# GSM

Global System for Mobile communication

# GPRS

General Packet Radio Service

# Examples of digital wireless systems

## (all originally specified by ETSI)

GSM (Global System for Mobile communication) is a *cellular mobile* system

- cellular concept
- high mobility (international roaming)

TETRA (TErrestrial Trunked RAdio) is an example of a *Professional/Privat Mobile Radio* (PMR) system

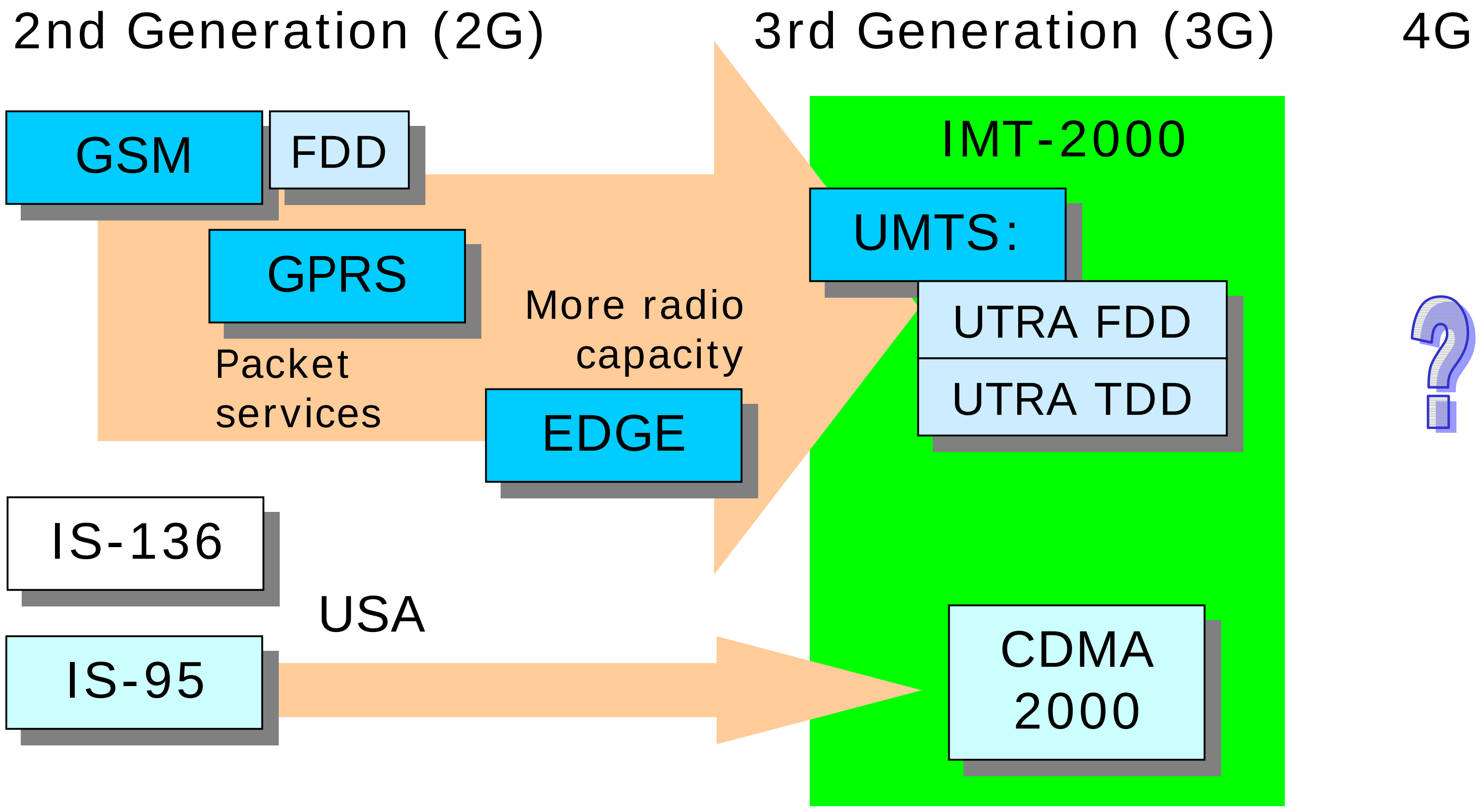
- limited access (mainly for professional usage)
- limited mobility (but other advanced features)

DECT (Digital Enhanced Cordless Telecommunications) is a *cordless* system

- low mobility (only within “isolated islands”)

# Digital PLMN systems (status 2004)

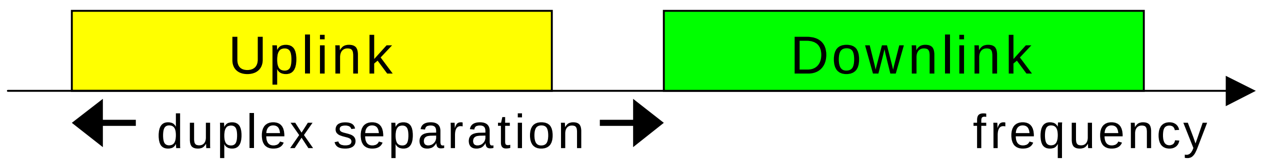
(PLMN = Public Land Mobile Network)



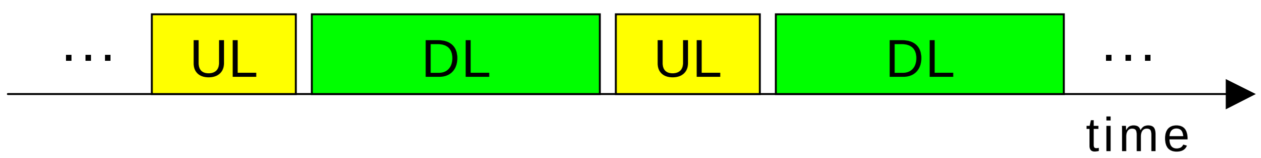
# Duplexing

(separation of uplink/downlink transmission directions)

FDD (Frequency Division Duplexing)
(GSM/GPRS, TETRA, UTRA FDD)




TDD (Time Division Duplexing)
(DECT, UTRA TDD)



# FDD vs. TDD

| FDD | TDD |
|---|---|
| Duplex filter is large and expensive | Large MS-BS separation => inefficient |
| | => indoor |
| Different fading in UL/DL | Same fading in UL/DL |

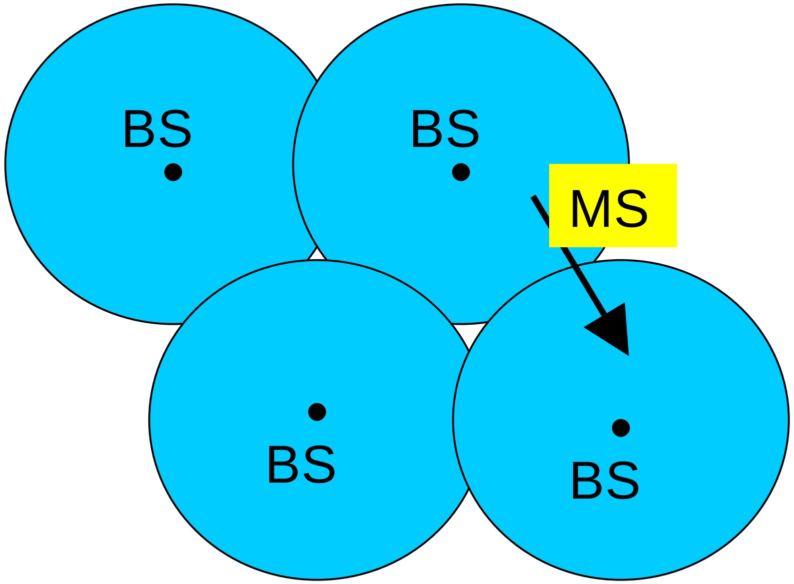
=> effect on power control

| FDD | TDD |
|---|---|
| Same UL/DL bandwidth | Flexible UL/DL bandwidth allocation |

asymmetric services

# GSM => cellular concept

The GSM network contains a large number of cells with a base station (BS) at the center of each cell to which mobile stations (MS) are connected during a call.

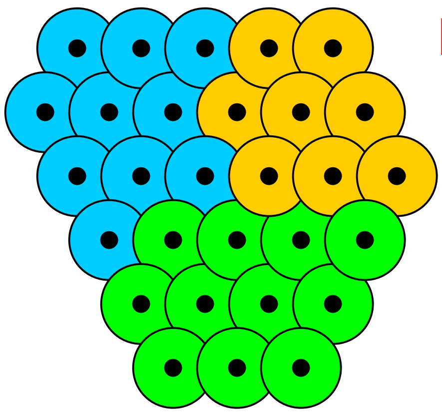



If a connected MS (MS in call phase) moves between two cells, the call is not dropped.

Instead, the network performs a handover (US: hand-off).

# GSM => mobility concept

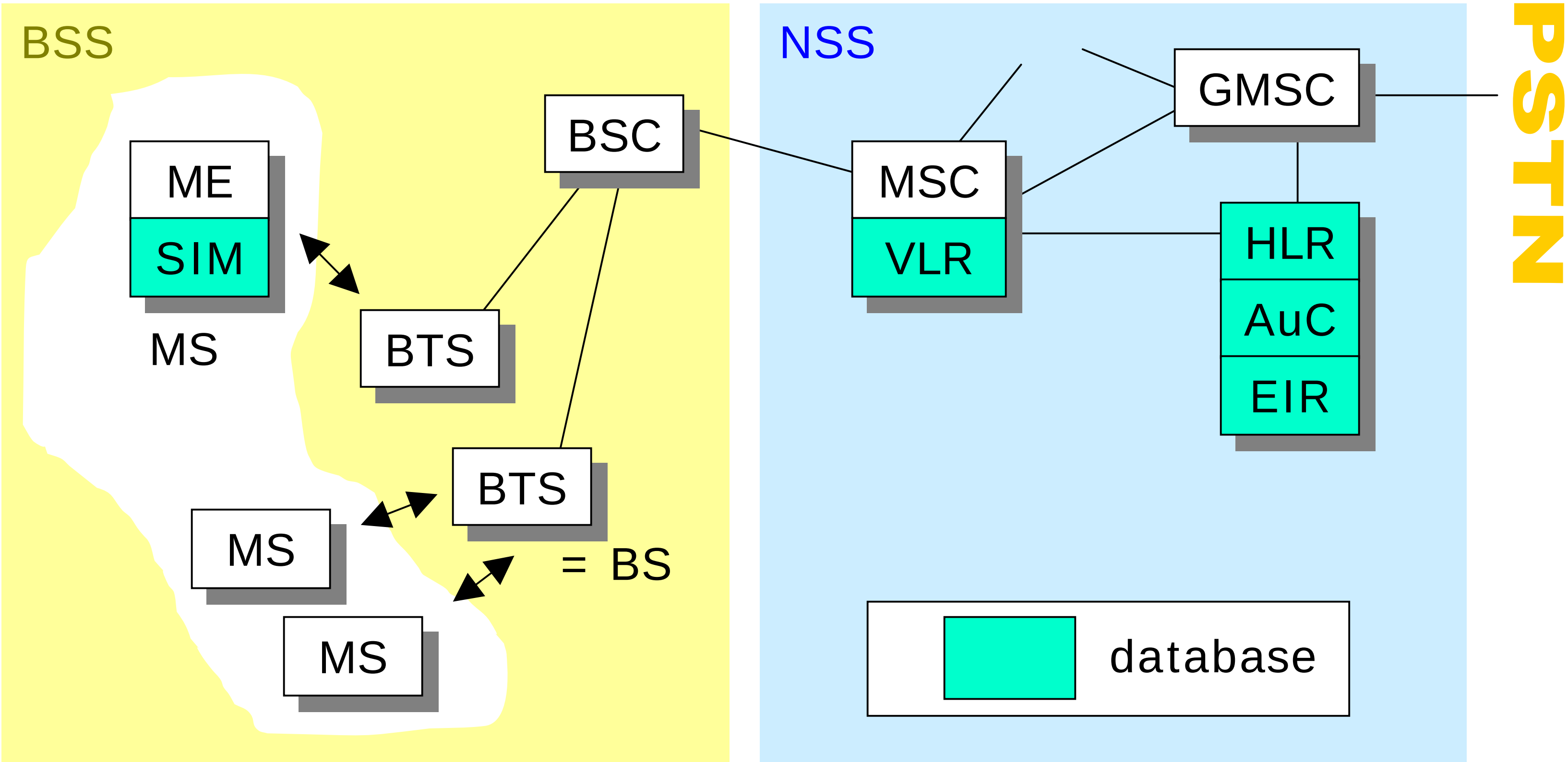
The GSM network is divided into location areas (LA), each containing a certain number of cells.



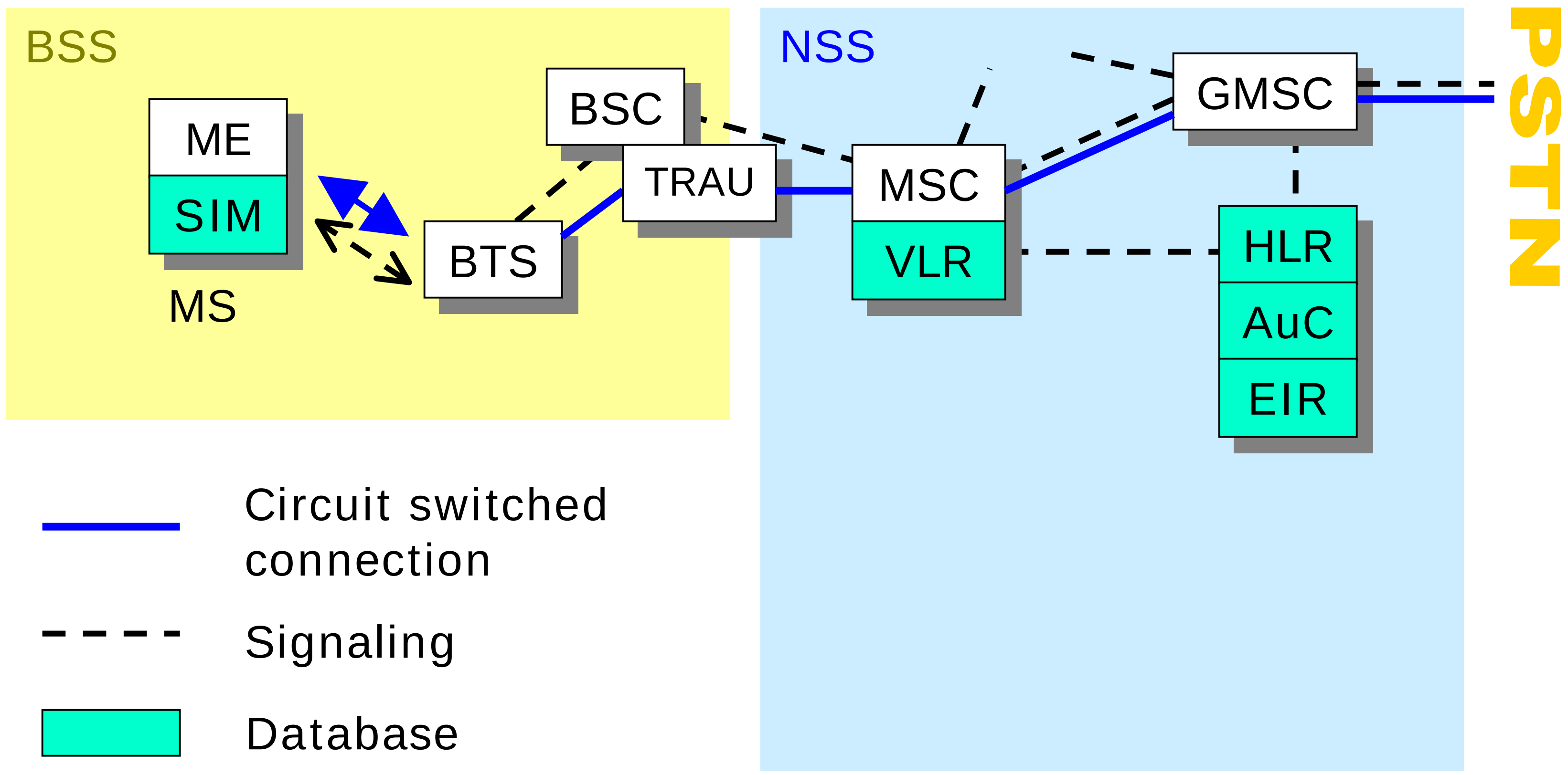

As long as an idle MS (idle = switched on) moves within a location area, it can be reached through paging.

If an idle MS moves between two location areas, it cannot be reached before it performs a location update.

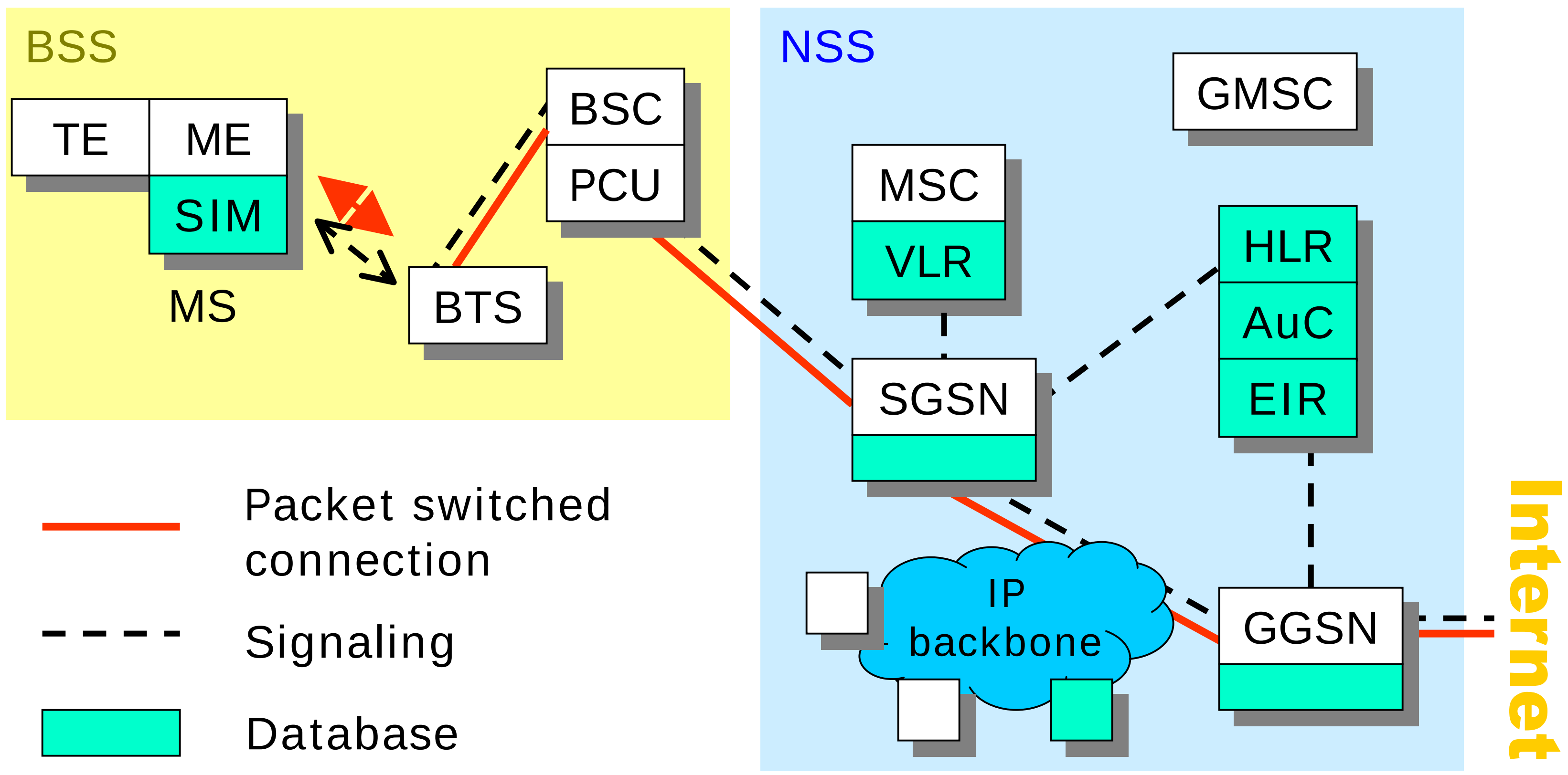
# Original GSM system architecture



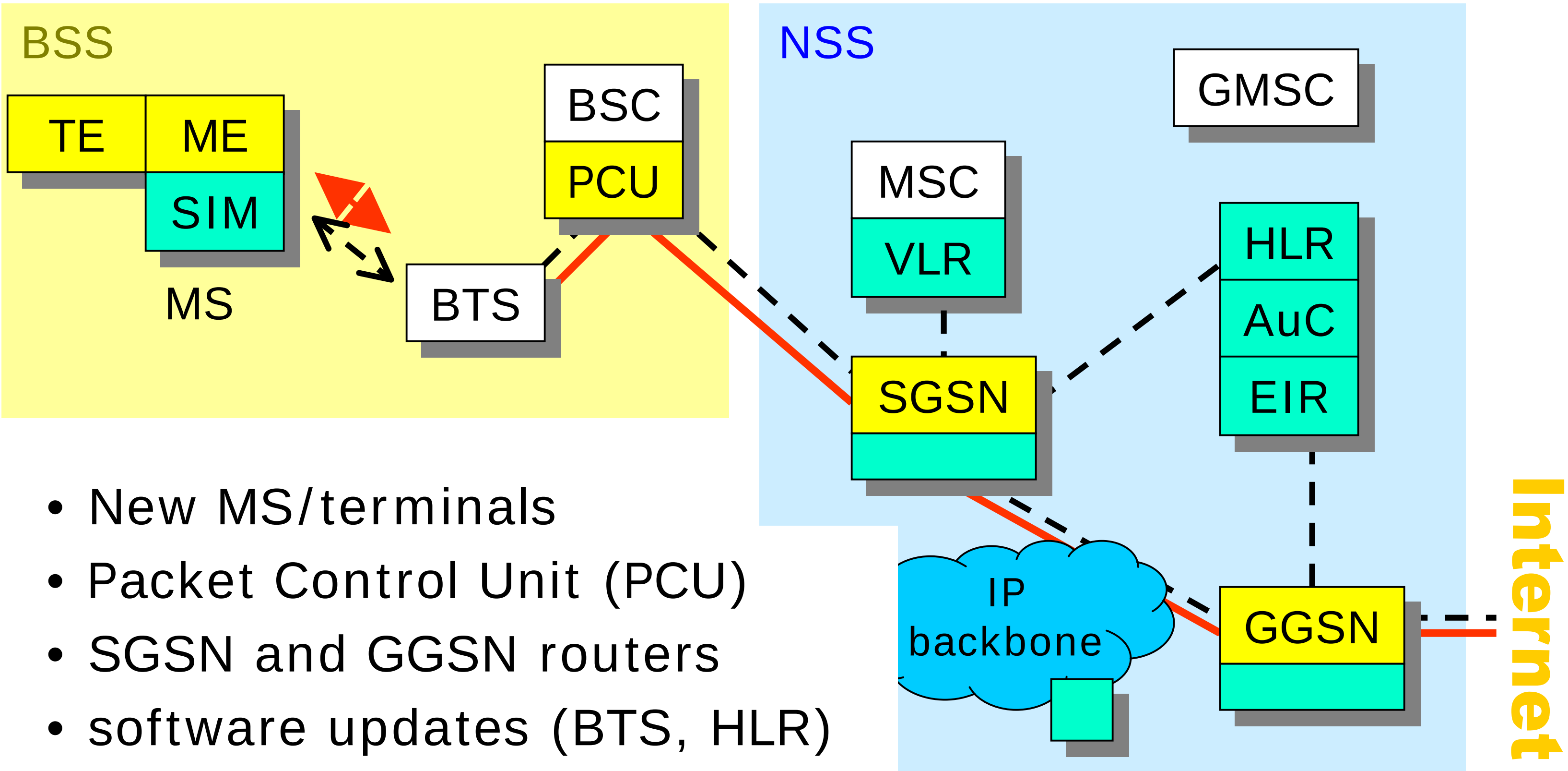
# GSM: circuit switched connections



# GPRS: packet switched connections



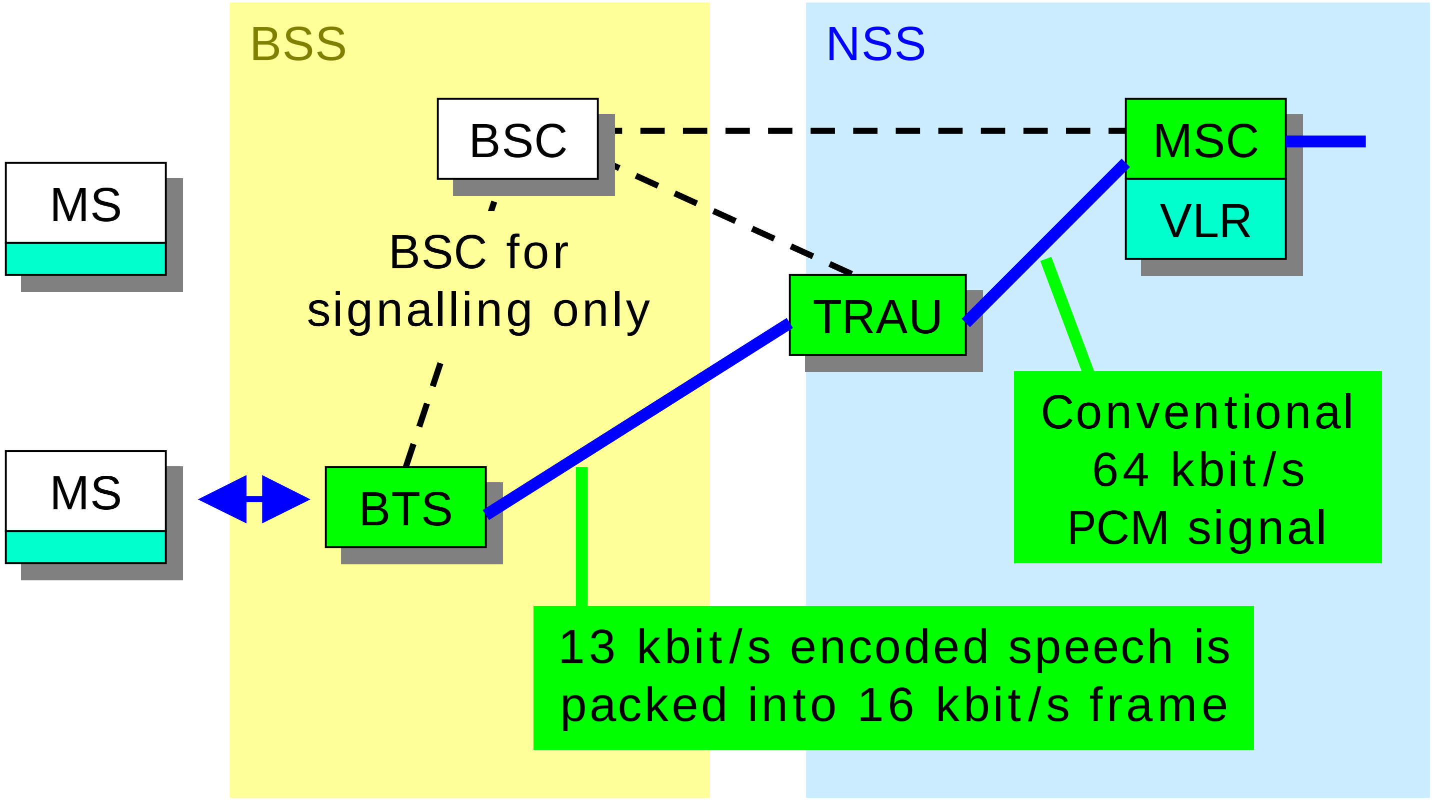
# Upgrading from GSM to GSM/GPRS



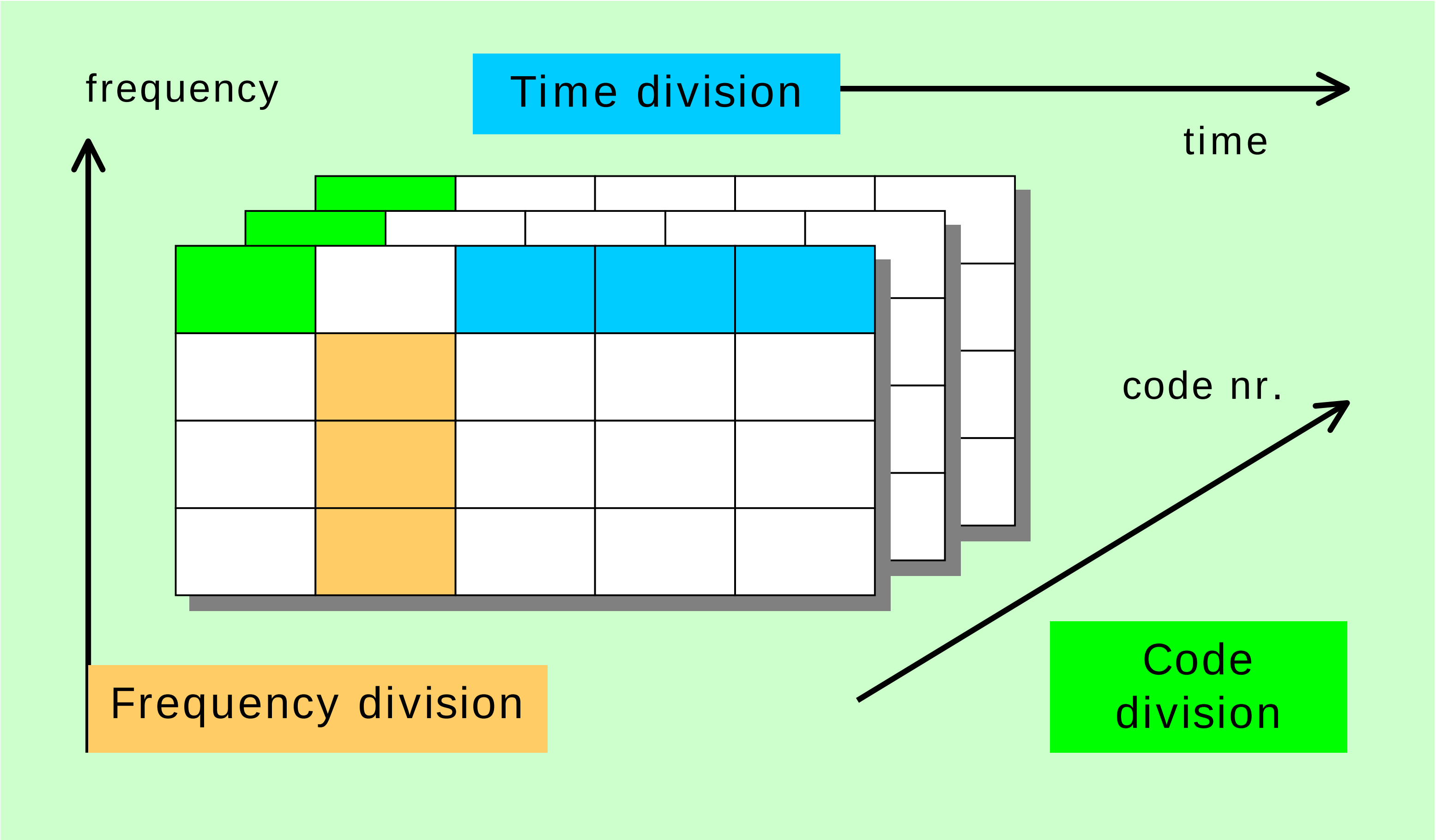

- New MS/terminals
- Packet Control Unit (PCU)
- SGSN and GGSN routers
- software updates (BTS, HLR)

# Purpose of TRAU

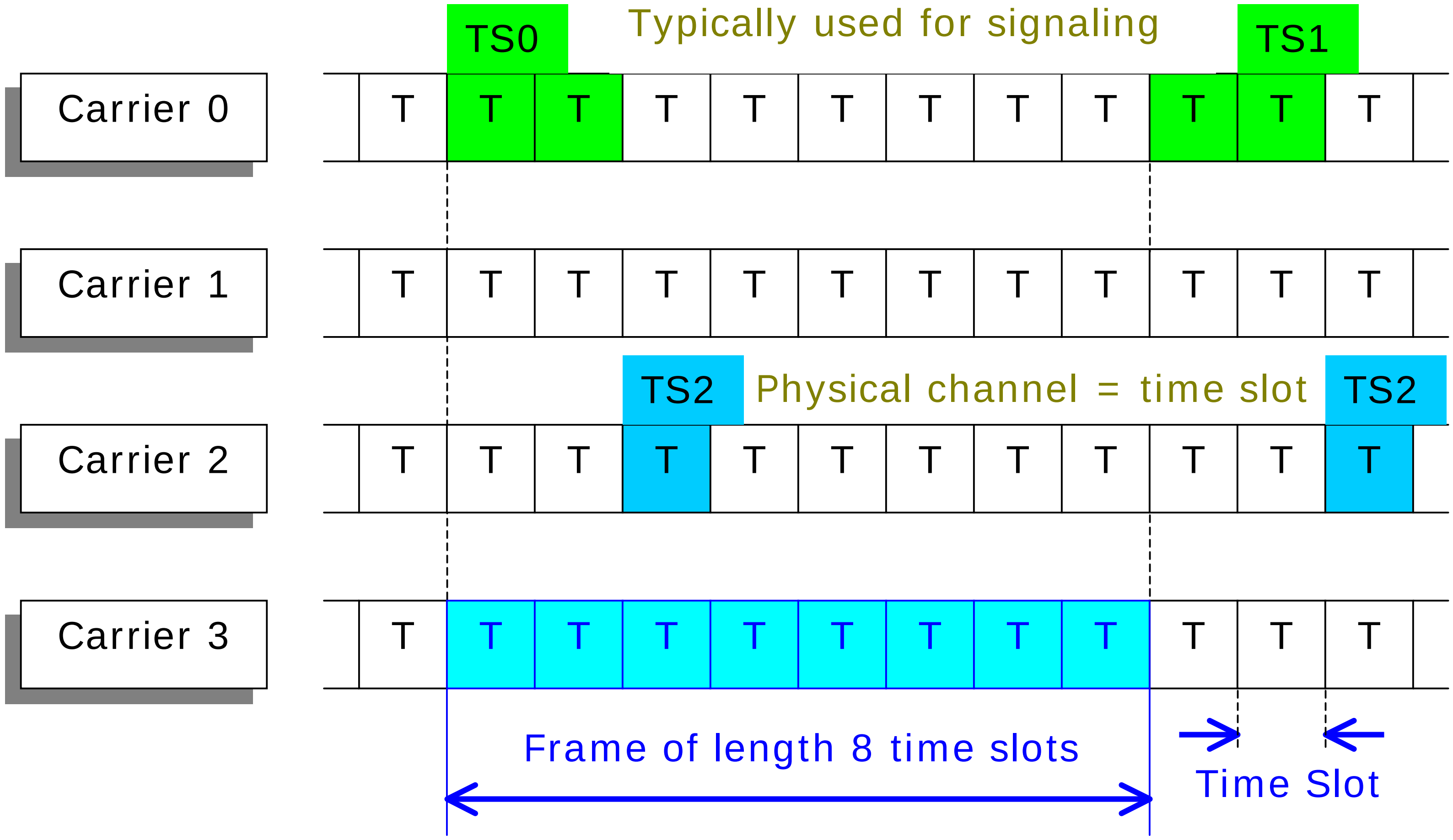
(TRAU = Transcoding and Rate Adaptation Unit)



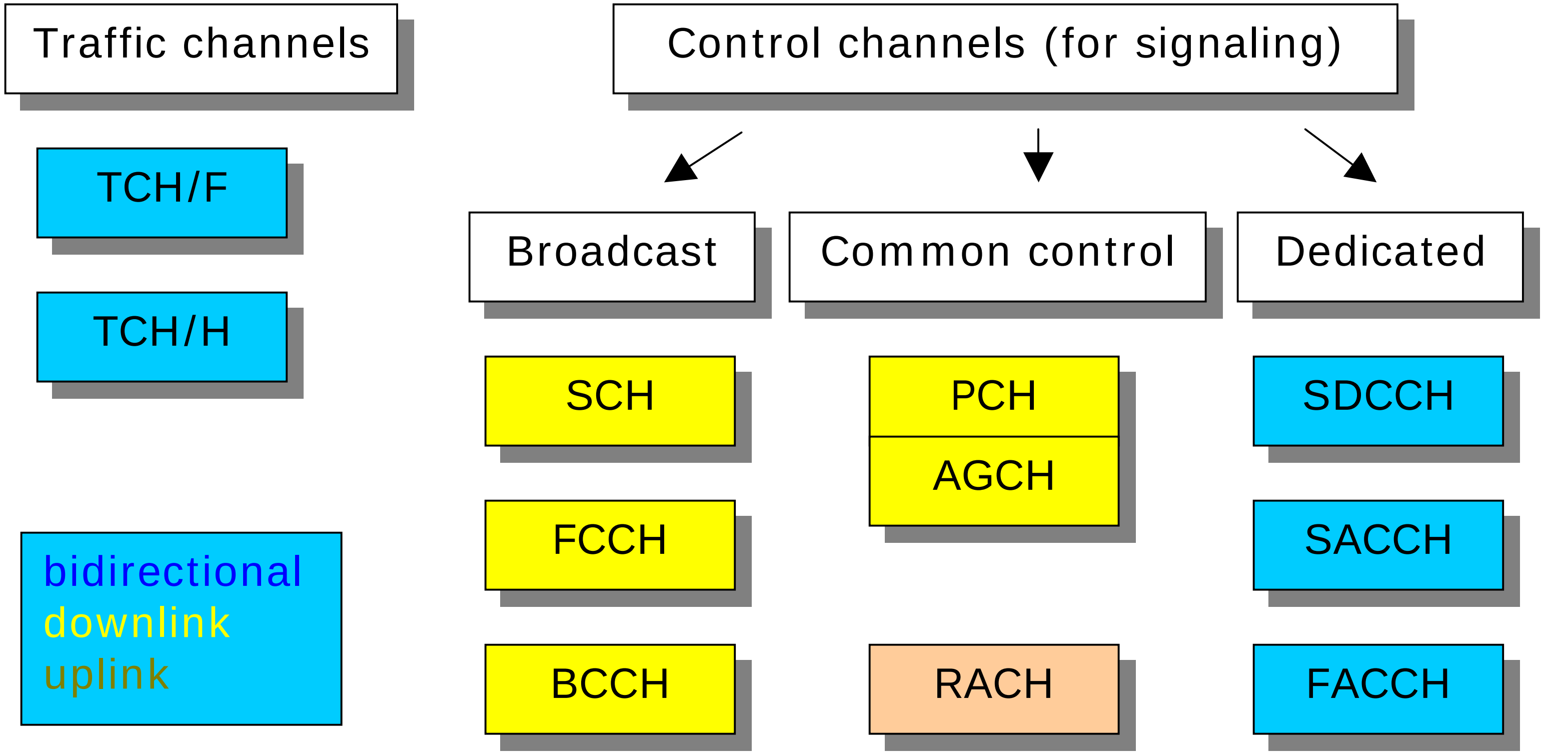
# Radio interface - multiple access techniques



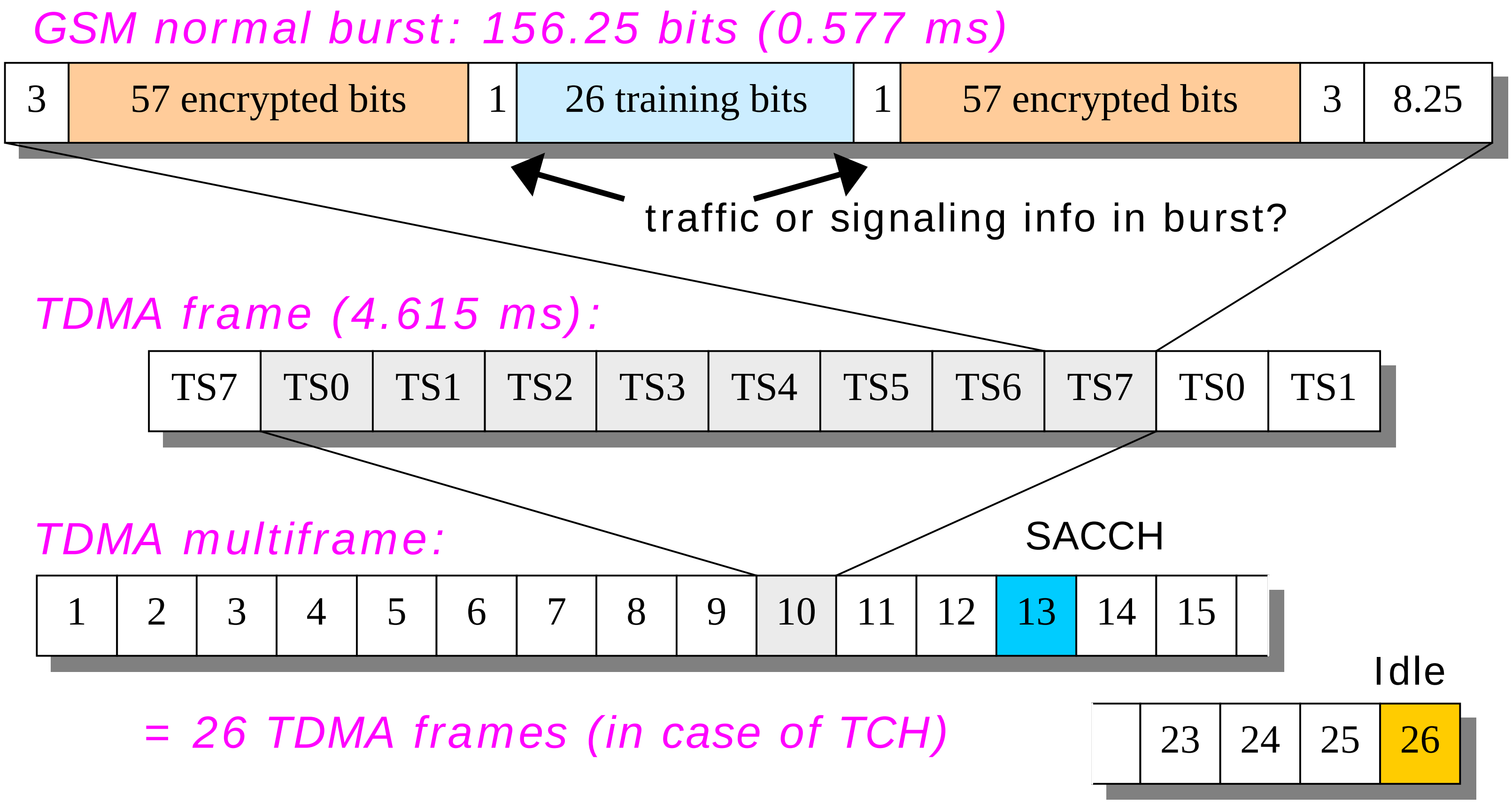
# Physical channel = repetitive time slot



# GSM logical channels

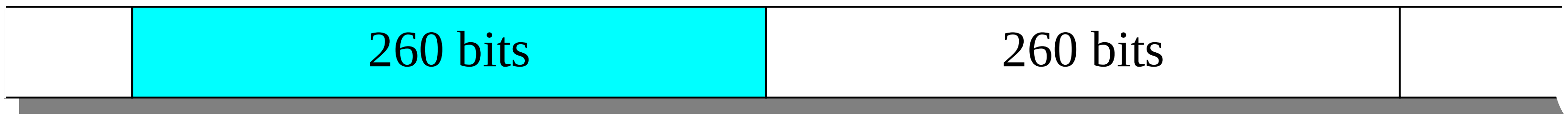


# GSM burst structure

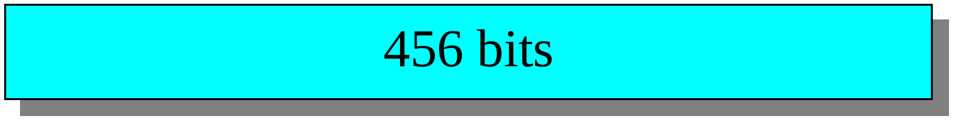


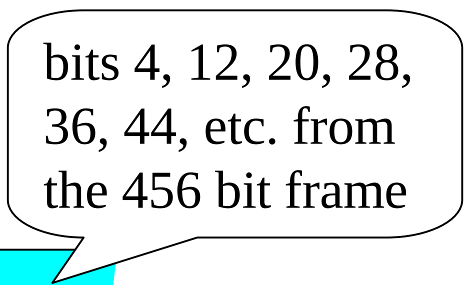
# GSM speech encoding

*Voice coding: 260 bits in 20 ms blocks (13 kbit/s)* *MS - TRAU*

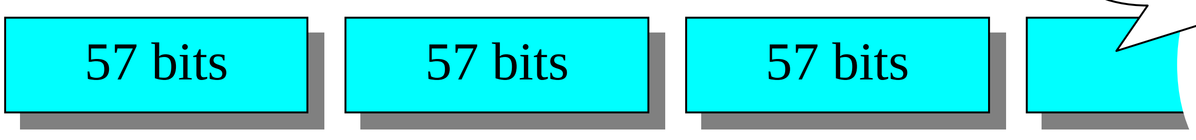



*Channel coding: 456 coded bits (22.8 kbit/s)* *MS - BTS*




*Interleaving: 8 x 57 bits (22.8 kbit/s)*



# GSM signaling message encoding

*Signaling message is segmented into blocks of 184 bits:*

184 bits

*Each block is coded into 456 bits (22.8 kbit/s)*

456 bits

*Interleaving: 8 x 57 bits (22.8 kbit/s)*

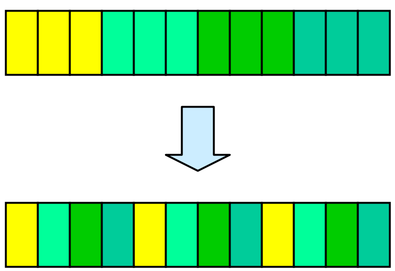
57 bits | 57 bits | 57 bits

bits 4, 12, 20, 28, 36, 44, etc. from the 456 bit frame

# Purpose of interleaving

**Transmitter**

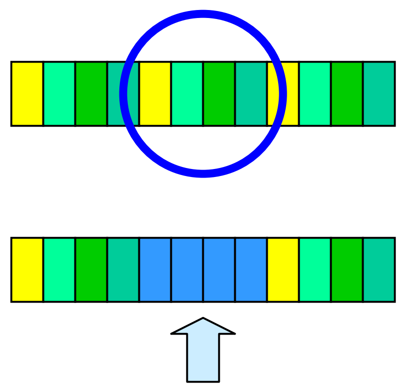
Bits are interleaved ...



... and will be de-interleaved in the receiver

**Channel**

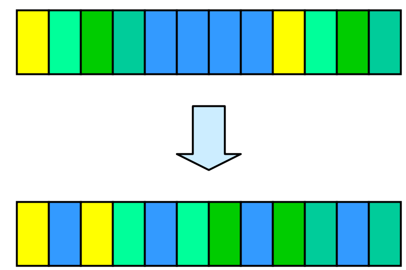
Fading affects many adjacent bits



Bit errors in the receiver

**Receiver**

After de-interleaving of bits, bit errors are spread



(better error correction)

# Task Management in GSM/GPRS

**Radio Resource Management (RM)**

1 Random access and channel reservation
Handover management
3 Ciphering (encryption) over radio interface

Number refers to the remaining slides

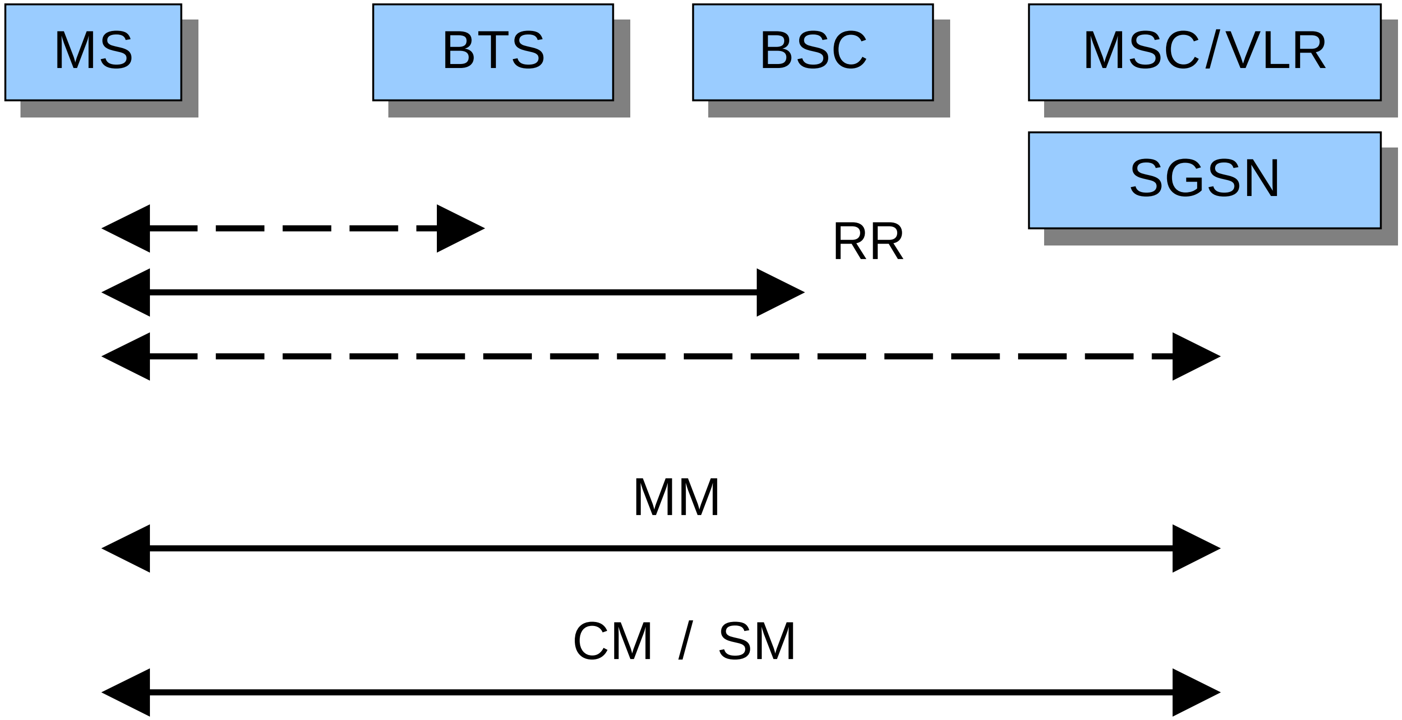
**Mobility Management (MM)**

IMSI/GPRS Attach (switch on) and Detach (switch off) 4
Location updating (MS moves to other Location/Routing Area)
2 Authentication

**Call Control (CC) in GSM** — MOC, MTC 5

**Session Management (SM) in GPRS** — PDP Context 6

# Who is involved in what?



# 1 Random access in GSM/GPRS (1)

Communication between MS and network is not possible before going through a procedure called *random access*.

Random access must consequently be used in

network originated activity

- paging, e.g. for a mobile terminated call in GSM

MS originated activity

- IMSI attach, IMSI detatch
- GPRS attach, GPRS detach
- location updating in GSM or GPRS
- mobile originated call in GSM
- SMS (short message service) message transfer

1

# Random access in GSM/GPRS (2)

1. MS sends a short access burst over the Random Access CHannel (RACH) in uplink using Slotted Aloha (in case of collision => retransmission after random time)

2. After detecting the access burst, the network (BSC) returns an ”immediate assignment” message which includes the following information:
   - allocated physical channel (frequency, time slot) in which the assigned signalling channel is located
   - timing advance (for correct time slot alignment)

3. The MS now sends a message on the dedicated signalling channel assigned by the network, indicating the reason for performing random access.

# Four security measures in GSM

1) PIN code (authentication of user using terminal
=> local security measure, network is not involved)

2) SIM authentication (performed by network)

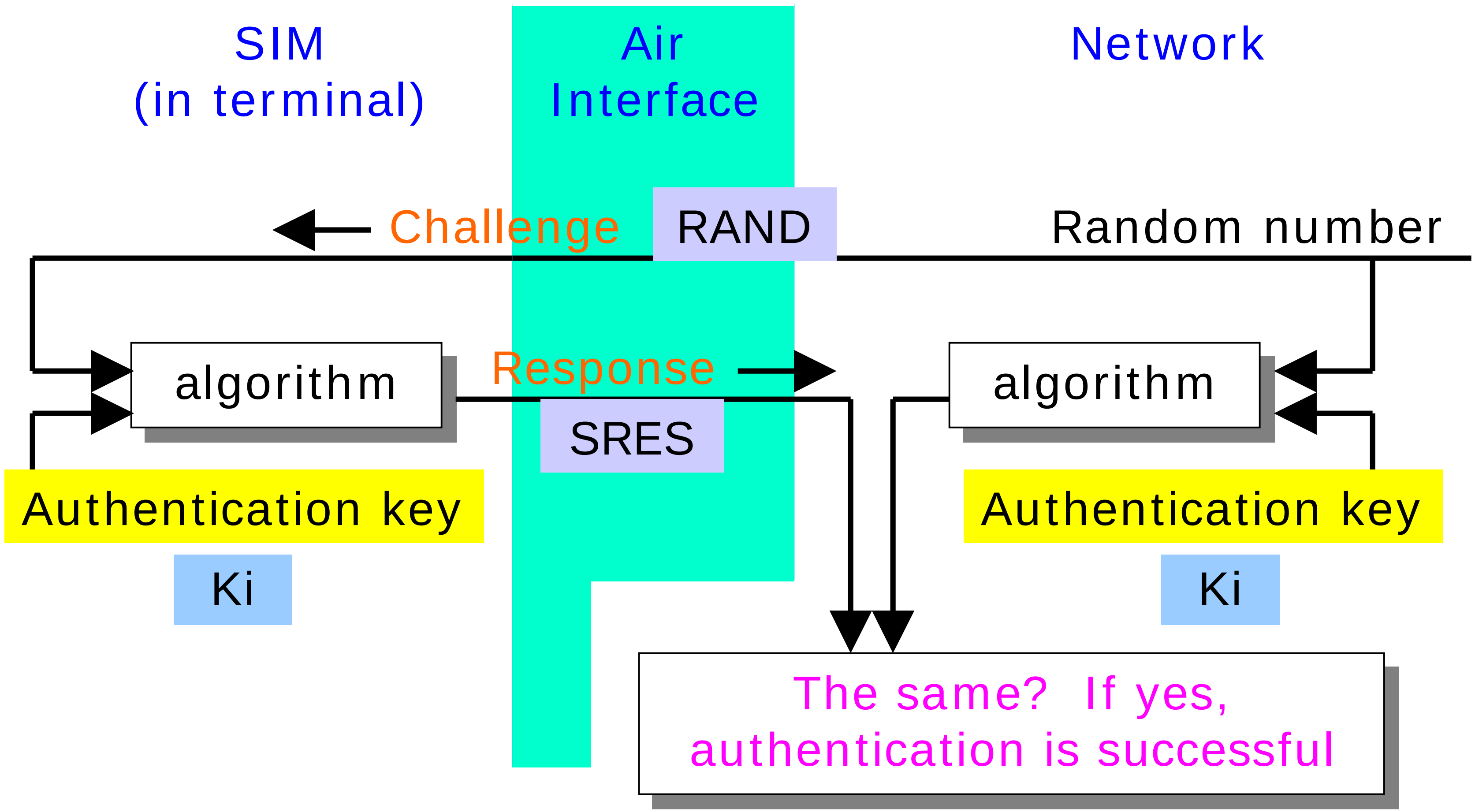
3) Ciphering of information sent over air interface

4) Usage of TMSI (instead of IMSI) over air interface

IMSI = International Mobile Subscriber Identity
(globally unique identity)

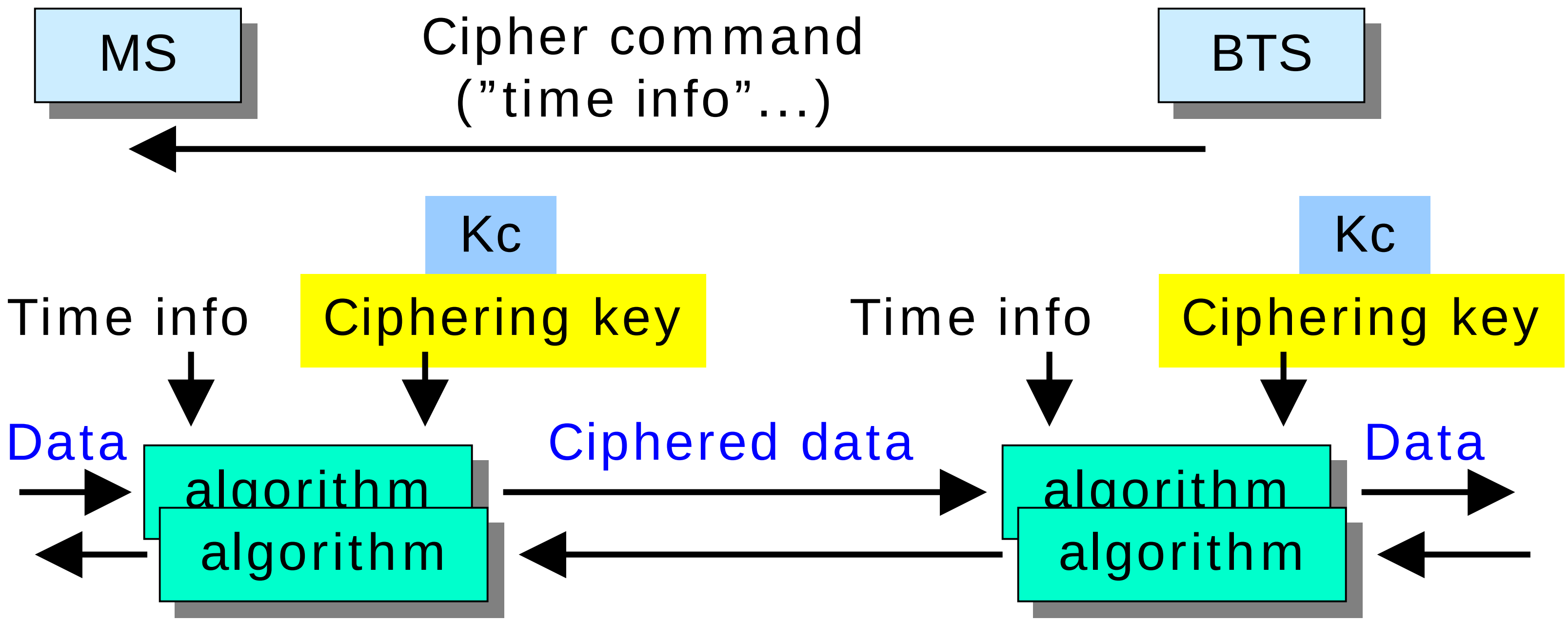
TMSI = Temporary Mobile Subscriber Identity
(local and temporary identity)

## ② Basic principle of user authentication



3

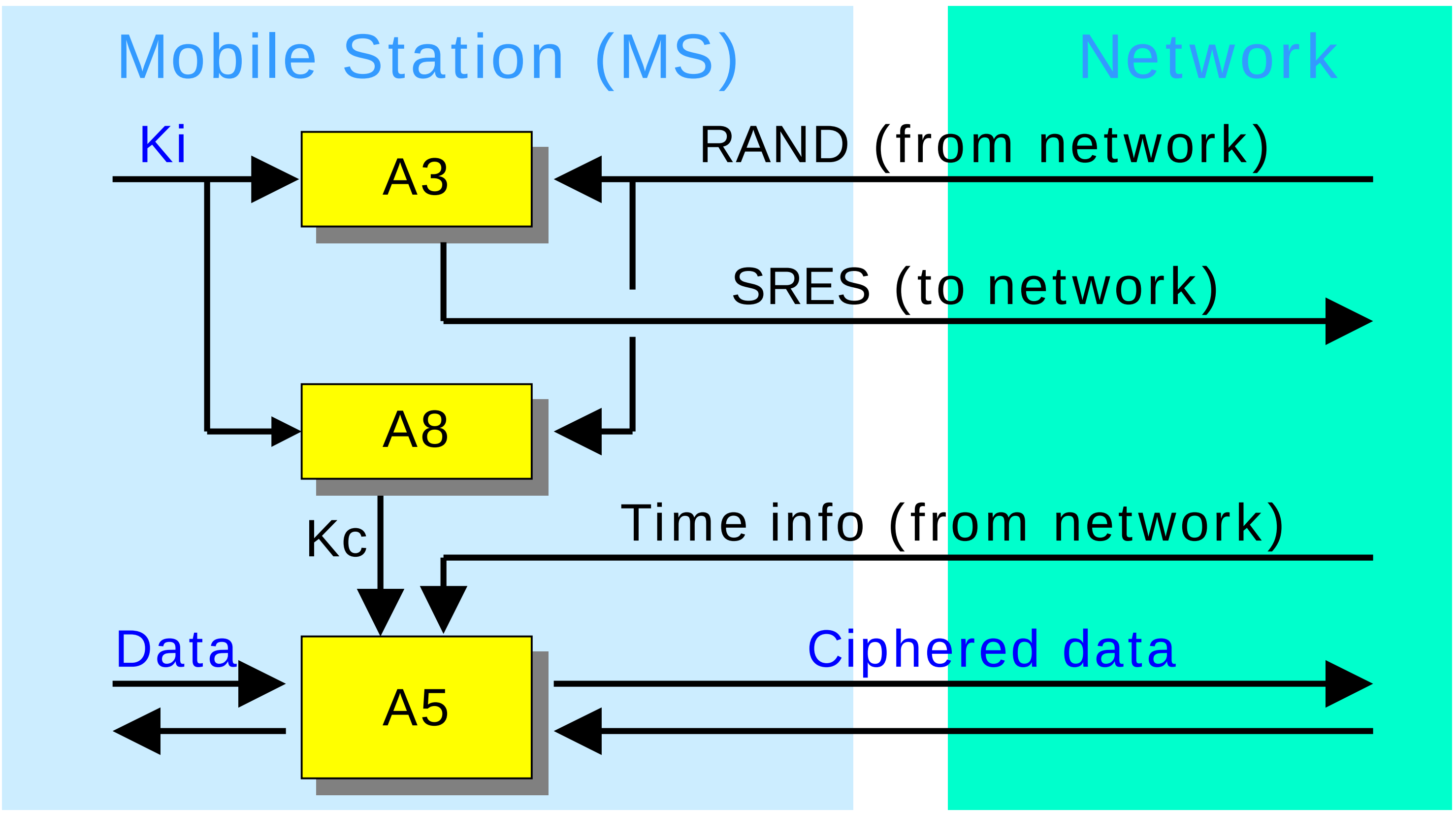
# Ciphering in GSM




For each call, a new ciphering key (Kc) is generated during authentication both in MS and MSC (in same way as authentication "response").

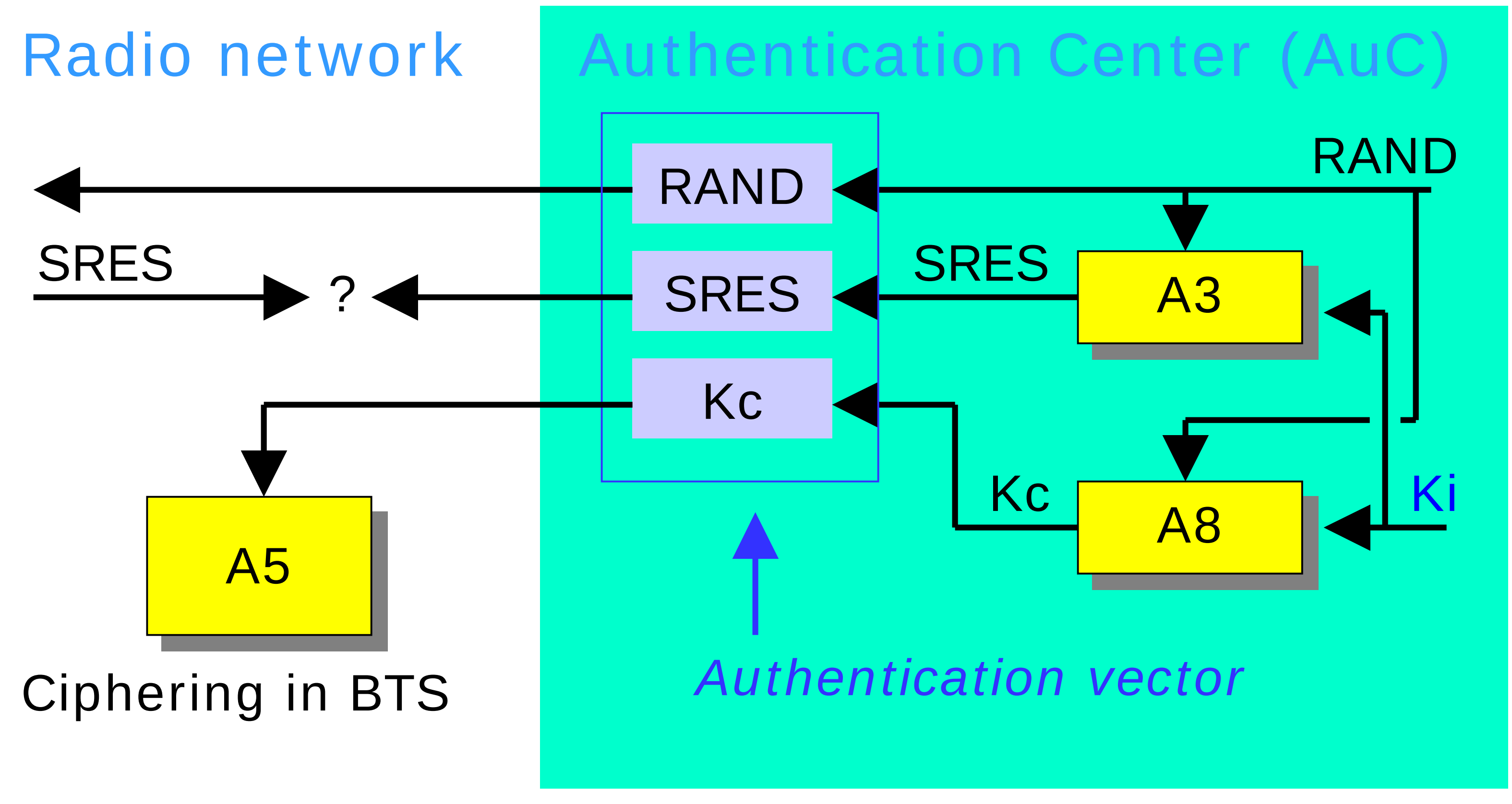
# Three security algorithms in GSM

(in UMTS many more ...)



# Three security algorithms in GSM

## at the network side ...



2 3

# Algorithm considerations

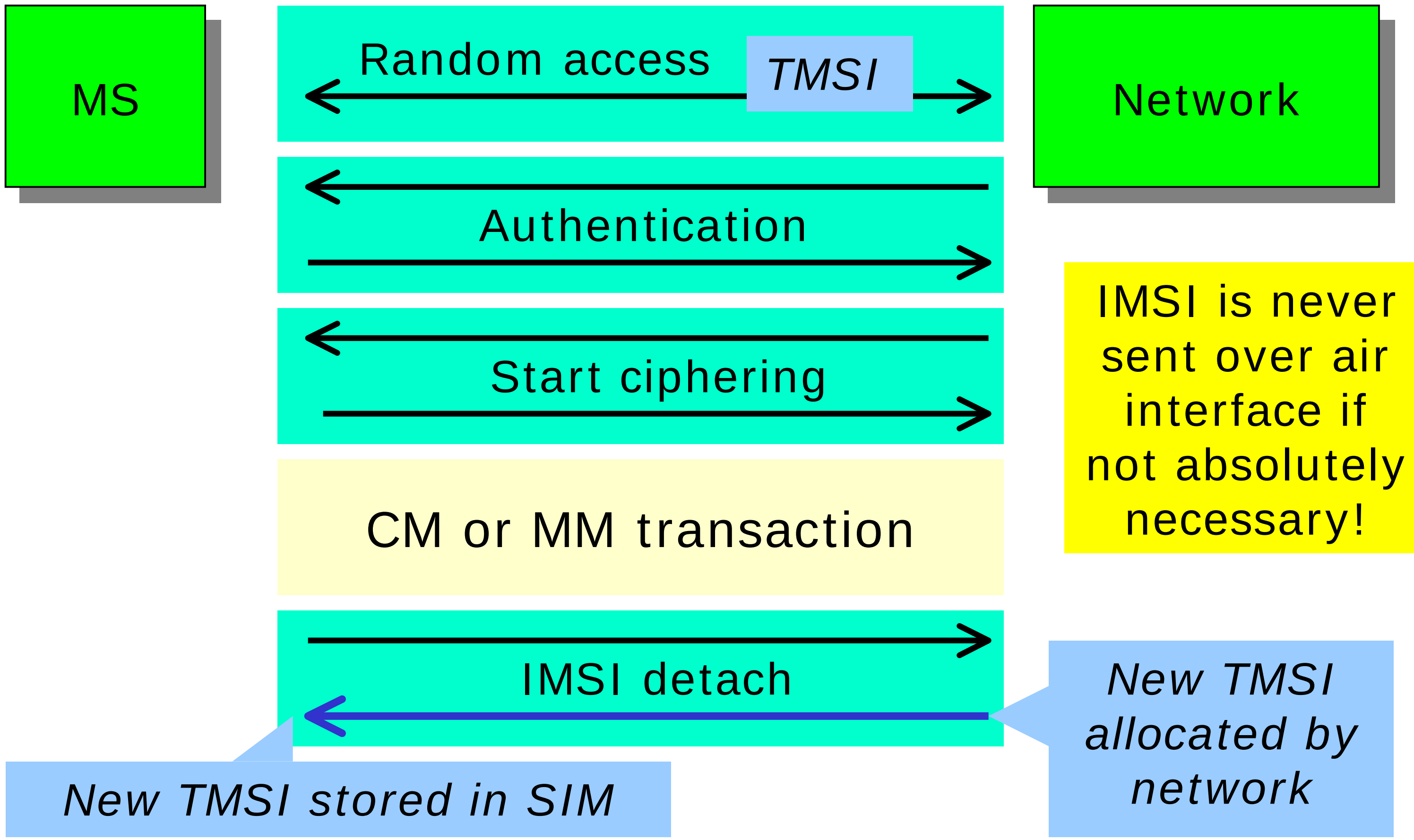
Using output and one or more inputs, it is in practice not possible to calculate "backwards" other input(s)
"brute force approach", "extensive search"

Key length in bits (*N*) is important (in case of brute force approach $2^N$ calculation attempts may be needed)

Strength of algorithm is that it is secret => bad idea!
"security through obscurity"

Better: open algorithm can be tested by engineering community (security through strong algorithm)

# Usage of TMSI in GSM



# 4 Connectivity states in GSM/GPRS

**GSM**

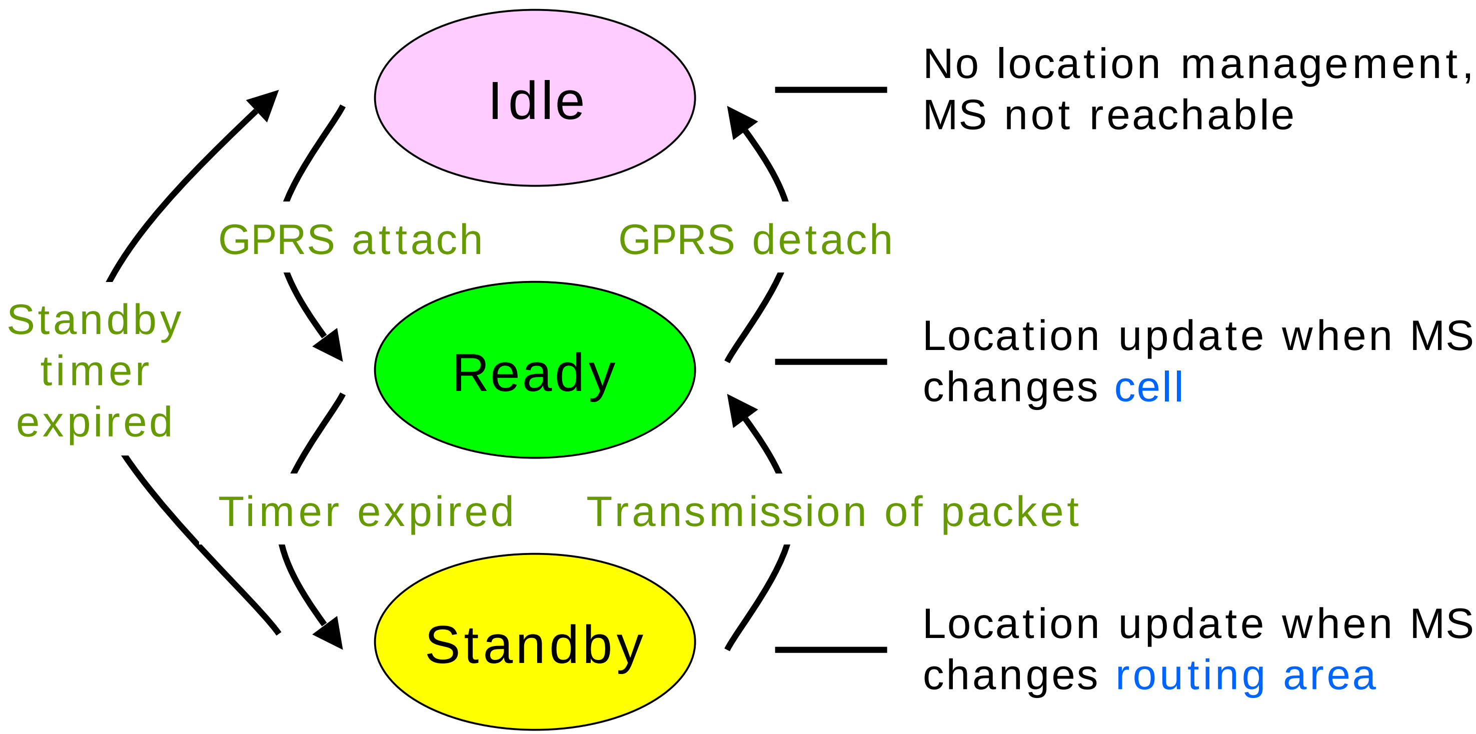
| | |
|---|---|
| Disconnected | MS is switched off (circuit mode) |
| Idle | location updates on LA basis |
| Connected | handovers, not location updates |

**GPRS**

| | |
|---|---|
| Idle | MS is switched off (packet mode) |
| Standby | location updates on RA basis |
| Ready | location updates on cell basis |

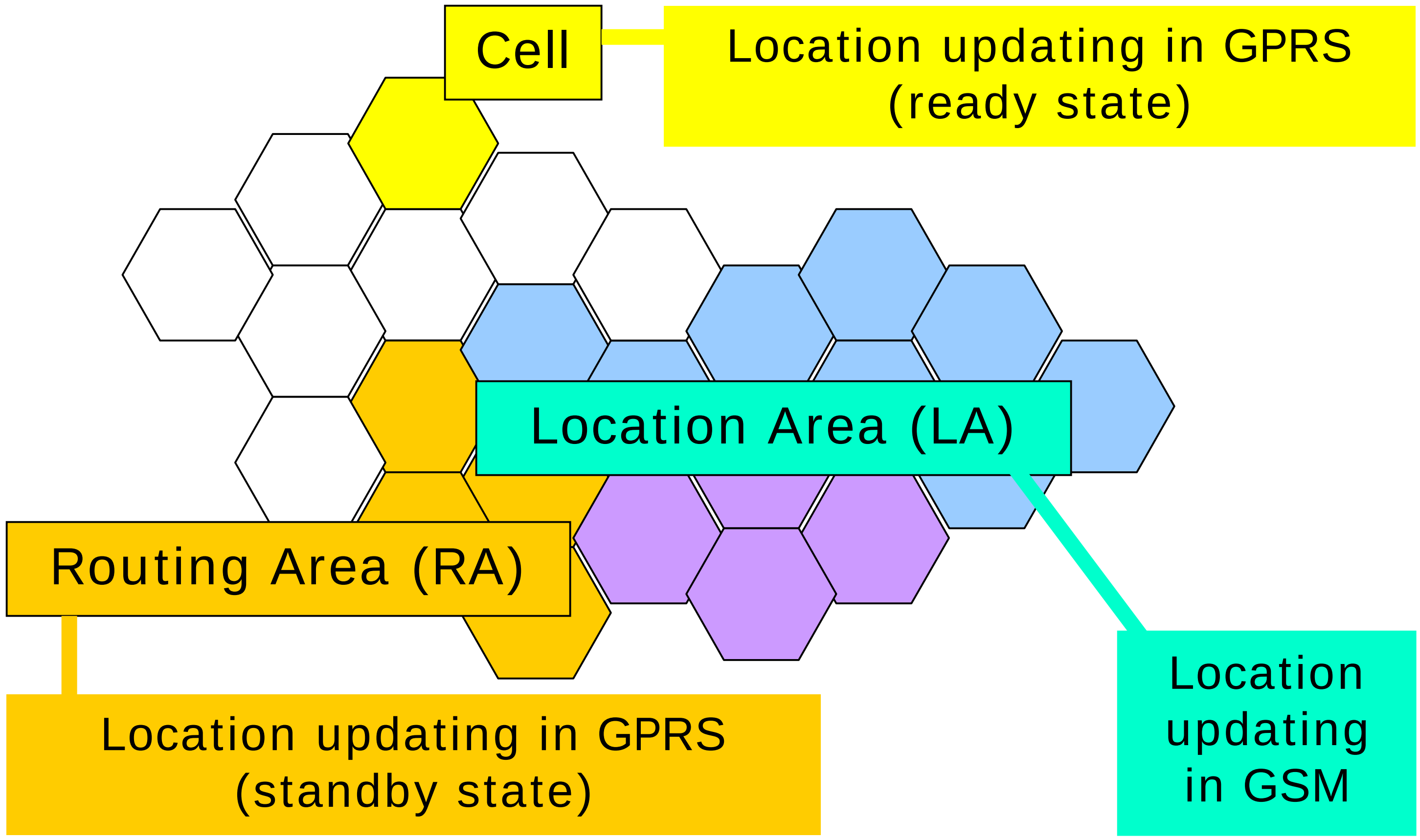
4

# GPRS connectivity state model



4

# MM “areas” in GSM/GPRS



# 4 Trade-off when choosing LA/RA size

If LA/RA size is very large (e.g. whole mobile network)

+ location updates not needed very often
– paging load is very heavy

Affects capacity

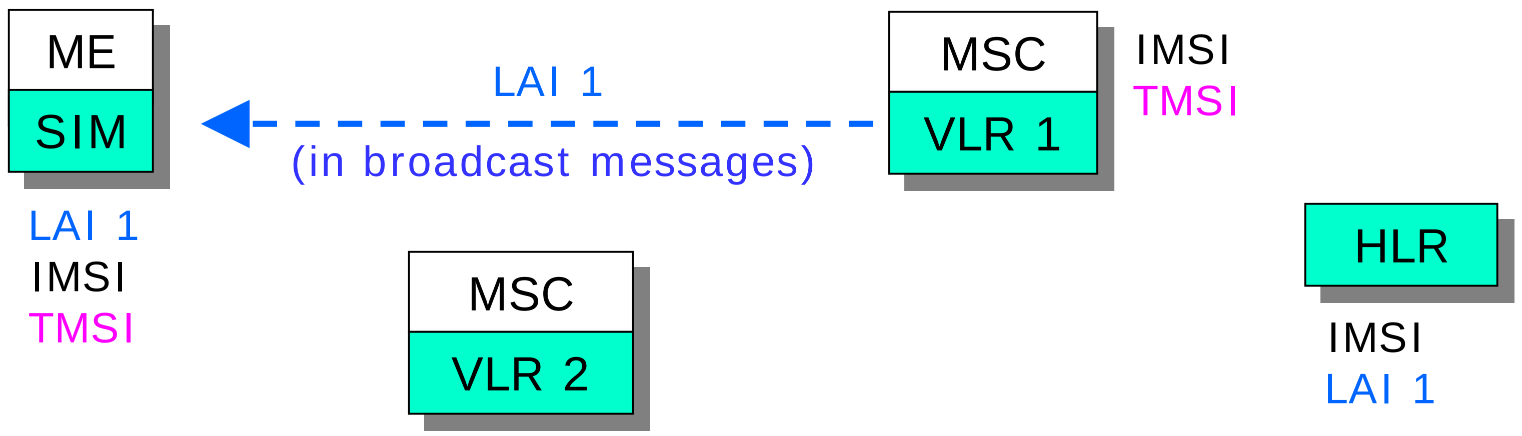
If LA/RA size is very small (e.g. single cell)

+ small paging load
– location updates must be done very often

Affects signalling load

# 4 Case study: GSM location update (1)

(most generic scenario)

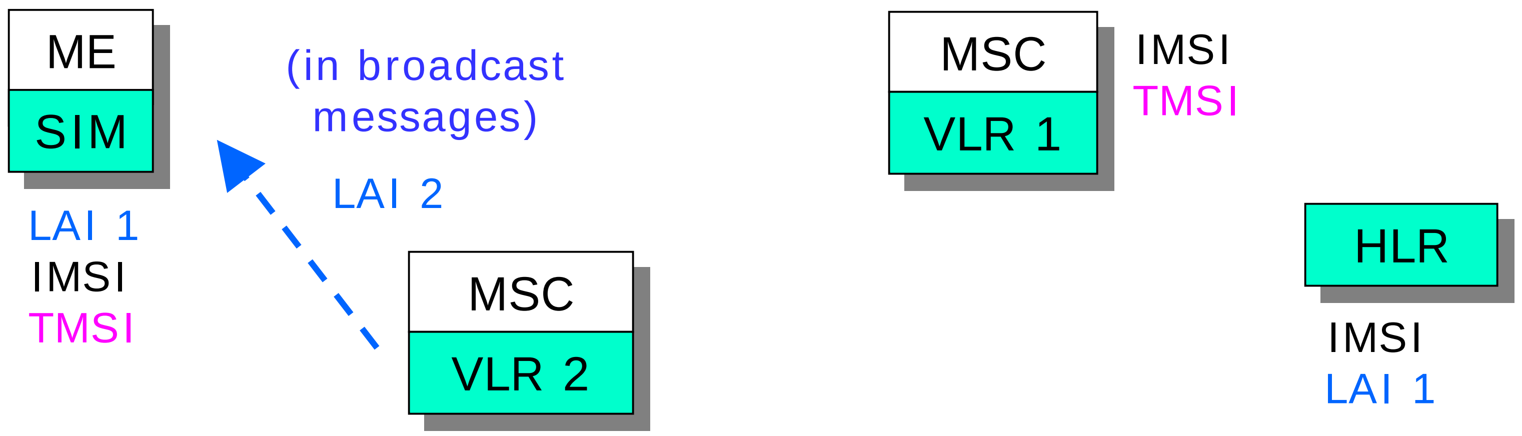



Most recently allocated TMSI and last visited LAI (Location Area ID) are stored in SIM even after switch-off.

After switch-on, MS monitors LAI. If stored and monitored LAI values are the same, no location updating is needed.

4

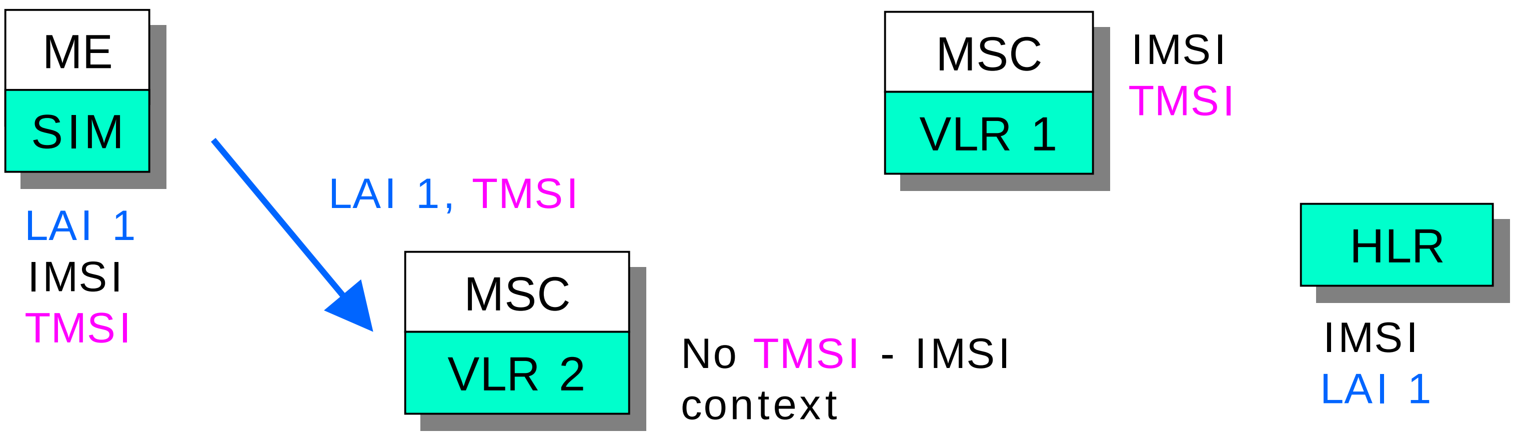
# GSM location update (2)




Different LAI values => location update required !

4

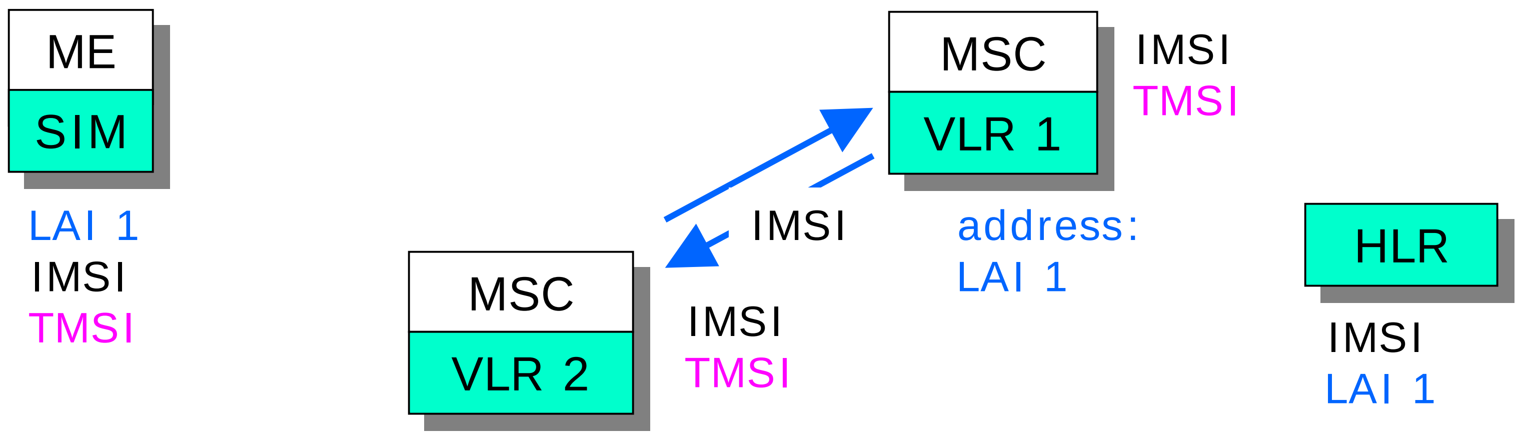
# GSM location update (3)




SIM sends old LAI and TMSI to VLR 2.

VLR 2 does not recognize TMSI since there is no TMSI-IMSI context. Who is this user?

# GSM location update (4)

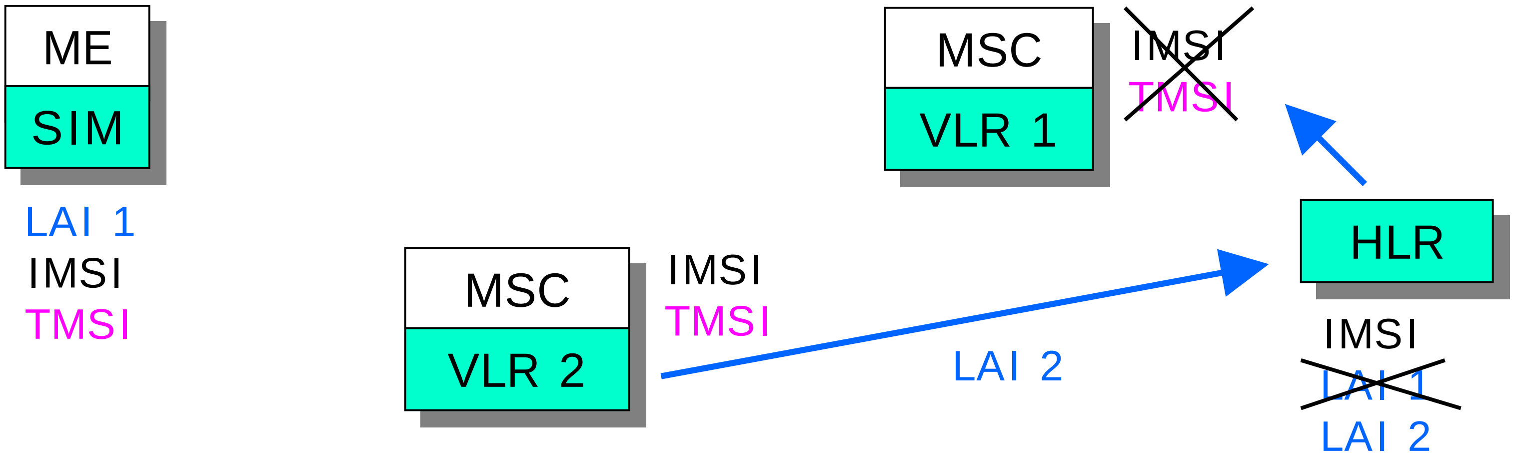



However, VLR 2 can contact VLR 1 (address: LAI 1) and request IMSI.

IMSI is sent to VLR 2.

4

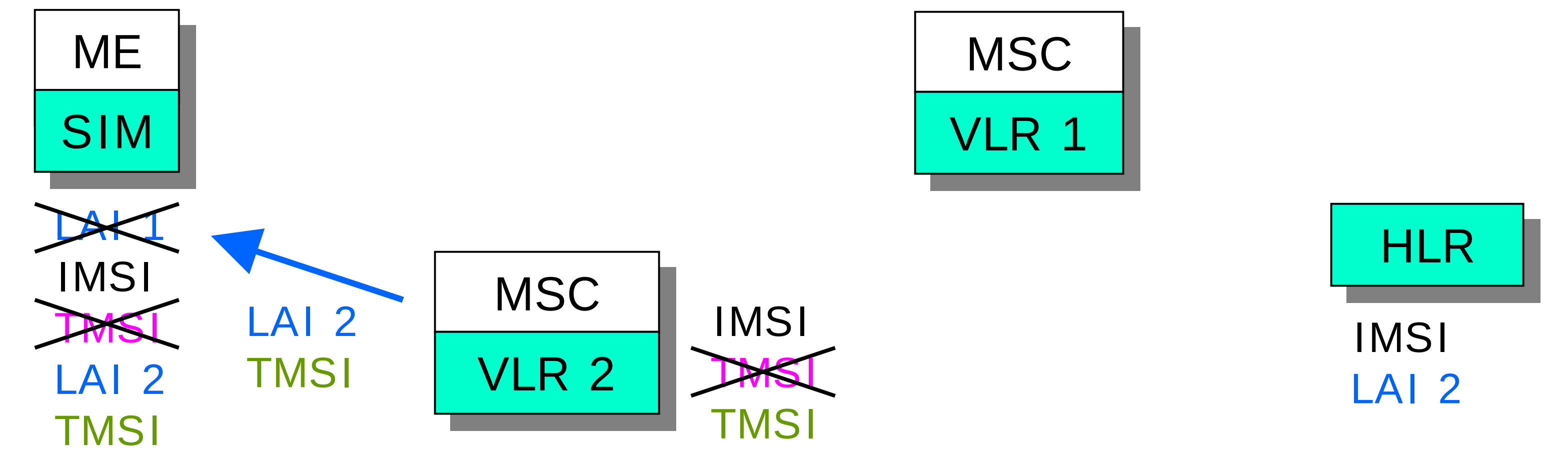
# GSM location update (5)




Important: HLR must be updated (new LAI). If this is not done, incoming calls can not be routed to new MSC/VLR.

HLR also requests VLR 1 to remove old user data.

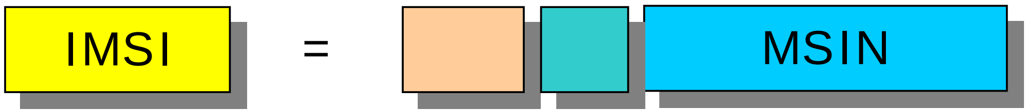
# GSM location update (6)




VLR 2 generates new TMSI and sends this to user. User stores new LAI and TMSI safely in SIM.

Location update successful !

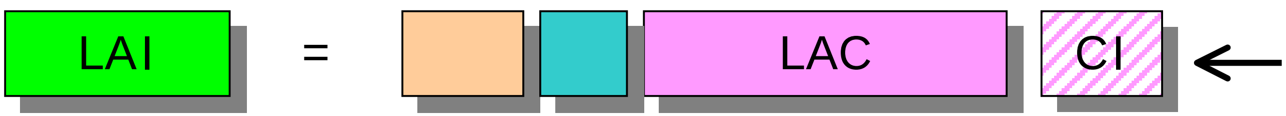
# GSM identifiers (1)




*GSM "internal information"*

*Globally unique*

MCC = Mobile Country Code (3 digits)
MNC = Mobile Network Code (2 digits)
MSIN = Mobile Subscriber Identity Number (≤10 digits)

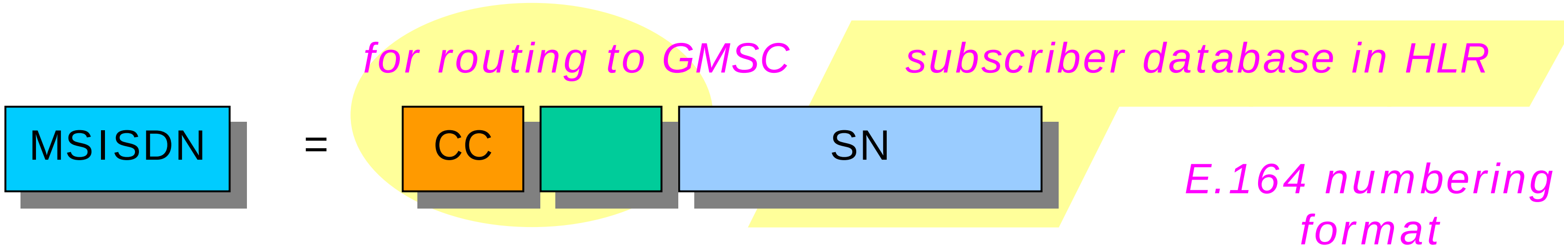



*LAI + CI = CGI Cell Global Identity*

*Globally unique*

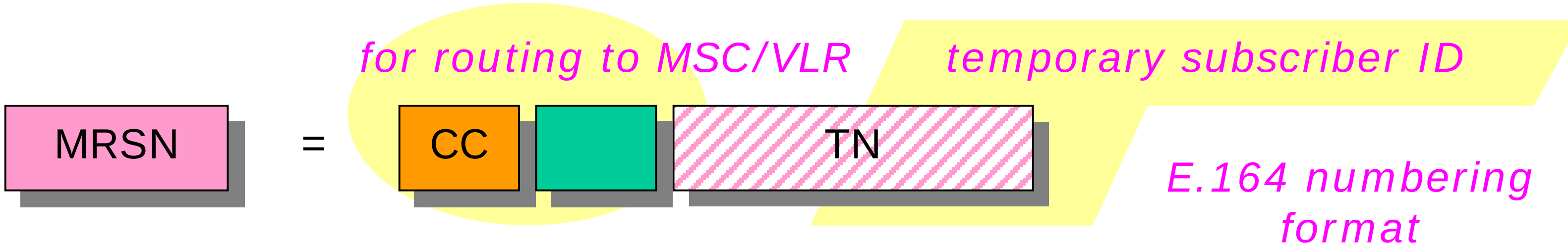
MCC = Mobile Country Code (3 digits)
MNC = Mobile Network Code (2 digits)
LAC = Location Area Code (≤10 digits)

# GSM identifiers (2)




*Globally unique*

CC = Country Code (1-3 digits)
NDC = National Destination Code (1-3 digits)
SN = Subscriber Number



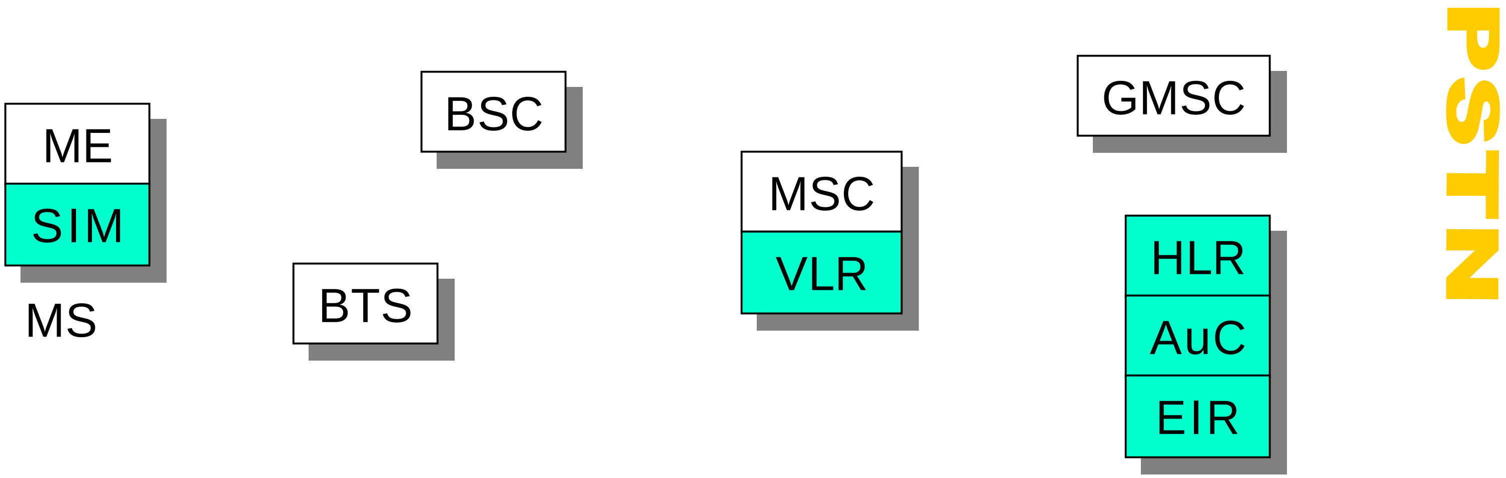

*Temporary allocation*

CC = Country Code (1-3 digits)
NDC = National Destination Code (1-3 digits)
TN = Temporary Number

5

# Case study: GSM MTC (1)

MTC = mobile terminated call

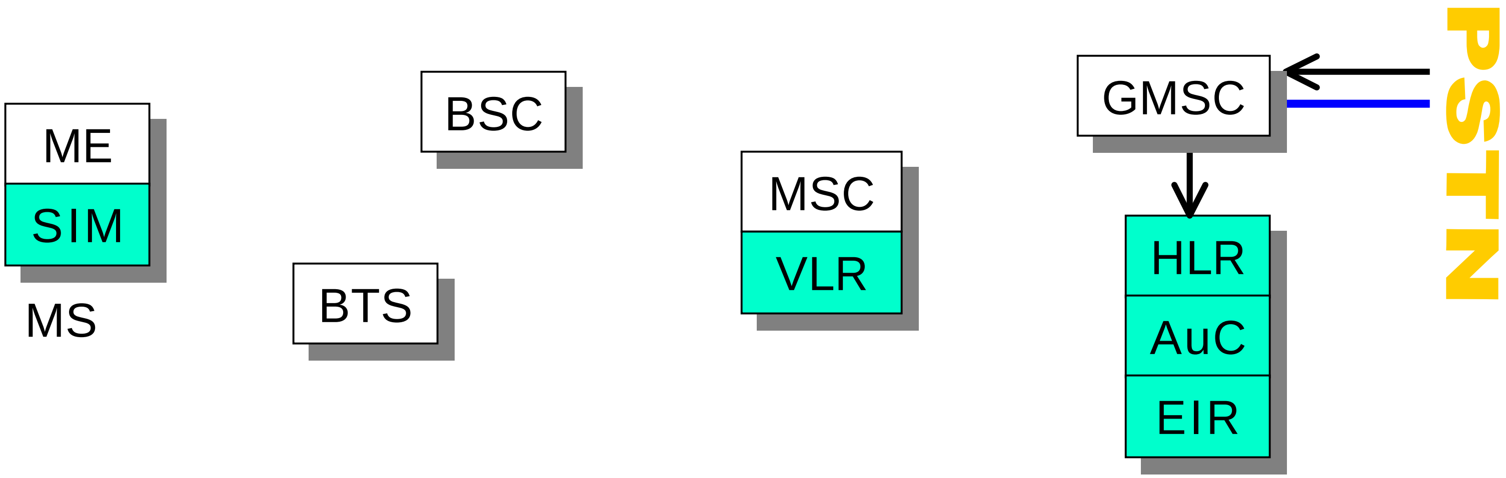



Circuit switched connection (64 kb/s PCM, 16 kb/s between TRAU and BTS, 13 kb/s encoded speech over air interface)

Signaling (ISUP, MAP)

Database

# GSM mobile terminated call (2)



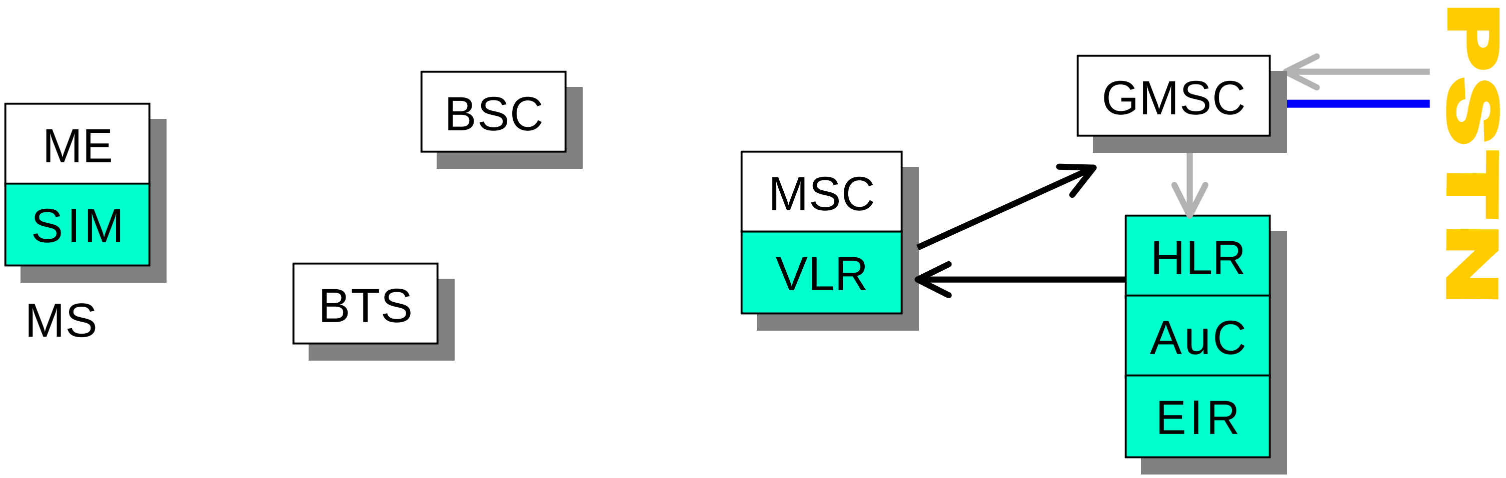

Call is routed to GMSC using MSISDN number of called user (e.g. 040 1234567).

MSISDN number in fact points to database in HLR.

HLR is contacted. Under which MSC/VLR is user?

5

# GSM mobile terminated call (3)



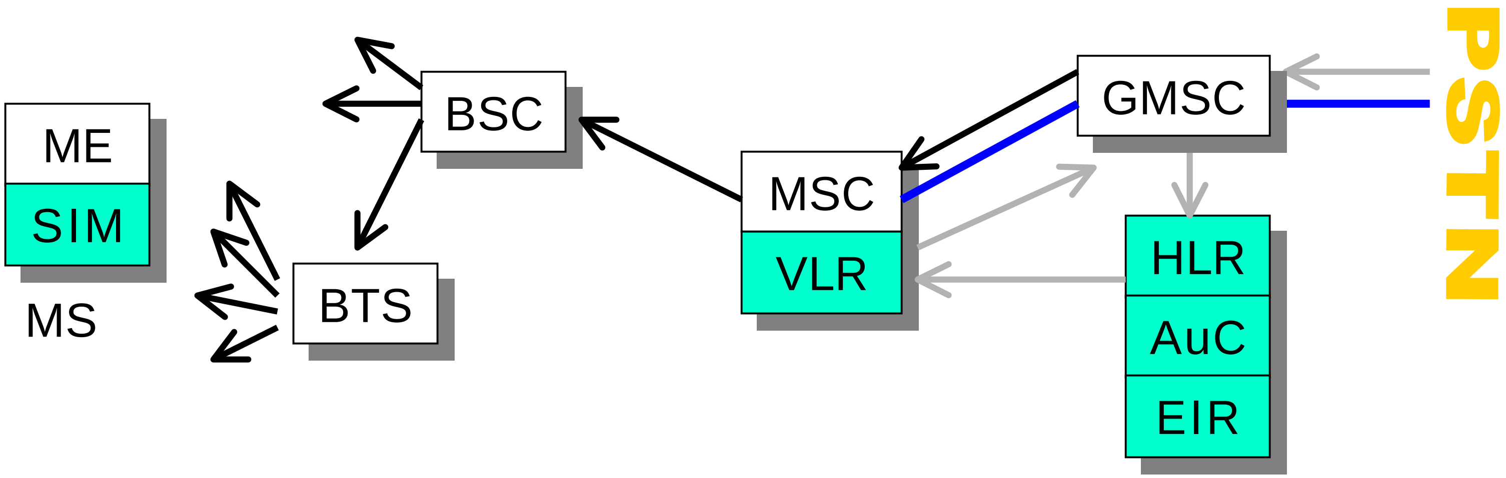

HLR knows location of Serving MSC/VLR (when user moves to another VLR, this is always recorded in HLR).

HLR requests MSRN (roaming number) from VLR.

MSRN is forwarded to GMSC.

5

# GSM mobile terminated call (4)

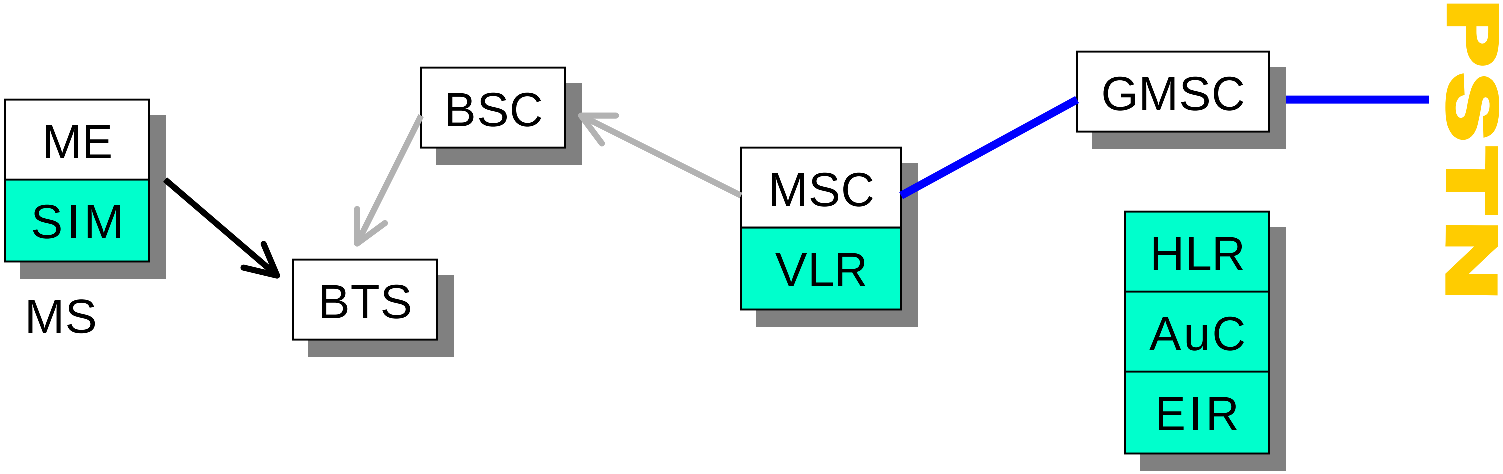



Call can now be routed to Serving MSC/VLR using ISUP (may involve several intermediate switching centers).

MSC/VLR starts paging within Location Area (LA) in which user is located, using TMSI for identification.

5

# GSM mobile terminated call (5)

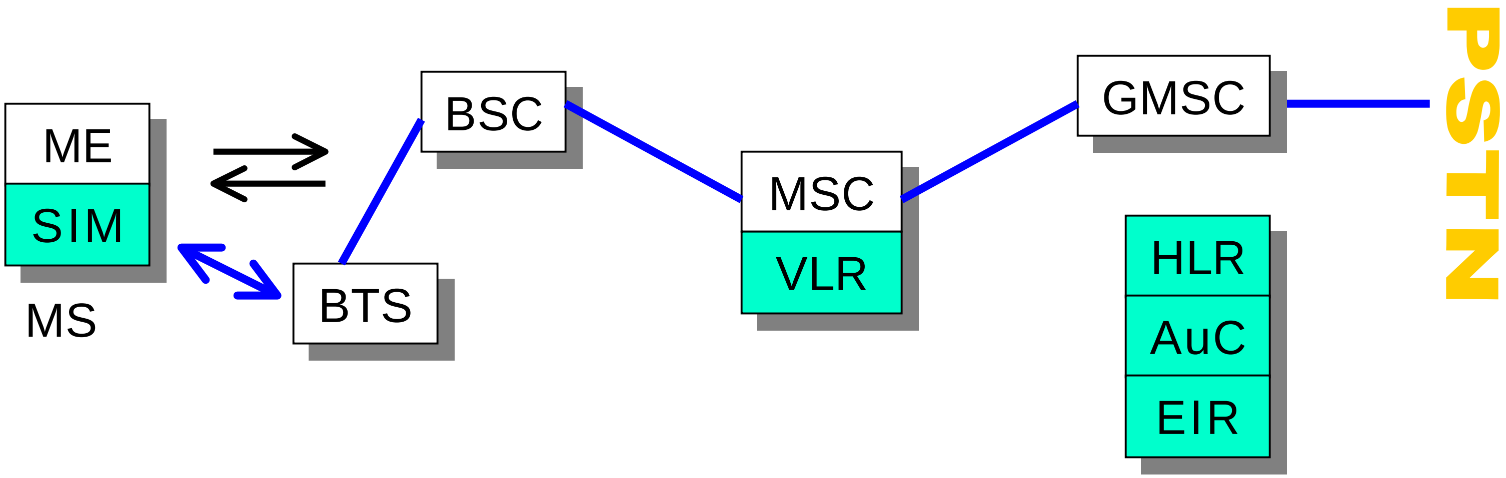



Only the mobile user with the corresponding TMSI responds to the paging.

Using random access procedure, user requests a channel, e.g. SDCCH, for call control signaling.

5

# GSM mobile terminated call (6)




Signaling channel is set up. After authentication and ciphering procedures, call control signaling continues.

Finally, a GSM traffic channel is set up over the radio interface. The circuit switched connection is now ready.

6

# GPRS attach / PDP session

## GPRS attach

Separate or combined GSM/GPRS attach
MS registers with an SGSN (authentication...)
Location updates possible

## PDP context is created

MS is assigned PDP (IP) address
Packet transmission can take place

In case of dynamic address allocation

DHCP (Dynamic Host Configuration Protocol)

## GPRS detach

PDP context terminated
Allocated IP address released

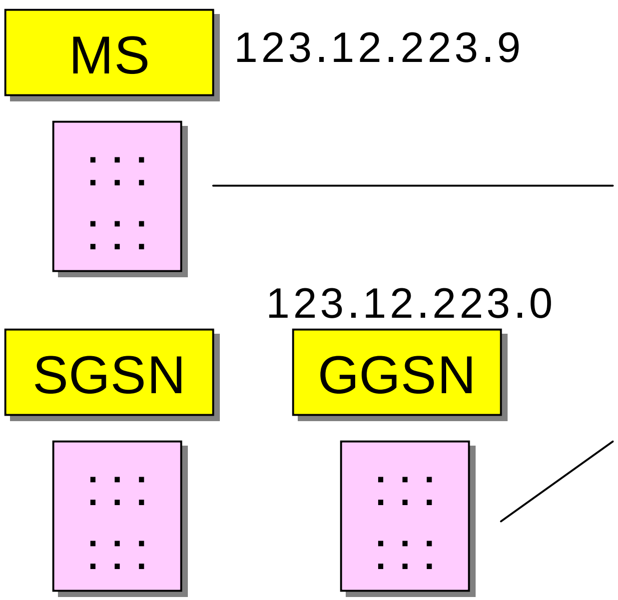
6

# PDP context

PDP context describes characteristics of GPRS session (session = “always on” connection)

PDP context information is stored in MS, SGSN and GGSN

One user may have several PDP context sessions active




PDP type (e.g. IPv4)

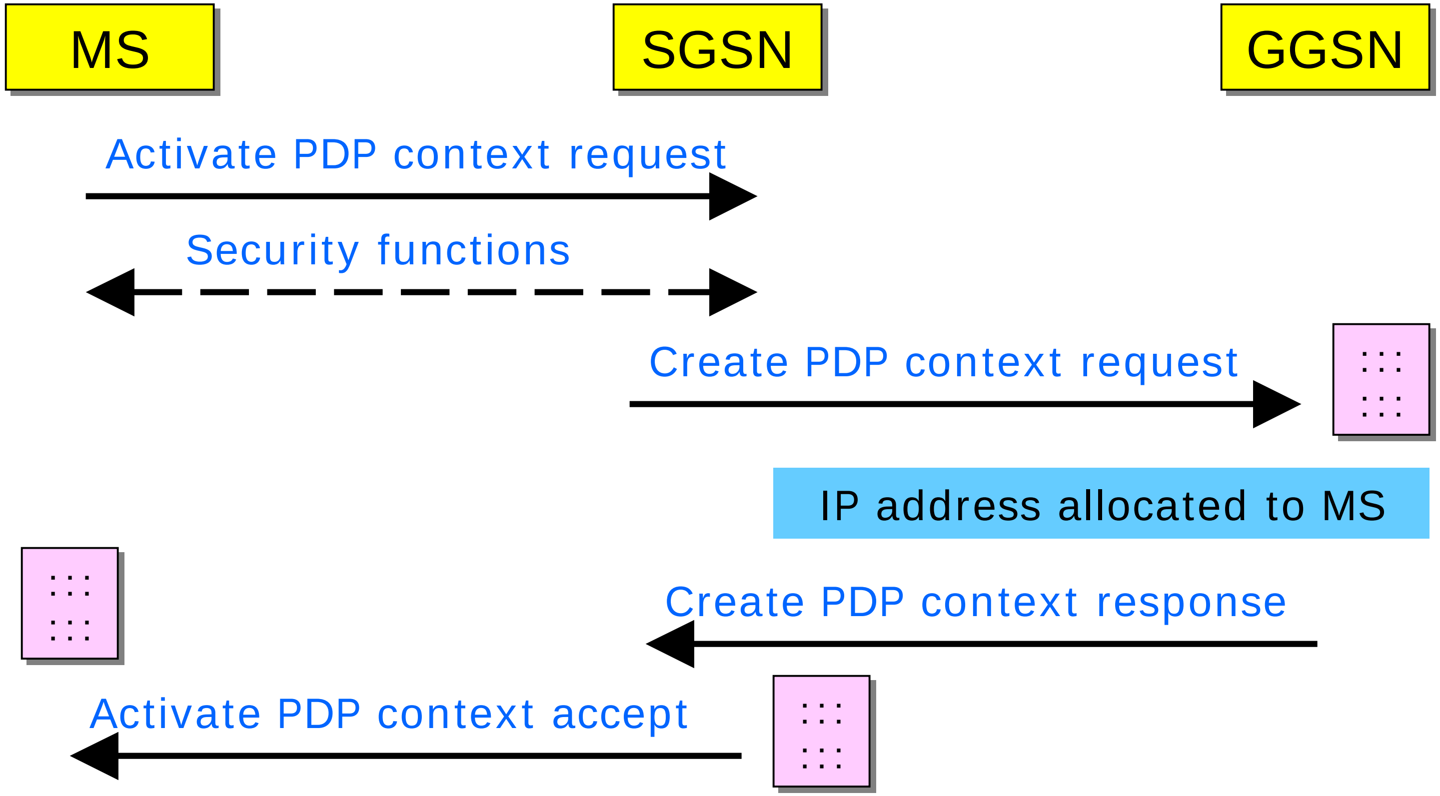
PDP address = IP address of MS (e.g. 123.12.223.9)

Requested QoS (priority, delay …)

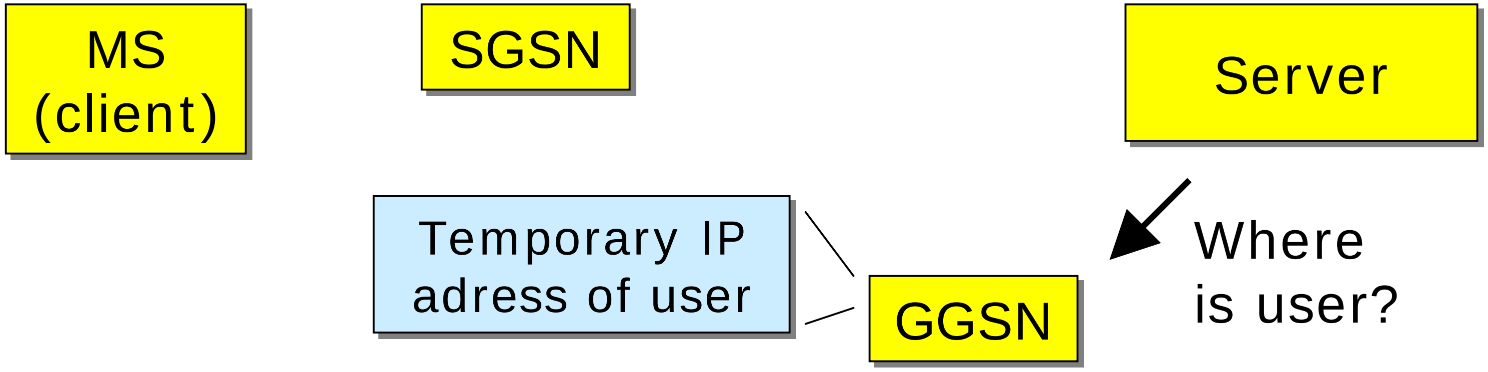
Access Point Name = IP address of GGSN (e.g. 123.12.223.0)

6

# PDP context activation



# Packet transmission (1)



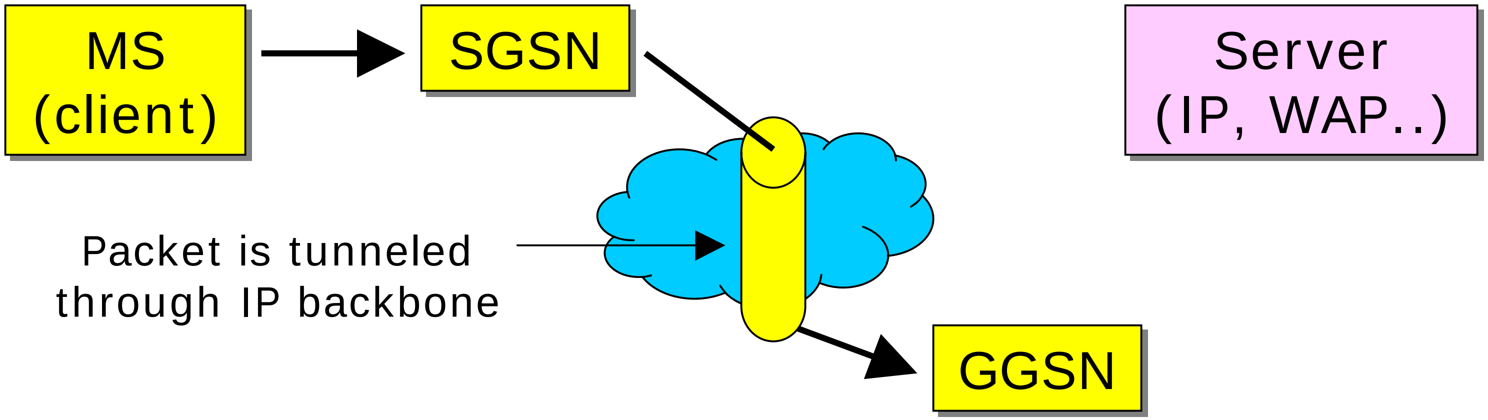

Dynamic IP address allocation has one problem:
it is difficult to handle a mobile terminated transaction
(external source does not know IP address of MS)

Fortunately, packet services are usually of client-server type

=> MS initiates packet transmission

6

# Packet transmission (2)




Packet is sent to SGSN. SGSN sends packet to GGSN through GTP (GPRS Tunneling Protocol) tunnel.

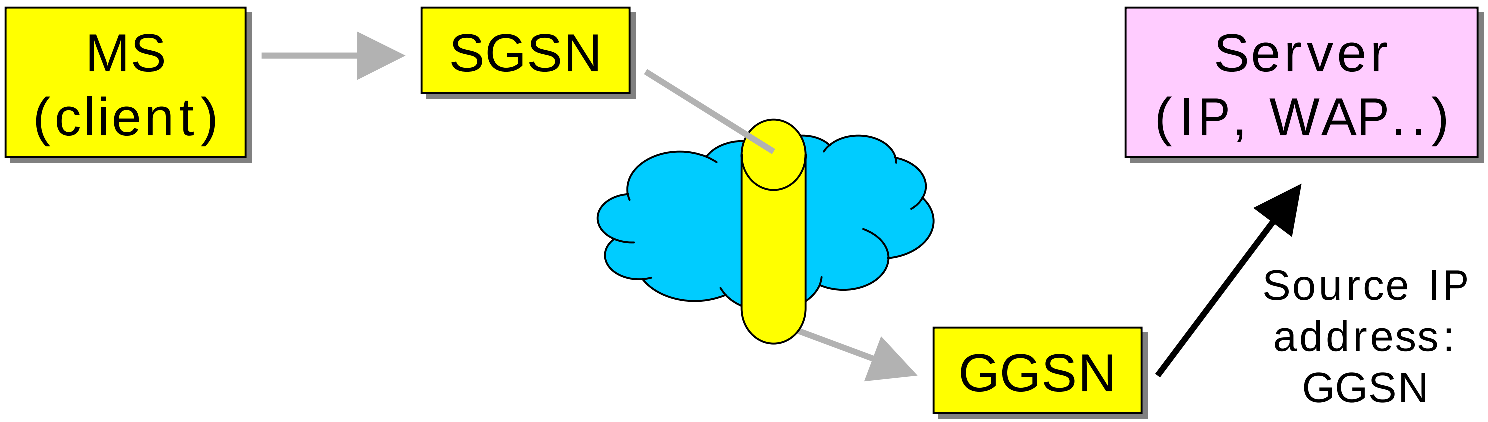
Tunneling = encapsulation of IP packet in GTP packet

| | | |
|---|---|---|
| IP address ... | IP address | IP payload |

... = APN of GGSN, used for routing through tunnel

6

# Packet transmission (3)

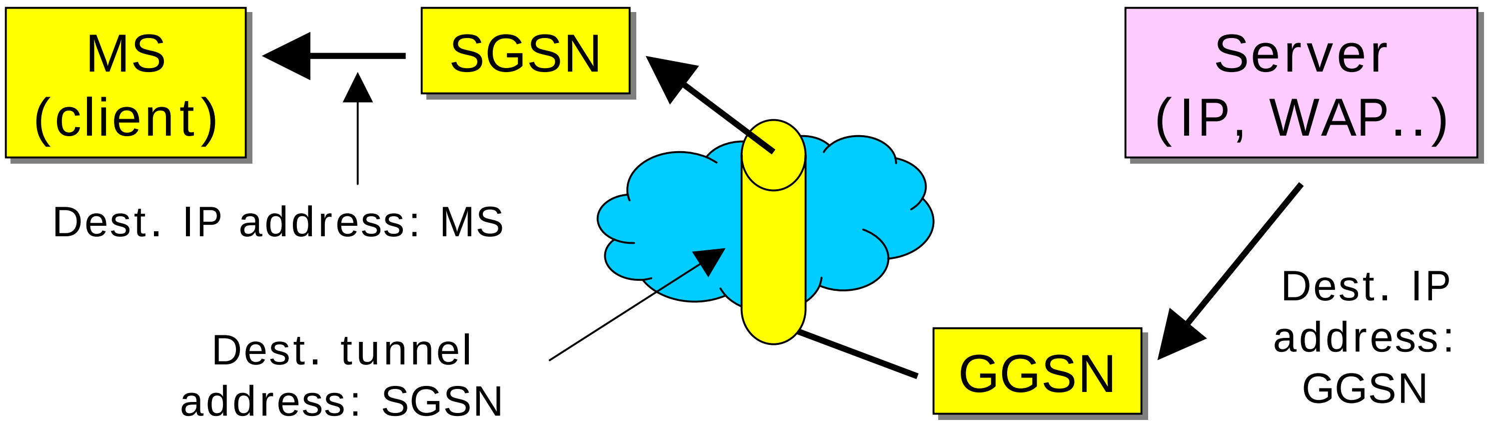



GGSN sends packet through external IP network (i.e. Internet) to the server.

| Source IP addr. | Dest. IP addr. | IP payload |
|---|---|---|
| GGSN | Server | |

6

# Packet transmission (4)




Server sends return packet via GGSN, GTP tunnel and SGSN to MS.

Packets from server to MS are always routed via GGSN (since this node has PDP context information).

# Further information on GSM/GPRS

**Books:**

Many good books available (GSM)

GPRS is more problematic ...

**Web link (GPRS basics):**

www.comsoc.org/livepubs/surveys/public/3q99issue/bettstetter.html