# MAP - Mobile Application Part

Mobility Management in GSM
GSM services

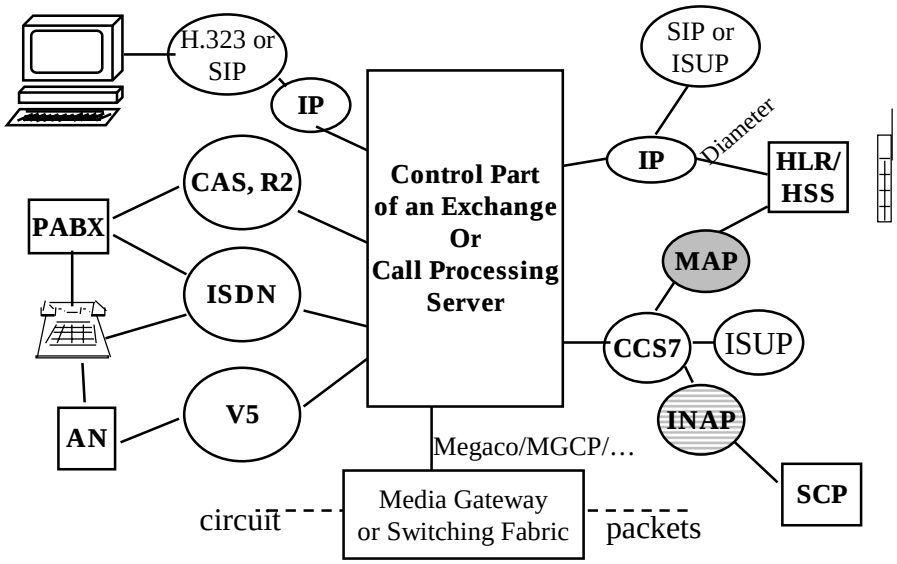
Short Message Service

Support of GPRS

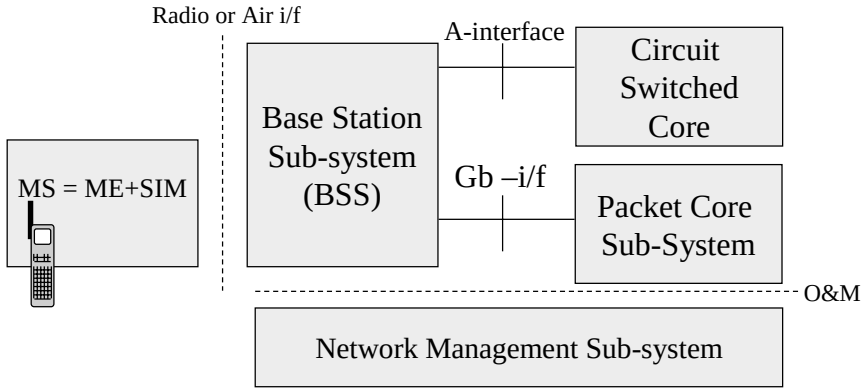
CAMEL = IN+GSM integration



# Summary of course scope



# GSM system consists of sub-systems




MS - Mobile Station
ME - Mobile Equipment
SIM - Subscriber Identity Module
BSS - Base Station Subsystem
HLR belongs to both CS and PS domains

Main differences cmp to wire-line networks
- air interface for the subscribers
- mobility and roaming of users

NB: the whole system is digital incl the ME.



# Mobility Management in General

Comparison of solutions for CS and PS networks

## Mobility requires logical subscriber numbers - are mapped dynamically to network topology bound routing numbers

- For most nodes it is enough to understand only the prefix of the routing number.
- Example: $10^9$ subscribers, number length = 13 digits

*Rough memory estimate for the analysis tree based on dialled digits (no separate routing nrs.*
*Tree is made of nodes of 64 octets. One node is used to analyse one dialled digit*

*Use of numbering space: on average 5 values in each position are used*

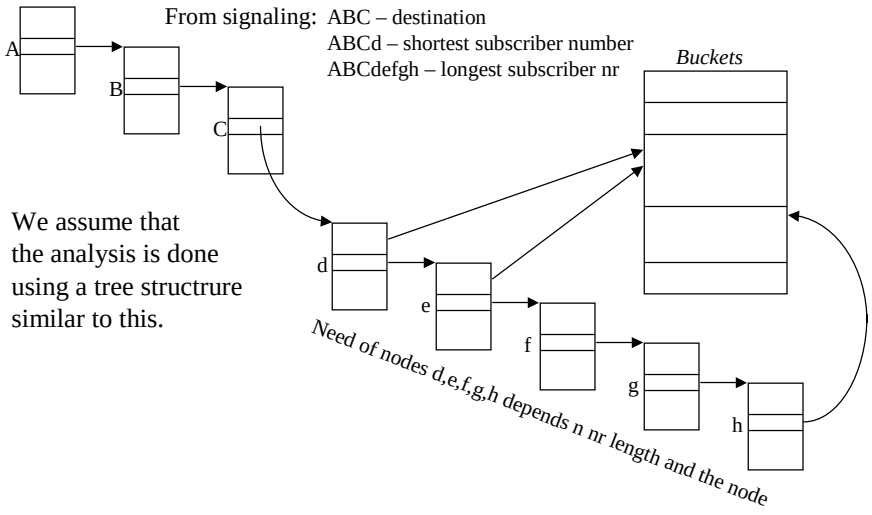
$m^{13} = 10^9 \Rightarrow 13 \lg m = 9 \Rightarrow m = 4.92$

Nrof nodes in the tree is (m is also the branching factor!)

$$1 + m + m^2 + \ldots m^{12} = \frac{m^{13} - 1}{m - 1} = 305 \text{ million}$$



## Analysis tree links signaling to routing



# Analysis tree calculus cont ...

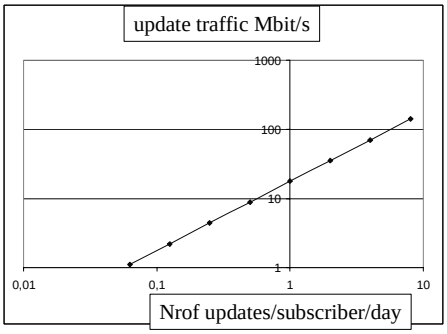
Memory requirement is 64 bytes * 305 * $10^6$ = 19 Gb

- Need to be available for any calls: replication will be expensive!
- A single read with full number requires 13 memory references, is not a problem
- Maintaining replicas is the problem:

Assumptions:
- an update takes a 50 bytes msg
- all updates in 6 hours

NB:
- updates/subscriber may need to be done significantly more often.

Problem needs to be partitioned!

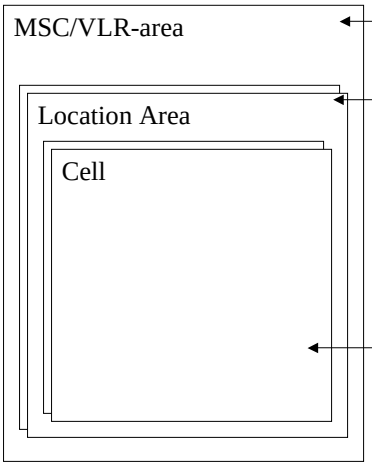





# In GSM the DB is partitioned by Operator and by Prefix of MSISDN nr

- An HLR the VLR of a few 100 000 subscribers
  - Operator code + prefix map to HLR
- Location area hierarchy decreases nrof updates
  - Not all location changes need be told to HLR
- MS-ISDN = “directory number” = what you dial is mapped to Mobile Subscriber Routing Number (MSRN) per call or per visit to another network

# Location Area Hierarchy in GSM reduces the need for HLR updates




HLR knows MSC/VLR

Visitor Location Register (VLR) knows
- = a set of cells
- update once/6 min….24h and when power switched o/off etc.
- update need to be authenticated

In case of GPRS the SGSN knows the Routing Area = a subset of Location area.

Final location is found by paging:
- call is sent to all cells in LA
- MS receives in favorite cell
- cell with best connectivity is chosen



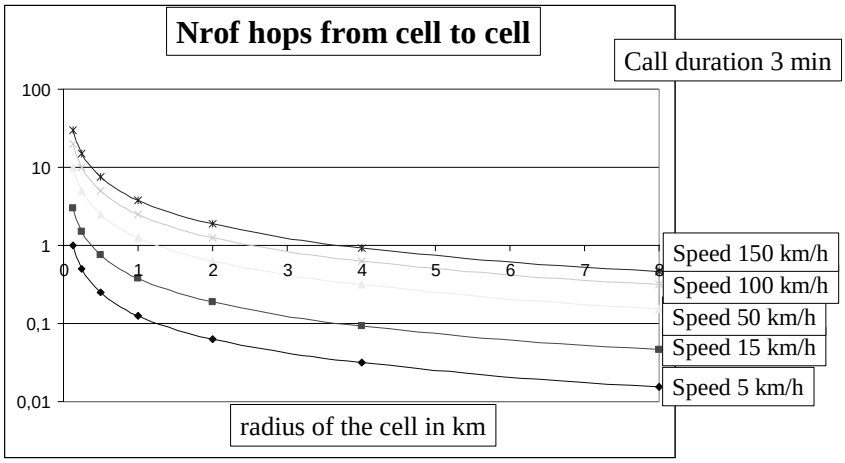
# Rough calculus of location update traffic in an HLR with 200 000 subs

- 200 000 subscribers
- 1 update/5min/subscriber
- Rough estimate: let one update = 100 octets

Traffic = 200 000 * 100 * 8/(5*60) = 0,53Mbit/s.

Can be transported on a single PCM-line (2 Mbit/s)!
-→ Makes sense, is clearly feasible.

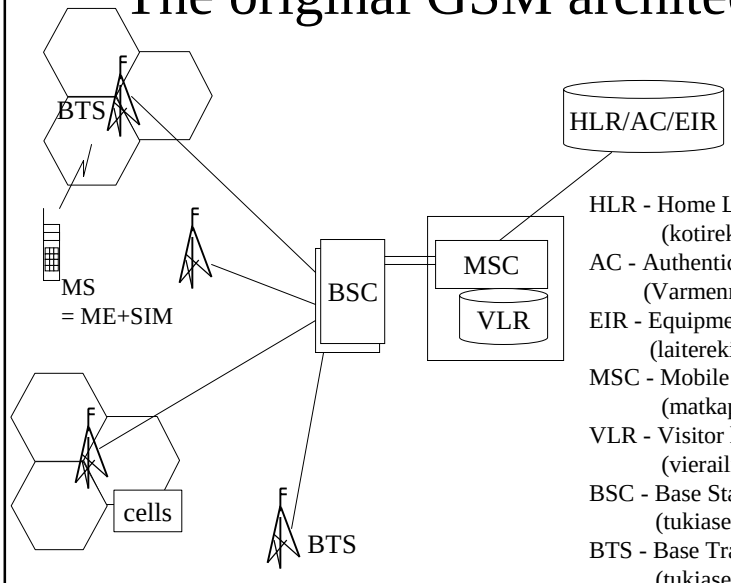
# Nrof probable hops from cell to cell during a telephone call




An architecture with less than one hop makes sense!

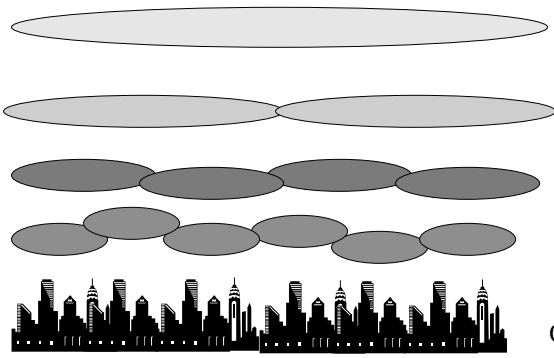


# The original GSM architecture




HLR - Home Location Register (kotirekisteri)
AC - Authentication Center (Varmennekeskus)
EIR - Equipment Identity Register (laiterekisteri)
MSC - Mobile Switching Center (matkapuhelinkeskus)
VLR - Visitor location Register (vierailijarekisteri)
BSC - Base Station Controller (tukiasemaohjain)
BTS - Base Transceiver Station (tukiasema)

# Multi-layer cell design increases radio network capacity




Cell selection tries to place fast moving MSs higher up in the hierarchy.



# What if subscriber numbers are binary?

- Example: $10^9$ subs, sub nr length is 128 bits

*Rough memory estimate for analysis: Analysis tree is made of node of 64 octets, each for analysing 4 bits.*

*Usage of hexa code points:*

$m^8 = 10^9 \Rightarrow 8 \lg m = 9 \Rightarrow m = 13.34$

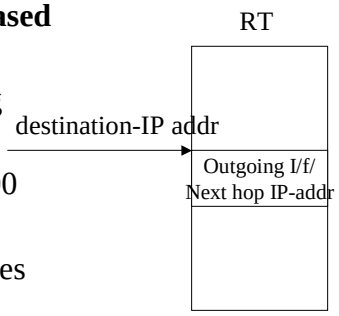
Nrof nodes in the tree is

$$1 + m + m^2 + \ldots m^7 = \frac{m^8 - 1}{m - 1} = 114 \text{ million}$$

⇨ *Result is of the same order of magnitude!*

# Background of mobility mgt for packet services terminals

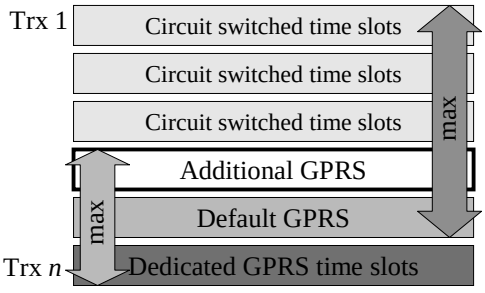
- **Packet forwarding/packet is based on routing tables.**
- Routers maintain RTs by routing protocols.
- Feasible size of the RT is 100 000 …300 000 entries =rows.
- Longest match search/packet takes many memory reads (<32).




- n x 100m users →provider addressing results feasible RT size
- search is based on address prefix not a full 32 bit address



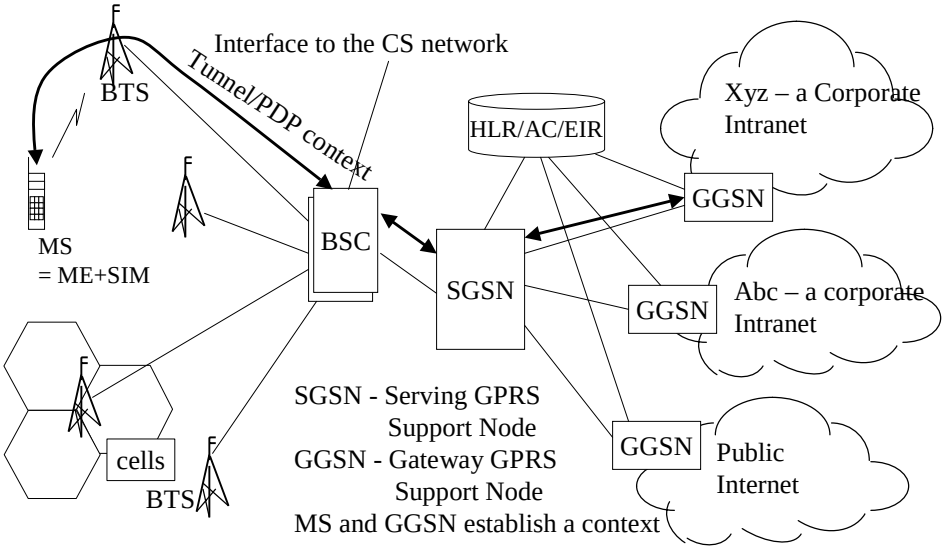
# GPRS shares TRX timeslots with CS services in GSM




Each trx has 8 time slots, classified to:
- purely CS (telephony) use
- purely PS use (optio)
- default packet traffic use (handovers may be used to keep these free of calls
-additional GPRS – may be used for packet traffic if there are no CS calls

By setting the parameters between PS/CS services appropriately an elastic boundary is created between GPRS and CS services – QoS, Revenues and network usage need to be optimised.

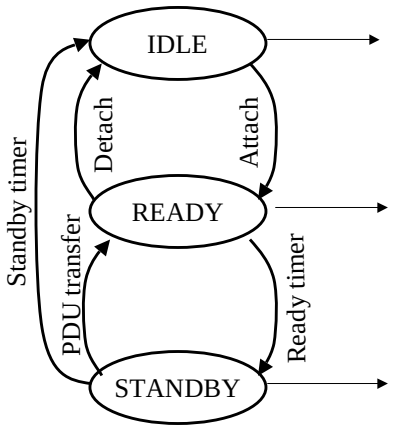
# SGSN takes care of mobility and GGSN is the interface node to other networks






# GPRS mobility management states/ MS in MS and in SGSN

this is a bit simplified




Mobility state model

Network does not follow MS location

User is active. Network follows the user with the accuracy of one cell

MS is online – but does not transfer packets. Network follows MS with the accuracy of a Routing Area:
cell < RA < location area. MS can be paged in the RA.

# Some GPRS key features

- GSM has two parallel MM systems: for CS and for PS serv
- GGSN allocates IP address for MS when MS needs it from the network GGSN is connected to.
  - GGSN = router from Internet and Intranet point of view
  - Several address allocation methods
- BSC-SGSN-GGSN (+HLR) network manages mobility using topology bound internal IP-addresses.
- In the tunnel MS - GGSN we have two IP networks on top of each other:
  - IP-based transport network: has its own DNS
  - and the “payload” network seen by users and applications.
  - Header overhead is high ( >100 octets)



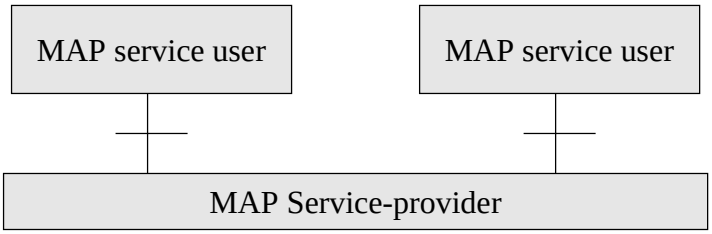
# Summary

- Two different MM solutions: one for CS one for PS services
  - CS solution is centralised: GMSC always asks HLR where the MS is located
- It is not feasible for ask per packet the location of the MS.
  - MM must be either adaptive or distributed.
  - Makes sense to limit paging to a smaller nrof cells

# MAP



# MAP works between MAP Service Users and MAP Service Providers



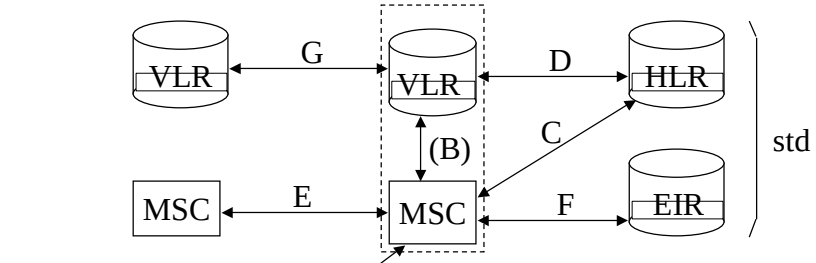

- MAP SUs and MAP SPs are network functions such as HLR, MSC etc

# MAP is used by many network elements

| | |
|---|---|
| EIR | Equipment Identity Register - usually integrated with HLR |
| GCR | Group Call Register |
| GGSN | Gateway GPRS Support Node - for interfacing to IP or other PD networks |
| GMLC | Gateway Mobile Location Center - for interfacing to Location Services |
| GMSC | Gateway MSC - for routing calls from visited network |
| gsmSCF | GSM Service Control Function - IN service control element |
| HLR | Home Location Register - the key database |
| MSC | Mobile services Switching Center |
| NPLR | Number Portability Location Center - for locating an HLR |
| SGSN | Serving GPRS Support Node - the "MSC/VLR" for PS services |
| SIWFS | Shared Interworking Function Server - for interfacing CS data services to IP or other PD networks |
| SMS GWMSC | SMS Gateway MSC - for terminating SMS routing |
| SMS IWMSC | SMS Interworking MSC - for originating SMS routing |
| USSDC | USSD Center - part of gsmSCF |
| VBS/VGCS Anchor MSC | Voice broadcast/group call service Anchor MSC - specified/not implemented |
| VBS/VGCS Relay MSC | Voice broadcast/group call service relay MSC - specified/not implemented |
| VLR | Visitor Location Register -in practice integrated with MSC |
| VMSC | Visited MSC |



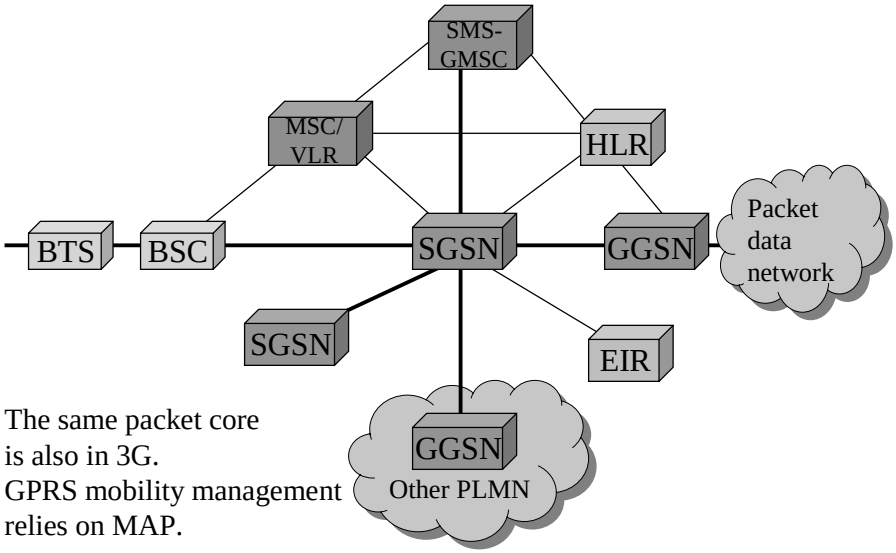
# CS Core interfaces are




MSC - Mobile Switching Center
HLR - Home Location Register
VLR - Visitor Location Register
EIR - Equipment Identity Register
NB: MSC+VLR always in the same node
+I - interface: MS - HLR (MS-MSC/VLR-HLR)

*All CS Core interfaces: B-G conform to the MAP protocol*

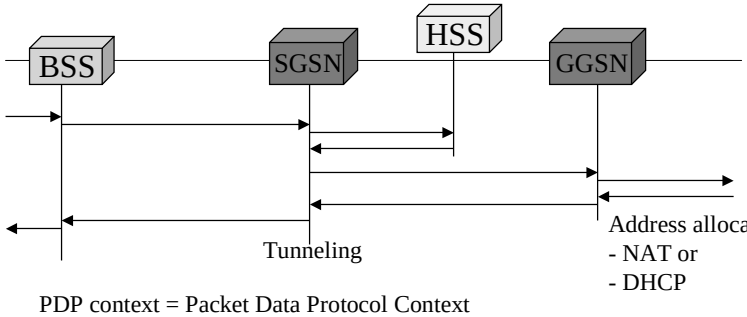
# GSM/GPRS Core Network




The same packet core is also in 3G.
GPRS mobility management relies on MAP.

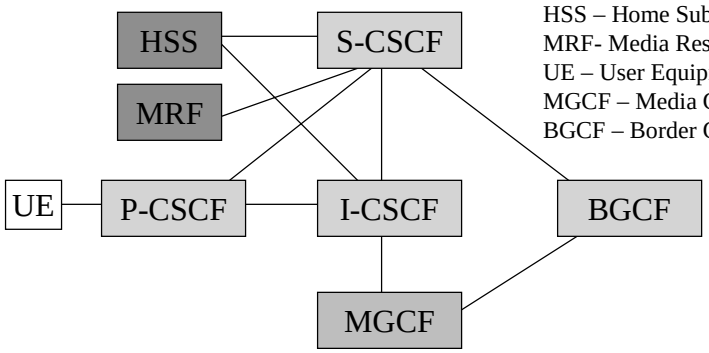


# To get on-line a GPRS device need to create a PDP Context




PDP context = Packet Data Protocol Context
- PDP = IP or X.25
- SGSN requests HSS for access authorization and to find the GGSN based on the so called APN name. An MS can be connected to several IP-networks thru different GGSNs.
- The GGSN allocates an IP address from the IP-network it is connected to. Result is that the MS has an IP address that it can use to communicate using the Internet Protocol. We say that a PDP context has been created.

# IP Multimedia System in 3G

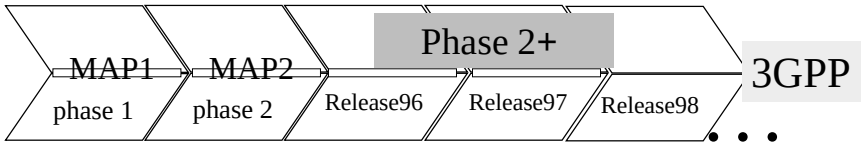



HSS – Home Subscriber Server
MRF- Media Resource Function
UE – User Equipment
MGCF – Media Gateway Control
BGCF – Border Gateway Control

- MM subsystem works on top of the packet core.
- CSCF – Call Session Control Function processes signaling and controls the MM services.



# Milestones in MAP development




- In phase 2+ … versioning is per operation package.
- This supports the idea of deploying small sets of features at a time in the network.
- If the remote systems does not understand the newest tricks, *fall-back negotiation* restores operation on the level of the previous version.
- Release98 3GPP TS 09.02 V7.11.0 in www.3gpp.org (03-2002), ETSI →3GPP
- Later releases have small improvements (not discussed here)
  - Release99: 3GPP TS 29.002 V3.15.0 (2002-12),
  - Release 4: 3GPP TS 29.002 V4.10.0 (2002-12), Release 5, jne…

# MAP -operations can be mapped to interfaces

| I/f | Elements | Mobility management | O&M | Call handling | Supple-mentary services | Short messages | Sum |
|---|---|---|---|---|---|---|---|
| B | MSC - VLR | 12 | 1 | 4 | 1 | 2 | 20 |
| C | GMSC - HLR | | | 1 | | | 1 |
| D | VLR - HLR | 9 | 3 | 1 | 10 | 1 | 24 |
| E | MSC - MSC | 5 | | | | | 5 |
| F | MSC - EIR | 1 | | | | | 1 |
| G | VLR - VLR | 1 | | | | 1 | 2 |
| | HLR - SMSGW | | | | | 3 | 3 |
| | MSC - SMSGW | | | | | 1 | 1 |
| Sum | | 28 | 4 | 6 | 11 | 8 | 57 |

*The table corresponds to MAPv2*



# MAP -operations in Release98/ETSI/3GPP

| i/f | Elements | Mobility Manage-ment | O&M | Call Handling | Supple-mentary Services | Short Messages | PDP Context | Location Services | Sum |
|---|---|---|---|---|---|---|---|---|---|
| B | MSC - VLR | 14 | 2 | | 13 | 3 | | | **32** |
| C | GMSC - HLR | | | 1 | | 2 | | | **3** |
| D | HLR - VLR | 9 | 2 | 4 | 12 | 1 | | | **28** |
| E | MSC - MSC | 5 | | 1 | | | | | **6** |
| F | MSC - EIR | 1 | | | | | | | **1** |
| G | VLR - VLR | 1 | | | | | | | **1** |
| J | HLR- gsmSCF | 1 | | | 3 | | | | **4** |
| L | MSC - gsmSCF | | | | 1 | | | | **1** |
| C | SMSGW - HLR | | | | | 2 | | | **2** |
| | MSC - SMSGW | | | | | 2 | | | **2** |
| | VBS/VGCS Anchor MSC - VBS/VGCS Relay MSC | | | 4 | | | | | **4** |
| I | VBS/VGCS aMSC - GCR | Vendor specific | | | | | | | **0** |
| K | vMSC - SIWFS | | | 2 | | | | | **2** |
| Gr | SGSN - HLR | 6 | | | | | | | **6** |
| Gc | GGSN - HLR | | | | | | 3 | | **3** |
| Gd | SGSN - SMSGW | | | | | 2 | | | **2** |
| Gf | SGSN - EIR | 1 | | | | | | | **1** |
| Gb | SGSN - BSS | Not discussed on this course - not a MAP interface | | | | | | | **0** |
| Gs | SGSN - MSC/VLR | optional - not a MAP interface | | | | | | | **0** |
| | GMSC - NPLR | | | 1 | | | | | **1** |
| Lh | GMLC - HLR | | | | | | | 1 | **1** |
| Lg | GMLC - MSC | | | | | | | 2 | **2** |
| | **use cases** | **38** | **4** | **13** | **29** | **12** | **3** | **3** | **102** |

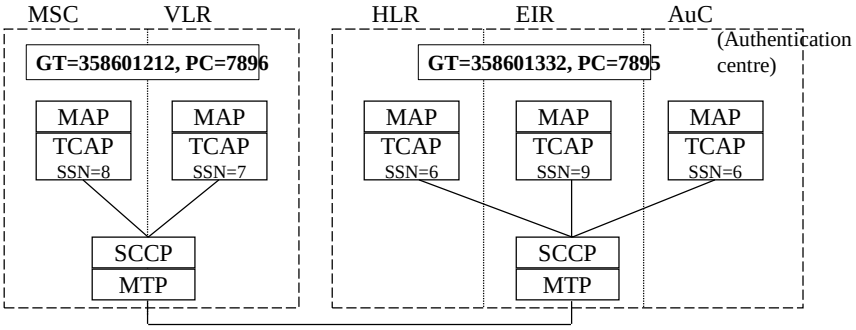
*The table corresponds to MAPv2+ Release98 (3GPP) This lecture does not discuss MSC-VLR interface operations nor O&M –operations, nor location services, nor Group Calls.*

# Upgrade from MAP -1997

- NB:
  - a service may be confirmed or non-confirmed in the previous tables
  - a service can appear on several rows – e.g. for many services VLR is the relay point between HLR and MSC
  - The table gives a feeling of what is MAP used for. (I believe the service use case count is 98% accurate)
- SGSN reuses most of the HLR to VLR services
- New services: Location Services, GPRS, IN, New Supplemetary Services, Group Calling
  - added complexity
  - the spec is approximately 1100 pages...



# Addressing MAP messages




GT formats:

| | | | | | | |
|---|---|---|---|---|---|---|
| IMSI | MCC | + | MNC | + | MSIN |
| MSISDN | CC | + | NDC | + | SN |
| Hybrid | CC | + | NDC | + | MSIN |

**GT - Global Title**
**PC - Point Code**
**MCC - Mobile Country Code**
**CC - Country Code**
**MNC - Mobile Network Code**
**NDC - National Destination Code**
**MSIN - Mobile Subscriber Identity Number**
**SN - Subscriber Number**

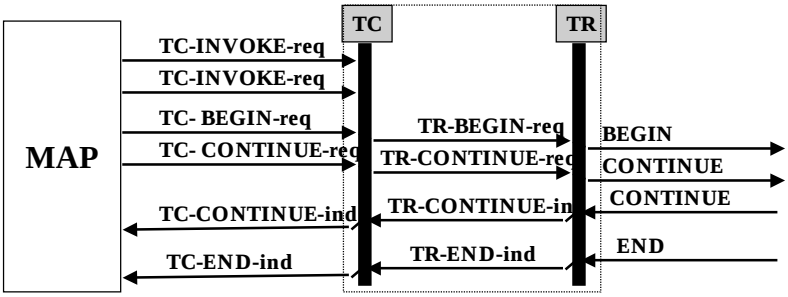
# Common MAP services

| | |
|---|---|
| • MAP-OPEN service<br>• MAP-CLOSE service | • For establishing and clearing MAP dialogues btw peer-MAP service users |
| • MAP-DELIMETER service | • access to functions below the application layer |
| • MAP-U-ABORT service<br>• MAP-P-ABORT service | • for reporting abnormal situations |
| • MAP-NOTICE service | • Notification from the Provider not affecting state of the dialogue |

These are used by the application on top of MAP.



# MAP uses the structured dialogue provided by TCAP



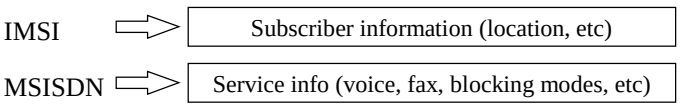

- **Begin causes a *transaction identifier* to be reserved.**
- **The remote system can either continue the transaction or close it.**
- **Continue - messages are exchanged in a full-duplex mode.**
- **Closing options:**
  - **based on pre-arrangement independently**
  - **normally by the End-message or "abnormally" by an Abort message**

# Mobility management is the most important feature in MAP

- Location management
- Handover MSC-MSC during a call
  - handover is supported on many levels - also BSSAP (A- i/f protocol) is needed, but we do not cover that here
- Authentication and security
- IMEI - mobile equipment id queries
- Subscriber management
- Fault recovery



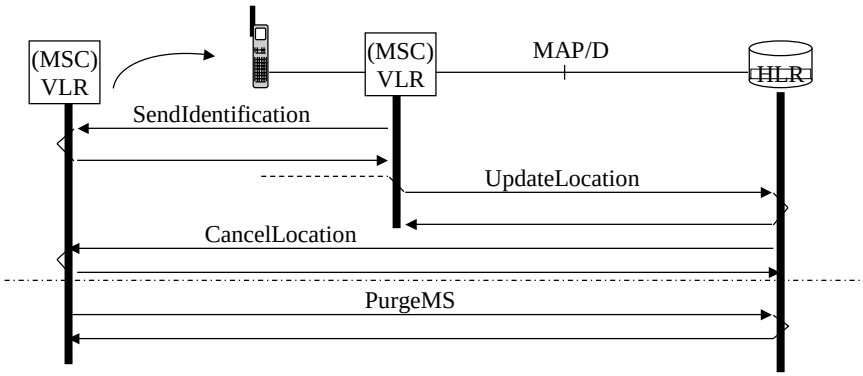
# Home Location Register - HLR - contains subscriber and service information




In a mobile terminated call, the right HLR can be found based on a *prefix in MSISDN* or if *free numbering within the operator network* is supported, a Global Title (MSISDN is embedded in the GT in SCCP) translation needs to be done first e.g. in a specific network element.

Release98 HLR database has
- location information (VLR number)
- basic telecommunications services subscription information
- service restrictions (e.g. roaming limitations)
- supplementary service parameters
- GPRS subscription data and routeing information

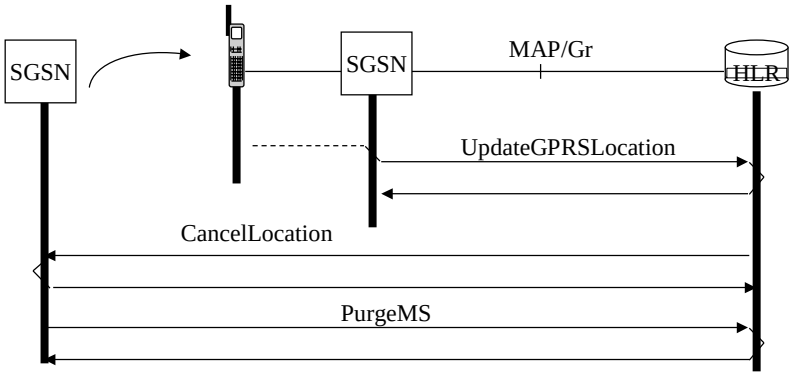
# Location management maintains the location of the MSs in the HLR




- **SendIdentification requests MS info (IMSI, authentication) from the previous VLR.**
- **UpdateLocation updates the new location with the accuracy of a VLR area**
- **With PurgeMS VLR tells to HLR that MS is unreachable (independent of the previous sequence).**

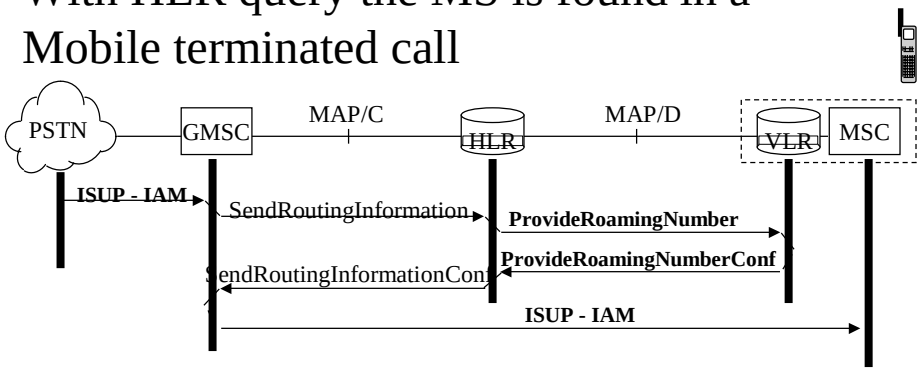


# Location management maintains the location of the GPRS MSs in the SGSN and HLR




- **SendIdentification requests MS info (IMSI, authentication) from the previous SGSN.**
- **UpdateLocation updates the new location with the accuracy of a SGSN area**
- **With PurgeMS (old) SGSN tells to HLR that MS is unreachable.**

# With HLR query the MS is found in a Mobile terminated call

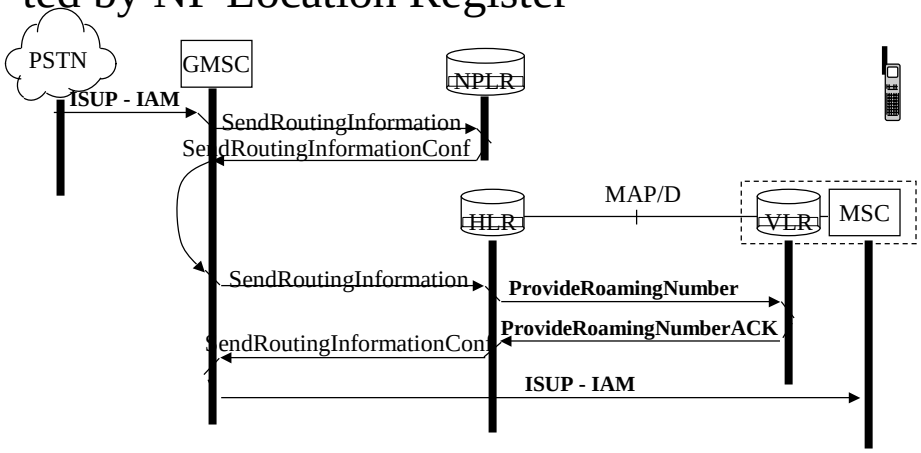



MSRN - Mobile Subscriber Roaming Number

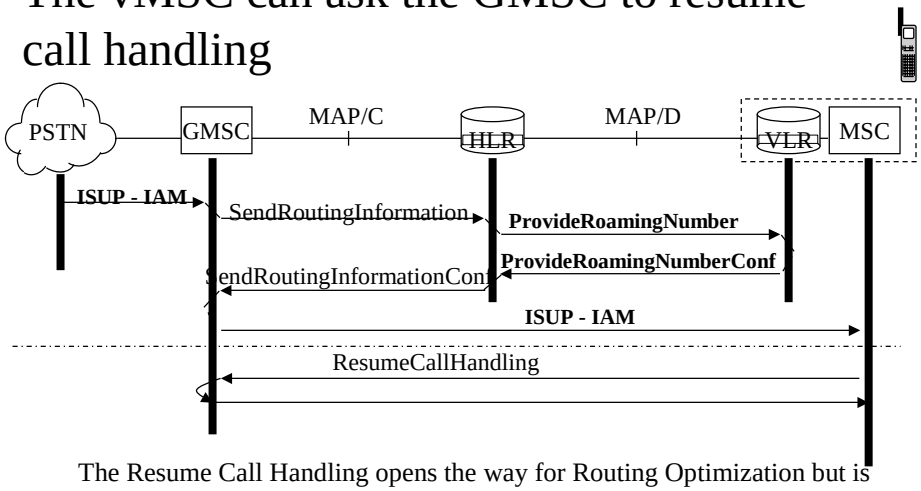
- conforms to E.164 format (any exchange can pass along the number)
- each MSC has a limited range of MSRNs
- MSRN has a validity timeout
- MSRN may be allocated on a call be call basis or for the duration of the visit



# GSM Number Portability can be implemented by NP Location Register



# The vMSC can ask the GMSC to resume call handling

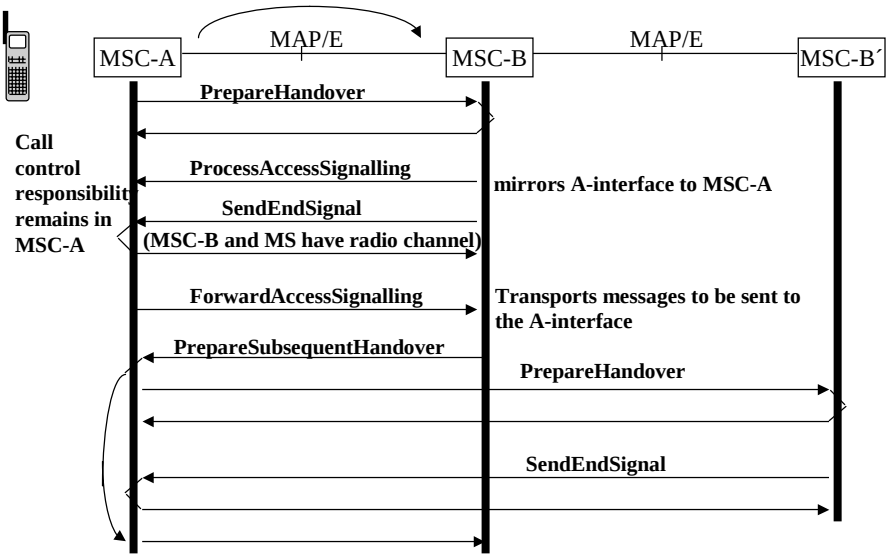



The Resume Call Handling opens the way for Routing Optimization but is not used:

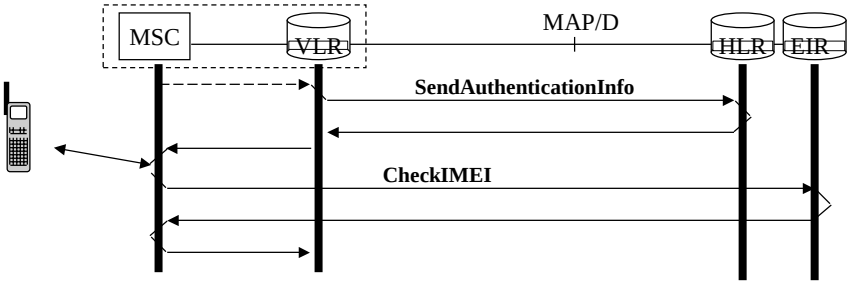
- calls are normally always routed through the Home Network due to charging reasons.



# Handover from MSC to MSC



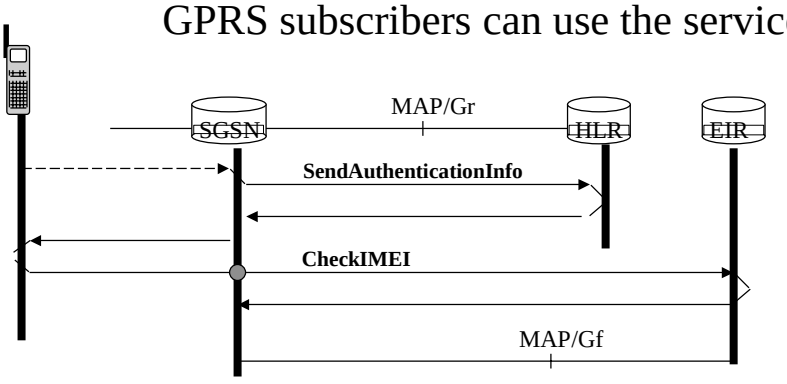
# Security operations ensure that only authorized subscribers can use the service




Black list of suspect stolen phones ensures that stolen equipment can not be used for long

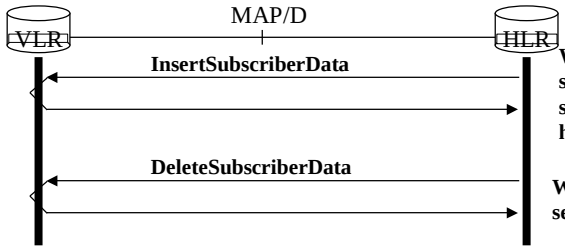


# Security operations ensure that only authorized GPRS subscribers can use the service




If SGSN does not have the IMEI, it asks it from the MS.
After authentication a PDP context is ready for packet transfer.

# Subscriber management takes care of the subscriber data in the VLR



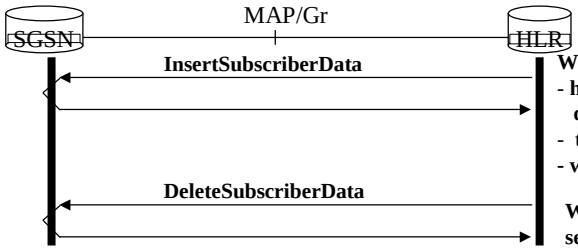

**When the operator or the subscriber have changed any of subscriber data. When location has been updated.**

**When a basic or a supplementary service is cancelled.**

***With these operations all information residing in the VLR, can be manipulated, when the HLR has the master copy of the information. (HLR does not have some detailed location info…)***



# Subscriber management takes care of the subscriber data in the SGSN



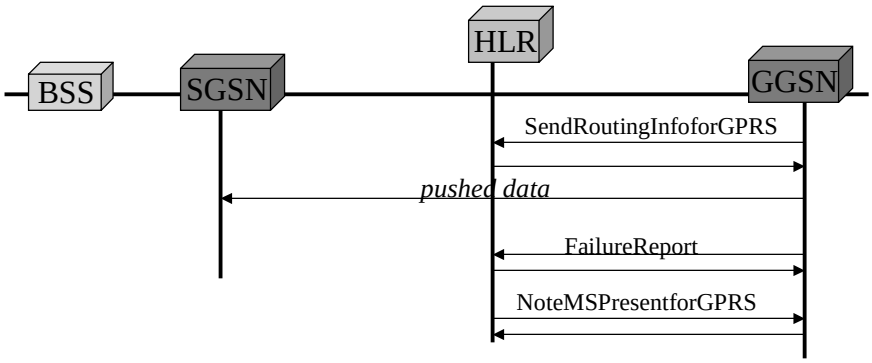

**When the operator or the subscriber**
**- have changed any of subscriber data (e.g. barring).**
**- the mode has changed**
**- when location is updated.**

**When a basic or a supplementary service is cancelled.**

***With these operations all information residing in the SGSN, can be manipulated, when the HLR has the master copy of the information. (HLR does not have some detailed location info…)***

There are 3 types of MS: (a) simultaneous CS + PS services,
(b) Alternate CS/PS services and (c) GPRS only. Type b has two modes.

# Network Requested PDP Context Activation facilitates data push




PDP context is Packet Data Protocol Context, includes a ”virtual connection” from MS to GGSN in an IP-tunnel.



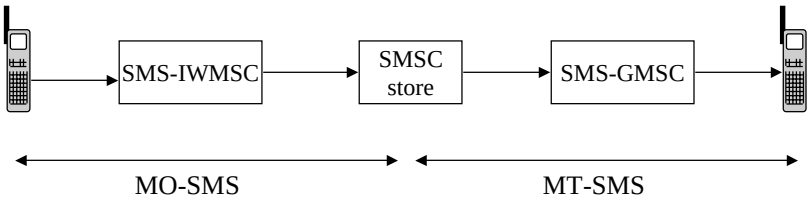
# Supplementary service operations are passed from MS via MSC/VLR to HLR

MS --> MSC/VLR --> HLR

| | |
|---|---|
| RegisterSS | Activation of call forwarding |
| EraseSS | Switching off supplementary services |
| ActivateSS | Activation of call blocking |
| DeactivateSS | Deactivation of supplementary services |
| InterrogateSS | Interrogation of supplementary service settings |
| RegisterPassword | Password setting for SS |

| | |
|---|---|
| GetPassword | Password query to MS |
| USSD operations | Unstructured SS data transport |

# Short Message Service



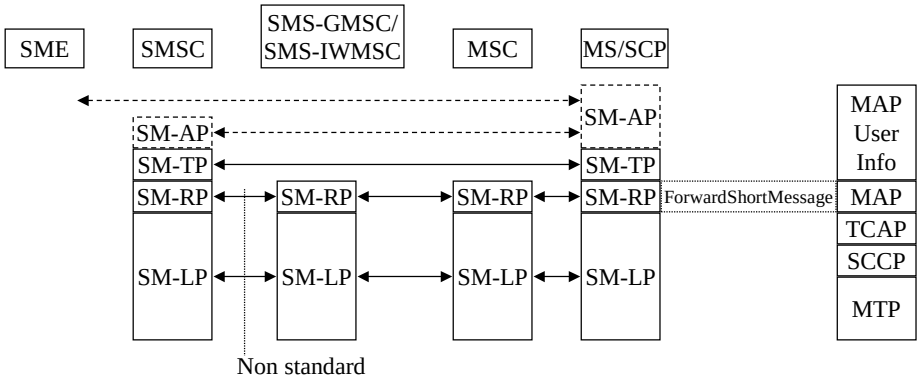

SMSC - Short Message Service Center (or SC - Service Center)
SMS-GMSC - Short message Gateway MSC, issuer of routing information query to HLR in MT-SMS
SMS-IWMSC - Short message Inter-working MSC, routing MSC in MO-SMS service
SMS-GW = SMS-IWMSC + SMS-GMSC

MO - Mobile Originated
MT - Mobile Terminated

SMSC - HLR operations:
- MS short message buffer full
- MS reachability
- successful delivery of message

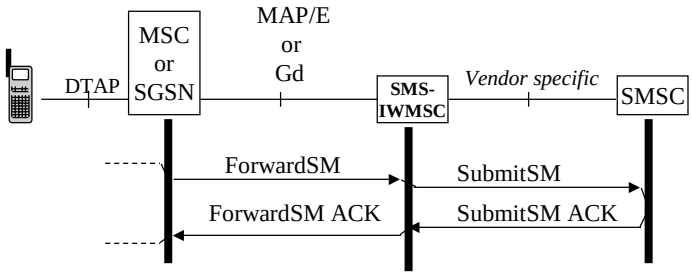


# Short message transport protocol stack




SME - Short Message Entity
SM-LP - Short Message Link Protocol
SM-RP - Short Message Relay Protocol
SM-TP - Short Message Transfer Protocol
SM-AP - Short Message Application Protocol

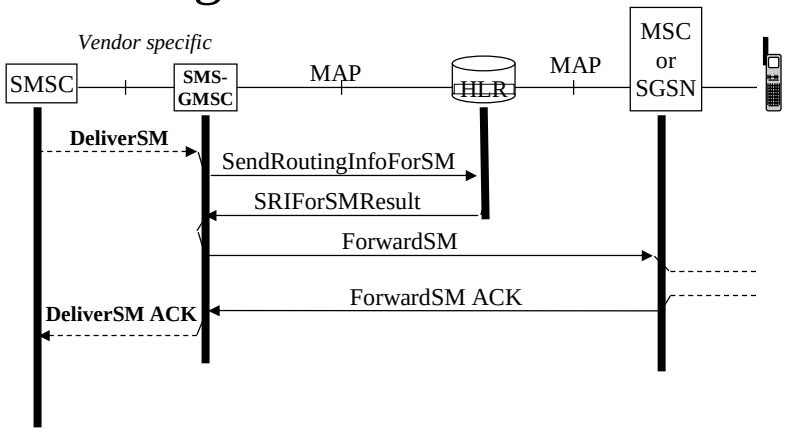
# Messages in MO-SMS service




Traditionally serving MSC send short messages to the SMS Interworking MSC. Alternatively, GPRS side can do the same: SGSN sends SMS instead of sMSC.

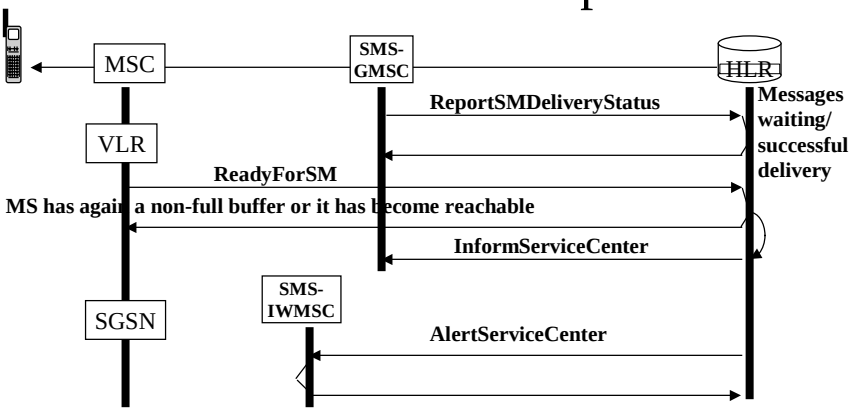


# Messages in MT-SMS service




The SMS can be delivered either by a serving MSC or the SGSN thru GPRS servce.

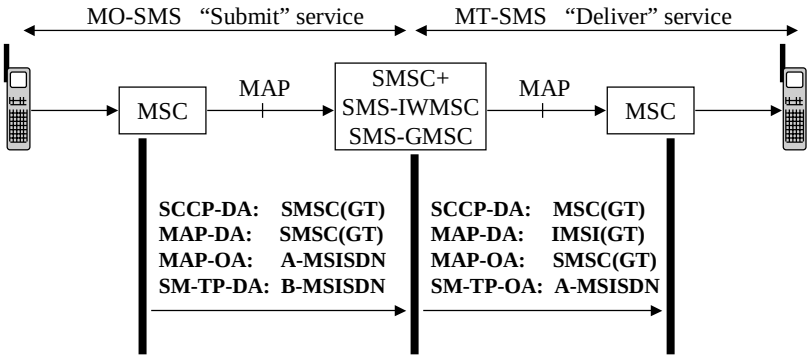
# Status information is kept in HLR




- **SM destination subscriber can tell the network, that its SM buffer is full or that the subscriber has become unreachable. HLR stores the status.**
- **When Status is good for receiving, VLR or SGSN gets the info and sends it to HLR.**
- **HLR informs those SMSCs that have reported themselves onto the waiting list.**



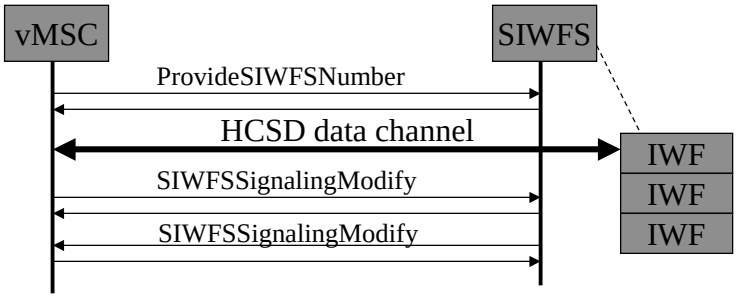
# Addressing of Short messages




SMSC gets the IMSI of the B subscriber and the address of the VMSC by SRIForSM operation from the HLR.

NB: Addresses are on three protocol layers!

# Shared IWF Server provides access to a PDN for CS data services

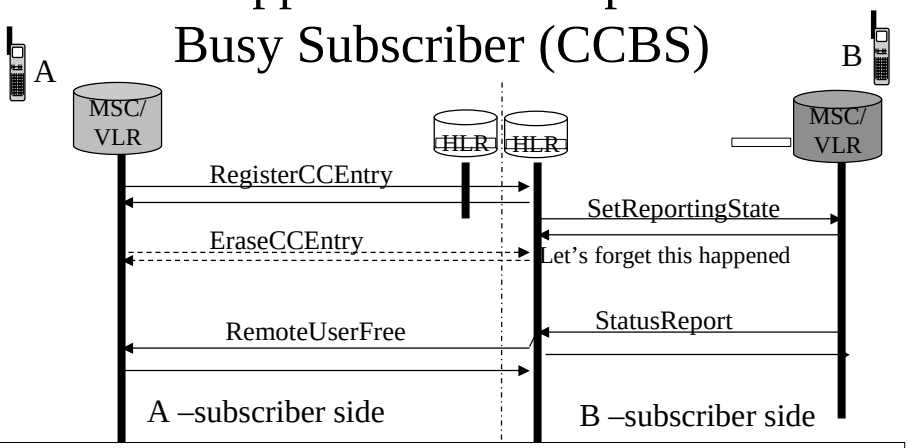



Signaling modify can e.g. modify number of time slots used for HSCSD

Compare this to what MGCP does!



# GSM supports Call Completion to Busy Subscriber (CCBS)




A calls, when B is busy, A registers that he/she wants to know when B becomes free. HLR sets the reporting state to B's VLR. When B becomes free, new status is reported to HLR. HLR tells A's VLR/MSC that B is now free and call can be completed so that A pays normally. There is a CCBS protocol (HLR-HLR) also …

## USSD - Unstructured Supplementary Service Data transports SS data between MS and the network

- Network destinations can be e.g.
  - MSC, VLR, HLR
  - HLR-> SCP, WWW-server
- Data is in “ascii”(cmp DTMF)
- E.g. WAP - Wireless Application Protocol can in principle use the USSD service
- a latecomer among features

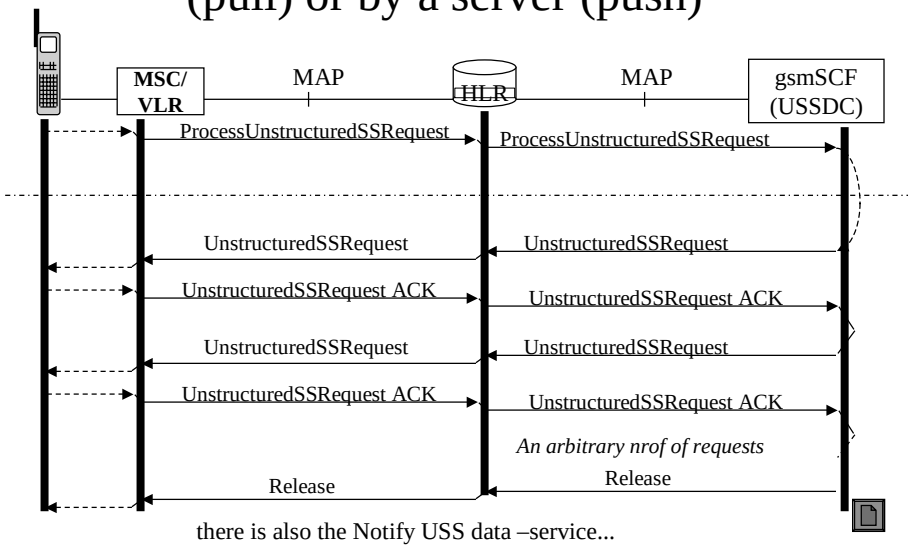


## USSD uses the structured dialogue of TCAP

- Dialogue is connection oriented
- A Dialogue has an identity
- Are independent of calls
- Message length is 80 octets, having max 91 Ascii characters a´ 7-bits


DCS - Data Coding Scheme

# USSD dialogue can be initiated by MS (pull) or by a server (push)



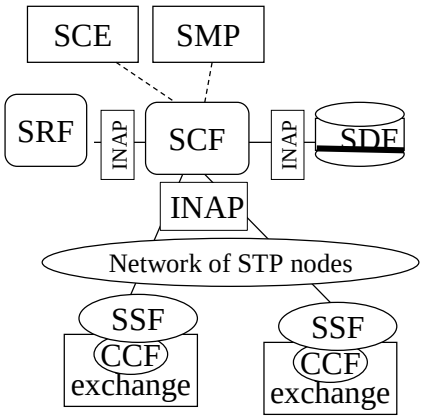

there is also the Notify USS data –service...



# CAMEL adapts the IN technology to GSM

- CAMEL - Customized Application for Mobile network Enhanced Logic
- The goal is the capability of providing the home network services to visiting subscribers
- CAP - CAMEL Application Part is a subset of ETSI CoreINAP
  - phases (Capability Sets) 1 and 2 are ready

# IN is a way of implementing services in nodes separate from exchanges



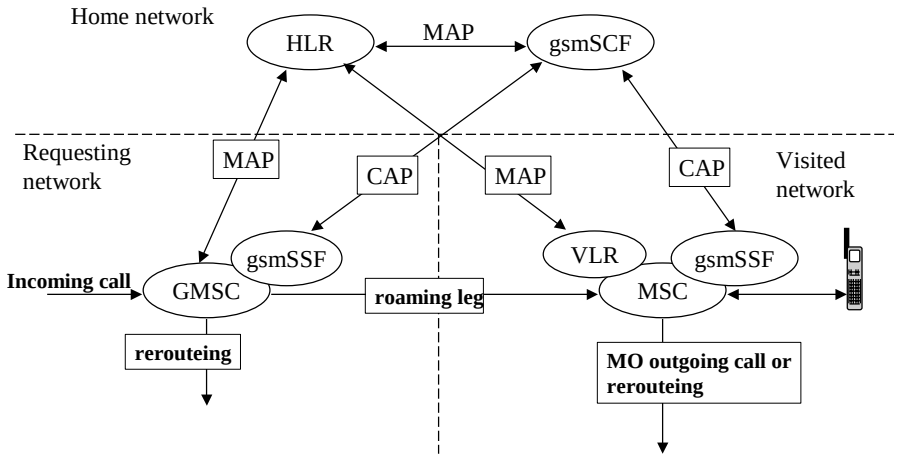

INAP = IN Application Part
= main protocol
SSF - Service Switching Function
maintains call state with CCF
SCF - Service Control Function
implements service logic
SRF - Special Resource Function
processes in-band signals
SDF - Service Data Function
is a database
SCE - Service Creation Environment
for creating new service logic
SMP - Service Management Point
implements mgt functions



# Features of the IN architecture ...

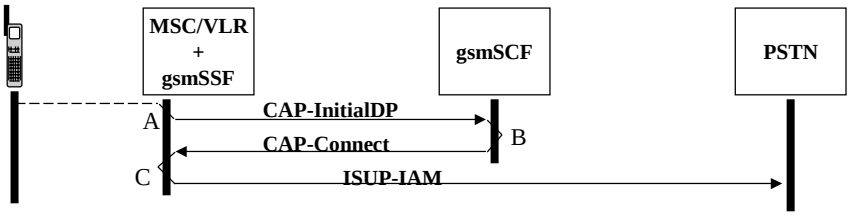
- BCSM - Basic Call State Model is a standardized state machine in SSP - couples/ de-couples IN service logic from connection resources
- BCSM states (detection points) can be programmed to trigger queries on conditions to an SCF concerning a certain call
- BCSM architectural issue is that a call is also a service and therefore the architecture is service dependent
- INAP messages are independent of voice channel connections

# Phase 1 CAMEL architecture






# MS originated CAMEL call

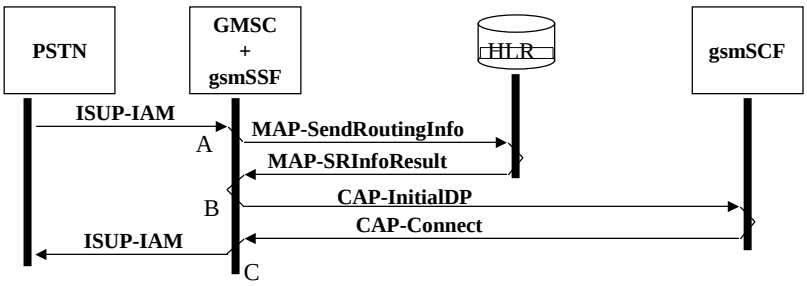



A - MSC gets the CAMEL service info from the VLR concerning the A subscriber, sees an active CAMEL service and hands the call to gsmSSF. gsmSSF queries gsmSCF:lle (service key, A-nr, B-nr, IMSI, location...

B - gsmSCF can for example do a number translation

C - MSC sets up a call using the received info

# Mobile terminated CAMEL call



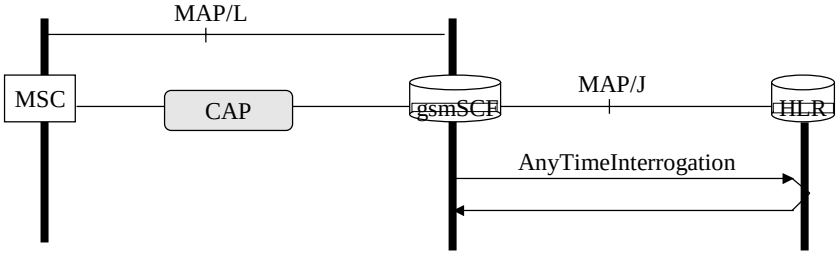

A - GMSC queries HLR of the location of the MS. HLR sends the terminating CAMEL service data of the subscriber.

B - GMSC hands the call to gsmSSF, which queries gsmSCF gsmSCF returns C-number that is used for routeing the call

C - GMSC sets up the call to C-number. If needed, GMSC can first do a new HLR query.



# An SCF can interrogate HLR at any time




This is a MAP98 (of 2002) feature.
See also slide nr 59:

# IN+GSM integration based on CAMEL is a step towards 3G

- CAPv1 supports only 7 operations
- CAPv1 call model has only a few triggering points (TDP - trigger detection point)
- CAPv2 has 22 operations
- Still no triggering for Short Messages
- CAMEL compatible equipment is in use in many networks



# MAP summary

- MAP has been introduced in several phases and releases.
- Provides a working solution to mobility including smooth handovers for CS services.
- Supports mobility for packet services (simplified handover) for GPRS Core.
- Is heavy on features.
- Future: MAP over IP? MAPSec (Release 4)?