Communication Networks

VITMAB06

Mobile Networks 0G, 1G, 2G

Gusztáv Adamis

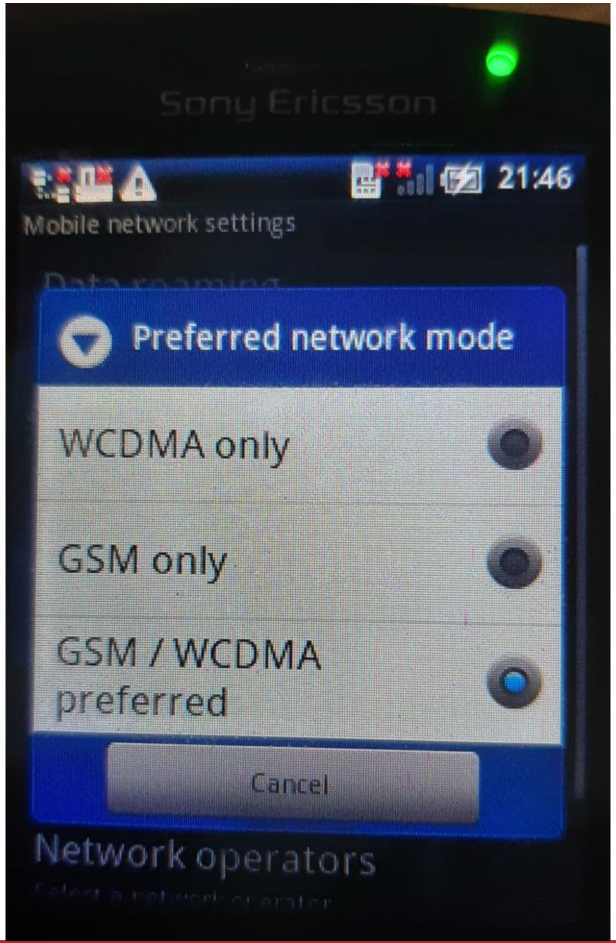
BME TMIT

2024

©

Motivation

- What do these mean on my phone at the top?
  - 2G
  - E
  - 3G
  - UMTS
  - WCDMA
  - H
  - H+
  - 4G
  - LTE
  - VoLTE
  - 5G



Mobile network settings

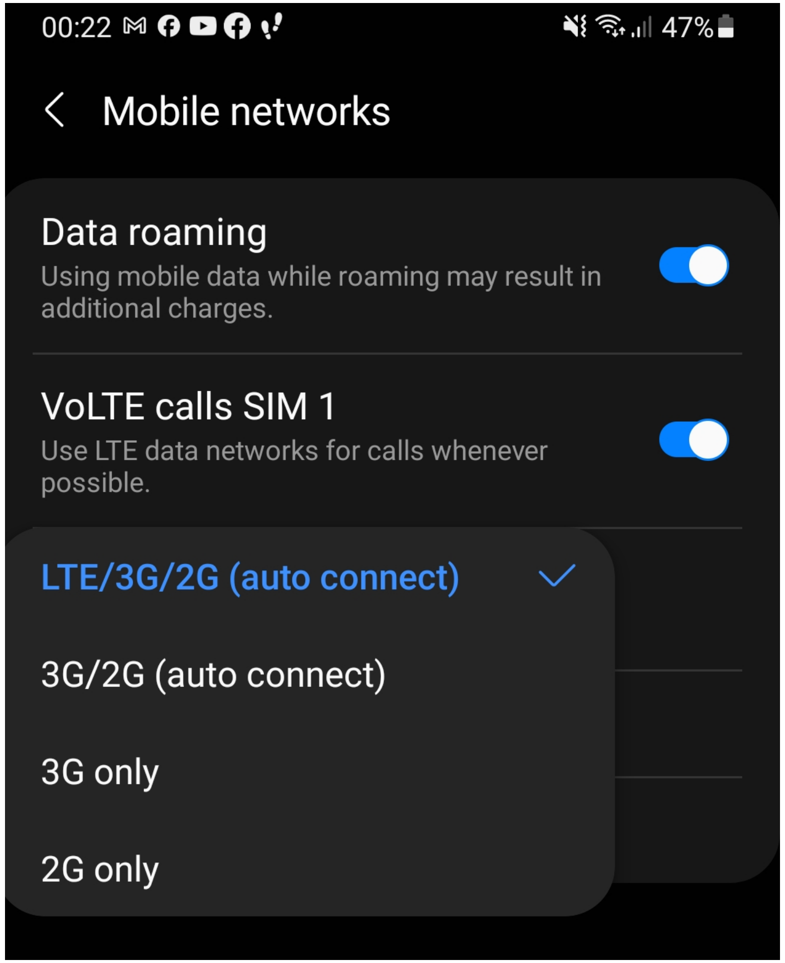
Data roaming

Preferred network mode

- WCDMA only ○
- GSM only ○
- GSM / WCDMA preferred ●

Network operators

Select a network operator



Mobile networks

Data roaming ●
Using mobile data while roaming may result in additional charges.

VoLTE calls SIM 1 ●
Use LTE data networks for calls whenever possible.

- LTE/3G/2G (auto connect) ✓
- 3G/2G (auto connect)
- 3G only
- 2G only

Mobile networks

- Early mobile networks (0G)
- Analog cellular networks (1G)
- GSM (2G)
- UMTS (3G)
- LTE (4G)
- 5G

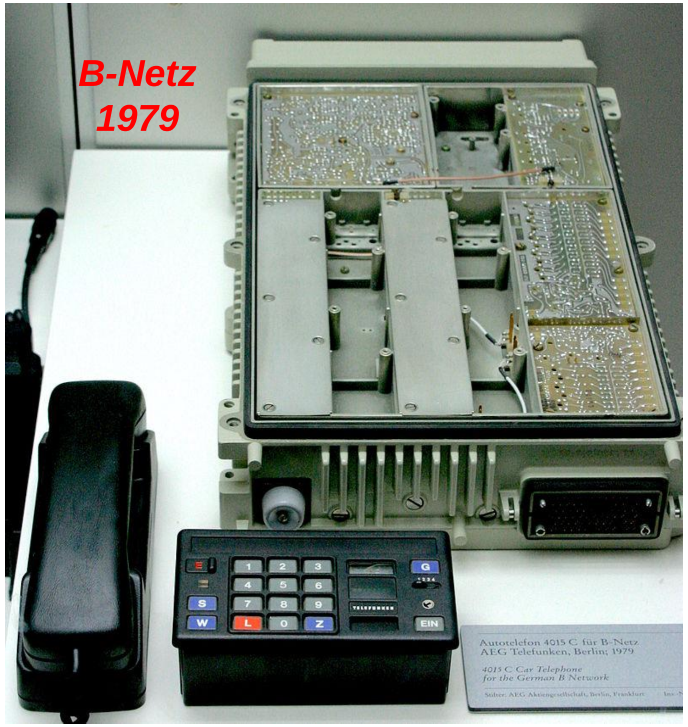
EARLY MOBILE NETWORKS

(0G)

0G

- Pre-1G mobile systems
- They were installed from 1946
- Analog systems, easy to eavesdrop
- Often built into a car
- They are simple, with few channels and few users
  - Typically non-public systems
- There was also a manual switching system

1964


EIN
Autotelefon 4015 C für B-Netz
AEG Telefunken, Berlin; 1979
4015 C Car Telephone
for the German B Network
Stifter: AEG Aktiengesellschaft, Berlin, Frankfurt

B-Netz
1979

0G

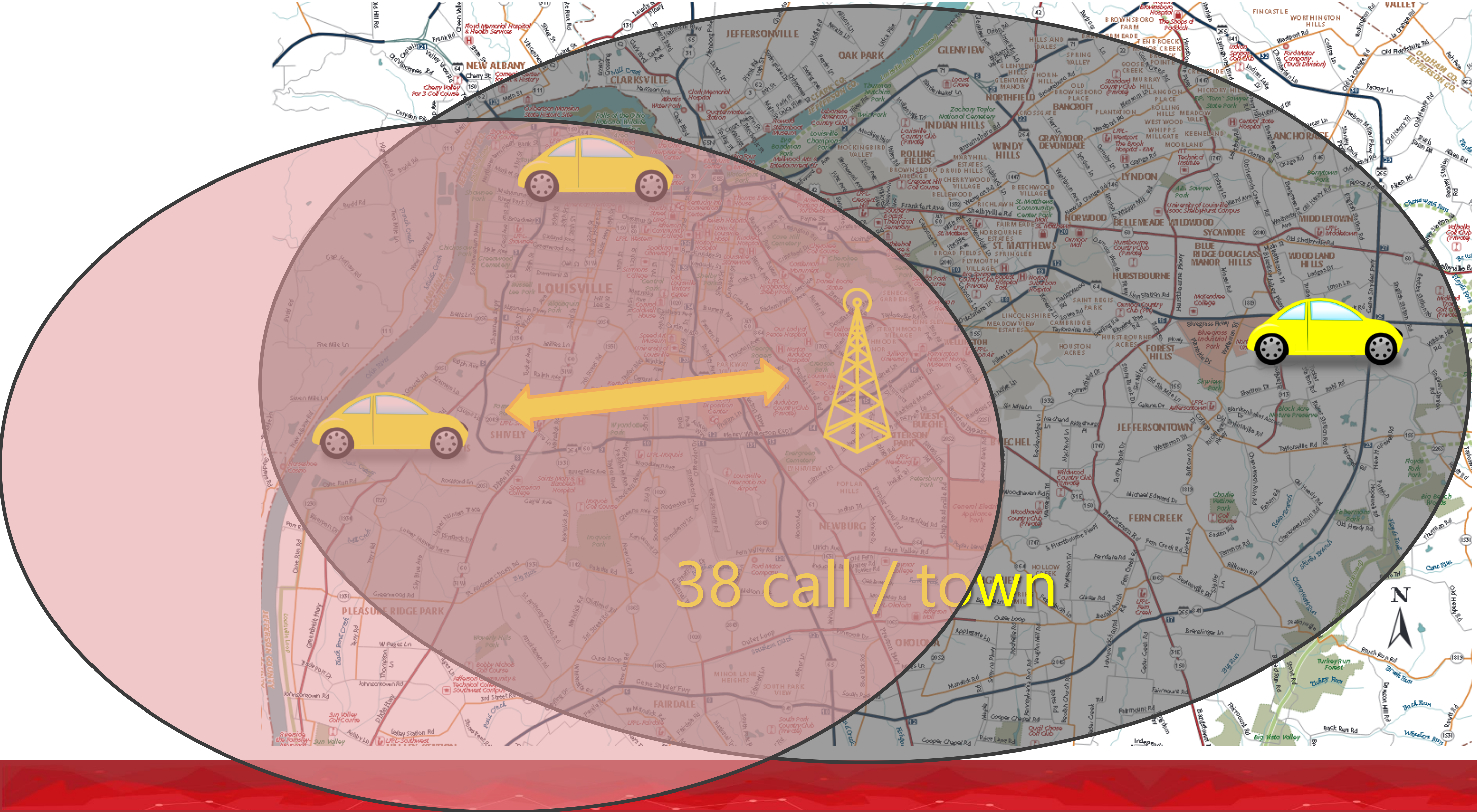
- Interestingly, a couple of such systems (in chronological order):
  - Mobile Telephone Service (MTS), USA, 1946 – cca 1990
  - A-Netz, West Germany, 1958 – 1977
  - System 1, UK (Manchester and neighbourhood), 1959
  - Алтай (Altaj), Soviet Union, 1963 –
  - Televerket, Norway, 1966
  - Autoradiopuhelin, Finnland, 1971 – 2000
  - B-Netz, West Germany, 1972 – 1994
  - Automatizovaný městský radiotelefon (AMR), Czechoslovakia, 1983 – 1999
    - 4 digit numbers -> 9999 users

0G

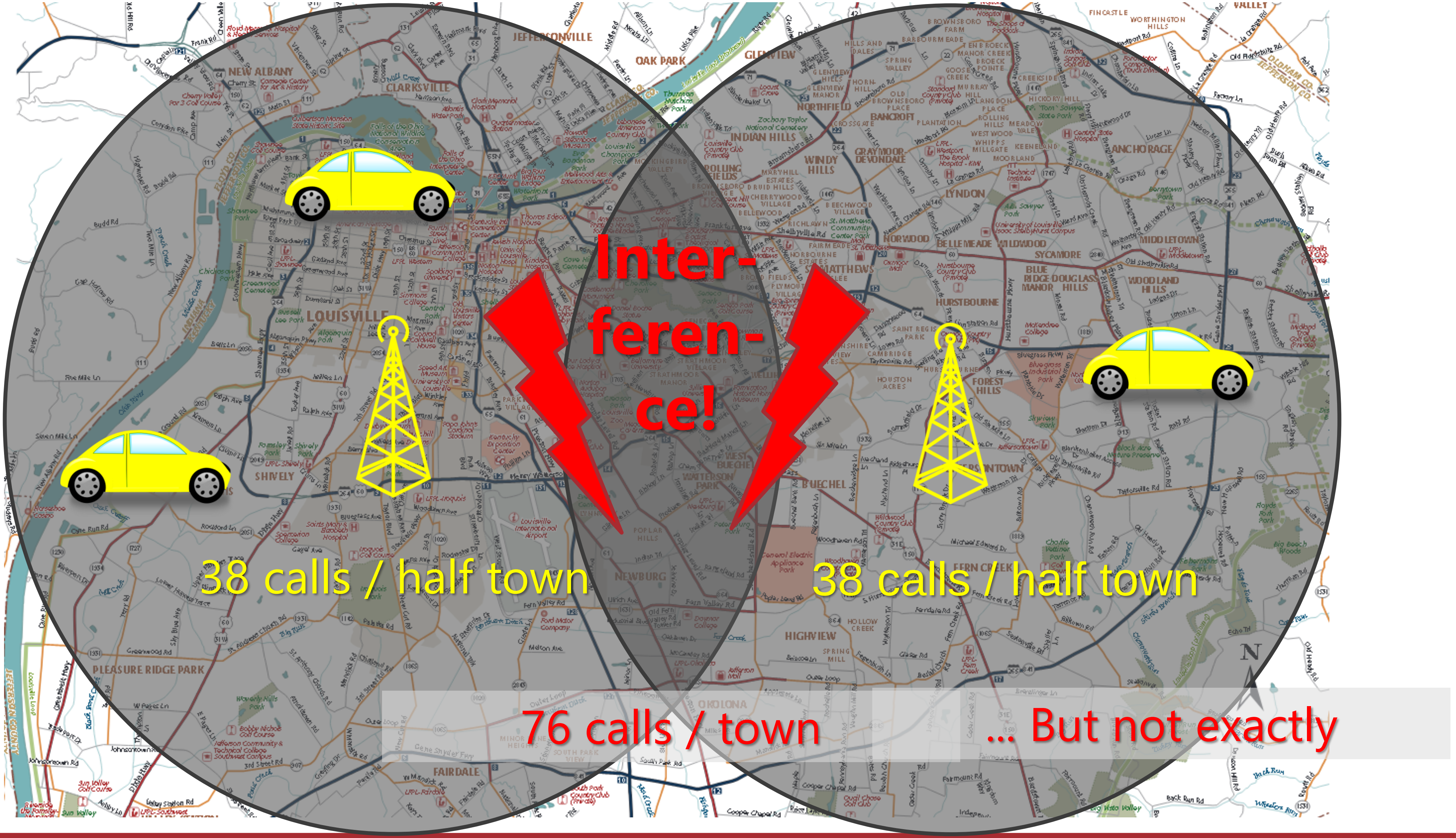
- Few users, not always public systems
  - The users often came from closed groups: state leaders, police, ambulance
- Why?
  - Because there are few usable frequency bands
  - E.g. West Germany B-Netz: 38 voice channels / town (!)
- Why?
  - Because the radio frequency spectrum is finite, and we want to use it for many things
- Solution: cellular division
  - This is typical from 1G systems

ANALOG CELLULAR NETWORKS
1G

Coverage with one base station



Coverage with two base stations



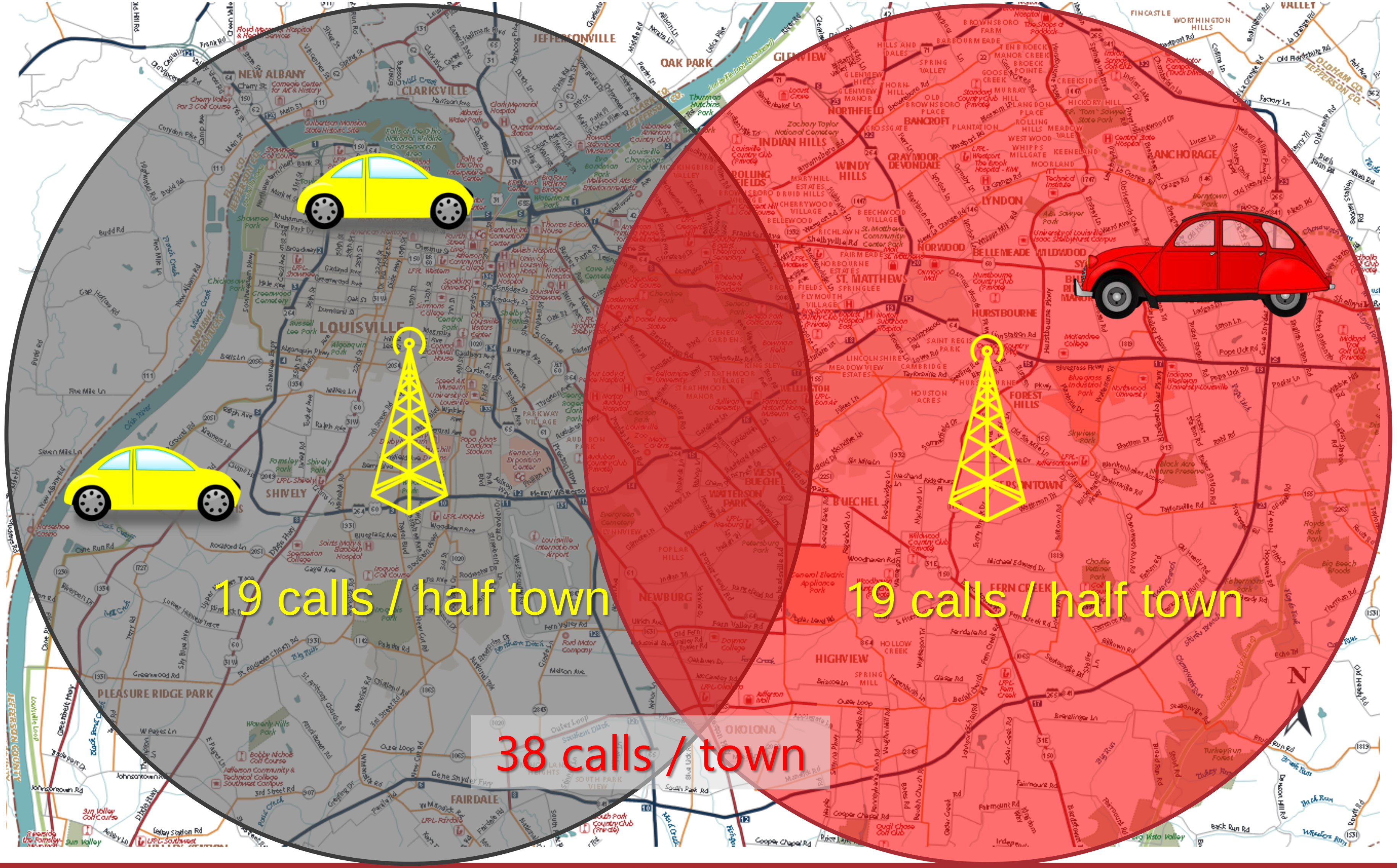
76 calls / town

… But not exactly

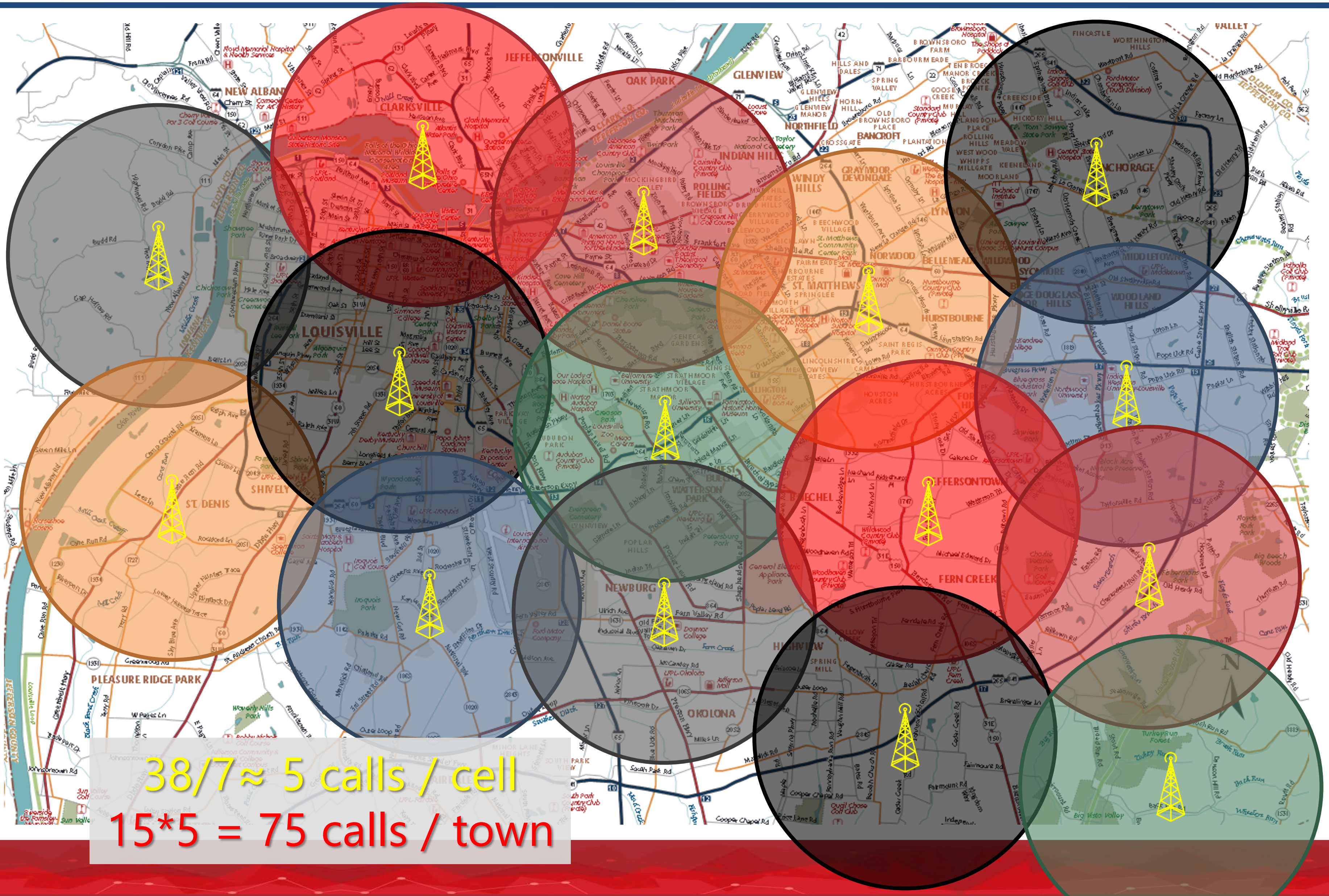
Interference

- “Addition” of waves
- In the case of radio waves,
  it happens when the signals of several transmitters come together
  - in space (i.e. coverage areas overlap) and
  - in time (transmission at the same time) and
  - in frequency (broadcast in the same frequency)
- This is a fundamentally harmful phenomenon, it destroys radio communication in the given place/time/frequency

Coverage with two base stations



Coverage with a lot of base stations



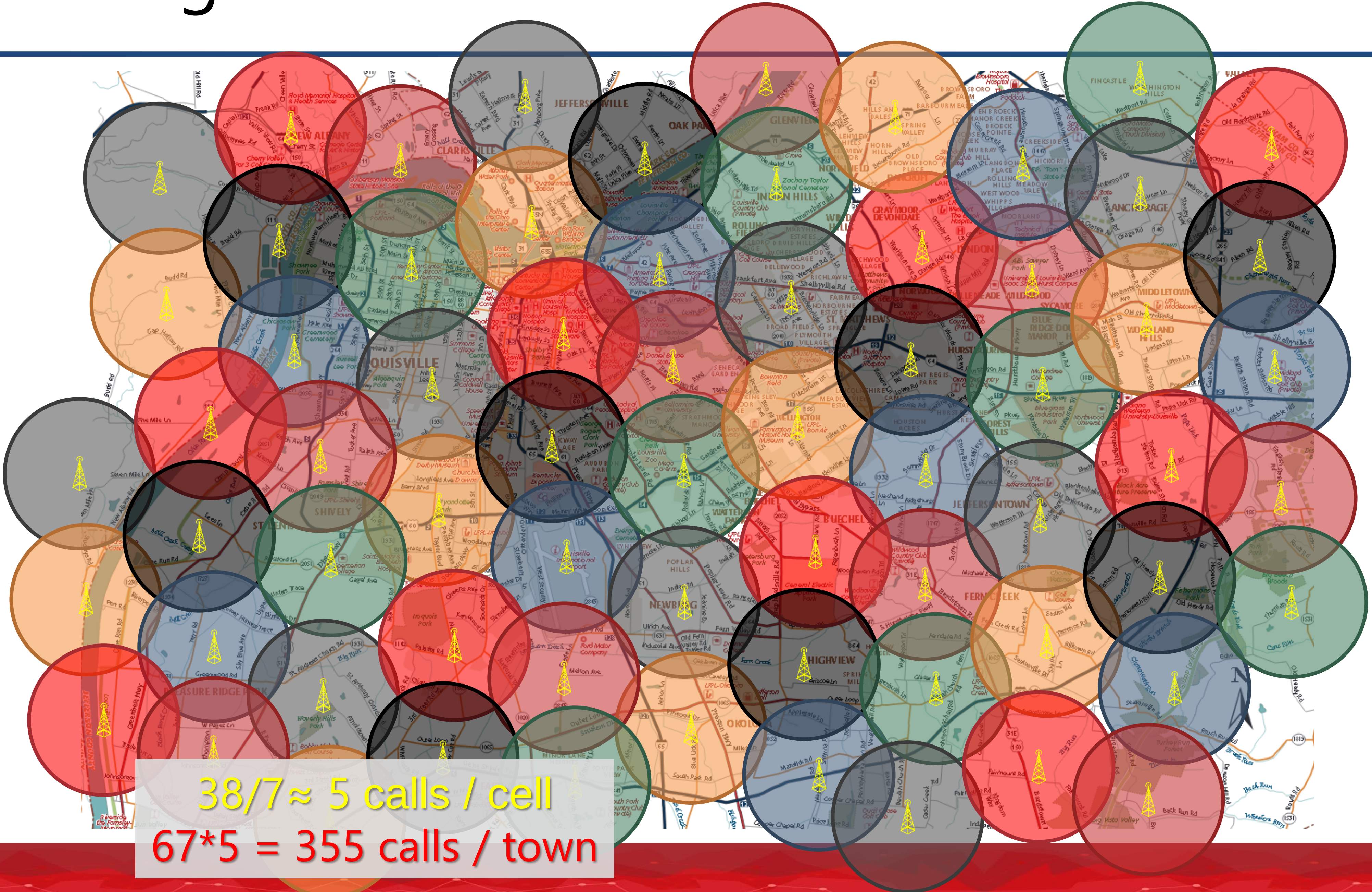
38/7≈ 5 calls / cell

15*5 = 75 calls / town

Explanation of previous slide

- Let's make many small cells, each using only a small part of the frequency range (channels).
  - There are seven types of cells in the slide (different colors). For this reason, only a seventh of the frequency can be used in a cell.
- It is essential that the cells using the same frequencies - marked with the same color - be far apart in space so that no interference occurs.
- The profit can be seen in the figure: more people can talk at the same time than before, even though the network itself uses the same amount of the radio frequency range as in the 0G case.
  - This is how all systems work from 1G upwards.

Coverage with even more base stations

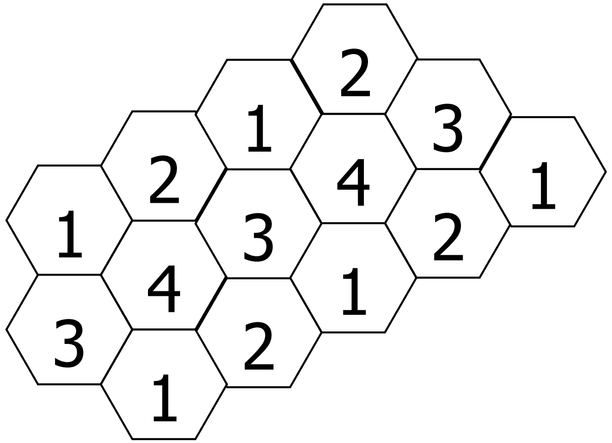


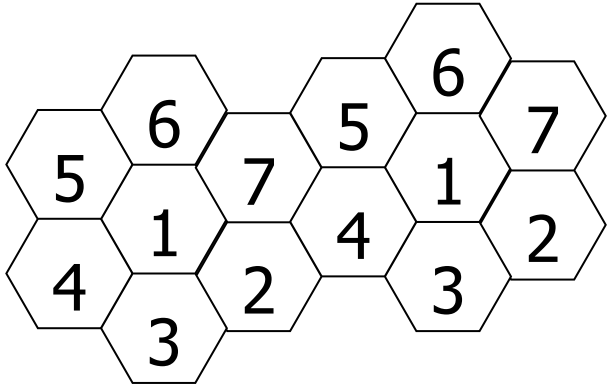
38/7≈ 5 calls / cell

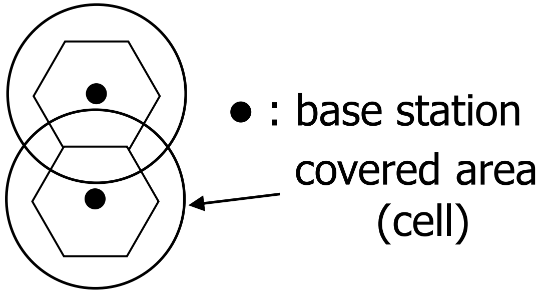
67*5 = 355 calls / town

Cellular concept

- Same frequency cannot be used in neighbouring cells – interference
  - 4-frequency set required as a minimum
  - Transmission power is large enough to cause interference in the second neighbouring cell
  - Frequency range is divided into 7 sets
  - This is only theoretical – in practice more complicated situations (base station in the „corner” of the cell, cell divided into several sectors, cells of different size, geographical circumstances, different traffic, etc.): ~10 (or even more) sets required







How large a cell shall be?

- What does the size of a cell depend on?
  - Geography
  - Frequency
    - ~900 MHz – 30-35 km
      - Follows the surface of the Earth more or less
    - ~1800 MHz – 2-3 km
      - Straight propagation
  - Transmission power
  - Height of transmitter (tower)
  - Traffic (!!)
- Advantages of small cells:
  - Small transmitter power enough
    - Minimisation of physiological risk
    - Smaller power consumption
      - Longer battery life
  - Higher traffic density
    - More parallel calls
- Disadvantages of small cells :
  - Lot of base stations needed
    - More expensive
    - More cell changes (handover)

1G systems

- End of 1970s / beginning of 1980s
- Analog systems
- Cellular, **public** networks
- Easy to eavesdrop and hack
- Lot of not compatible systems
  - No roaming, even if the technology was the same
  - E.g.: NMT (Nordic Mobile Telephone System)
    - Scandinavia since 1981
    - In Hungary 1990-2003 (Westel 0660)
    - Typically, around 450 MHz frequency
    - Relatively large cells, with 30-50 km of diameter
    - Poor voice transmission quality, few services (no number presentation, SMS)
    - No SIM: the phone number belongs to the device
    - Veeeery expensive (1/3 of a car)
  - More examples for 1G systems:
    - USA: Advanced Mobile Phone Service (AMPS),
    - GB: Total Access Communication System (TACS)
    - West Germany: C-Netz (C450)

GSM (2G)

The picture shows the Nokia 2110 GSM phone, which was considered a benchmark in its time (mid-1990s) and deservedly popular.

2G

The first public GSM call was made on 1st July 1991 in a Finnish network.

- 2G: second generation mobile telecommunications systems
  - from the beginning of the 1990s
  - digital systems
    - encrypted communication
    - more efficient usage of the radio spectrum
    - more people can talk at the same time
    - newer services: SMS, data transmission, …
  - GSM is the most common
  - There are/were other 2G systems, e.g.:
    - USA Digital Advanced Mobile Phone System (D-AMPS)
    - USA: Interim Standard 95 (IS-95), avagy cdmaOne
    - Japan: Personal Digital Cellular (PDC)
    - …

2G

The Ericsson GH 198, which was quite popular at that time, had dimensions of 141 x 59 x 29 mm and weighed 330 g. A competitor, the Nokia 1610: 168 x 58 x 28 mm, 255 g

- The size and weight of the devices decreased rapidly
  - "Half a brick" instead of briefcase size
- Prices also dropped quickly
  - technical development
  - more providers, competition
- Around 2000 in roughly 5 years, "everyone" had a mobile phone
  - huge business success
  - transformed our lives
    - the still “dumb” phone ;)

www.mobilgyujtemeny.hu

GSM

- Originally: „Groupe Spécial Mobile”,
  later: „Global System for Mobile communications”
- European standard (!): made by ETSI
  - European Telecommunications Standards Institute
- New concepts in GSM
  - Common, unified system in Europe
    - Later spread worldwide, pushing out other 2G szstems
  - Only the calling party pays (In USA both!)
  - Roaming
  - SIM card (subscriber data is device-independent)
  - SMS
  - encrypted voice transmission
- Even today, it still works in most countries of the world

GSM

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- Originally: „Groupe Spécial Mobile”, lat
- Eu
  - European Telecommunications Standards Institute

If we look at an early GSM phone now, of course we smile, but 3 decades have passed since then. Cars are different, but computers, for example, are very, very different. However, today's smartphones are also "GSM compatible", i.e. they can easily be used in purely GSM networks, i.e. they cooperate with a network of that time.

- New concepts in GSM
  - Common, unified system in Europe
- Ev

Around 2000, here in Europe, everyone was running around with a mobile phone, but in the USA, there were hardly any mobile phones. There were several reasons for this. On the one hand, there the mobile phone numbers were integrated into the landline system, and, say, a mobile phone in Chicago had a local (landline) area code. Since this way the caller could not know whether she/he was calling a landline or a mobile phone, it would not have been fair if she/he was made to pay more for mobile calls than for a landline one (which was accepted in Europe anyway). The problem was solved by having the mobile phone owner also pay for the received calls. This did not make the system popular, since it was not the case that till that time that the called party also paid. On the other hand, the option of pre-paying (pre-paid SIM card) appeared in GSM, which was also incredibly popular: many people bought such SIM cards for their children and thus could keep costs under control. Of course, sooner or later this advantage of Europe disappeared.

GSM – Main Services

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- Incremental development:
  - phase 1 (1991)
    - Digital voice transmission,
      - codec speed 13 kb/s (later: also 5.6 kb/s)
      - compromise: relatively poor voice quality, better frequency utilization
      - encryption of voice,
    - 9.6 kbps data transmission (circuit switched!!!)
    - SIM concept, SMS, roaming
  - phase 2 (1995)
    - backward compatibility, calling number presentation, call hold, call waiting, conference call, call forwarding (voicemail), half rate codec, etc.
  - phase 2+ (1998)
    - Mainly improvement in data transmission (HSCSD, EDGE)
    - Packet switched data (GPRS), 14.4 kbps
    - Virtual Private Networks, improvement of SIM, enhanced codecs, etc.
  - MMS (Multimedia Messaging Service) (2002)
    - multimedia message: image, written text, voice together
    - sometimes still used today

Dates and phases not exam material, only the services

GSM – Main Services

GSM GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- Incremental development:
  - ph

These are emphatically GSM services. Newer things like video calls have already appeared with 3G systems. These are natural today, but at that time even calling number presentation was a big deal: it wasn't introduced right away, you had to pay for it, but we liked it. We could still talk about WAP, which was an early mobile-optimized web browsing system, but it is now completely extinct.

    - 9.6 kbps data transmission (circuit switched!!!)
    - SIM concept, SMS, roaming
  - phase 2 (1995)
    - backward compatibility, calling number presentation, call hold, call waiting, conference call, call forwarding (voicemail), half rate codec, etc.
  - phase 2+ (1998)
    - Mainly improvement in data transmission (HSCSD, EDGE)
    - Packet switched data (GPRS), 14.4 kbps
    - Virtual Private Networks, improvement of SIM, enhanced codecs, etc.
  - MMS (Multimedia Messaging Service) (2002)
    - multimedia message: image, written text, voice together
    - sometimes still used today

GSM

- Digital transmission:
  - Voice codec (A/D converter) in the mobile
  - Encrypted (ciphered)
  - Both data and voice transmission possible
    - In GSM only circuit switched
- Cell diameter: 0.5 – 35 km
  - Design decision within that range
  - Depends on
    - the applied frequency
    - the **planned traffic** (number of calls)
    - propagation field conditions

GSM

- Digital transmission:
  - Voice codec (A/D converter) in the mobile
  - Encrypted (ciphered)
- C

The encryption lasted a surprisingly long time, but now someone has cracked it. This is also an interesting story. When designing the security system, great care was taken to ensure that the network (the base station and what is behind it) identifies the mobile. This was important so that it would not be possible for a mobile phone to pretend to be someone else, and thus make calls in someone else's name, on someone else's account, or receive incoming calls addressed to others. They thought that someone would try to imitate another mobile device (more precisely, the SIM card, because it identifies the user).

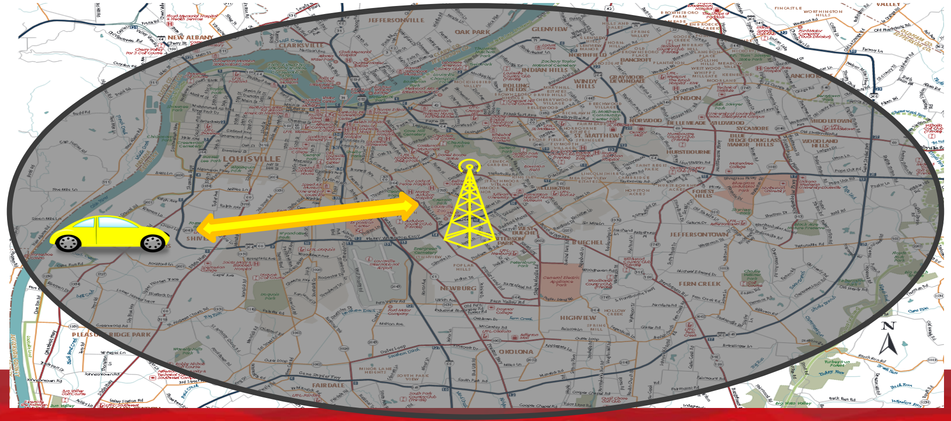
However, they did not think that someone was trying to imitate a network***. To do this, you should imitate the entire network system, which large manufacturers have developed over many years of work, and only service providers have this. It didn't go quickly, but after a while it did. From then on, however, by building a mini base station, the mobile device was willing to connect to it if it had the highest field strength of all the base stations. This pirated device presented itself as a network to the mobile phone, and as an end device to the real network, and embedded itself in the communication, making it eavesdropping (or thwarting).***

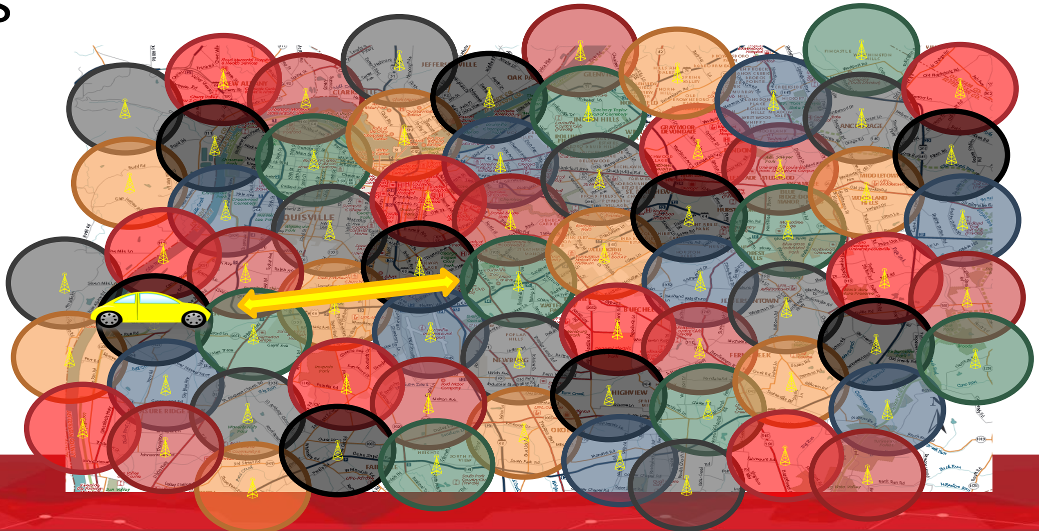
propagation field conditions

GSM power control

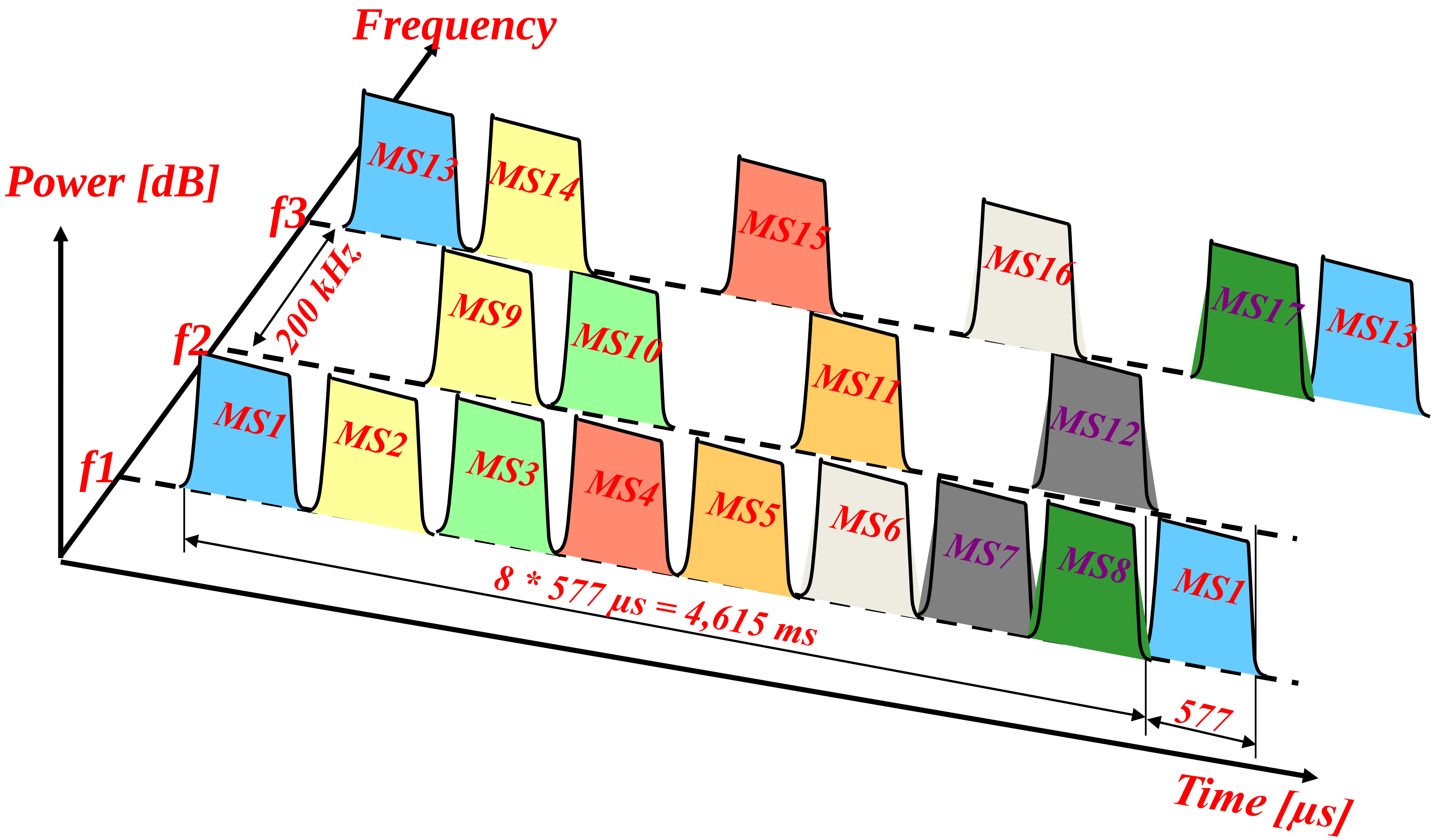
- Radiation output: max. 2W
  - Adaptive: the terminal transmits with the minimal necessary power
  - The phone may change the transmission power twice every second
    - Longer battery life
    - Minimisation of physiological risk
    - Not to interfere with further cells

If the mobile is closer to the base station, it transmits with a lower power, if it is further away, with a higher power. Smart ;)

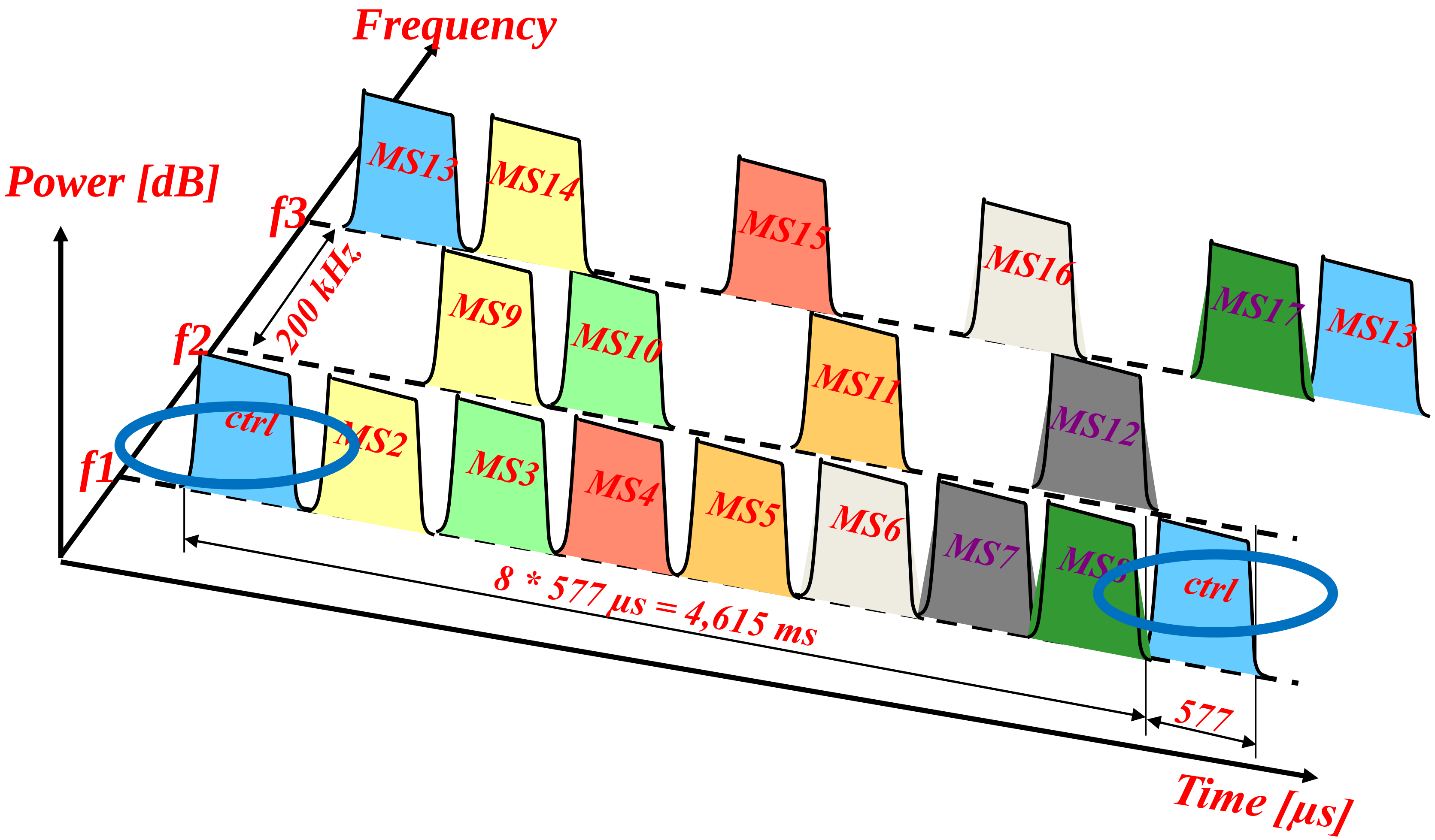




GSM Radio Access – Combined FDMA+TDMA



GSM Radio Access – Combined FDMA+TDMA



GSM – Radio Access – 900 MHz

You don't need to know the specific frequency ranges (890-915, 935-960), but you shall know that it is about 900 MHz, and the bandwidths.

- GSM 900 (Primary-GSM, P-GSM)
  - mobile station (uplink): 890-915 MHz,
  - base station (downlink) 935-960 MHz
  - lower frequency suffers smaller attenuation, so it requires less power -> mobiles (uplink traffic) use the lower frequency band
  - max. 35 km cell diameter: waves around 900 MHz somewhat follow the Earth's surface, therefore, **the technology is suitable for countrywide coverage**
  - 1 band = 25 MHz, 1 carrier = 200 kHz: 124 carriers (FDMA)
    - shared among service providers
    - in a country with 3 providers: appr. 40 frequencies/service provider; with 4 providers: appr. 30 frequencies/service provider in this band
  - 8 time slots/carrier (TDMA)
  - (40/10)*8 ≈ 32 channels / cell or (30/10)*8 ≈ 24 channels / cell
    - 10: typically ≈ 10 different frequency sets used in cells (more realistic than 7 as we could see before)
    - with Half Rate codecs: twice as much

GSM – Radio Access – 1800 MHz

- GSM 1800
  - Mobile: 1710-1785 MHz, base station: 1805-1880 MHz
  - 1 band = 75 MHz (three times larger capacity)
  - BUT: worse wave propagation
    - propagates straight
    - attenuates more quickly
  - **Not** (so…) **suitable for countrywide coverage**, only for small cells (where the traffic is high)
    - Cities, highways
- Several other bands: (not to learn, but interesting)
  - Extended-GSM 900, E-GSM: +10 MHz/direction: +50 carriers
  - R-GSM: Railways GSM: 876-880/921-925 MHz
  - GSM 1900: 1850-1910/1930-1990 MHz (USA)
  - GSM 850: 824-849/869-894 MHz (USA)
- 2-norm equipment: automatically select/change frequency range
  - 3-norm (900/1800/1900) and 4-norm equipment (850/900/1800/1900)

You don't need to know the specific frequency range, but you shall know that it is about 1800 MHz, and the bandwidth (75 MHz).

GSM – Radio Access – 1800 MHz

- GSM 1800
  - Mobile: 1710-1785 MHz, base station: 1805-1880 MHz
  - 1 band = 75 MHz (three times larger capacity)
  - BUT: worse wave propagation
    - propagates straight
    - attenuates more quickly
  - **Not** (so...) **suitable for countrywide coverage**, only for small cells (where the traffic is high)
    - Cities, highways
- Se
  - GSM 850: 824-849/869-894 MHz (USA)
- 2-norm equipment: automatically select/change frequency range
  - 3-norm (900/1800/1900) and 4-norm equipment (850/900/1800/1900)

You don't need to know the specific frequency range, but you shall know that it is about 1800 MHz, and the bandwidth (75 MHz).

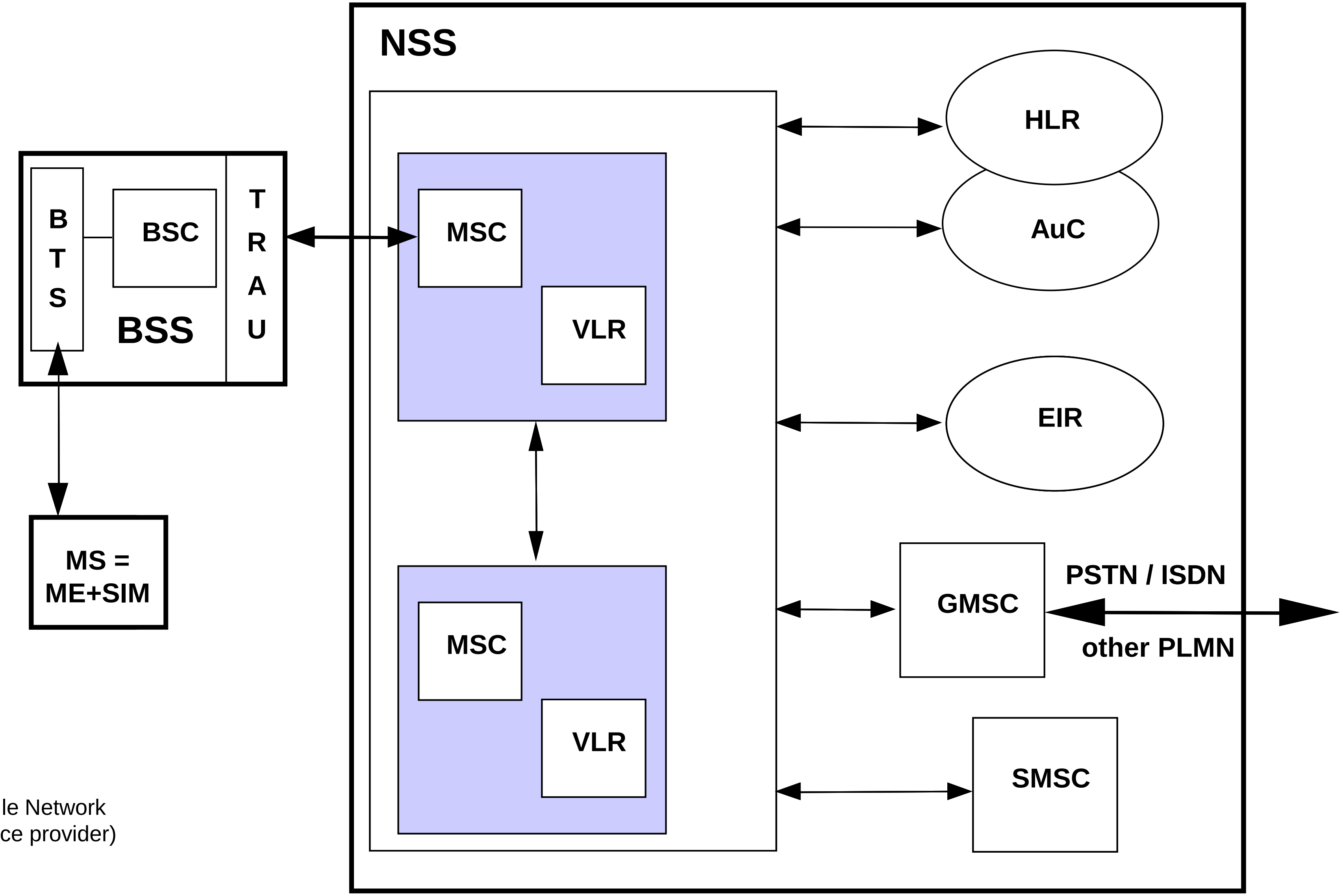
The 3- and 4-norm devices were needed because the frequencies around 900 and 1800 MHz were reserved for other uses in the USA, so they could free up slightly different frequencies for GSM there. It was also GSM, only the frequency was different, everything else was unchanged.

Since then, with the appearance of 3G, 4G, and 5G, more and more ranges have been freed up for the purpose of mobile communication, which of course the new devices are also capable of using.

GSM handover/handoff

- GSM: circuit switching
- When the mobile station enters another cell: handover (handoff)
  - Continuous connection
    - Mobile station initiates: measures, if the signal in one of the neighbouring cells is stronger
    - Network controls
      - the network can postpone the cell change if the „new” cell is overloaded

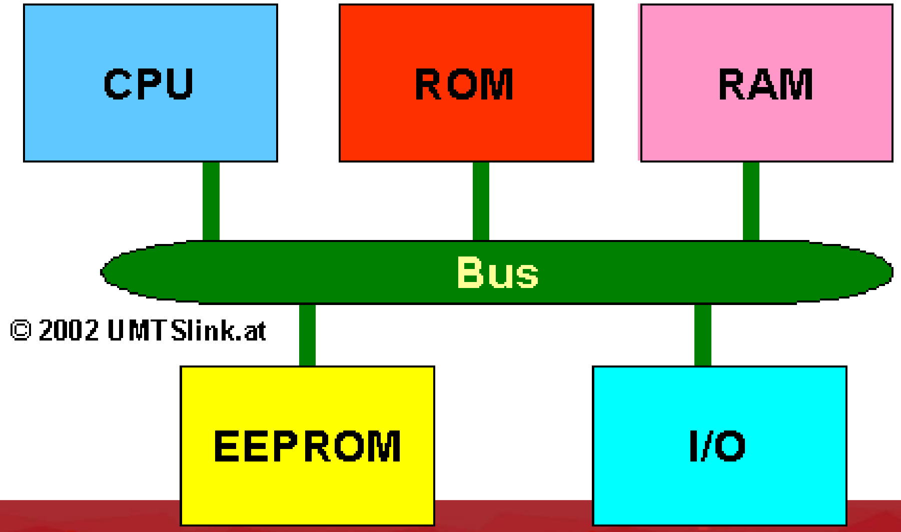
Architecture of GSM networks (PLMN)



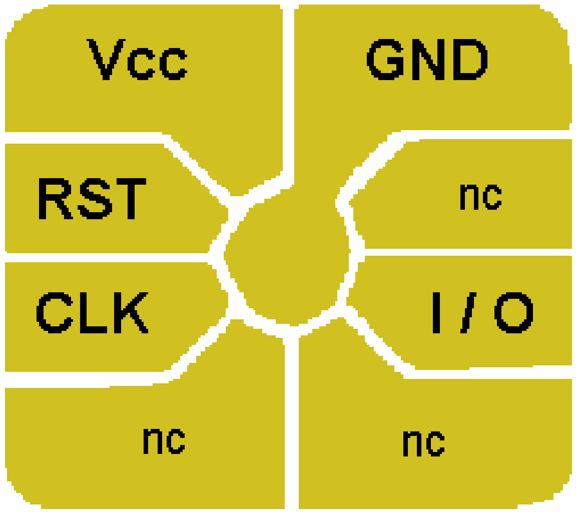
PLMN: Public Land Mobile Network
(network of a mobile service provider)

Mobile Station

- MS – Mobile Station
- ME – Mobile Equipment
- Subscriber Identity Module („SIM card”)
  - Identifiers
  - Authentication
  - Ciphering
  - User data (phone book, SMS)



© 2002 UMTSlink.at



© 2002 UMTSlink.at

Base Station Subsystem (BSS)

- Base Transciever Station (BTS)
  - One or more elementary transmitter/receiver
  - Transcoder/Transmission and Rate Adapter Unit, TRAU
    - FR, HR, EFR codec ⇔ 64 kbps PCM
      - Full Rate (13 kbps),
      - Half Rate (5.6 kbps),
      - Enhanced Full Rate (12.2 kbps, but better quality than FR)
    - Rate adaptation also at data transmission: 14.4 kbps ⇔ 64 kbps
- Base Station Controller (BSC)
  - Controls one or *more* BTSs
  - Radio channel assignment
  - Handover control

Network and Switching Subsystem (NSS)

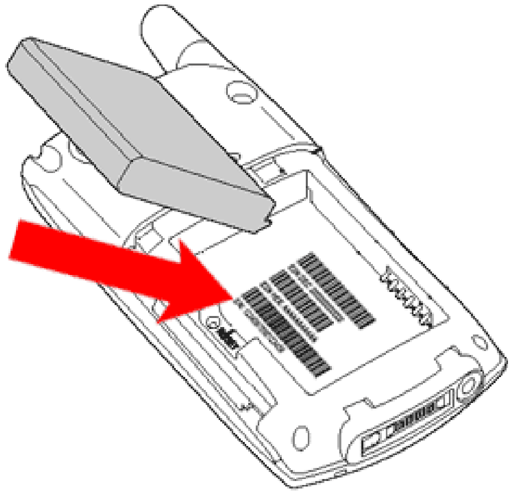
- Mobile Switching Center (MSC)
  - A digital switch
  - With mobile-specific extensions
    - authentication
    - location management (VLR)
    - inter-BSC handover
    - roaming
- Visitor Location Register (VLR)
  - Always integrated with MSC
  - Stores temporarily some parts of the HLR info about the currently served mobile stations
- Home Location Register (HLR)
  - Subscriber data, subscription information (services), current location
  - One HLR in every network
- Authentication Center (AuC)
  - Typically integrated with HLR
  - It verifies that the subscriber is the same in reality as is told to be

Permanent Identifiers in GSM

- **IMSI**: International Mobile Subscriber Identity
  - in GSM network **this** identifies the subscribers
    - in data bases (HLR, VLR - index)
  - assigned to SIM cards
  - unique worldwide
  - IMSI = Mobile Country Code (Hungary: 216) + Mobile Network Code (Hungary:01/30/70) + Mobile Subscriber Identifier (10 digits)
  - at operator change: MSISDN may be kept (number portability) but SIM card and therefore the IMSI must be changed
- **MSISDN**: Mobile Station ISDN Number
  - telephony number
  - unique worldwide
  - MSISDN = Country Code (Hungary: 36) + Network Identifier (National Destination Code) (Hungary:20/30/70) + Subscriber Number

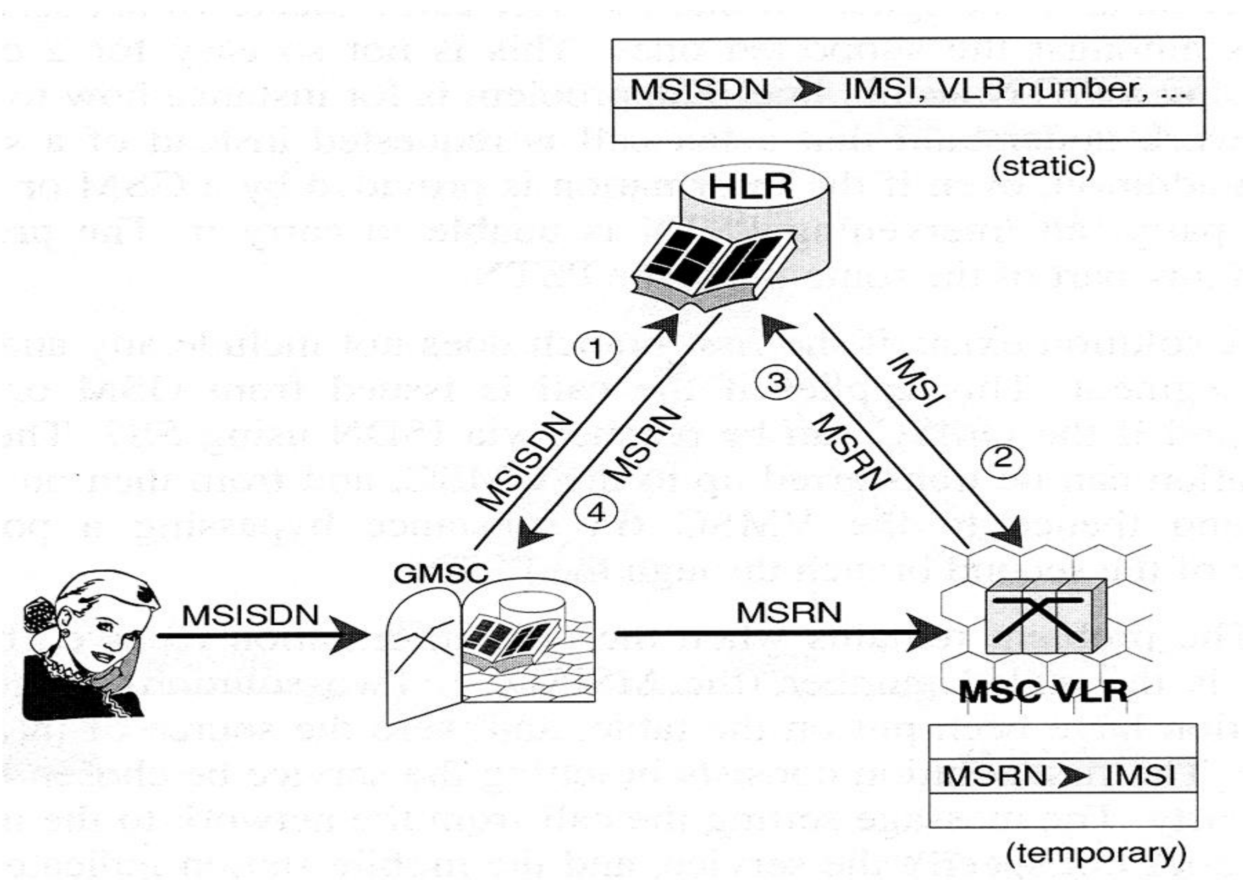
Permanent Identifiers in GSM

- **IMEI**: International Mobile Equipment Identity
  - identifier of the mobile equipment
  - unique worldwide
  - IMEI = <equipment type+producer id> (8 digits) + <serial number> (6 digits) + <control digit> (1 digit) (+<software version id> (1 digit))
  - To query: *#06#
    - works on every GSM terminal
    - also written under the battery
    - if they are different (or the latter is not present): the mobile is probably stolen!
      - exception:
        the SW version number is not always displayed by *#06#
        or it is not written under the battery



Temporary Identifiers in GSM

- **MSRN**: Mobile Station Roaming Number
  - used when a MS is called
  - assigned to MSC(VLR)
  - a telephone number belonging to a local number range belonging to an MSC/VLR, which is temporarily used, when a mobile device which is connected to it, is called
  - transparent to the user
  - MSRN refers to the geographical location: from this number the call control knows where to look for the given subscriber when called

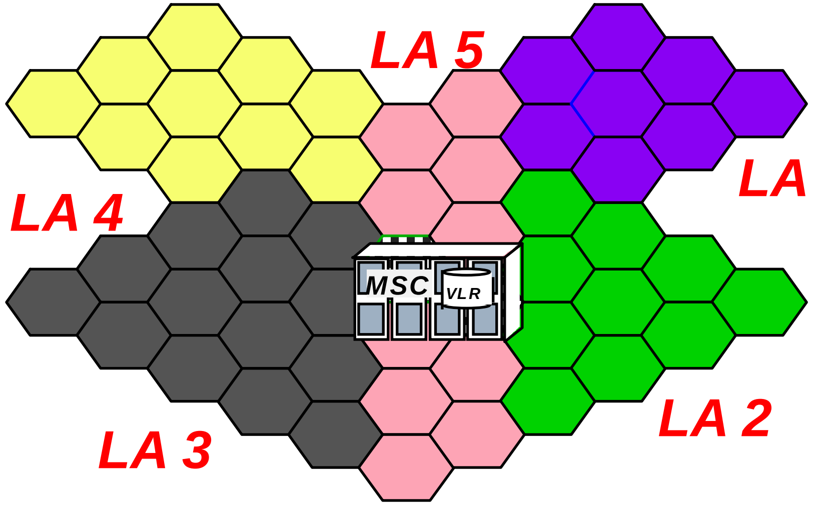


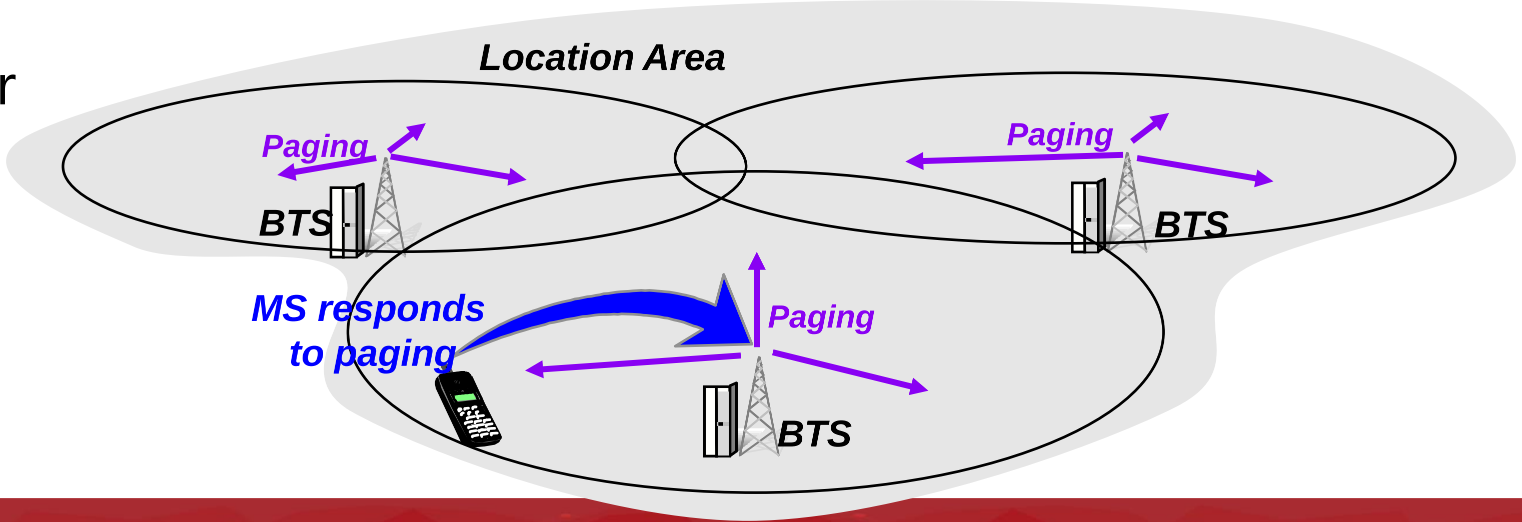
Mobility Management (MM)

- The network must know the location of a MS to be able to connect a call, or deliver an SMS to it
  - If the world were just one area
    - No need for location management
    - But Paging in every cell of the world ☹
  - If we always knew the cell
    - Paging only in one cell, but too many cell-change messages
  - Compromise: Divide the world to not too large areas – to Page an MS only in a limited part of the world, but in more than one cell
    - Location Area – LA
      - Group of several (20-50) neighbouring cells, which are served by the same MSC
  - But then the network must keep track the movement of MSs
    - Additional signaling needed
      - Location Update – when a mobile changes a LA

Location Areas

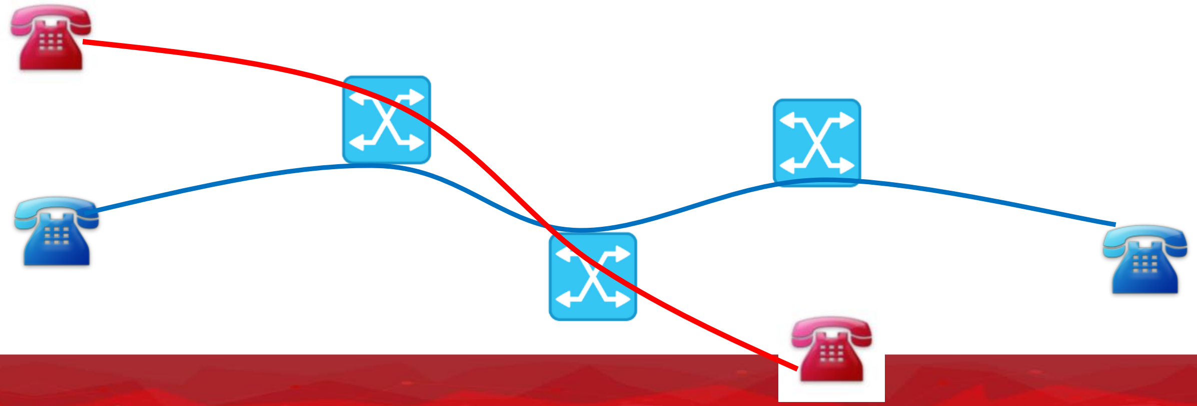
- Area served by an MSC/VLR can be divided into smaller units: **Location Area**
- The maximum size of LA can be one MSC area and the minimum size is one cell
- A subscriber can move within this area without having to make a normal Location Update
- Paging is done in all cells of the LA in which the subscriber is currently located





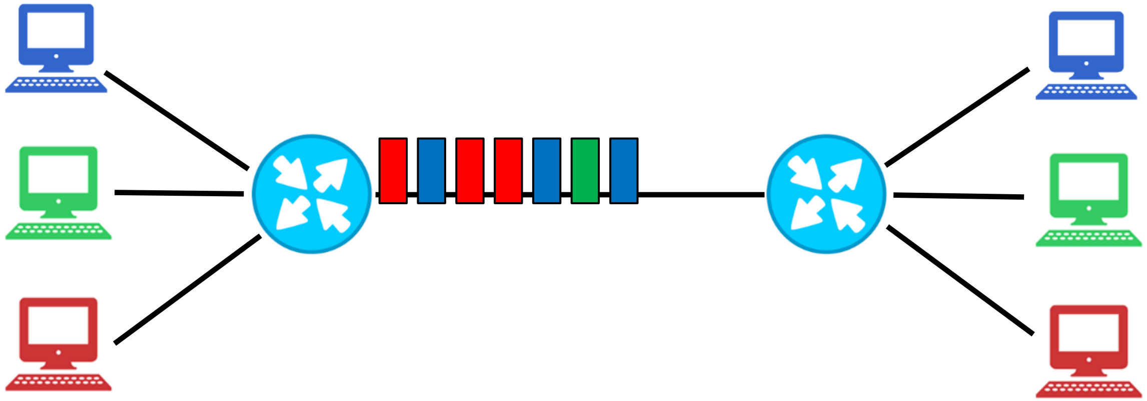
Circuit switching

- this is the case in classic telephone networks
- end-to-end channel with *guaranteed quality*
- *call establishment* before communication
- *call release* after communication
- the channel can only be used by the caller and the called party
- if they are not talking, the channel is empty
  - but must be paid
- it can be physically a circuit (originally), but it can be a channel in a more general sense (later)
  - e.g. given time slot, given frequency in a multiplex transmission system



Packet switching

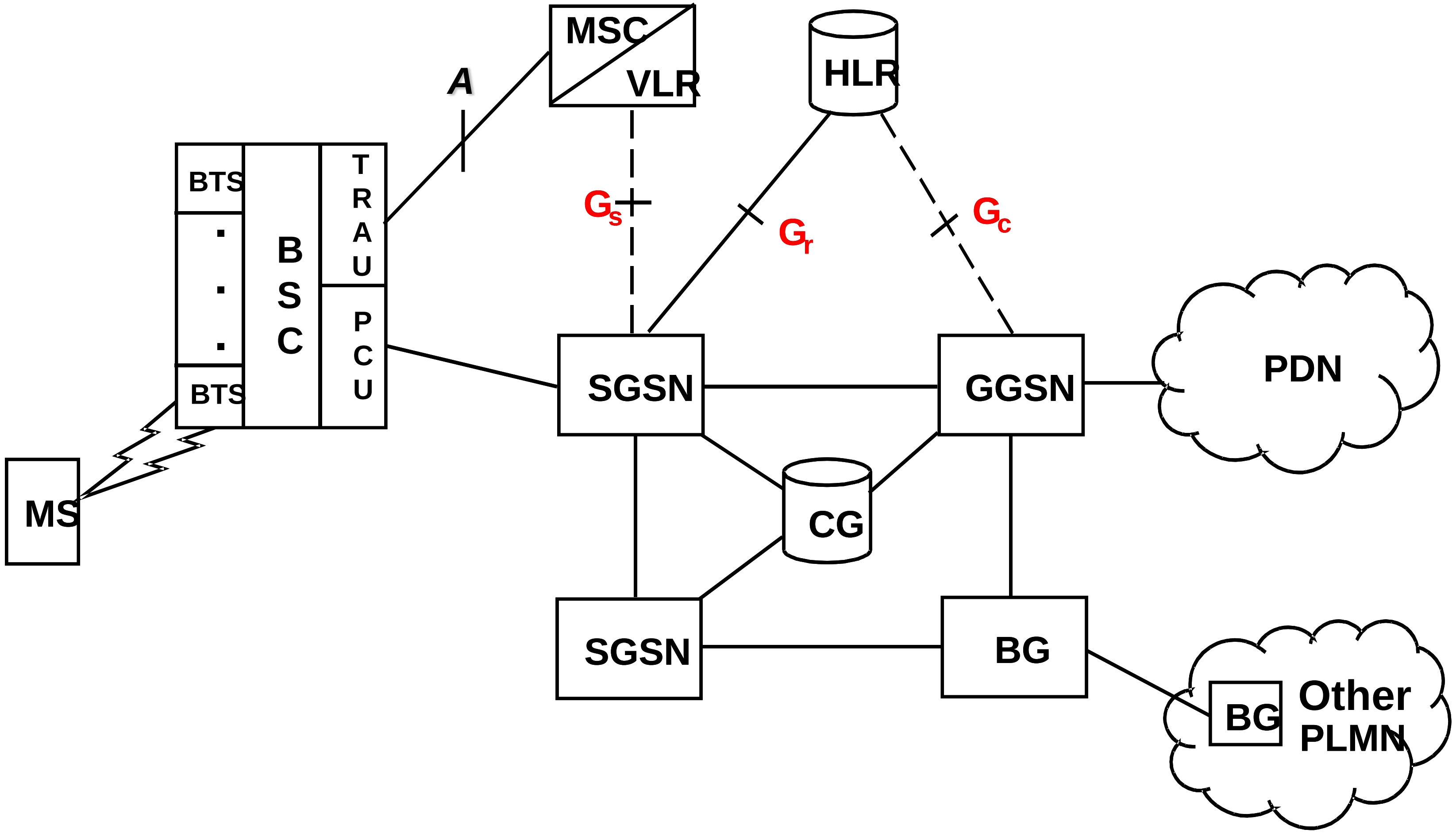
- it was the novelty of computer networks
- the transmitted information is divided into small packets and forwarded
- no need to set up and break down a call
- advantage: statistical multiplexing
  - if there is no communication, someone else can use the channel
  - larger traffic can be handled on the same channel
  - = cheaper!
- disadvantage: quality is not guaranteed
  - ensuring quality of service (QoS) is a separate task



GSM/GPRS: „2.5 G”

- GPRS (General Packet Radio Service)
  - since 2001
  - packet switched data transmission, extension to GSM
  - advantage:
    - better utilisation of network, frequency
    - payment on basis of amount of transmitted data (kB), not on basis of duration of connection
  - speed
    - originally max. 56 kbps
    - theoretical max.: 8 x 20 = 160 kbps
    - typically, 60-80 kbps downlink, 20-40 kbps uplink
      - fewer channels used in uplink direction
  - usage:
    - Internet access
  - requires significant extensions in the network (next slide)

GPRS architecture

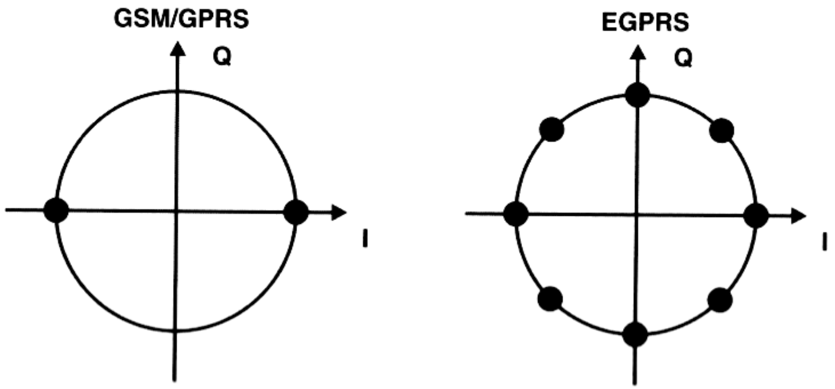


GPRS architecture

- CS: Circuit Switched Subsystem
- PS: Packet Switched Subsystem – new extensions
  - SGSN: Serving GPRS Support Node
  - GGSN: Gateway GPRS Support Node (to other public data networks (PDN) e.g. Internet)
  - BG: Border Gateway (gateway to other GPRS service providers)
  - CG: Charging Gateway
- Extended GSM elements
  - HLR: stores also the data service-related parameters
    - Serving SGSN
  - BSS:
    - PCU – Packet Control Unit – code conversion, encryption
- Important New Interfaces
  - SGSN – HLR
    - Routing Area (Similar to Location Area, but smaller) Update
  - MSC – SGSN
    - Paging, SMS can be inserted among the data packets, mobile does not need to listen to an other control channel if it has a data connection

GSM/EDGE: „2.75 G”

- *EDGE* (Enhanced Data Rate for Global/GSM Evolution – no comment...)
  - improved modulation procedure
    - originally it was 1 bit/symbol (Gaussian minimum shift keying, GMSK)
    - EDGE: 8PSK, 3 bits/symbol ⇒ three times larger data transfer rate
    - this only works if the signal/noise ratio is better (less interference-tolerant)
  - data transmission rate approx. 150-180 kb/s
  - "E" on the phone on the top line
    - sometimes we still see it today (and we are not happy about it)



GMSK = 1 bit per symbol

8PSK = 3 bits per symbol