**Mobility Management**

Mobility management operations can be divided into the following categories:

* Location Management
* Paging and Search
* Access Management
* Handover
* Authentication Management
* Security Management
* IMEI Management
* Subscriber Management
* Identity Management
* Fault Recovery

The following section examines the MAP operations that are used in each of these categories, excluding Paging and Search, Access Management, Security Management and Identity Management because these categories were removed at Phase 2.

**Location Management**

To minimize transactions with the HLR, it only contains location information about the MSC/VLR to which the subscriber is attached. The VLR contains more detailed location information, such as the location area in which the subscriber is actually roaming. See Chapter 12, "Cellular Networks," for more information about location areas. As a result, the VLR requires that its location information be updated each time the subscriber changes location area. The HLR only requires its location information to be updated if the subscriber changes VLR.

Location management operations include the following:

* updateLocation
* cancelLocation
* sendIdentification
* purgeMS

**updateLocation**

This message is used to inform the HLR when an MS (in the idle state) has successfully performed a location update in a new VLR area. In this way, the HLR maintains the location of the MS (VLR area only). In Appendix L, "Tektronix Supporting Traffic," [Figure 13-3](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig03.gif')) contains a trace that shows an HLR's decode calling a VLR (to perform cancel location). In [Figure 13-1](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig01.gif')), the MS has roamed from a VLR area that is controlled by VLR-A to an area that is controlled by VLR-B. Note that the purgeMS operation is optional in a location update procedure.

[13fig03.gif](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig03.gif'))

[Figure 13-3](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig03.gif')) MAP Operation Sequences in a Handover

[13fig01.gif](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig01.gif'))

[Figure 13-1](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig01.gif')) Showing the MAP Operation Sequences Involved in a Location Update

**cancelLocation**

The cancelLocation operation is used to delete a subscriber's profile from the previous VLR, following registration with a new VLR—in other words, following an updateLocation. When the HLR receives an updateLocation from a VLR other than the one that is currently stored in its tables, it sends a cancelLocation to the old VLR. The cancelLocation includes the International Mobile Subscriber Identity (IMSI) and the Local Mobile Subscriber Identity (LMSI) to identify the subscriber whose profile should be deleted as parameters. For details of the IMSI and LMSI see Chapter 12, "Cellular Networks." In Appendix L, "Tektronix Supporting Traffic," Example L-3 contains a trace that shows an HLR's decode calling a VLR (to perform cancel location).

Operators can also use the operation to impose roaming restrictions following a change in the subscriber's subscription. It is also used as part of the process of completely canceling a subscriber's subscription. When the HLR receives a request from the Operation and Maintenance Center (OMC) to delete the subscriber, the HLR deletes the subscriber's data and sends a cancelLocation to the VLR that serves the subscriber. [Figure 13-2](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig02.gif')) shows a subscriber's subscription being cancelled, thereby disabling their service.

[13fig02.gif](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig02.gif'))

[Figure 13-2](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig02.gif')) MAP Operation Sequences in Which a Subscriber's Service is Disabled

In addition, a cancelLocation operation is sent from the HLR to the VLR if the authentication algorithm or authentication key of the subscriber is modified.

**sendIdentification**

When the MS changes to a new VLR area, the new VLR queries the old VLR using a sendIdentification operation to obtain authentication information. The sendIdentification operation sends the TMSI as its argument, and the result contains the IMSI and other authentication information (RAND, SRES, and optionally KC). If it is unable to obtain this information, it can retrieve the information from the HLR via a sendAuthenticationInfo operation.

**purgeMS**

This message is sent if an MS has been inactive (no call or location update performed) for an extended period of time. The VLR sends this message to the HLR to indicate that it has deleted its data for that particular MS. The HLR should set a flag to indicate that the MS should be treated as not reached; as a result, the HLR no longer attempts to reach the MS in the case of a mobile terminated call or a mobile terminated short message.

**Handover**

Handover between MSCs is known as inter-MSC handover: basic inter-MSC handover and subsequent inter-MSC handover. A basic inter-MSC handover is where the call is handed from the controlling MSC (MSC-A) to another MSC (MSC-B). A subsequent inter-MSC handover is an additional inter-MSC handover during a call. After a call has been handed over from MSC-A to MSC-B, another handover takes place, either to a new MSC (MSC-C) or back to the original MSC (MSC-A).

The following sections describe these MAP handover operations:

* prepareHandover
* sendEndSignal
* processAccessSignalling
* forwardAccessSignalling
* prepareSubsequentHandover

**prepareHandover**

The prepareHandover message is used to carry a request and response between the two MSCs at the start of a basic inter-MSC handover (MSC-A to MSC-B). It is used to exchange BSSAP messages, such as HAN\_REQ and HAN\_ACK, for this purpose. It is the decision of MSC-A to hand over to another MSC. The prepareHandover message does not contain subscriber information—only information that is necessary for MSC-B to allocate the necessary radio resources and possibly some optional information, such as an IMSI.

**sendEndSignal**

Following a successful inter-MSC handover (from MSC-A to MSC-B in the case of a basic handover), MSC-B sends a sendEndSignal message to MSC-A to allow it to release its radio resources. If the call was originally established with MSC-A, it keeps control of the call and is known as the *anchor* MSC following the handover. As a result, MSC-B does not receive information about the release of the call. To solve this problem, MSC-A sends a sendEndSignal to MSC-B to inform it that it can release its own radio resources.

**processAccessSignaling**

The messages processAccessSignaling and forwardAccessSignaling are used to pass BSSAP messages between the MS and the anchor MSC transparently and between the anchor MSC and the MS, respectively. As stated previously, MSC-A keeps control of the call after a successful inter-MSC handover from MSC-A to MSC-B. The BSSAP messages travel from the MS to MSC-A via MSC-B. The message processAccessSignaling carries data from the MS to MSC-A and is sent from MSC-B to MSC-A. The message forwardAccessSignaling is the reverse; it carries data from MSC-A to the MS via MSC-B, as shown in [Figure 13-3](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig03.gif')).

**forwardAccessSignaling**

See processAccessSignaling. If call control information is required to be passed to the serving MSC (MSC-B), the anchor (controlling MSC, MSC-A) sends the information using a forwardAccessSignaling message.

[13fig04.gif](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig04.gif'))

[Figure 13-4](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig04.gif')) Direction of processAccessSignaling and forwardAccessSignaling

**prepareSubsequentHandover**

If another inter-MSC is required (back to MSC-A or to another MSC, C), then MSC-B sends this message to MSC-A. It contains the information required for MSC-A to send a prepareHandover message to MSC-C. Refer to [Figure 13-3](javascript:popUp('/content/images/bok_1587050404/elementLinks/13fig03.gif')).

**Authentication Management**

MAP operation sendIdentificationInfo is the only operation in Phase 2 that falls under the category of authentication management. See sendIdentification for a description of this operation.

**IMEI Management**

The only MAP operation in the IMEIs management category is checkIMEI, which is used to check whether a piece of mobile equipment is on a black, gray, or white list. To perform an IMEI check, the serving MSC requests that the MS provide its IMEI. On receiving the IMEI from the MS, the MSC sends the IMEI to the EIR in a MAP checkIMEI operation. The EIR checks the status of the IMEI and sends the result back to the MSC. The equipment status can be white listed, gray listed, blacklisted, or unknown.

Blacklisted equipment is equipment that has been reported stolen and is, therefore, not granted permission to use the network (barred). If the status indicates that the equipment is blacklisted, an alarm might be generated on the operation and maintenance interface; this is network operator-dependent. The network operator can use the gray listed equipment list to block a certain model of equipment (or even a particular software version) from using his network if, for example, a certain handset type has proven to act erroneously on the network. Gray listed equipment cannot be barred; instead, it can be chosen to track the equipment for observation purposes. The white list contains all the equipment identities that are permitted for use and to which service should therefore be granted.

Criminals have been able to change mobile handsets' IMEI fairly easily using a data cable (to connect it to a PC) and specialist software. Because of this and the abundance and the high price of mobile handsets, theft has hit epidemic levels in many parts of the world. Recently, the United Kingdom passed legislation known as the Mobile Telephones (Re-programming) Act making it illegal to reprogram the IMEI, and manufacturers were pressed (with limited success) to make the IMEI tamper-proof. In addition, the operators and the GSM association set up a nationwide EIR, known simply as the Central Equipment Identity Register (CEIR) so that stolen mobile equipment could be reported as easily as a stolen credit card. Before CEIR, if the equipment had been blacklisted with one operator, in most cases you could simply put in an SIM card for another operator because the operators failed to pool information.

**Subscriber Management**

An HLR uses subscriber management procedures to update a VLR with specific subscriber data when the subscriber's profile is modified. A subscriber's profile can be modified, because the operator has changed the subscription of the subscriber's basic services or one or more supplementary services. A subscriber's profile might also be modified, because the subscriber himself has activated or deactivated one or more supplementary services.

Subscriber management uses the insertSubscriberData and deleteSubscriberData operations.

**insertSubscriberData**

The HLR uses the insertSubscriberData operation to provide the VLR with the current subscriber profile—for example, during a location update or restore data procedure. It is also used if the operator (via the OMC) or the subscriber himself modifies the data—for example, barring all or certain types of calls. The operation insertSubscriberData is sent as many times as necessary to transfer the subscriber data from the HLR to the VLR.

**deleteSubscriberData**

The HLR uses the deleteSubscriberData operation to inform the VLR that a service has been removed from the subscriber profile. The subscriber might have subscribed to a number of services, such as international roaming. The operator can use this operation to revoke such subscriptions.

**Fault Recovery**

The fault recovery procedures ensure that the subscriber data in the VLR becomes consistent with the subscriber data that is stored in the HLR for a particular MS, and that the MS location information in the HLR and VLR is accurate following a location register fault.

3GPP TS 23.007 gives the detailed specification of fault recovery procedures of location registers.

The fault recovery procedures use the following three MAP operations:

* reset
* forwardCheckSsIndication
* restoreData

**reset**

The HLR that returns to service following an outage sends this operation to all VLRs in which that HLR's MSs are registered according to any available data following the outage.

**forwardCheckSsIndication**

This operation is optionally sent to all MSs following an HLR outage. The MSs are requested to synchronize their supplementary service data with that which is held in the HLR.

**restoreData**

When a VLR receives a provideRoamingNumber request from the HLR for either an IMSI that is unknown to the VLR or an IMSI in which the VLR entry is unreliable because of an HLR outage, the VLR sends a restoreData message to the HLR to synchronize the data.