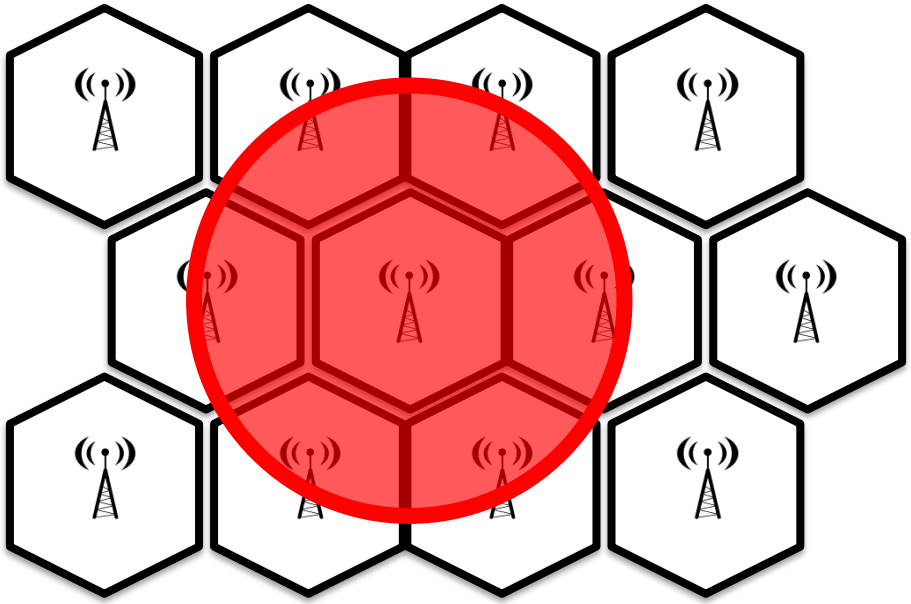
Base Transceiver Station

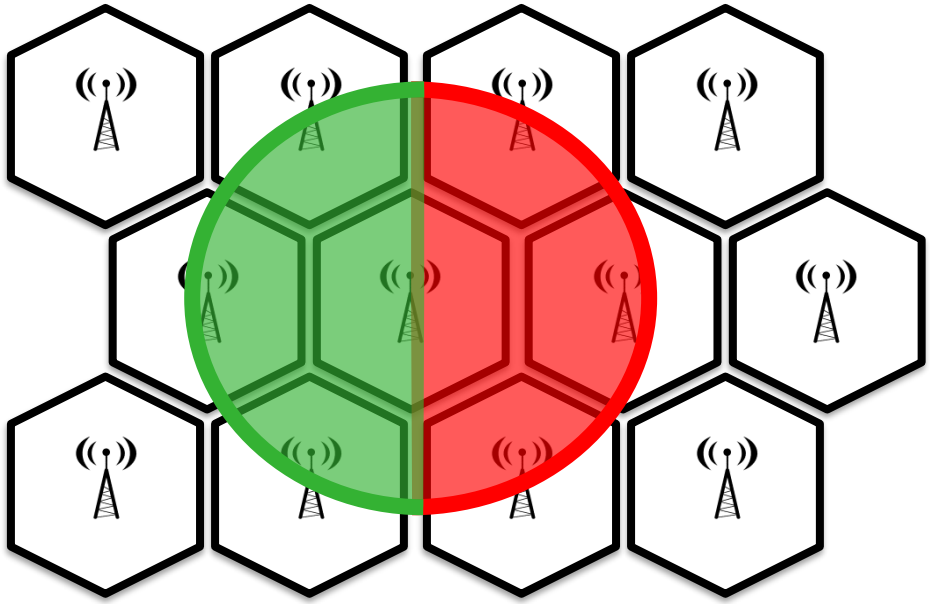
- O2 has around ~18000 BTS in Germany
- A BTS can cover an area ("*cell*") with a radius of up to 35km
  - But a BTS can only serve a limited number of users
  - In cities, cells of only 3-4 km or even down to a few 100 m in shopping centers etc.

Wikimedia.org

Cellular structure

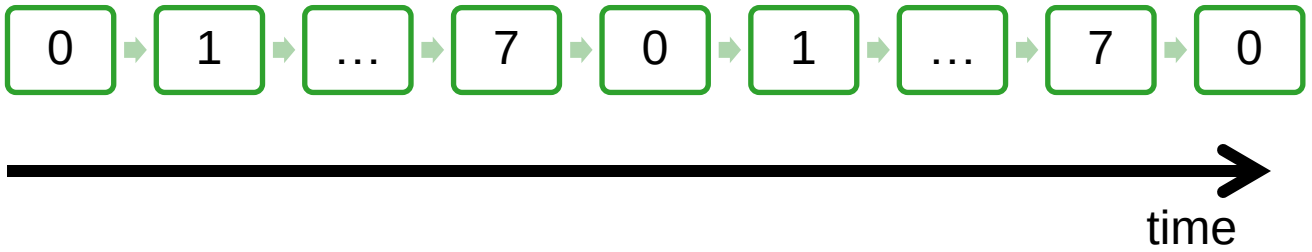
- Each BTS can use only a limited number of frequencies because of interferences with neighbor cells
- To increase capacity, the coverage area of a BTS is usually split into two or three sectors





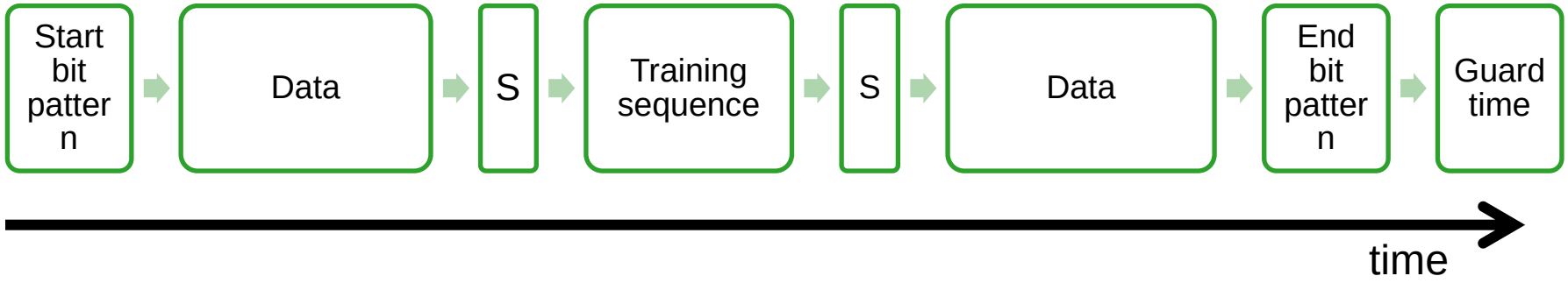
Timeslots

- Each carrier frequency is divided into 8 repeating timeslots ("bursts") of 0.577ms -> TDMA



- The 8 timeslots of a carrier frequency are called "*physical channels*"
  - A physical channel is identified by its frequency and timeslot number
- Example: base station with 6 frequencies -> 48 physical channels
  - Number of physical channels determines how many simultaneous active MS the base station can handle

Normal burst structure



- Guard time: prevents overlap between bursts
- Data: 2 fields of 57 bits = 114 bits per burst
- S bits: indicate that the data fields contain urgent signaling information instead of normal data
- Training data: contains a fixed bit pattern, used by the receiver to optimize its filter parameters in order to compensate for interferences

- This is the *Normal Burst* type used for voice and data
- There are special burst types for synchronization etc.

Timing

- TDMA requires exact timing
  - But signal propagation time depends on distance between phone and base station!
  - Guard times at the end of the Normal Burst help but they are very short in GSM

- How can we assure that phones stay in their timeslots?
- The base station measures the delay and sends signaling information to phone to adjust its timing (“Timing Advance”)