MAP - Mobile Application Part

Mobility Management in GSM
GSM services
Short Message Service
CAMEL = IN+GSM integration

Course scope - lecture scope
GSM system consists of 4 sub-systems

- Base Station Sub-system (BSS)
- Network Sub-System (NSS)
- Network Management Sub-system
- MS = ME + SIM

Main differences compared to wire-line networks:
- Air interface for the subscribers
- Mobility and roaming of users
- NB: The whole system is digital including the ME.

NSS interfaces are:

- VLR - Visitor Location Register
- MSC - Mobile Switching Center
- HLR - Home Location Register
- EIR - Equipment Identity Register

All NSS interfaces: B-H conform to the MAP protocol

MSC+VLR always in the same node
+H-interface: MSC - SMS Gateway interface
+I-interface: MS - HLR (MS-MSC/VLR-HLR)

NB: MSC+VLR always in the same node
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, *fallback negotiation* restores operation on the level of the previous version.

MAP -operations can be mapped to interfaces

<table>
<thead>
<tr>
<th>ID</th>
<th>Elements</th>
<th>Mobility management</th>
<th>O&amp;M Call handling</th>
<th>Supplementary services</th>
<th>Short messages</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>MSC - VLR</td>
<td>12</td>
<td>4</td>
<td>2</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>GMSC - HLR</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>VLR - HLR</td>
<td>9</td>
<td>3</td>
<td>10</td>
<td>1</td>
<td>24</td>
</tr>
<tr>
<td>E</td>
<td>MSC - MSC</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>F</td>
<td>MSC - EIR</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>G</td>
<td>VLR - VLR</td>
<td>1</td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HLR - SMSGW</td>
<td></td>
<td></td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MSC - SMSGW</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Sum</td>
<td></td>
<td>26</td>
<td>4</td>
<td>11</td>
<td>8</td>
<td>57</td>
</tr>
</tbody>
</table>

The table corresponds to MAPv2

*This lecture does not discuss MSC-VLR interface operations nor O&M -operations.*
Addressing MAP messages

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

<table>
<thead>
<tr>
<th>IMSI</th>
<th>Subscriber information (location, etc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSISDN</td>
<td>Service info (voice, fax, blocking modes, etc)</td>
</tr>
</tbody>
</table>

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.
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.

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 MSRN
- MSRN has a validity timeout
- MSRN may be allocated on a call be call basis or for the duration of the visit
Handover from MSC to MSC

Call control responsibility remains in MSC-A

PrepareHandover

ProcessAccessSignalling

SendEndSignal

(MSC-B and MS have radio channel)

ForwardAccessSignalling

PrepareSubsequentHandover

Transports messages to be sent to the A-interface

PrepareHandover

SendEndSignal

Security operations ensure that only authorized subscribers can use the service

SendAuthenticationInfo

CheckIMEI

Black list of suspect stolen phones ensures that stolen equipment can not be used for long
Subscriber management takes care of the subscriber data

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…)

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

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RegisterSS</td>
<td>Activation of call forwarding</td>
</tr>
<tr>
<td>EraseSS</td>
<td>Switching off supplementary services</td>
</tr>
<tr>
<td>ActivateSS</td>
<td>Activation of call blocking</td>
</tr>
<tr>
<td>DeactivateSS</td>
<td>Deactivation of supplementary services</td>
</tr>
<tr>
<td>InterrogateSS</td>
<td>Interrogation of supplementary service settings</td>
</tr>
<tr>
<td>RegisterPassword</td>
<td>Password setting for SS</td>
</tr>
<tr>
<td>GetPassword</td>
<td>Password query to MS</td>
</tr>
<tr>
<td>USSD operations</td>
<td>Unstructured SS data transport</td>
</tr>
</tbody>
</table>
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
USSD dialogue can be initiated by MS (pull) or by a server (push)

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
Messages in MT-SMS service

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 gets the info and sends it to HLR.
- HLR informs those SMSCs that have reported themselves onto the waiting list.
Addressing of Short messages

MO-SMS “Submit” service  —  MT-SMS “Deliver” service

SMSC  —  SMS-IWMSC
SMS-GMSC  —  MSC

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!

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 on conditions queries 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**

- **Home network**
  - HLR
  - MAP
  - gsmSCF

- **Requesting network**
  - MAP
  - CAP
  - MAP
  - gsmSSF

- **Visited network**
  - VLR
  - gsmSSF
  - MSC

**Incoming call**
- GMSC
- roteing

**MS originated CAMEL call**

- MSC/VLR + gsmSSF
- gsmSCF
- PSTN

**Steps:**

**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.

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