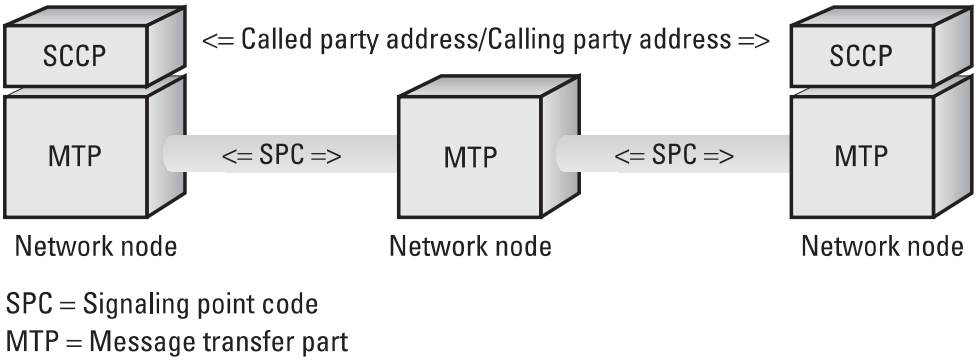


Figure 9.7 End-to-end addressing of the SCCP.

other than the dialed directory number. That is exactly what a global title is. The global title consists of a regular directory number and information as to how to interpret that number. The example in Figure 9.8 shows a called-party address with a global title taken from a MAP trace. Not a subscriber but a particular VLR of the D1 network in Germany is addressed in the figure. The addressing scheme is formatted according to ITU Recommendations E.163 and E.164. The ISDN address of the VLR is 49 171 062 6666.

```
Called Party Address

    reserved for national use : 0

    routing indicator : routing based on global title

    global title indicator : 4 = global title includes translation

    type,numbering plan,encoding scheme and nature of address indicator

    SSN indicator : address contains a subsystem number

    point code indicator : address contains no signaling point code

    subsystem number : 7 = GSM-VLR

    translation type : 0

    numbering plan : 1 = ISDN/telephony numbering plan (recommendation

    E.163 and E.164)

    encoding scheme : 2 = BCD, even number of digits

    nature of address indicator : 4 = international number

    address information : 491710626666
```

Figure 9.8 Example for a CdPA with global title.

Format of Calling-Party Address and Called-Party Address

Figure 9.9 presents the format of CaPA and CdPA as used by the MAP. This illustration also is valid for other applications.

- The first byte defines the structure of the remainder of the information, that is, how the following data shall be processed. Bits 0 through 5 of the first byte indicate whether a parameter is included and what parts the global title consists of, if included. Bit 6 of the first byte determines how the routing of a SCCP message shall be done. When bit 6 equals 0, the global title shall be used for routing. If bit 6 equals 1, the SSN and the SPC shall be used for routing.
- The second and third bytes carry the SPC. The two most significant bits of the SPC are coded with a 0 value, since the SPC, as defined by ITU-SS7, has only 14 bits.

<table>
<tr><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>bit</td></tr>
<tr><td>Reserved for national use</td><td>Routing indicator</td><td colspan="5">Global title indicator
(value for MAP inter-PLMN = 0100)</td><td>SSN indicator</td><td>Point code indicator</td><td>byte 1</td></tr>
<tr><td colspan="8">SPC (signaling point code)/bits 1–8 of 14</td><td>byte 2</td></tr>
<tr><td>0</td><td>0</td><td colspan="6">SPC (signaling point code)/bits 9–14 of 14</td><td>byte 3</td></tr>
<tr><td colspan="8">(SSN) subsystem number (e.g., BSSAP, EIR, HLR, SCCP management)</td><td>byte 4</td></tr>
<tr><td colspan="8">How to translate the global title (translation type)</td><td>byte 5</td></tr>
<tr><td colspan="4">Numbering plan
(e.g. ISDN; E.163/E.164)</td><td colspan="4">How is the global title coded
(e.g., BCD, even/odd number of digits)</td><td>byte 6</td></tr>
<tr><td>Even/odd number of digits</td><td colspan="7">Structure of the address information
(international number, subscriber number, …)</td><td>byte 7</td></tr>
<tr><td colspan="4">2nd digit</td><td colspan="4">1st digit</td><td>byte 8</td></tr>
<tr><td colspan="4">4th digit</td><td colspan="4">3rd digit</td><td>byte 9</td></tr>
<tr><td colspan="4">……</td><td colspan="4">……..</td><td>…</td></tr>
<tr><td colspan="4">'1111' (fill digit ↔ in case of odd number of digits)</td><td colspan="4">last digit</td><td>byte N</td></tr>
</table>

Figure 9.9 Format of a CaPA and CdPA in the SCCP.

- The fourth byte carries the SSN.
- All the remaining data belong to the global title, when present.

9.3.2.2 Credit (1 Byte)

The credit (C) parameter indicates for a secured SCCP transmission the number of SCCP messages that may be unacknowledged at any given time. Only the protocol classes 1 and 3 allow for secured transmission.

9.3.2.3 End of Optional Parameters (1 Byte)

The end-of-optional-parameters (EO) parameter is found only in SCCP messages that may contain optional parameters. It indicates the end of the part, which hosts all the optional parameters of a SCCP message and, hence, the end of the SCCP message as such.

9.3.2.4 Message Type (1 Byte)

The message type (MT) parameter defines the SCCP message type. Its values are presented in Figures 9.6(a) and Figure 9.6(b).

9.3.2.5 Protocol Class (1 Byte)

The protocol class (PC) parameter indicates the service class of a message. Four protocol classes are defined (0, 1, 2, 3), where 0 and 1 represent the connectionless services, while 2 and 3 represent the connection-oriented services. Not all messages can be sent in any service class.

Two protocol classes are defined for both connection-oriented and connectionless service, where classes 0 and 2 form the basic version and classes 1 and 3 allow for additional data security in the form of acknowledgements. Over the A-interface, only protocol classes 0 and 2 are used, while the GSM MAP uses protocol classes 0 and 1. The protocol class 3 is not used at all by GSM.

It is important to distinguish between connection-oriented and connectionless service classes, when analyzing the PC parameter (Figure 9.10). Bits 0 through 3 describe, in both cases, the actual protocol class. Bits 4 through 7 are

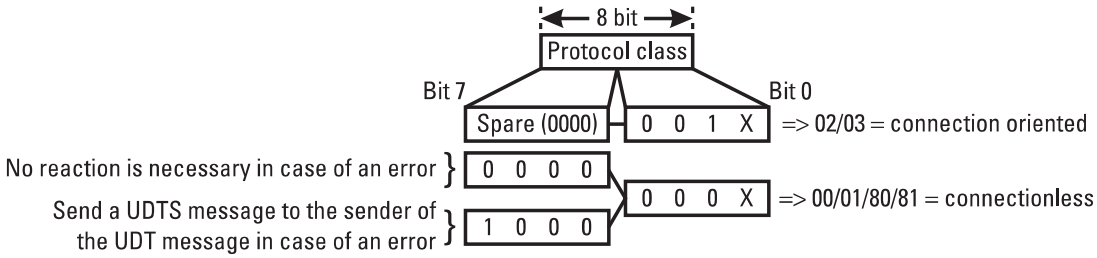


Figure 9.10 Possible formats of the SCCP PC parameter.

not used, in the case of connection-oriented service classes 2 and 3, while bits 4 through 7, in the case of connectionless service classes 0 and 1, indicate whether a UDT message has to be answered in case of an error.

9.3.2.6 Release Cause (1 Byte)

The release cause (RC) parameter provides information about the cause of a SCCP connection being released. Note that the value $0F_{hex}$ (unqualified) is used in the case of normal clearing of a SCCP connection.

9.3.2.7 Refusal Cause (1 Byte)

The refusal cause (RF) parameter provides the reason for a request for a SCCP connection setup being refused. There is, in particular, a distinction between overload of the SCCP and overload of a subsystem.

9.3.2.8 Return Cause (1 Byte)

The return cause (RT) parameter is present only in UDTS messages. It indicates why the sender of a UDTS message could not process a UDT message.

9.3.2.9 Source Local Reference/Destination Local Reference (Each 3 Bytes)

The source local reference (SLR) and destination local reference (DLR) parameters are present only in connection-oriented messages. Their task is to identify a virtual connection.

9.3.2.10 Segmenting/Reassembling (1 Byte)

The segmenting/reassembling (S/R) parameter is present only in DT 1 messages. The data part of DT 1 messages is limited to 256 bytes. When information larger than 256 bytes has to be transmitted, the data has to be segmented, that is, distributed over several DT 1 messages (compare the segmentation of $LAPD_m$, described in Chapter 7).

9.3.2.11 Sequencing/Segmenting (2 Bytes)

The sequencing/segmenting (S/S) parameter is used only in the DT 2 message and the IT message. It contains SCCP internal information, the send sequence number P(S) and the receive sequence number P(R), as well as information on segmentation, which is similar to S/R. The task of P(S) and P(R) corresponds to that of N(S) and N(R) of LAPD, or FSN and BSN in SS7 respectively.

9.3.2.12 Subsystem Number (1 Byte)

The subsystem number (SSN) specifies the user from which a SCCP message stems or to which it is addressed. The SSN may be part of CaPA/CdPA or part of an SCCP management message. Table 9.3 lists the subsystems of the SCCP.

Table 9.3
Subsystems of the SCCP

SSN (Hex)	Subsystem
00	SSN not known or not available
01	SCCP management
02	Reserved
03	ISUP
04	OMAP
05	MAP
06	HLR
07	VLR
08	MSC
09	EIR
0A	AuC (future)
FE	BSSAP

9.3.3 Decoding a SCCP Message

Figure 9.11 shows a RLSD message that was recorded by a protocol tester. The explanation is intended to clarify the relationship between the hexadecimal and the mnemonic representations.

9.4 The Principle of a SCCP Connection

The same principle is always used to establish and release an SCCP connection. Figure 9.12 illustrates that principle for the BSC-to-MSC example. One side requests a SCCP connection by sending a CR message. An important part of the CR message is the SLR, which is used as a reference by the requesting side like some kind of ticket number, to identify the requested SCCP connection.

The peer entity confirms the establishment of the SCCP connection by sending a CC message. The CC message contains the SLR of the responding side and the DLR (which corresponds to the original SLR of the requesting side). Hence, the SLR on the side of the BSC corresponds to the DLR on the MSC side and vice versa. Both sides know the SLR, DLR, and when the CC message was received, and the two parameters are then used as identifiers for sender and addressee.

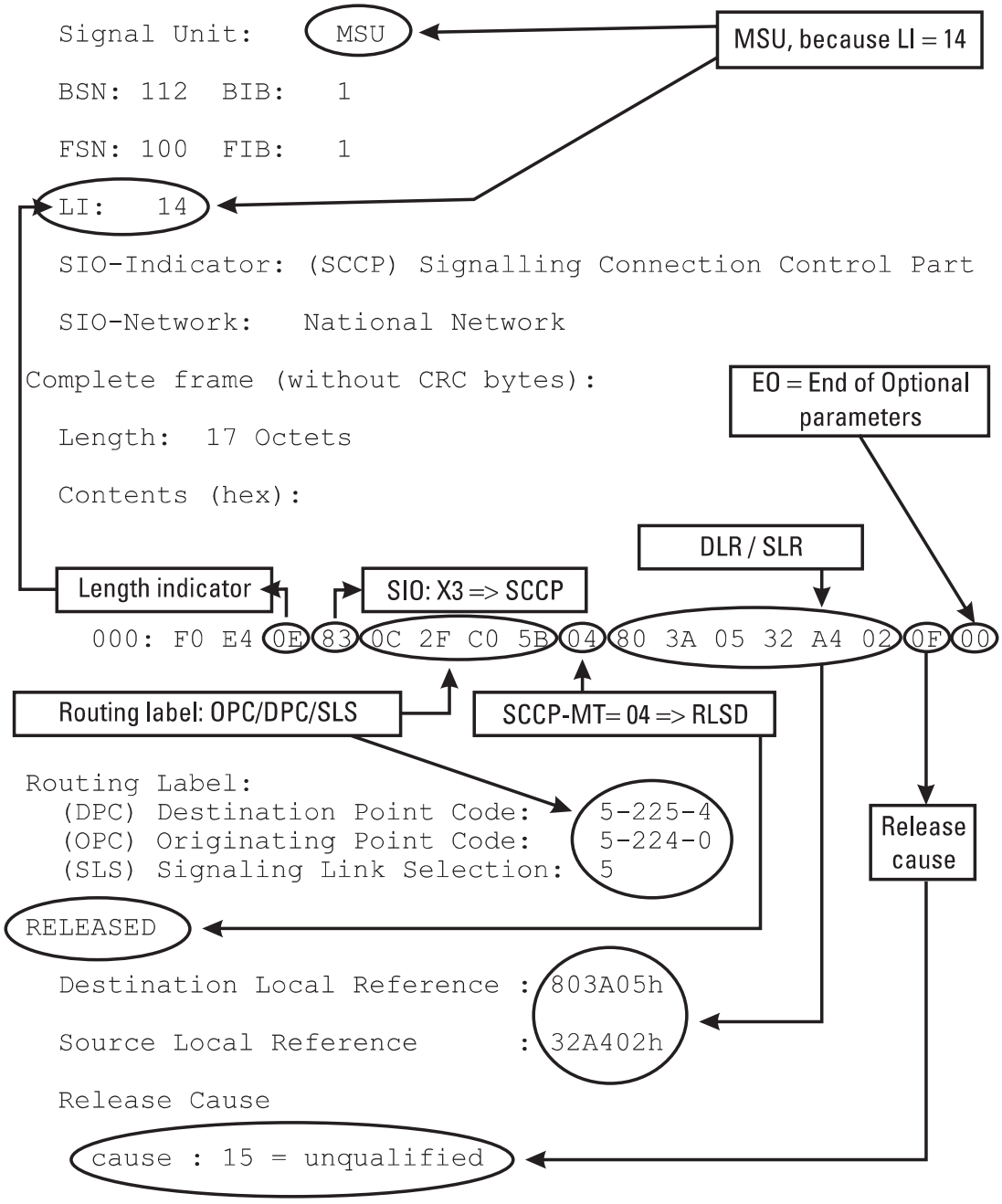


Figure 9.11 An RLSD message.

When a connection is set up and each side knows the "ticket number" (the reference number (DLR) of the peer entity) the DT 1 message is used for further exchange of data (the DT 2 message is not used by GSM).

Note that the establishment of a radio connection or a call on the A-interface is performed via DT 1 messages. This shows the transparency of

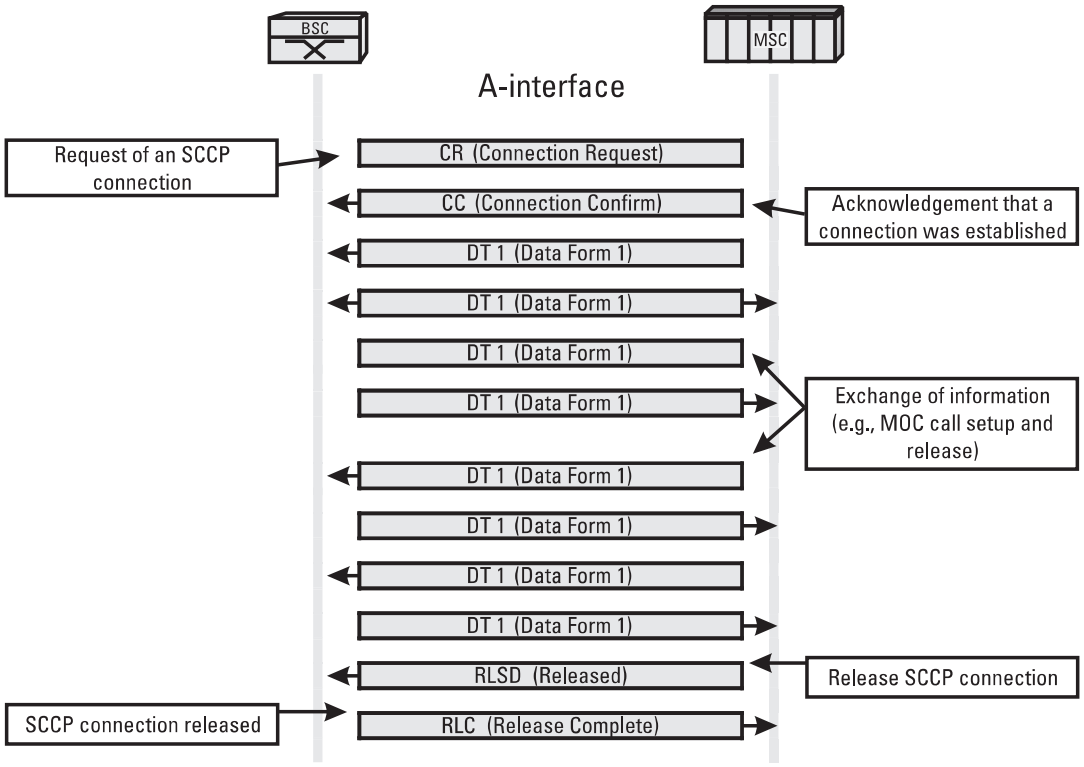


Figure 9.12 Principle to establish and release an SCCP connection for BSC-to-MSC.

the SCCP for its users (the BSSAP is this user on the A-interface). Only after release of the radio connection is the SCCP connection also released.

An SCCP connection is released by an RLSD message, which in the BSC-to-MSC example is always sent by the MSC. The receiving side confirms with an RLC message that the RLSD message was received, the SCCP connection was released, and the resources were cleared.

10

The A-Interface

On the physical level, the A-interface consists of one or more PCM links between the MSC and the BSC, each with a transmission capacity of 2 Mbps. The TRAU, which typically is located between the MSC and the BSC, has to be taken into consideration when examining this interface. Consequently, the A-interface can be separated into two parts.

- The first part is between the BTS and the TRAU, where the transmitted payload still is compressed. Figure 10.1 shows a possible channel configuration for three trunks. As on the Abis-interface, a single traffic channel occupies only two of the eight bits of a PCM channel. That is why it is possible to transport four fullrate traffic channels on one PCM channel. The exceptions are TSs, where signaling information is carried. Signaling information requires the entire 64 Kbps of a channel (e.g., TS 16 in Figure 10.1).
- The second part of the A-interface is the one between the TRAU and the MSC. There, all data are uncompressed. For that reason, every traffic channel requires the complete 8 bits or occupies an entire 64-Kbps PCM channel. The position of a signaling channel may be different before and after the TRAU, as Figure 10.1 shows.

10.1 Dimensioning

An examination of the channel configuration in Figure 10.1 makes it obvious that the transmission resources between the BSC and the TRAU are used only

Samsung Ex. 1032, Page 176 of 417

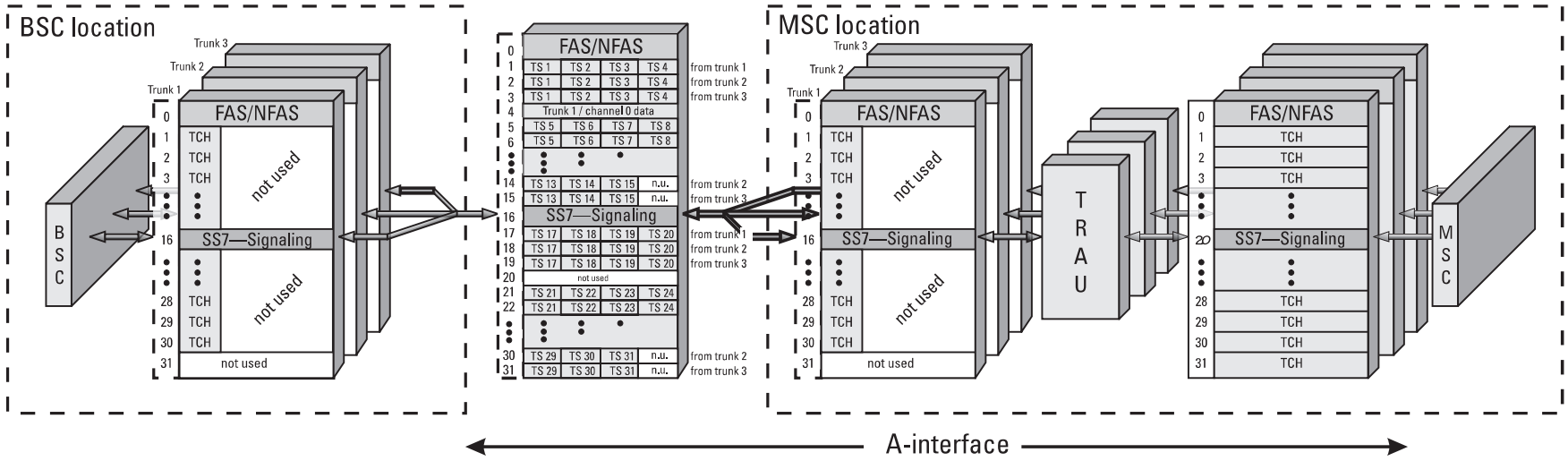


Figure 10.1 Possible channel configuration between the BSC and the MSC.

inefficiently. Only 2 bits of the PCM channel are actually occupied, while the remaining 6 bits stay vacant. In that respect, the A-interface between the BSC and the TRAU can be compared to the Abis-interface in a star configuration.

It is possible, by means of multiplexing, to transport the data of several trunks from the BSC over only one physical 2-Mbps link before the data are actually handed over to the TRAU for decompression. That allows a savings of about two-thirds of the line costs if the TRAU is installed at the MSC location. Multiplexing between the TRAU and the MSC does not deserve any consideration, since every traffic channel there requires 64 Kbps.

10.2 Signaling Over the A-Interface

As on all the other interfaces except for the Air-interface and the Abis-interface, the A-interface uses SS7 with the SCCP as the user part. Similar to the Abis-interface, GSM uses an already existing signaling standard (SS7 plus SCCP) on the A-interface and simply defines a new application.

This new application is the BSSAP, which itself can be separated into the base station subsystem management application part (BSSMAP) and the direct transfer application part (DTAP).

That results in the OSI protocol stack are presented in Figure 10.2. DTAP data are user information and therefore completely transparent for the A-interface, while the BSSMAP data are part of Layer 3.

10.2.1 The Base Station Subsystem Application Part

The BSSAP, with its two parts, the DTAP and the BSSMAP, represents the GSM-specific user signaling on the A-interface.

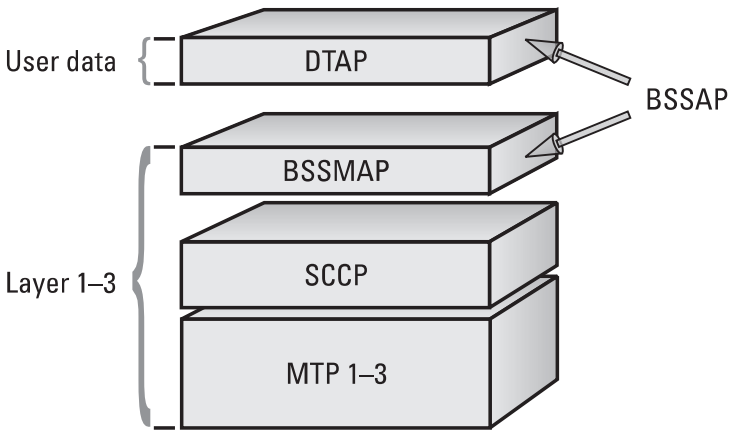


Figure 10.2. The A-interface in the OSI protocol stack.

- The BSSMAP includes all messages exchanged between the BSC and the MSC that are actually processed by the BSC. Examples are PAGING, HND_CMD, and the RESET message. More generally, the BSSMAP comprises all messages exchanged as RR messages between the MSC and the BSC, as well as messages used for control tasks between the BSC and the MSC.
- The DTAP comprises all messages exchanged between a subsystem of the NSS and the MS. The messages are transparent for the BSS. This definition applies to all but three messages of MM. These exceptions are the LOC_UPD_REQ, the IMSI_DET_IND, and the CM_SERV_REQ messages. All three are part of DTAP but nevertheless are partly processed by the BSC.

Figure 10.3 illustrates the task sharing between BSSMAP and DTAP. It is important to note that there is not a 100% correspondence between DTAP and CC/MM on one side and BSSMAP and RR on the other. There are cases when the BSC and the MS exchange RR messages without informing the MSC about the content of the messages. The same applies for BSSMAP messages between the BSC and the MSC.

10.2.2 The Message Structure of the BSSAP

Figure 10.4 shows the general structure of BSSAP messages. The entire BSSAP message is embedded in an SCCP message. The first 8 or 16 bits of the BSSAP distinguish between BSSMAP and DTAP. The DTAP header is

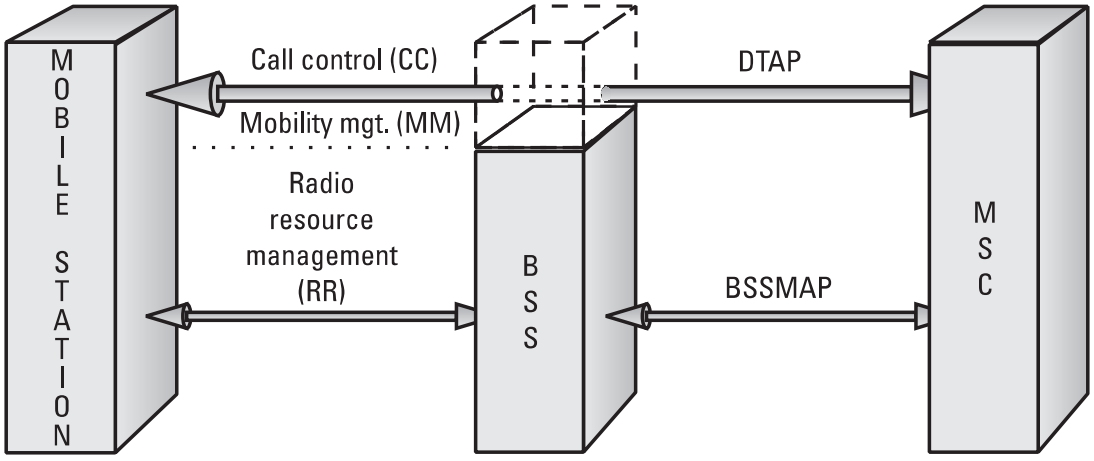


Figure 10.3 The relation between DTAP corresponding to CC and MM, and BSSMAP corresponding to RR.

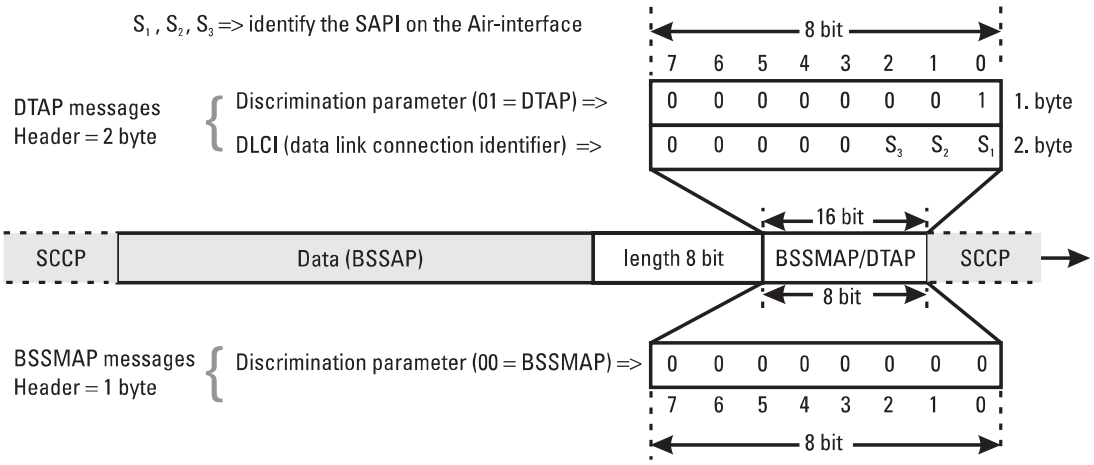


Figure 10.4 The format of BSSAP messages.

2 bytes (16 bits) long and consists of the discrimination parameter (01 = DTAP) and the data link connection identifier (DLCI). The first 3 bits of the DLCI identify the service access point identifier (SAPI), which is used on the Air-interface (SAPI = 0 for RR, MM, and CC; SAPI = 3 for SMS and SS).

The BSSMAP header is only 1 byte (8 bits) long and consists only of the discrimination parameter (00 = BSSMAP). In BSSMAP, there is no DLCI octet.

A length indicator, indicating the length of the following data field, follows the header in both cases of BSSMAP and DTAP. DTAP messages exactly follow the format as presented in Figure 7.14. BSSMAP messages are formatted as shown in Figure 10.5. The actual parameters follow the 1-octet-long message type. Independent of being mandatory or optional, each parameter always consists of an information element identifier (IEI), length indicator, and the actual data.

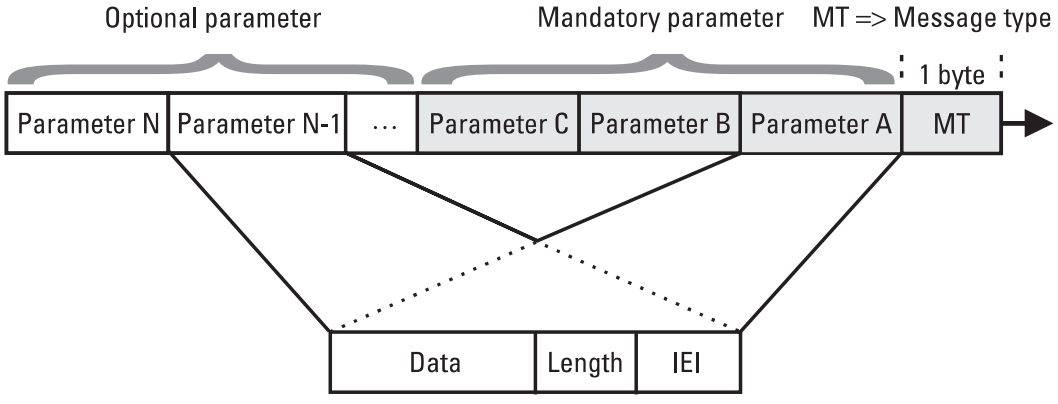


Figure 10.5 The internal structure of BSSMAP messages.

10.2.3 Message Types of the Base Station Subsystem Management Application Part

Table 10.1 lists all BSSMAP messages, along with brief descriptions of their tasks. The uppercase letters indicate the abbreviations used in this context.

Table 10.1
BSSMAP Messages

ID (Hex)	Name	Direction	Description
01	ASSignment REQuest	MSC → BSC	Is sent from the MSC to the BSC during a connection set up in order to assign a channel on the Air- and the A-interface. The ASS_REQ message does not specify the Air-interface channel in more detail. Rather, the BSC selects one TCH out of the available radio resources and assigns this channel by means of the ASS_CMD message. The ASS_REQ message, however, contains a specification of the channel on the A-interface. There is no TCH available on neither the Air-interface nor on the A-interface before the ASS_REQ message is received and the complete communication between NSS and MS occurs via control channels.
02	ASSignment COMplete	BSC → MSC	This is the positive response to an ASS_REQ for TCH assignment. The MS has changed to the TCH and the Layer 3 connection is established.
03	ASSignment FAILure	BSC → MSC	This is the negative response to the MSC, when a channel assignment was not successful (not used for errors during handover). ASS_FAIL should not be confused with ASS_FAI, a message, defined in GSM 04.08 for the Air-interface. The cause values, for example, are different between the two messages.
10	HaNDover REQuest	MSC → BSC	If the BSC needs to be changed during handover, this message is sent by the MSC to the new BSC. The MSC reacts with HND_REQ to HND_RQD originating from the old BSC. The new BSC selects the appropriate radio resources and sends the detailed information (e.g., frequency, time slot, handover reference) in a HND_REQ_ACK message, back to the MSC. The HND_REQ message, like the ASS_REQ, contains a specification of the resources to be used on the A-interface.

Table 10.1 (continued)

ID (Hex)	Name	Direction	Description
11	HaNDover ReQuireD	BSC → MSC	The BSC uses this message to request a handover from the MSC (only intra-MSC and inter-MSC handover). The best candidates for the handover are the most important content. The possible destinations are derived from the measurement results of the MS and neighbor cell relations of the serving cell.
12	HaNDover ReQuest ACKnowl-edge	BSC → MSC	Answer of the BSC to a HND_REQ message. The HND_REQ_ACK message contains the HND_CMD message, which was prepared by the new BSC and shall be sent to the MS via the MSC and the old BSC.
13	HaNDover CoMmanD	MSC → BSC	Is used for every handover that is controlled by the MSC, in order to provide detailed information about the new radio resources to the MS. Please note that this HND_CMD message has a different format compared to the one with the same name, defined by GSM 04.08 for the Air-interface.
14	HaNDover CoMPlete	BSC → MSC	A HND_CMP message has to be sent to the MSC for every successful handover, which is controlled by the MSC. In case of an intra-BSC handover (which most likely is controlled by the BSC), HND_PERF is used to inform the MSC about the change of channels within the BSC, instead of HND_CMP.
16	HaNDover FAILure	BSC → MSC	A HND_FAIL is always sent from the BSC to the MSC when a handover fails, e.g., due to insufficient resources (answer to HND_REQ) or when handover as such fails (answer to HND_CMD).
17	HaNDover PERFormed	BSC → MSC	Is sent to the MSC for every handover, which is controlled by the BSC (only intra-BTS and intra-BSC) in order to inform the MSC about a channel change. HND_PERF corresponds to HND_CMP in case of the MSC controlled handover.
18	HaNDover CaNDidate ENQuire	MSC → BSC	There might be cases when it is required to lower the traffic load on one or more cells. For this purpose, the MSC has the ability to send a HND_CND_ENQ message to the BSC. The message identifies the cell, where the load shall be reduced and possible neighbor cells, and where already active calls could be transferred. For every connection, which can—from a radio perspective—be transferred, the BSC responds with a HND_RQD message to the MSC.

Table 10.1 (continued)

ID (Hex)	Name	Direction	Description
19	HaNDover CaNDidate RESponse	BSC → MSC	With an HND_CND_RES message, the BSC confirms to the MSC that a HND_CND_ENQ message was received and processed. The confirmation that the message was processed refers, in particular, to the fact that HND_RQD messages were sent for all possible candidates for handover.
1A	HaNDover ReQuireD REJect	MSC → BSC	This message is only sent by the MSC as a response to HND_RQD when: a) the HND_RQD was not processed within the time defined by timer T7 (i.e., if no HND_CMD is sent) and b) the Response Request parameter was set in the HND_RQD message. In this case, the MSC has to answer each not processed HND_RQD. If the Response Request parameter is not active then the BSC may simply repeat the HND_RQD after the expiration of timer T7.
1B	HaNDover DETect	BSC → MSC	The BSC reacts with this message when it receives a HND_DET from the BTS (same name as the message on the Abis-Interface). The HND_DET message informs the MSC at the earliest possible time about a change of the radio resources. This measure, on the other hand, allows for rapid switch of the terrestrial resources (reduction of "dead air"-time during handover).
20	CLeaR CoManD	MSC → BSC	This message is always used to release the radio resources to a specific MS. A CLR_CMD may be: a) the answer to a CLR_REQ, that is, a problem that was detected by the BSS; (b) the reaction to a problem detected by the NSS; or (c) used in case of normal termination of the radio resources. Only further analysis provides details on the reason for a CLR_CMD.

Table 10.1 (continued)

ID (Hex)	Name	Direction	Description
21	CLeaR CoMPlete	BSC → MSC	When the BSC receives a CLR_CMD message it clears the radio resources to a particular MS. This is confirmed by sending a CLR_CMP message. Sometimes, the CLR_CMP message is sent even before the radio resources are actually released, i.e., before the RF_CHAN_REL message is sent on the Abis-interface.
22	CLeaR REQuest	BSC → MSC	A CLR_REQ message with the appropriate cause is sent to the MSC, if the BSC detects severe problems with an existing connection to a MS on a control channel or a TCH. The BSC reacts with a CLR_REQ message when a CONN_FAIL message is received from the BTS, but also in case of some error situations during handover. The MSC reacts with a CLR_CMD message (for more details see Chapter 13, "Quality of Service").
25	SAPI"n" REJect	BSC → MSC	The BSC responds with a SAPI_REJ message if it receives a DTAP message from the MSC with a SAPI value other than zero, and no corresponding connection to a MS exists or can be established. This message contains an appropriate cause value and the 'wrong' DLCI (Data Link Connection Identifier).
26	CONFUSION	BSC ↔ MSC	When the BSC or the MSC receives a message with apparently the wrong content in the BSSAP header (protocol error), then a CONFUSION message is sent back to the sender. This message contains a diagnosis element that allows the sender of the faulty message to draw conclusions on the type of problem.
30	RESET	BSC ↔ MSC	In case of fatal errors, which reveal serious inconsistencies regarding the communications data between BSC and MSC (used SCCP reference, data about active calls, etc.), the reset-procedure is performed. The RESET message is then used to synchronize the BSC and the MSC. It is sent in connectionless mode (protocol class 0) in a UDT-SCCP message by that network element that detects the inconsistency. The RESET message is also utilized when the A-interface is originally initialized in order to bring both sides into a defined state. (Note that after the reset-procedure, the BSC has to repeat BLO/CIR_GRP_BLO messages, for all channels, which were in a blocked state before a RESET was sent.)

Table 10.1 (continued)

ID (Hex)	Name	Direction	Description
31	RESet AC-Knowledge	BSC ↔ MSC	The RES_ACK message confirms that a RESET message was received and that all resources were actually reset.
32	OVERLOAD	BSC ↔ MSC	The BSC sends this message to the MSC in order to indicate an overload situation in a BTS or even the whole BSS. It is possible to specify the type of overload and which BTSs are affected. This message can be sent by the MSC as well, e.g., in order to indicate processor overload. The OVERLOAD message is sent to the peer within a UDT-SCCP message (connectionless mode, protocol class 0).
34	RESet CIRCuit	BSC ↔ MSC	The RES_CIRC message is used like the RESET message, to reset resources between BSC and MSC. However, the RES_CIRC message applies only to individual time slots on the A-interface, while the RESET message is used on a per trunk basis. Therefore, the RES_CIRC message contains a parameter that identifies the respective time slot.
35	RESet CIRCuit AC-Knowledge	BSC ↔ MSC	The RES_CIRC_ACK message confirms to the peer entity that a RES_CIRC message was received and the respective channel was reset.
36	MSC IN-Voke TRaCe	MSC → BSC	GSM allows to track a single connection from the beginning to the end. For this purpose, the OMC allows the activation of a supervisory function, which translates on the message level in the direction from MSC to BSC into an MSC_INV_TRC message (MSC BSC) and in the reverse direction, from the BSC to the MSC into a BSS_INV_TRC message (BSC MSC). The connection to be supervised is determined by SLR/DLR, with which the message is sent. Other parameters, like the type of connection, identity of the MS, and identity of the OMC are included.
37	BSS INVoke TRaCe	BSC → MSC	See MSC_INV_TRC.
40	BLOck	BSC → MSC	Individual traffic channels sometimes need to be disabled for traffic. Like in ISUP, this request is sent in a BLO message, which the BSC sends to the MSC. The BLO message allows to single out an individual channel.
41	BLOcking ACKnowl-edge	MSC → BSC	This is the acknowledgment that a BLO message was received and processed. The channel indicated in the BLO message is no longer assigned.

Table 10.1 (continued)

ID (Hex)	Name	Direction	Description
42	UnBLOck	BSC → MSC	The UBLO message is used to cancel the blockage of a single channel on the A-interface. Hence, the UBLO message is the counter part of the BLO message.
43	UnBLOcking ACKnowl-edge	MSC → BSC	This is the acknowledgment that a UBLO message was received and processed. The channel, indicated in the UBLO_ACK message, can now be assigned again.
44	CIRCuit GRouP BLOck	BSC → MSC	Frequently, not only a single channel needs to be blocked, but a complete PCM trunk. If a single BLO message had to be sent for each individual time slot of a trunk, then the SS7 system would experience unnecessary load, or even overload. Therefore, the CIRC_GRP_BLO message allows to block a complete area or a whole PCM link.
45	CIRCuit GRouP BLOcking ACKnowl-edge	MSC → BSC	Acknowledgement by the MSC that it received and processed a CIRC_GRP_BLO message. The area or the trunks, which were specified in the CIRC_GRP_BLO message will no longer be assigned.
46	CIRCuit GRouP UnBLOck	BSC → MSC	The CIRC_GRP_UBLO message is used to cancel the blockage of an area on the A-interface. The CIRC_GRP_UBLO message is the counterpart to the CIRC_GRP_BLO message.
47	CIRCuit GRouP UnBLOcking ACKnowl-edge	MSC → BSC	Acknowledgement by the MSC that a CIRC_GRP_UBLO message was received and processed. The area, defined in the CIRC_GRP_UBLO_ACK message can now be assigned again.
48	UNEQipped CIRCuit	BSC ↔ MSC	If the BSC or the MSC receives a message, e.g., RES_CIRC from its peer, where channels are referenced that are unknown to the receiving side, then a UNEQ_CIRC message is returned.
50	RESource REQuest	MSC → BSC	When the MSC sends a RES_REQ message, it requests the BSC to provide updated information on the available radio resources of a BTS. The MSC selects the BTS and sends its identity (CI) within the RES_REQ message.
51	RESource INDication	BSC → MSC	Answer to a RES_REQ message. The RES_IND message contains all information about the radio resources of a BTS.

Table 10.1 (continued)

ID (Hex)	Name	Direction	Description
52	PAGING	MSC → BSC	In case of a Mobile Terminating Call (MTC), the MSC sends PAGING messages to all the BSCs of a location area. The particular location area is where the MS was last registered and is identified by the Location Area Code (LAC). Exactly one MS can be paged with a single PAGING message. The PAGING message always contains the IMSI, if assigned also the TMSI of the called MS.
53	CIPHER MODE CoManD	MSC → BSC	The MSC sends a CIPHER_MODE_CMD message to the BSC in order to start ciphering on the Air-interface. The most important information is the ciphering key Kc, which is required by the BTS to begin ciphering the encryption algorithm (A5/X), which is selected by the MSC/VLR. The CIPH_MOD_CMD message is another, different message of the Air-interface, which should not be confused with the one with a similar name of the A-interface, since the ciphering key Kc must not be sent over the Air-interface.
54	CLaSsMaRK UPDate	BSC ↔ MSC	It is possible that the technical information related to a MS, the Classmark information, changes during a call or just needs to be queried again. An example of such a situation when the characteristics of a mobile change during usage is when a class handheld is connected to a booster in a car. The MS sends, in this case, a CLS_MRK_UPD message to the MSC.
55	CIPHER MODE CoMPlete	BSC → MSC	The MS confirms that a CIPHER_MODE_CMD message was received and that encryption begins.
56	QUEUing INDication	BSC → MSC	The QUEU_IND message is used only when TCH queuing is active. If this is the case, then QUEU_IND is sent to the MSC as a response to a HND_REQ or a ASS_REQ message if no radio resources are immediately available. The corresponding connection is put in a queue until a traffic channel becomes available.

Table 10.1 (continued)

ID (Hex)	Name	Direction	Description
57	Complete Layer 3 Information	BSC → MSC	The CL3I message is used to transport all initial messages by which a connection can be established (IMSI_DET_IND, PAG_RSP, CM_SERV_REQ, LOC_UPD_REQ). Note that the SCCP message, which carries a CL3I, is not a DT 1 message, but a CR message. The CL3I message is used in particular to piggyback those DTAP messages that need to be processed by the BSC. This applies for the LOC_UPD_REQ, the IMSI_DET_IND an d the CM_SERV_REQ messages.
58	CLaSsMarK REQuest	MSC → BSC	The MSC uses this message to request the MS to transmit its technical specification (Classmark information), which has possibly changed. The response by the MS is sent in a CLS_MRK_UPD message.
59	CIPHER MODE REJect	BSC → MSC	The BSC uses this message to respond to a CIPHER_MODE_CMD message if the ciphering information, received from the MSC, can not be processed properly (e.g., when the requested ciphering algorithm is not supported).
5A	LOAD INDication	BSC ↔ MSC	The BSC sends the LOAD_IND message to the MSC, in order to be forwarded to all neighboring BSCs. This message may be used to indicate an overload situation of a BTS, and is intended to influence handover decisions in the neighboring cells. The major parameters are the identity of the affected BTS and its neighbor cells, as well as the duration, for which the overload situation is anticipated to last.

10.2.4 Decoding of a BSSMAP Message

Figure 10.6 shows an extract from a trace file captured by a protocol tester. It shows a CLR_CMD message in both hexadecimal and decoded forms.

The intention here is to emphasize the message structure of BSSMAP, where a number of parameters follow the message type identifier. These parameters are, in the case of CLR_CMD, the two information elements: Layer 3 header information and cause.




```
Decoded:  CLEAR COMMAND
            Layer 3 Header Information
              Protocol Discriminator: Radio Resource
              management messages
              Transaction Identifier: 0  -  msg sent from TI orig. side
            Cause
              09h = Normal Event - call control
```

Figure 10.6 Decoding of a CLR_CMD message.

- The Layer 3 header information contains the PD and the TI that are to be used on the Air-interface.
- The cause identifies the reason why a specific radio resource will be released. Normal values are 09, which stands for CC and indicates that CC requests the release of a connection when the call is terminated, and $0B_{hex}$, which indicates a successful handover.

11

Transaction Capabilities and Mobile Application Part

The TCAP and the MAP are "on top" of SS7 (MTP 1–3) and SCCP, the basis for signaling on all NSS interfaces. Both are dealt with in this one chapter, because the functionality of the MAP cannot be understood without knowing about the TCAP. The TCAP, with its Layers 4 through 6 provides the GSM-specific MAP with a standardized interface to the transmission medium and to SS7. The clearly separated border between TCAP and MAP, as shown in Figure 11.1, is in practice more difficult to identify. The transition between the two layers is rather fuzzy. An essential precondition to understanding MAP is the study of TCAP. Above MAP, there are the applications themselves, in the GSM case there are the NSS subsystems HLR, VLR, MSC, and EIR.

11.1 Transaction Capabilities Application Part

TCAP uses SS7 or, more precisely, the SCCP, as shown in Figure 11.1. The TCAP protocol is, to some extent, the most important piece of the protocol stack for GSM or any other mobile system, because it provides the core functionality to support roaming.

Like the SCCP, TCAP is not restricted to being used by only mobile services but is utilized by many other applications for database access and similar tasks. In that respect, TCAP is different from all previously presented protocols. TCAP allows its users to access databases and switching exchanges via the worldwide SS7 network and to invoke services or modify parameters. That does

Samsung Ex. 1032, Page 190 of 417

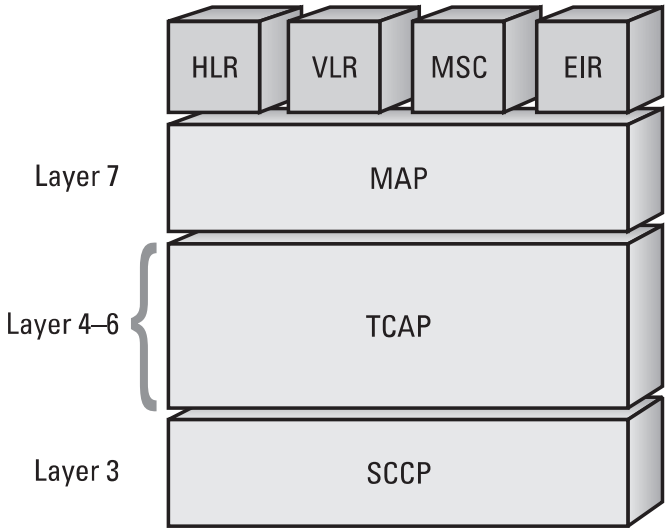


Figure 11.1 Positioning of MAP and TCAP in the SS7 protocol stack.

not exclude TCAP from being used as a platform for pure data transfer, as in GSM, after an inter-MSC handover.

TCAP is the typical implementation of the OSI layers 4 through 6. In that function, it allows integration of some translation functionality into a message, for instance, to provide a means for users of a transaction to discuss or synchronize on an application protocol. An example of this is the GSM networks of Phase 1 and Phase 2, which come with different sets of features. Therefore, those GSM networks need to exchange some information in order to synchronize the feature sets and the respective protocol elements. TCAP provides that functionality.

Figure 11.2 illustrates a generic communication process via TCAP, where, initially, both partners need to agree on the protocol to be used. The receiving side finds the respective information in the dialog control information, which in TCAP is called the dialog portion. Figure 11.2 describes the successful case only. Figure 11.2 separates the parameter part which in TCAP is called the component portion. The component portion carries the actual user data. This is MAP traffic in the case of GSM.

11.1.1 Addressing in TCAP

With respect to addressing, TCAP relies completely on the services of the SCCP. Although ITU does not explicitly exclude alternatives for the future, SCCP currently is the only platform for TCAP. TCAP uses exclusively the connectionless services of SCCP (PCs 0 and 1). The consequence is that SCCP-UDT messages are the only candidates for the transport of TCAP

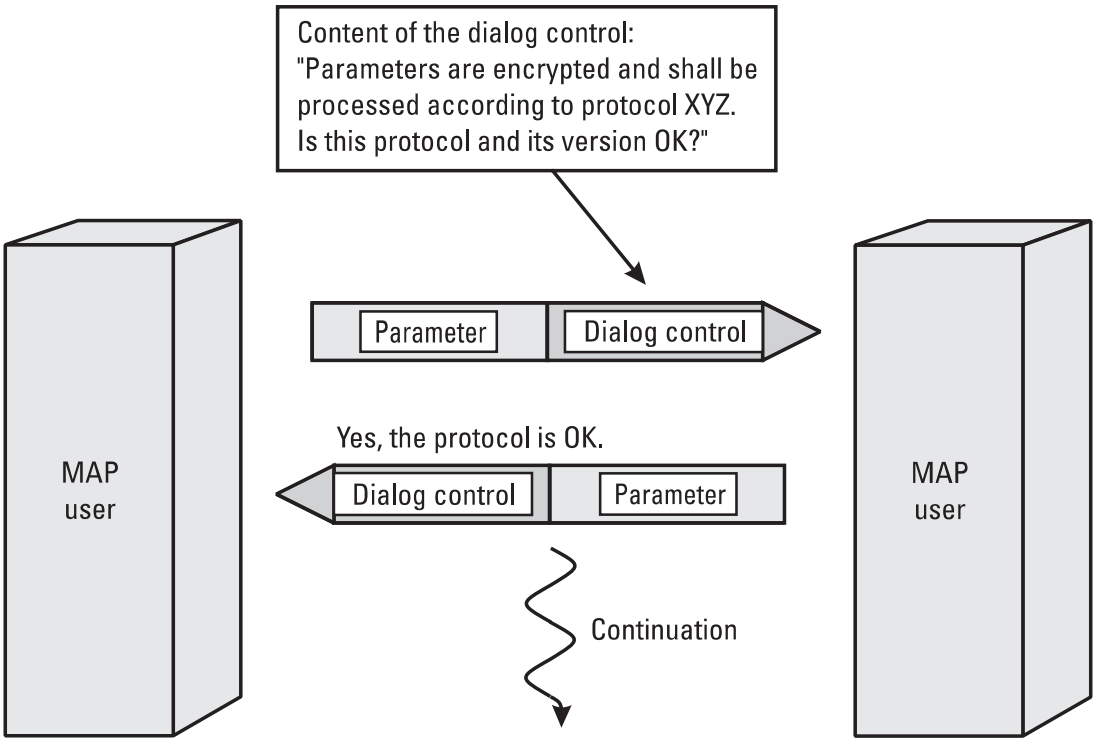


Figure 11.2 The (optional) dialog at the begin of a communication via TCAP.

messages. The sender of a TCAP message directly addresses the destination via the SCCP. The SCCP routes the message via STPs, where the actual path lies in the discretion of the SCCP.

Consider the example of addressing in TCAP/SCCP in the context of a scenario where the MSC and the HLR communicate. Figure 11.3 shows the SCCP header of a TCAP BEGIN message, where an MSC in Australia accesses an HLR in Germany. Both sender and addressee are identified by the global title. Consequently, the MSC in Australia uses the ISDN number of the HLR in Germany for addressing.

11.1.2 The Internal Structure of TCAP

TCAP can be separated into two parts or layers, as shown in Figure 11.4.

- The transaction layer in OSI Layer 4 deals with setting up and maintaining an end-to-end communication. It expects sufficient information from its user about the sender and addressee of a message. As shown in the example in Section 11.1.1, that value is not used by TCAP itself but passed to the SCCP for addressing. In most cases, the transaction layer assigns to a process an additional TCAP-internal

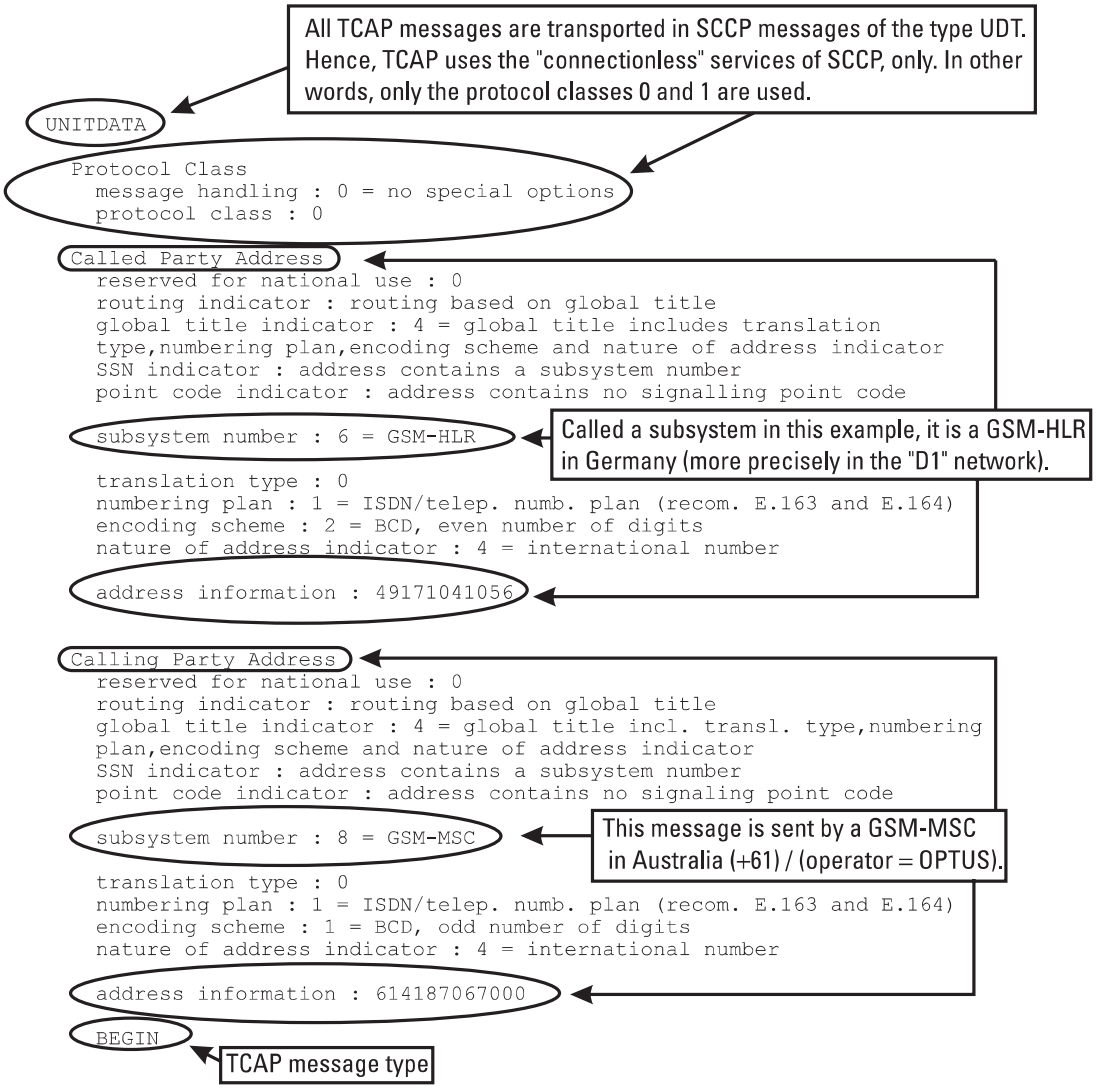


Figure 11.3 Important information in the SCCP header of a TCAP message.

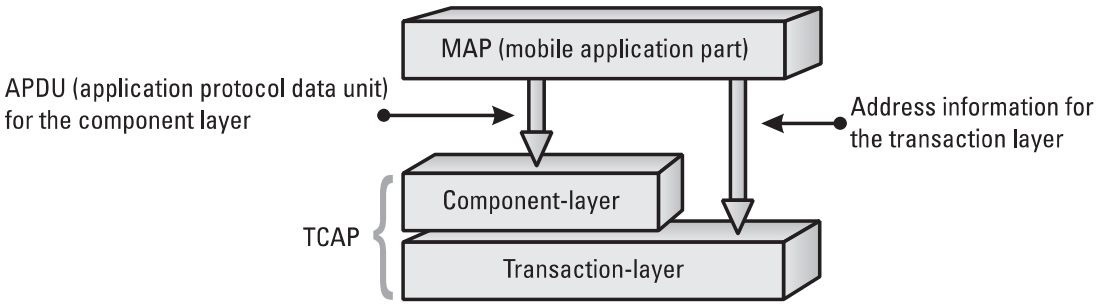


Figure 11.4 Separation of TCAP into component and transaction layers and its communication with MAP.

identifier, the transaction ID, which is comparable to SLR and DLR of the connection-oriented mode of the SCCP.

- The component layer in the OSI Layers 5 and 6 is responsible for synchronization and coordination of a communication. It also provides a uniform data interface to its users, represented by the application protocol data unit (APDU). In TCAP, APDUs are also referred to as components. They transport the payload, which MAP and the component layer exchange.

11.1.3 Coding of Parameters and Data in TCAP

One of TCAP's major advantages is its flexibility, which allows for processing of all kinds of parameter types and data formats. Take this example: TCAP (equals a shipping company) transports data (goods) of all kinds (pets, dishes, bulldozer, etc.). More technically speaking,

- TCAP has to be able to process length indicators from one byte to several thousands of bytes. That requires that a sufficiently large area is reserved for length indicators.
- It must be possible to distinguish among various parameter types. Parameter types are of little significance for the lower layers of the OSI Reference Model. In contrast, OSI Layer 6—in this case, TCAP—has the task of distinguishing and preprocessing the data for Layer 7 (MAP).

Examples for parameter types are:

- Strings (i.e., a combination of characters, e.g., "the GSM system");
- Integer numbers (0, 1, 2, 3, …);
- Real numbers (π = 3.14159…).

Recommendations ITU X.208 and X.209 provide a complete definition of the coding of the various parameter types in ASN.1. GSM uses only a subset of those parameter types (which will be described later). There are some practical limitations with respect to the coding of parameters and length that are a consequence of the limited capacity of the data field of a UDT message (maximum 255 bytes).

In general, all data and message parts in TCAP are coded according to the same scheme (Figure 11.5), and there is no distinction between mandatory and



Figure 11.5 Coding of data in TCAP.

optional parameters. Every message starts with a TAG, which is an identifier, followed by a length indicator. The TAG indicates the data type of the following content.

- TAG: type, classification;
- Length: length of the content field;
- Content: The actual information.

Note that the field "content" itself also may consist of a number of TAGs, length, and content fields, which then results in an interlaced, overall structure. That can lead to a confusing structure in which significant space is consumed by type and length indicators.

Note further that the TAG field and the length indicator can be formatted in different ways, whereby the actual format is derived from the coded information and the application in use. This is more closely examined in the next section.

11.1.3.1 Formatting of the TAG Field

The TAG field is used to identify the data part, in which distinctions have to be made among data classes, formats, and types. For that reason, the TAG field itself is composed of three parts that provide the information. Note that the length indication and bit information in Figure 11.6 refer to a TAG with a length of 1 byte, only.

The meaning of the various fields is as follows:

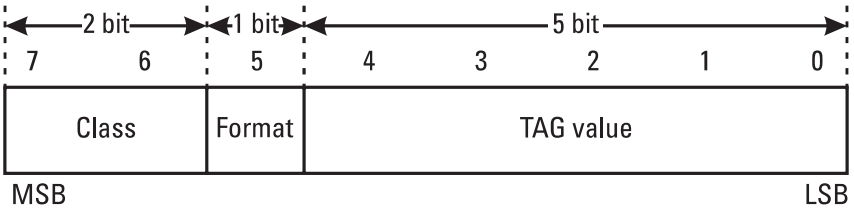


Figure 11.6 Format of TAG field (short form with length of 1 byte).

Class

Class defines the data type. Four classes need to be distinguished and are listed in Table 11.1. (The definitions provided in Table 11.1 are taken from ITU X.208.)

Format

Format distinguishes between two possible formats. It has to be noted that the distinction is valid only on the interface between MAP and TCAP.

- Format = 0_{bin}: The data field contains a primitive, which means that the parameter is not further partitioned.
- Format = 1_{bin}: The data field contains a constructor. Here, the TAG field is only a generic reference for the parameters that follow in the data field, which again are constructors or primitives.

TAG Value

The TAG value indicates to the recipient what kind of parameter type the data field carries. ITU provides a number of proposals that are mandatory within ITU applications (i.e., the universal, applicationwide, and context-specific data classes). The private-use data class can be used for proprietary data types.

11.1.3.2 Primitive Versus Constructor

The difference between a primitive, a single parameter and a constructor, and a collection of parameters is valid only in the context of formatting in TCAP. It can be explained by the example of transmitting an IMSI.

Table 11.1
Classification of Data in TCAP

Value (Bin)	Class, Explanation
00	Universal: Universal data types are specified in X.208. These data types are independent of an application, and all users of SS7 have to be able to recognize them.
01	Applicationwide: Valid only within an ITU Recommendation (e.g., TCAP message types and data types).
10	Context-specific: Valid only in an ITU application (e.g., MAP data types).
11	Private use: Network- or service-provider-specific data types, which will never be assigned by ISO or ITU.

The IMSI is a constructor per definition. It consists of MCC, MNC, and MSIN (mobile sunbscriber identification number), as presented in Figure 11.7.

In TCAP, the IMSI can be coded in two ways. Although the second way of representation may seem unusual, it still demonstrates the alternatives.

- If the IMSI is coded as a primitive, TCAP does not distinguish among MNC, MCC, and MSIN. The complete IMSI is coded as shown in Figure 11.8. The format value 0 indicates that this is a primitive and thus a single parameter message.
- If, however, the individual parameters of the IMSI are coded separately as individual parameters, then a constructor is used for the IMSI where the parameters MCC, MNC, and MSIN are the primitives (Figure 11.9). Note that the fill digit *F* is required for the MCC, because the MCC has a length of 3 bytes (uneven number of bytes). The following remarks are given: (1) Because the MCC, MNC, and

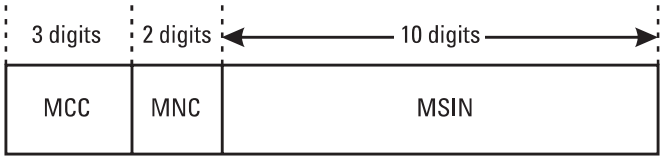


Figure 11.7 The IMSI.

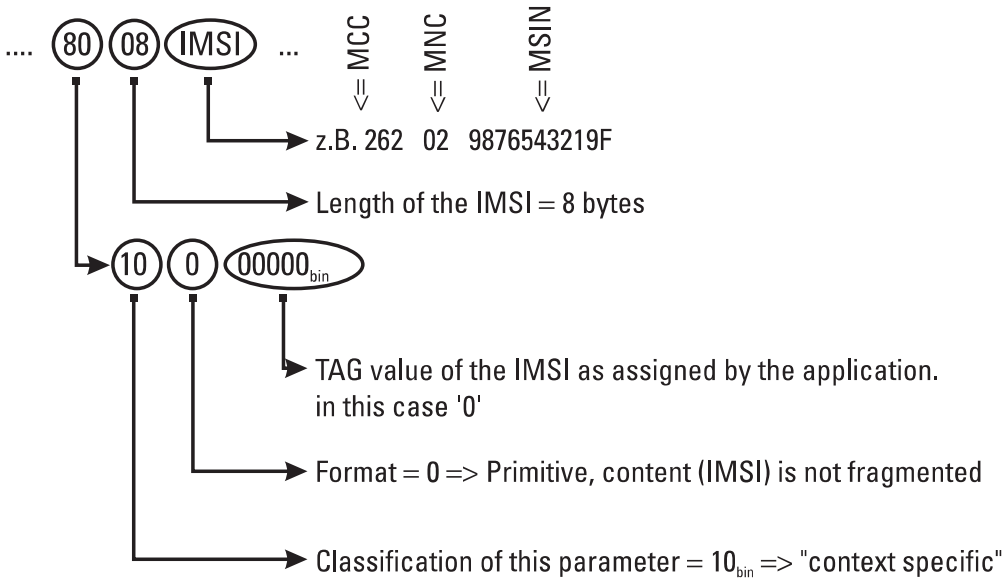


Figure 11.8 Coding of an IMSI as a primitive (with TAG and length indicator).

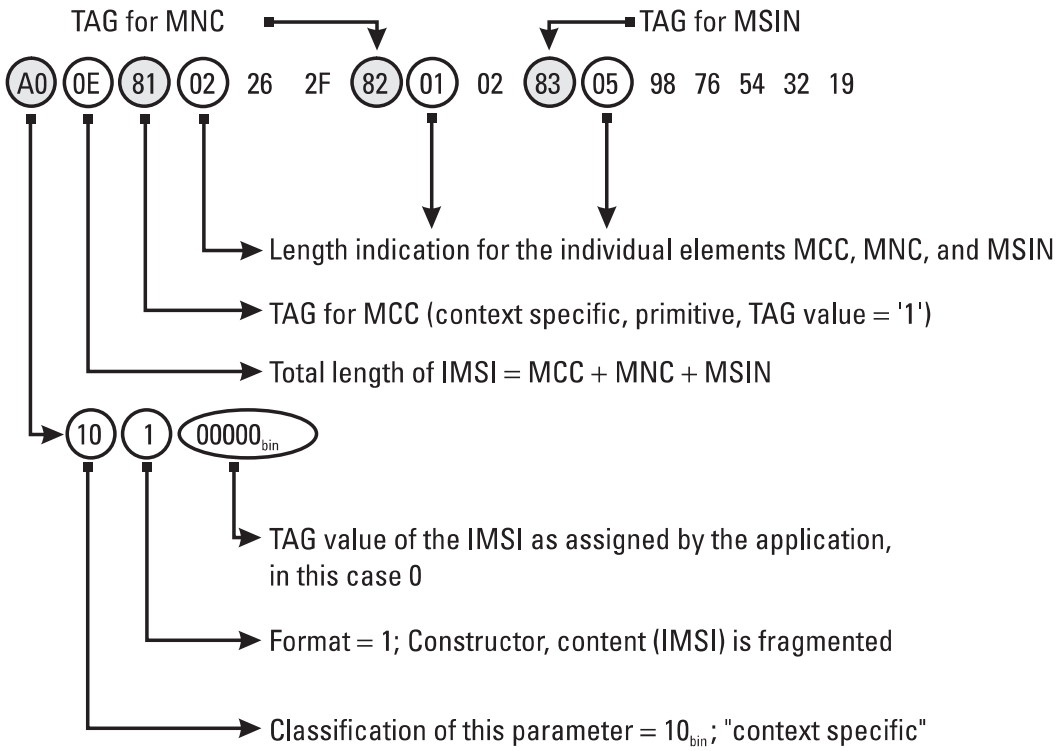


Figure 11.9 Coding of an IMSI as a constructor (with TAGs and length indicators).

MSIN are formatted as separate parameters, each requires its own TAG and length indicator, and (2) the overall length of the message increases by 6 bytes, compared to the first version.

11.1.3.3 More Options for Coding the TAG

Expansion Let us, once more, come back to Figure 11.6. The 5-bit of the TAG value field allows addressing of 31 different parameter types. That may not be enough for certain applications. Furthermore, ASN.1 has predefined most of the values (refer to the Glossary).

In addition, it may be necessary for the internal purposes of an application to assign a TAG value outside that value range (0–31).

The solution to the problem consists of the extension of the TAG to any necessary length. To do so, a special method is used, which is illustrated in Figure 11.11 and explained as follows.

- A TAG with a length of 1 byte is used for all TAG values smaller than 31_{dez}. The TAG value is binary coded. Hence, the maximum TAG value is 30_{dez} and its binary representation is 11110_{bin}.

- If the TAG value exceeds 30_{dez}, then more than one octet is required to code that value. Therefore, the value 11111_{bin} for the first byte of the TAG is reserved to indicate that the TAG is extended. In this way of coding, bits 0 through 6 of the following octets contain the actual value of the TAG. To be more precise, bits 0 through 6 represent the TAG value, while bit 7 always indicates whether another octet with a TAG value field follows. If bit 7 is set to 1, the next octet also contains TAG information; if bit 7 is set to 0, the TAG ends with this octet. Bit 6 of the *second* octet is the most significant bit (MSB), while bit 0 of the *last* octet represents the least significant bit (LSB).

Data Type Octetstring Two variants of TAG coding have been presented, the "short" and the "long" versions, which can be assigned by the user based on data type and TAG value. GSM uses yet another TAG borrowed from ASN.1. This data type is the octetstring, which is always used as the TAG when the data type does not require that an explicit identification be provided.

Data type octetstring has a fixed TAG value of 00100_{bin}, which is the representation of 4_{dez}.

For the class = universal = 00 and format = primitive = 0, the result for the TAG is 04_{hex}.

The data type octetstring was defined by ITU, in particular, to transport strings, where the individual characters are ASCII coded. The Glossary provides a complete list of all variable types and the assigned TAGs.

An example of "GSM" coded as octetstring in shown in Figure 11.10.

Note a peculiarity of MAP when it uses the octetstring TAG. When numbers need to be transmitted, the respective digits are not coded in ASCII.

Figure 11.11 illustrates the various formats for TAG and length indicators.

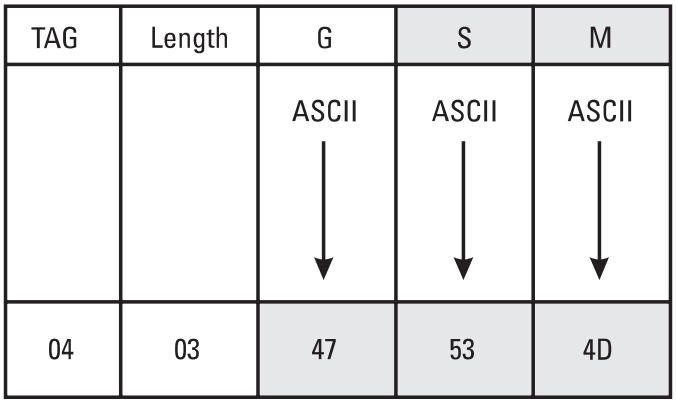


Figure 11.10 Format of octetstring.

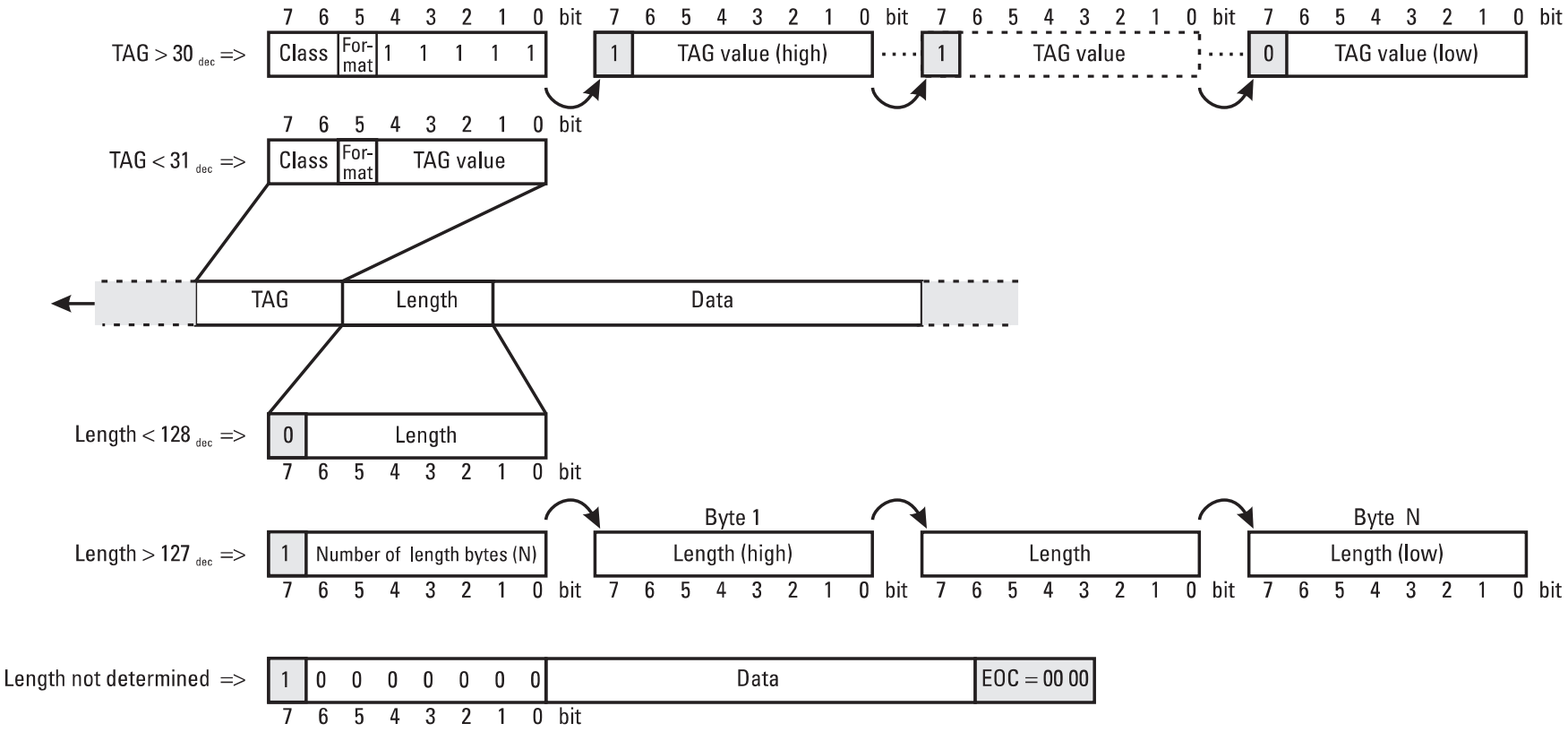


Figure 11.11 Various formats for TAG and length indicators in TCAP. Note that bit 0 is always sent first, despite the information about the direction, right to left.

11.1.3.4 Presentation of the Length Indicator

Problems similar to those described for the coding of the TAG arise in the coding of the length of a message or a parameter. The theoretical limit for coding the length field with just 1 byte is 255 bytes. For all practical purposes, that value would be suitable for the time being, because SCCP UDT messages are limited to 255 bytes. However, to be safe in the future and allow for additional applications, a solution was needed that allowed the coding of a field of any necessary (arbitrary) length.

Another requirement was that fields of undefined length be allowed, at least for constructor parameters, where MAP possibly does not know the actual length. Therefore, three different representations needed to be distinguished (see Figure 11.11).

- For "small" length (less than 128 bytes), the length indicator field is 1 byte long. Only bits 0 through 6 are used, which allows coding of values between 0 and 127_{dez} ($0111\ 1111_{bin}$). Bit 7 is always zero; hence, the limit of 255 cannot be reached.
- For a "large" length (greater than 127 bytes), the length indicator field needs to be extended by the necessary number of bytes. For that purpose, bit 7 is set to 1 and bits 0 through 6 then indicate the number of bytes to follow, which carry length information. For example, when the first byte of the length indicator field is coded as $1000\ 0111_{bin}$, then 7 bytes ($111_{bin} = 7$) of length information will follow, for a total of 8 bytes of length information.
- For an undefined length, the length indicator field is 1 byte long and is fix-coded with 80_{hex}. Here, bits 0 through 6 are all of 0 value and bit 7 is set to 1. However, the end of a parameter with undefined length needs to be indicated, too. For that purpose, a special end mark, the end of contents (EOC), is added. The EOC consists of 2 bytes, coded with all zeroes. Note that an undefined length indication may be used only for constructor parameters.

11.1.3.5 "Large" TAG and Length Indicator

In this example, a parameter needs to be coded for the transmission via TCAP. TAG and length are as follows:

$$\text{TAG type} = 2222_{dez} = 08AE_{hex} = 0000\ 1000\ 1010\ 1110_{bin}$$

$$\text{length} = 3333_{dez} = 0D05_{hex} = 0000\ 1101\ 0000\ 0101_{bin}$$

This represents a parameter of class "constructor" with the format "context specific." In both cases, 1 byte is not enough to code the particular fields. The value for TAG is greater than 30 and the length is greater than 127. For that reason the expanded form has to be applied.

The TAG

Three bytes are necessary to represent the TAG, as shown in Figure 11.12(a). Byte 1 is used to define class and format, while bytes 2 and 3 contain the actual TAG value.

- The value for class is 10_{bin} = context specific.
- The value for format (F) is 1_{bin} = constructor.
- The value for TAG of the first byte is 11111_{bin} and indicates that the TAG is expanded.
- The actual TAG value of 0000 1000 1010 1110_{bin} needs to be coded within bytes 2 and 3 and then be inserted right-aligned. Bit 7 may not be used and leading zeros are omitted.

Coding of the type TAG, therefore, is BF 91 $2E_{hex}$.

The Length Indicator

The length indicator itself requires 2 bytes ($0D05_{hex}$). Together with the first byte (to indicate an extended length field), that totals 3 bytes, as shown in Figure 11.12(b):

Byte 1								Byte 2								Byte 3							
Class F				TAG extended				E	TAG value (high)							E	TAG value (low)						
bit								bit								bit							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
1	0	1	1	1	1	1	1	1	X	X	X	X	X	X	X	0	X	X	X	X	X	X	X
1	0	1	1	1	1	1	1	1	0	0	1	0	0	0	1	0	0	1	0	1	1	1	0
B				F				9				1				2				E			

11.12(a) Coding a large TAG.

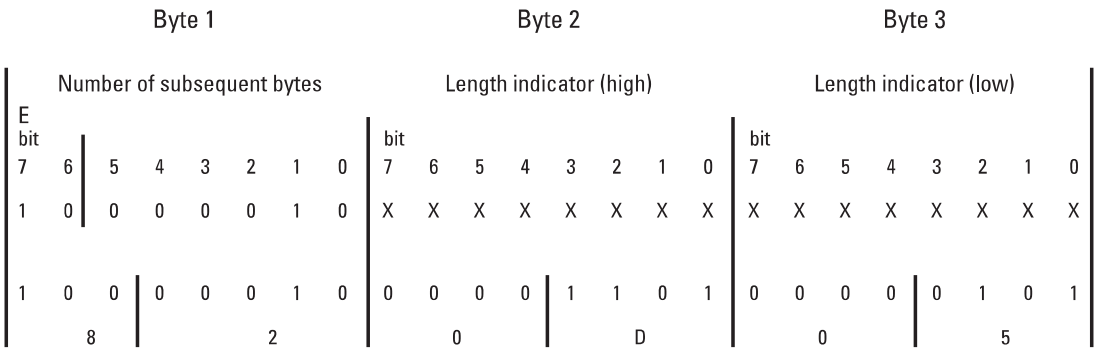


Figure 11.12(b) Coding a large length indication.

- Bit seven of the first byte is the extension mark and needs to be set to 1.
- Because the actual length requires 2 additional bytes, bits 0–6 have to be coded with a value of $000\ 0010_{bin} = 2$.
- Now, the value for the length ($0D05_{hex}$) is inserted into bytes 2 and 3, starting from the right.

Coding of the length, therefore, is $82\ 0D\ 05_{hex}$.

11.1.4 TCAP Messages Used in GSM

ITU-T, in its Recommendations Q.772 and Q.773, has defined five TCAP messages, of which GSM uses four. The four messages used in GSM are illustrated in Figure 11.13. The white areas in Figure 11.13 are optional parts; the mandatory parts are shaded.

Table 11.2 provides details on the various TCAP messages. Note that the messages form only the transport container for the MAP content.

11.1.4.1 The Dialog Portion

The dialog control of TCAP messages was mentioned at the beginning of this chapter. The dialog control is, together with some further information, part of the optional dialog portion of a TCAP message (see Figure 11.15).

Structured Versus Unstructured Dialog

The term *dialog portion* has a meaning different from that of the term *dialog*. A dialog refers to the whole communication process of exchanging information between users. One has to distinguish between an unstructured dialog and a structured dialog. GSM uses the services of the structured dialog only. For that

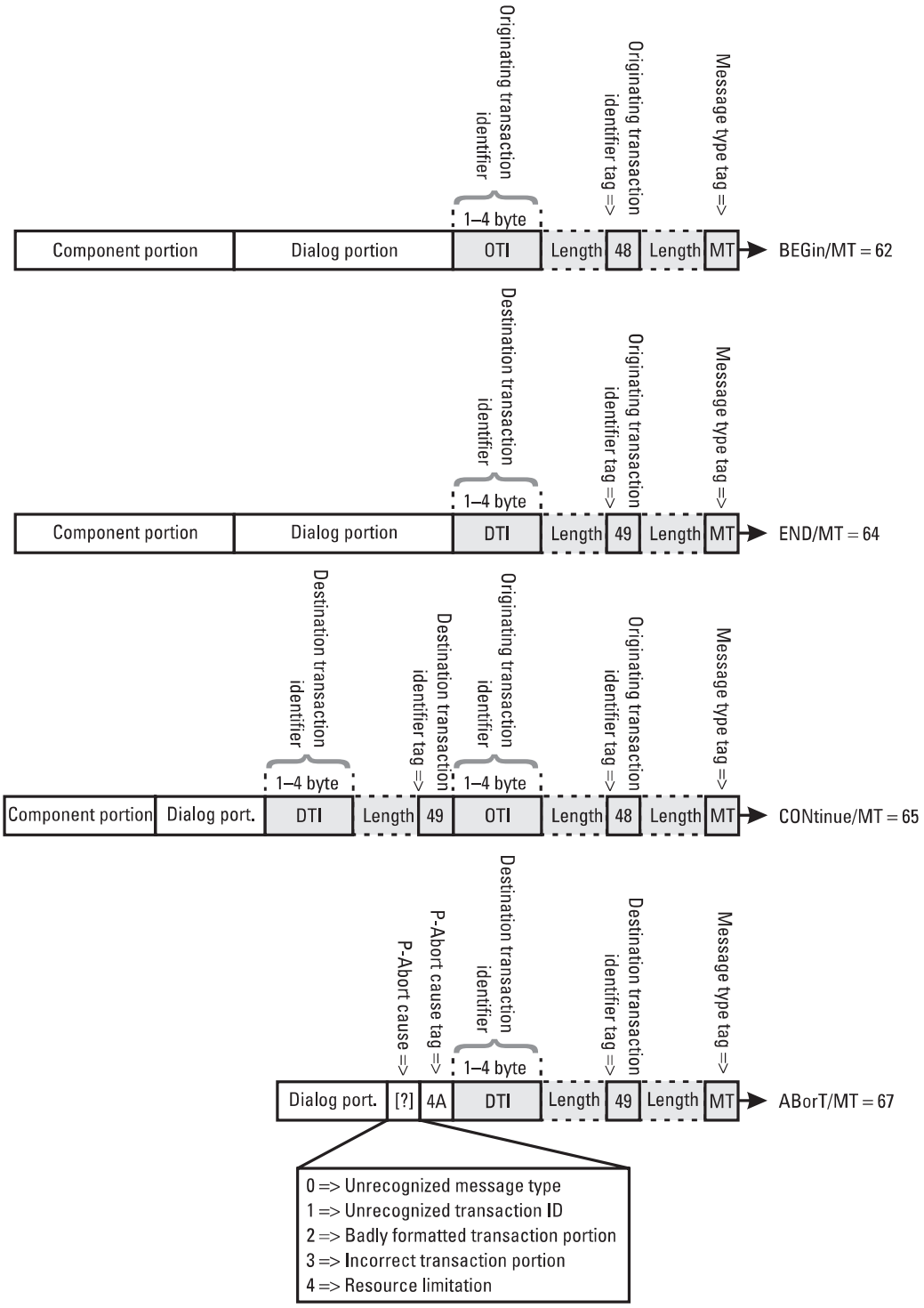


Figure 11.13 TCAP messages used in GSM.

reason, unstructured dialog will not be dealt with in more detail. However, it should be mentioned that unstructured dialog, when used, is transmitted in a

Table 11.2
TCAP Messages Used in GSM

ID (Hex)	Name	Abbr.	Interface	Description
62	BEGin	BEG	all NSS	By sending a BEG message, TCAP opens a dialog for one user (this is MAP in the case of GSM) to another user. The BEG message comprises the originating transaction identifier, which identifies a dialog within TCAP, or more precisely, within the transaction layer. Additionally, the invoke ID of the optional component part may be used to identify the dialog.
64	END	END	all NSS	An END message is sent specifically, when a process needs to be terminated, which was started by a BEG message. An END message may be the direct response to a BEG message. The END message also has an optional component part, which may contain MAP data.
65	CONtinue	CON	all NSS	The CON message is used between the begining and ending of a process in order to transport information between MAP users. A CON message comprises both an originating transaction identifier as well as a destination transaction identifier. The first CON message, which is sent after a BEG message, confirms that the requested protocol and application context are accepted.
67	ABorT	ABT	all NSS	Both TCAP and MAP may use the ABT message to terminate a process at any time if an error occurs or if a request cannot be processed. A reason for termination may or may not be provided. A distinction is made, however, between the source for termination. When the *service provider*, which is TCAP, initiates the termination, *P-ABORT* is used, when the *user*, which is MAP initiates the termination, U-ABORT is used. For the first category, the ABT message provides a P-Abort-Cause field. In the second case, the reason for abortion is sent within the field *Dialog Control*. A frequent reason for the abortion of a process is the incompatibility between the protocol versions of MAP (application context name) in the two peers of a dialog. One side, for example, requests an old or a new protocol, which the partner does no longer or not yet support.

UNI message. The difference between the two dialog types is that unstructured dialog actually is not a real dialog but a one-time data transmission, in which the sender does not expect any feedback or answer. In contrast, structured dialog consists of the beginning, the execution, and the termination of a communication process between two peers, as illustrated in Figure 11.14.

A user opens a structured dialog by sending a BEG message. The BEG message identifies a transaction on the serving side by means of the originating transaction identifier. If the addressee is able to accept the dialog, then it answers with a CON message, which contains both an originating transaction identifier and a destination transaction identifier. Following that, both sides may continue to send additional CON messages. To end a dialog, one side sends an END message.

In the case of a very short dialog, the process consists only of a BEG message and an END message.

The Dialog Unit

This optional area in a TCAP message is used to allow both end points of a connection to synchronize processing of the data, contained in the component part. Three different dialog units have been defined as part of the dialog portion:

- The dialog request: proposal of a protocol;
- The dialog response: confirmation of the proposed protocol;
- The dialog abort: termination of a dialog (may or may not be related to the proposed protocol).

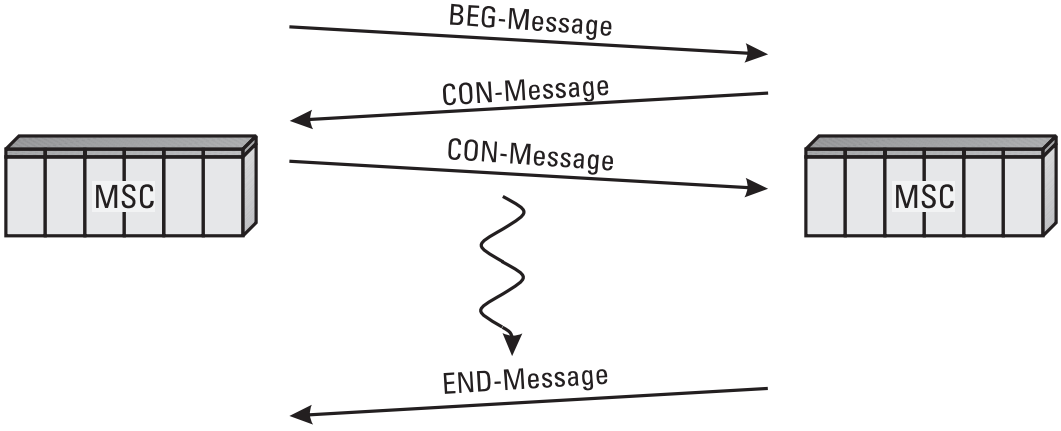


Figure 11.14 The structured dialog in an MSC-to-MSC transaction.

Figures 11.15(a) and 11.15(b) show the formatting of the dialog request, dialog response, and dialog abort. Exactly one dialog unit may be present per TCAP message.

The dialog request can be compared to a negotiation between two individuals about which language their conversation will be in. TCAP uses the application context name for those discussions that contain an identifier for the standard and the protocol that will be used for a transaction.

In GSM, the string

Ccitt-identified-organization.etsi.mobileDomain.gsm-Network.ac-id
Application Context Name. Version

tells the recipient exactly which MAP module in what version is proposed by the sender. Every parameter of that string is represented in a TCAP message by exactly 1 byte. In this context, *parameter* means a part of the string that lies between two dots. Depending on the position and the value of a byte, the meaning of the value, for example, 01 for the fourth byte is gsm-Network. For the GSM-MAP, only the last three bytes are actually usable:

- Byte 5: ac-id application context identification (always the same);
- Byte 6: value for ac-id (assigned by GSM);
- Byte 7: version number of ac-id (e.g., Phase 1 or Phase 2).

For example, in the context of a location update or an IMSI detach, the application context [networkLocUp V2] is used by the VLR for communication with the HLR. That corresponds to the byte sequence 01 02 (examined in more detail in Chapter 12). The information is sent to the HLR, together with the leading five bytes, which are always coded with a fixed value. The received application context name allows the HLR to derive the information, which software module needs to be used, or how the data within the component portion shall be treated.

As already indicated, TCAP and MAP follow the ASN.1 when coding data. The same applies for the dialog unit. That explains terms like *object descriptor* and *external*, the values of which are listed in the Glossary entry *ASN.1*.

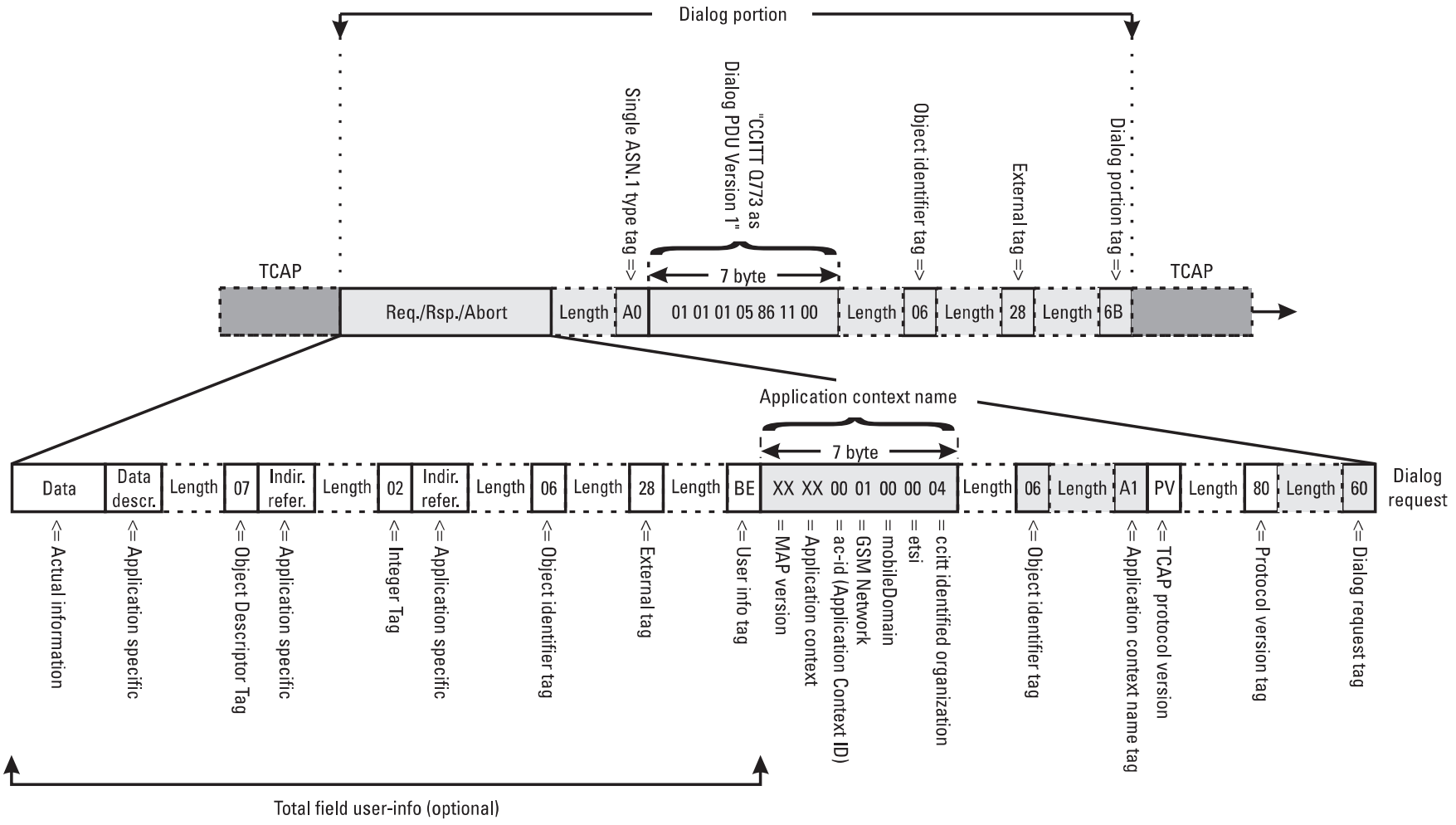


Figure 11.15(a) The dialog portion (part 1).

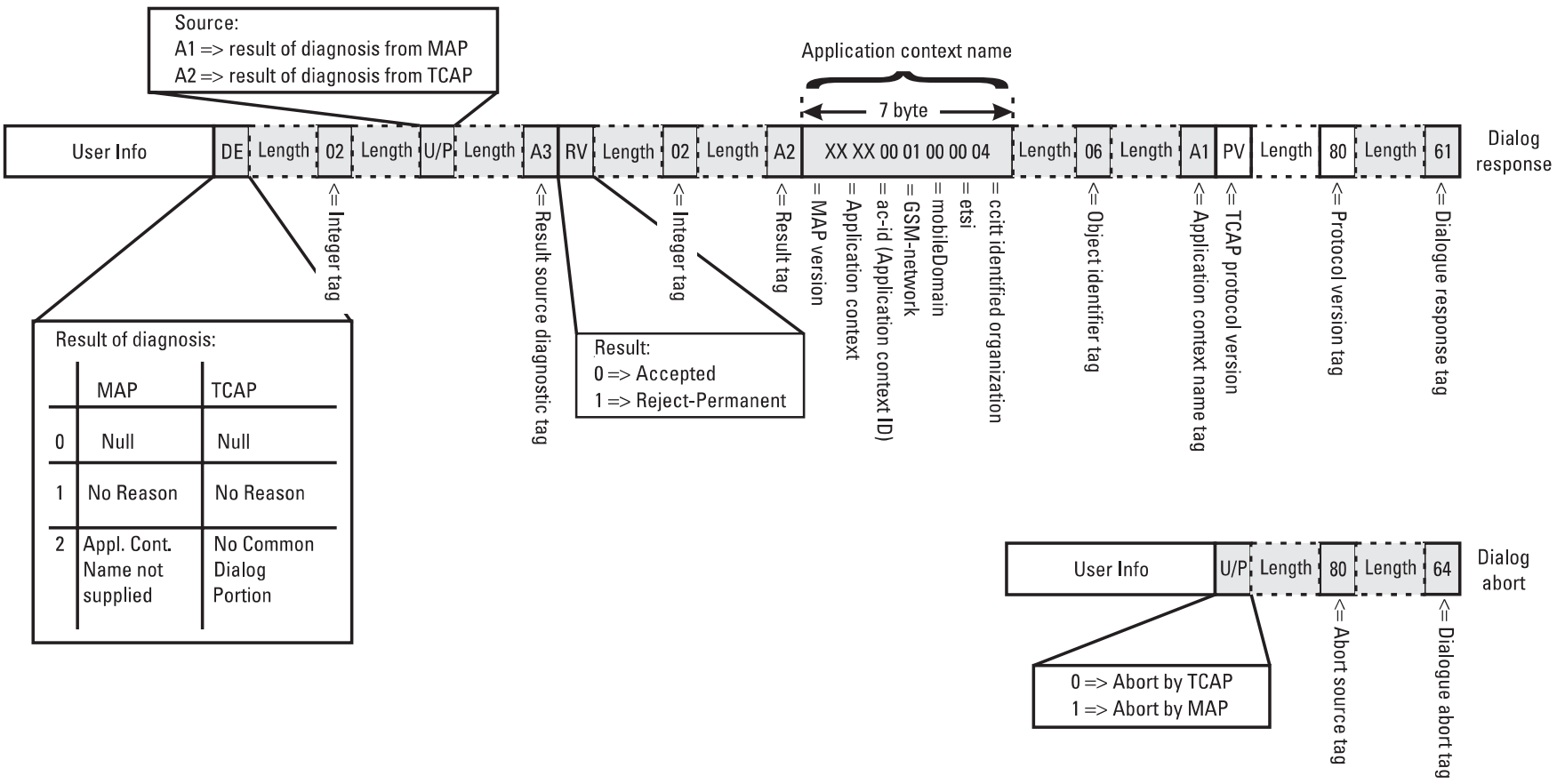


Figure 11.15(b) The dialog portion (part 2).

11.1.4.2 The Component Portion

The component portion, if present, contains the actual user data. This is MAP signaling information in the case of GSM. Different units have been defined for the component portion, just as for the dialog portion. Figures 11.16(a) and 11.16(b) describe these components.

Invoke Component

The invoke component starts an operation on the receiver side. An operation is defined by the operation code and is application specific. In GSM, the MAP operation codes correspond to these operation codes (see Section 11.2.3). Similar to the message types in other signaling standards like SS7, these values indicate the composition of the parameter field that follows.

Every component contains an invoke ID, to allow for different components to be unambiguously dedicated to an operation or a dialog. The invoke component also may contain a linked ID, to allow relations between different dialogs. The linked ID contains the value of the invoke ID of the second dialog, which is linked to the first.

The MAP user data are carried in the optional parameter field of an invoke component.

Return Result Component

The return result component (*last* and *not last*) is the result of a dialog opened by an invoke component and is transported in a return result component. Note that because of the limited capacity of UDT messages the transmission of result data might be segmented. In that case, the return result (*not last*) component is used for all data segments but the very last one (as shown in Figure 11.17). Note that the last result data segment is always transferred in a return result (*last*) component. Of course, that also applies if no segmentation was necessary.

Return Error Component

A return error component is the answer to an invoke component if an operation cannot be completed successfully. "Not successful" does not necessarily mean some sort of protocol error; it could refer to other problems, like a subscriber not responding to paging or that a particular IMSI is unknown in the HLR. Figure 11.16(b) shows examples of local error codes. Furthermore, the example in Section 11.1.4.3 shows the decoding of a TCAP message that contains a return error component.

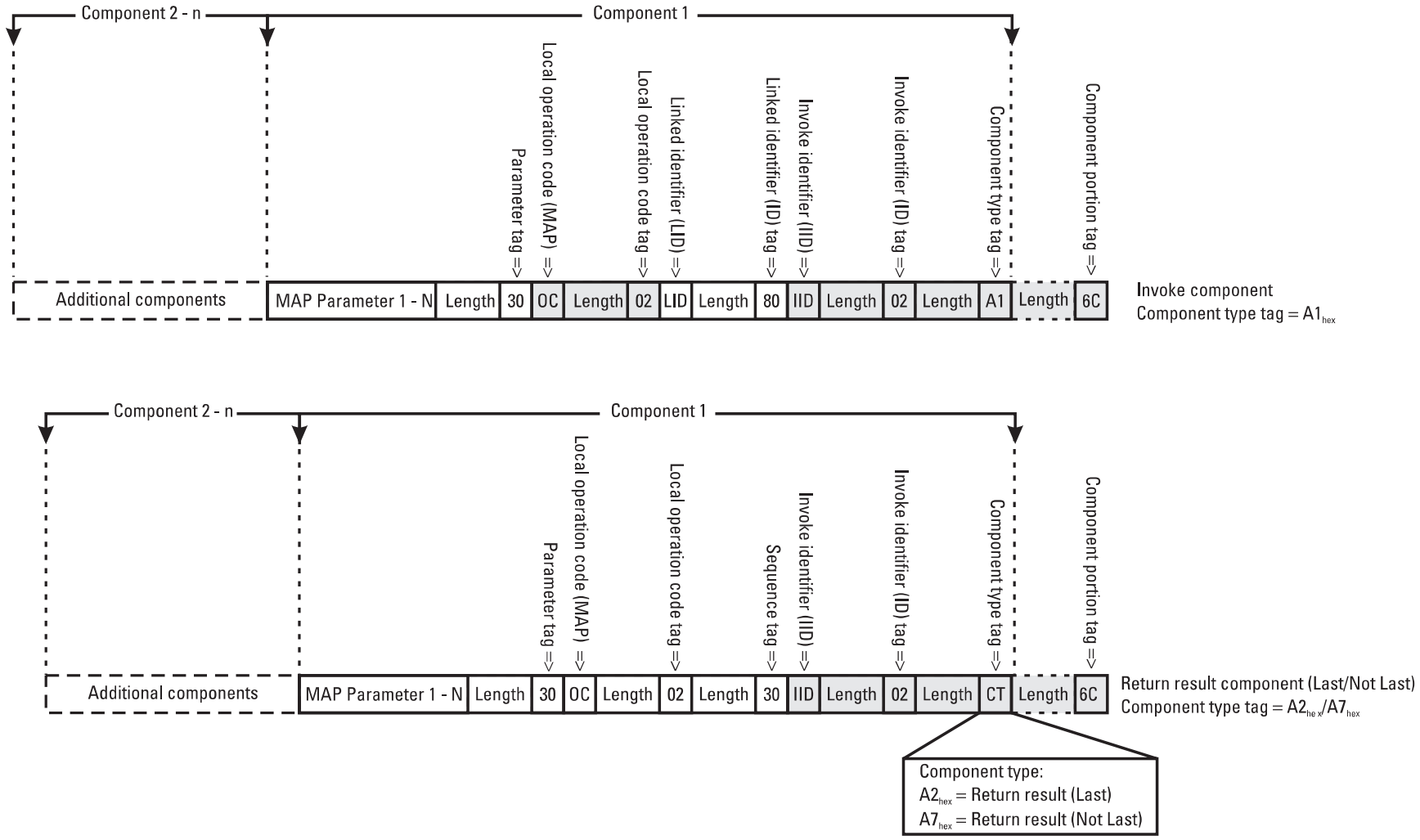


Figure 11.16(a) The component portion (part 1).

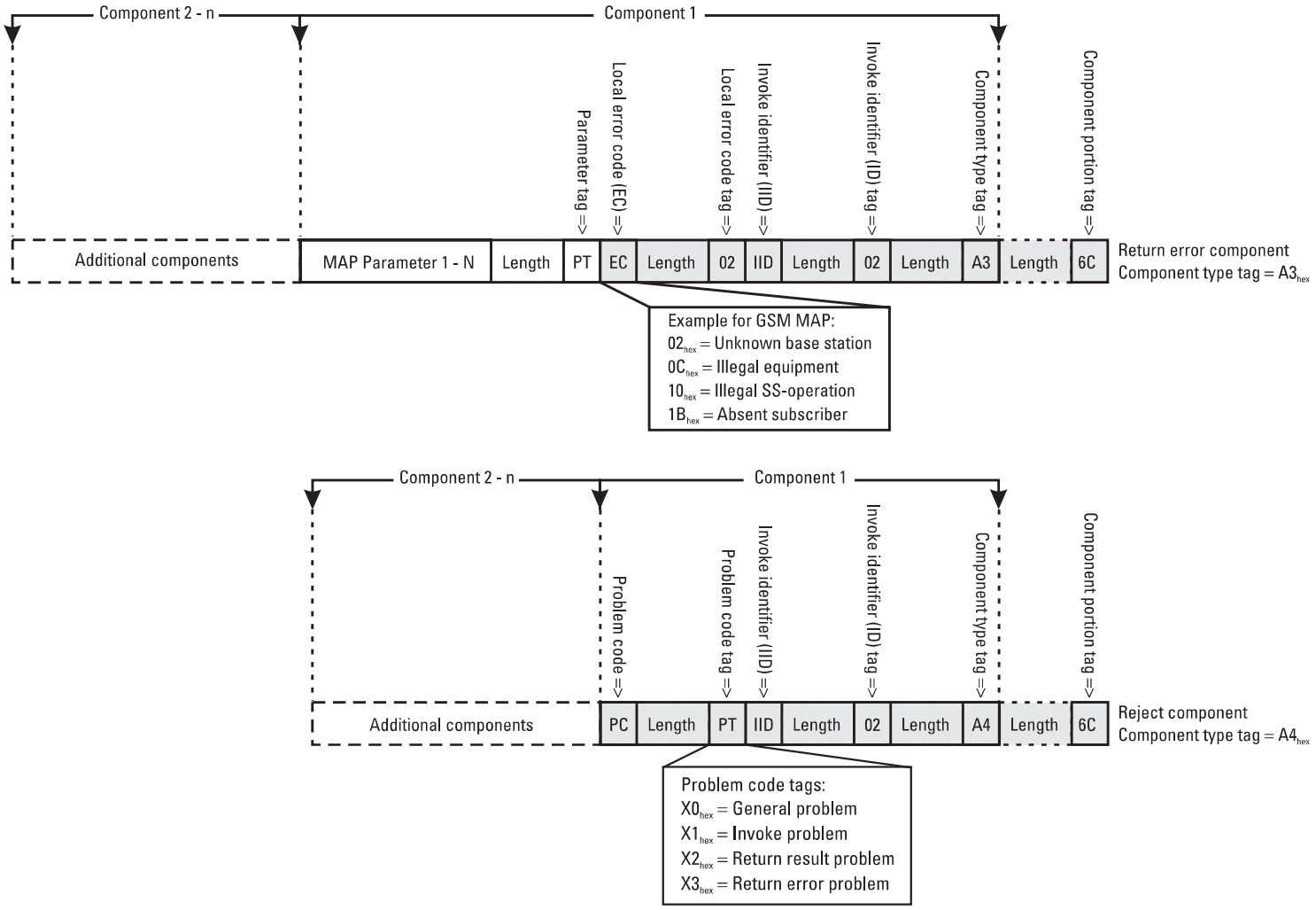


Figure 11.16(b) The component portion (part 2).

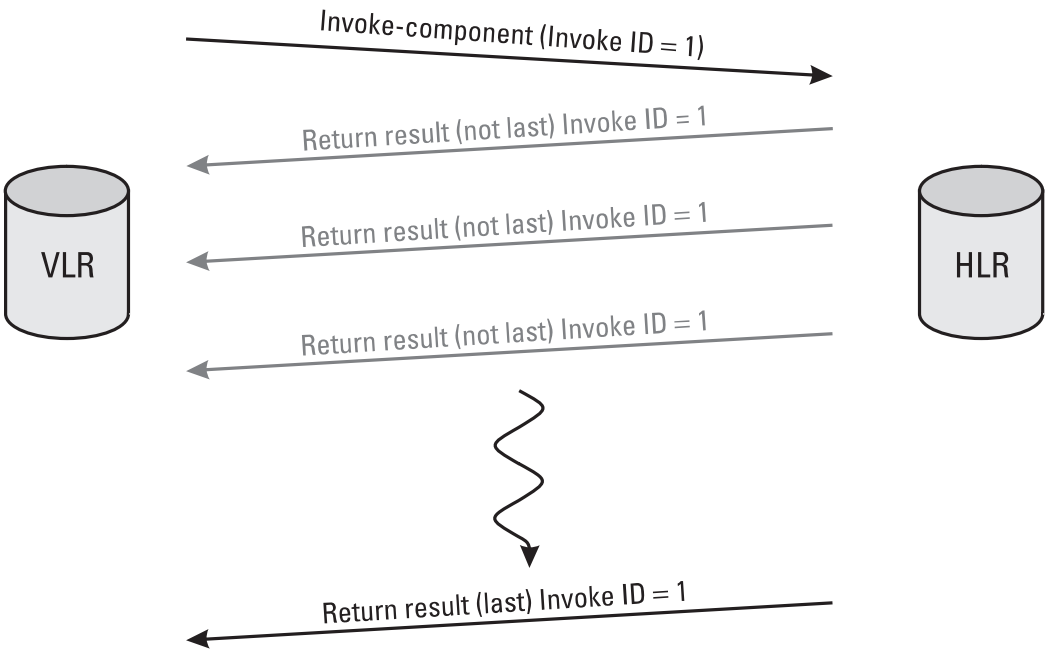


Figure 11.17 Use of the return result (*last*) and (*not last*) components.

Reject Component

If an application is unable to process a component because of errors, the problem is conveyed to the sender by a reject component. With the exception of the reject component itself, every component may be rejected.

The available error causes are categorized into four groups, as listed in Table 11.3. The numbers in the table correspond to the Problem Code (PC) in Figure 11.16(b).

11.1.4.3 Decoding of an END Message With Dialog and Component Portions

Figure 11.18 shows an extract of a trace file that was captured by a protocol tester. The trace file presents the TCAP content of an END message, sent from a VLR to an HLR. Although a return error is reported, there is no real error, simply the feedback that paging for a subscriber was unsuccessful. This example also illustrates how TAG and length indications affect the size of a message.

11.2 Mobile Application Part

The MAP was mentioned frequently in the first part of this chapter. The reason for this is the tight cooperation between MAP and TCAP in the NSS. This second section focuses on the processes and procedures within MAP itself; the

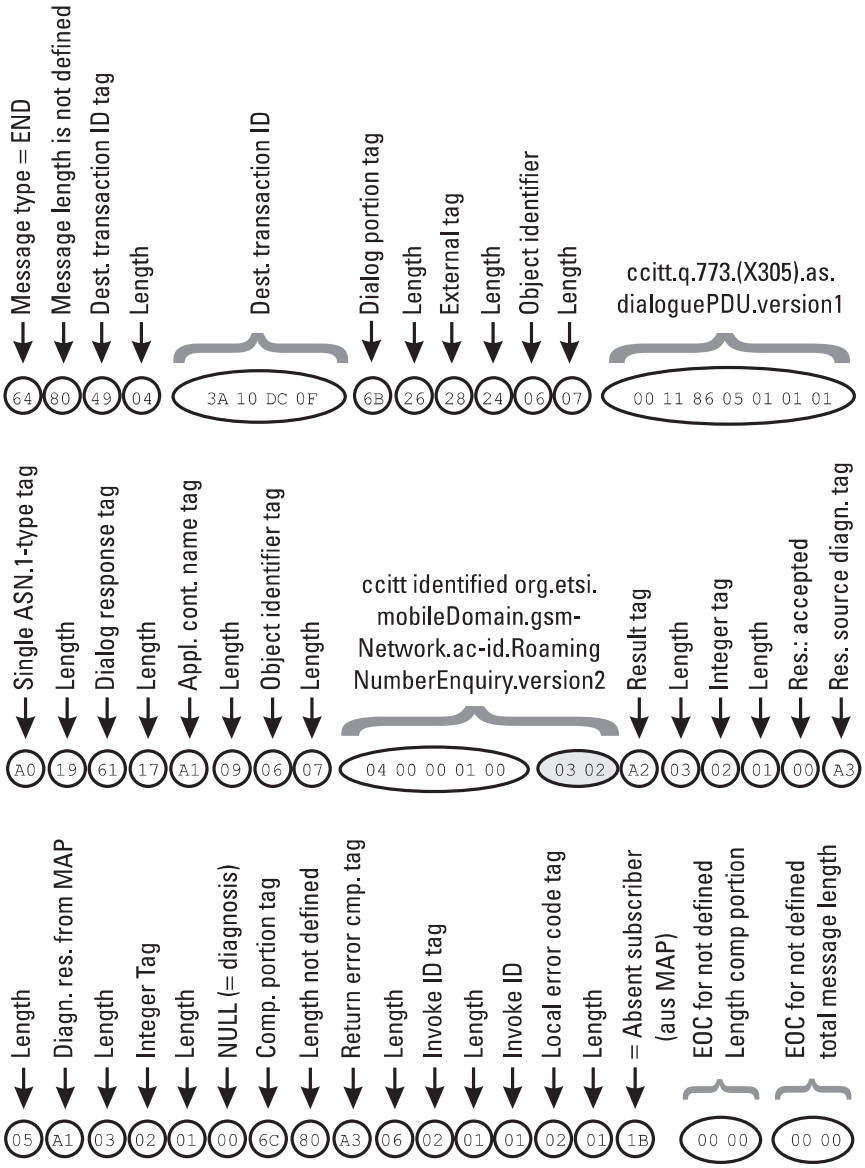
Table 11.3
Problem Codes for the Reject Component

General problem (X0):	
0	Unrecognized component
1	Mistyped component
2	Badly structured component
Invoke problem (X1)	
0	Duplicate invoke ID
1	Unrecognized operation
2	Mistyped parameter
3	Resource limitation
4	Initiating release
5	Unrecognized linked ID
6	Linked response unexpected
7	Unexpected linked operation
Return result problem (X2)	
0	Unrecognized invoke ID
1	Return result unexpected
2	Mistyped parameter
Return error problem (X3)	
0	Unrecognized invoke ID
1	Return error unexpected
2	Unrecognized error
3	Unexpected error
4	Mistyped parameter

emphasis will be on MAP as the interface or adapter between TCAP and the application.

11.2.1 Communication Between MAP and its Users

All the signaling protocols introduced so far, from LAPD through TCAP, are peer-to-peer protocols, that is, horizontal protocols, in the way the OSI



In plain text:

```
END
  Destination Transaction ID (hex) : 3A 10 DC 0F
  Dialogue Portion
    Protocol : {ccitt.Q.773.as.dialoguePDU.version1}
    Dialogue Response
      Application Context Name : {ccitt-ident-org.etsi.mobileDomain.gsm-Network
      ac-id.RoamingNumberEnquiry.version2}
      Result : 0 = accepted
      Result-Source-Diagnostic
        dialogue-service-user : 0 = null
  Component
    Return Error
      Invoke ID : 1
      Error Code
        Local Value : 27 = Absent Subscriber
```

Figure 11.18 Decoding of an END message.

Reference Model considers them. The primitives, as the carrier of vertical data exchange, were neglected. Nevertheless, LAPD, SCCP, and TCAP all need primitives to communicate with the adjacent higher or lower layer. For the reader's comprehension, these primitives were of less importance. The situation is different for the communication between MAP and TCAP, so this is the time to discuss primitives in more detail. Figure 11.19 illustrates the relevant part of the OSI Reference Model.

Because the application itself (HLR, VLR, etc.) is not part of the OSI Reference Model, so-called MAP services are required for control tasks and data exchange between the different applications and MAP. The MAP services actually are primitives. Let's use the expression *MAP application* as a collective term for all involved GSM subsystems, from the MSC to the EIR.

11.2.2 MAP Services

The communication between MAP and an application is done via MAP services, in which we have to distinguish between common MAP services for pure communication control between MAP and application and special MAP services as the carrier of signaling data. Both variants are dealt with in the following sections.

11.2.2.1 Direction Dependency of MAP Services

The tasks of Layers 1 through 7 of the OSI Reference Model are transparent for the MAP application; they can be considered as some kind of black box. The MAP application sees only the communication with MAP, which is performed by MAP services. MAP in Layer 7 receives commands and answers from the application that are conveyed to the peer entity via TCAP and the remaining layers of the OSI Reference Model. On the other hand, MAP receives commands and answers from TCAP (Layer 6) that actually come from the peer

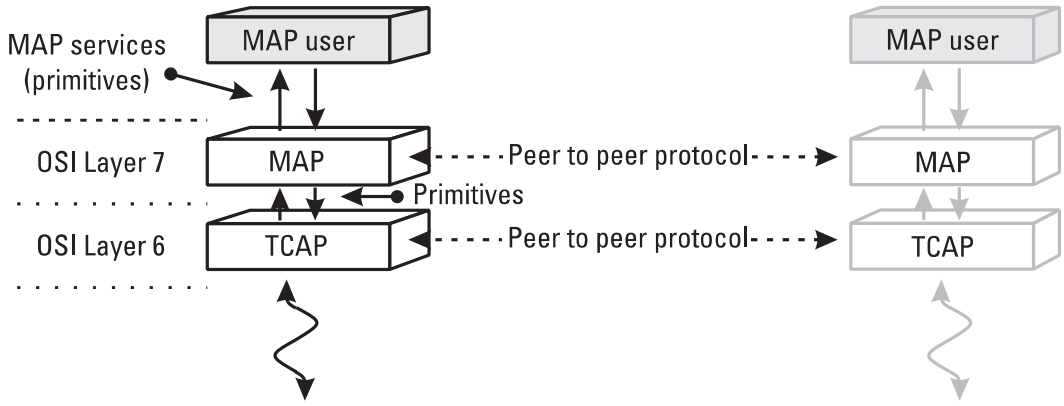


Figure 11.19 MAP in the OSI Reference Model.

entity and need to be forwarded to the application. It is important for MAP and for the MAP applications to distinguish not only between the various MAP services but also between the two possible directions of those services. For that reason, up to four different variants were defined for every MAP service (as for primitives in general). An overview is provided in Figure 11.20. Let the initiating MAP application be A and the responding MAP application be B. A sends a *request*, which translates into an *indication* on the side of MAP application B. B's answer is sent back in a *response* and translated into a *confirmation* from MAP to A. Although the differentiation is of little significance during protocol testing, it is important for a thorough comprehension of MAP.

11.2.2.2 Common MAP Services

Six common MAP services can be used to control a communication between MAP and its application. Depending on the task of the MAP service, all four or only some of the primitives—*Request*, *Indication*, *Response*, and *Confirmation*—are needed.

MAP-DELIMITER Service

By sending this primitive, the application indicates that a data packet is complete and ready to be passed to the peer entity. Such a data packet may contain a MAP-OPEN service for communication control, special MAP services (with signaling data), or both. Only the *Request* and *Indication* variants are defined for the MAP-DELIMITER service.

MAP-OPEN Service

By means of this primitive, an application requests MAP to establish a dialog with another application. The MAP-OPEN service includes the specification of the requested transaction (application context name) and identifies sender and addressee. Neither parameters nor data are included. All four primitives—*Request*, *Indication*, *Response*, and *Confirmation*—are defined for the MAP-OPEN service.

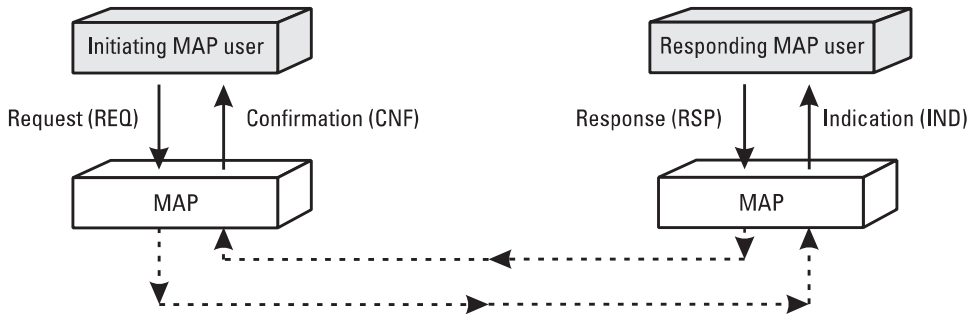


Figure 11.20 Direction dependency of MAP services.

MAP-CLOSE Service

The MAP-CLOSE service is used to terminate an existing process. The primitive is passed to the MAP and then forwarded to TCAP when a MAP application intends to terminate (not interrupt) a dialog. Only the *Request* and *Indication* variants are defined for the MAP-CLOSE service.

MAP-U-ABORT Service

The abbreviation stands for MAP User Abort and indicates that an application wants to interrupt a dialog. Only the *Request* and *Indication* variants are defined for the MAP-U-ABORT service.

MAP-P-ABORT Service

The abbreviation stands for MAP Service Provider Abort and indicates that TCAP wants to interrupt or has already interrupted a dialog. Only the *Indication* variant is defined for the MAP-P-ABORT service.

MAP-NOTICE Service

The MAP-NOTICE service provides an application with information about problems on the peer side. Only the *Indication* variant is defined for the MAP-NOTICE service. In particular, when a TCAP message with a reject component and specific problem codes is received, the MAP application gets a MAP-NOTICE service. Reasons might be protocol errors (e.g., duplicate invoke ID) or unexpected data values and parameter types.

11.2.2.3 Special MAP Services

The purpose of the common MAP services is to control the communication between MAP and its applications. Although the MAP-OPEN service already contains the application context name and, hence, the requested protocol for the dialog to be established, only a special MAP service such as *updateLocation* contains the actual parameters. Like the message type for other signaling standards, the local operation codes identify the special MAP services within MAP. As for all primitives, up to four variants (Request, Indication, Response, and Confirmation) are defined for the special MAP services. Two examples are the following:

- The local operation code *forwardAccessSignaling* is a service for transparent transmission of BSSAP data between MSCs after an inter-MSC handover. This service is nonconfirmed, that is, no acknowledgment is returned when a *forwardAccessSignaling* code is received. Therefore, only the Request and Indication variants are necessary for the *forwardAccessSignaling* service.

- The local operation code *updateLocation* is required directly after a location update for the new VLR to update the location information in the HLR. Because this is a confirmed service, it requires all four variants: Request, Indication, Response, and Confirmation.

The strange representation style of the local operation codes becomes obvious in the preceding examples. The words are concatenated without any blanks, and the first letter of the first word is in lowercase, while the first letters of all other words are uppercase. That is the defined way to present local operation codes.

11.2.3 Local Operation Codes of the Mobile Application Part

This section presents the special MAP services (local operation codes) as they are defined for GSM Phase 2. Note that GSM does not consider the B-interface, that is, the interface between MSC and VLR, to be an external interface. Therefore, no binding recommendations were made for that interface nor for the information that needs to be sent over it. For that reason, this section contains no local operation codes that are used exclusively on the B-interface.

Table 11.4 explains the tasks and the meanings of the various MAP local operation codes. The information provided in the third column indicates which interfaces the respective local operation code have used. (The Glossary and Chapter 4 provide definitions of the interfaces.)

Table 11.4
MAP Local Operation Codes

Op.-Code (Hex)	Name	Interface	Description
02	updateLocation	D	When a MS has successfully performed a location update in a new VLR area, this message is used to inform the HLR. If several MSCs are served by one VLR, then this message is also sent when the MS changes the MSC within the VLR area.
03	cancelLocation	D	When a MS roams into a new VLR area this message is used to inform the old VLR that it will delete the related subscriber data.

Table 11.4 (continued)

Op.-Code (Hex)	Name	Interface	Description
04	provideRoaming-Number	D	Is used between VLR and HLR in case of an MTC (mobile terminating call) to provide routing information to the HLR. This information, the roaming number (MSRN), is then sent to the Gateway-MSC (see also local operation code 16: sendRoutingInfo).
07	insertSubscriber-Data	D	The HLR uses this operation code to provide the VLR with the current subscriber profile, e.g., during a location update procedure.
08	deleteSubscrib-erData	D	The HLR uses this message to inform the VLR that a service (in particular a supplementary service) was removed from a subscriber profile.
0A	registerSS	B D	Is used to enter supplementary service data for a specific subscriber. This may be accompanied by an automatic activation of this supplementary service, e.g., when the subscriber enters a call forwarding number. In this case the supplementary service is automatically activated at the same time. For the MSC and the VLR, the respective data is transparent. This data is only relevant for the HLR.
0B	eraseSS	B D	This local operation code is used to delete supplementary service data for a specific subscriber that was previously entered by registerSS.
0C	activateSS	B D	By this local operation code a supplementary service is switched on for a specific subscriber. Supplementary services to be activated by the subscriber, are, for example, CLIP and CLIR. Like the other SS messages, this message is transparently passed from the MSC to the VLR and then to the HLR.
0D	deactivateSS	B D	This "turns off" a Supplementary service that was previously activated. It is the reverse operation to activateSS.
0E	interrogateSS	B D	This local operation code allows to query the state and the details regarding a Supplementary service in the HLR for a specific subscriber. With one interrogateSS message exactly one Supplementary service can be queried.

Table 11.4 (continued)

Op.-Code (Hex)	Name	Interface	Description
11	registerPassword	B/D	Is used to enter or modify a password for a Supplementary service. After the HLR has received this message, it responds with getPassword messages in order to request the old password, the new password, and to verify the new password. This operation is blocked if the old password was incorrectly entered for three consecutive times.
12	getPassword	B/D	If a subscriber wants to change the current password or modify or activate a Supplementary service, which is password protected, then the HLR requests this password in a getPassword message. This operation is blocked if the old password is incorrectly entered for three consecutive times.
16	sendRoutingInfo	C	The Gateway-MSC sends this message in case of an MTC (mobile terminating call) to the HLR of the called subscriber in order to obtain routing information. This routing information consists of the MSRN (mobile station roaming number), which is formatted like an ordinary telephone number (see in Glossary). When the HLR receives a sendRoutingInfo request it sends a provideRoamingNumber request to the VLR in which area the respective subscriber is currently roaming.
1D	sendEndSignal	E	The sendEndSignal request is used after a inter-MSC handover. After a successful handover from MSC A to MSC B, MSC B sends a sendEndSignal request to MSC A, which allows MSC A to release the radio resources. If MSC A is the MSC where the call was originally established, then it keeps the overall call control even after the inter-MSC handover. In this case, MSC A is referred to as "anchor MSC." Consequently, MSC B does not receive any information on when that call is released, i.e., when MSC B may trigger the release of its own radio resources. To cope with this situation, MSC B receives the respective information in the sendEndSignal response from MSC A.

Table 11.4 (continued)

Op.-Code (Hex)	Name	Interface	Description
21	ProcessAccess Signaling	E	An anchor-MSC keeps control of a call, even after successful handover from MSC A to MSC B. In order to establish a transparent connection between MSC A and MS, the local operation codes processAccessSignaling and forwardAccessSignaling were defined. Their task is to transfer BSSAP messages between MS and MSC A, i.e., on the path MS MSC B MSC A. The difference between the two operation codes is the direction. ProcessAccessSignaling is sent from MSC B to MSC A, hence, it carries data from the MS to MSC A, while forwardAccessSignaling is used in the reverse direction, i.e., it carries data from MSC A towards the MS.
22	ForwardAccess Signalng	E	Please refer to processAccessSignaling.
25	reset	D	Reset is only used when a HLR is brought back to service after an outage. The HLR sends this local operation code to all VLR's, in which mobile stations of that HLR are registered according to the data that is still available after the outage.
26	Forwardcheck SS-Indication	B / D	ForwardcheckSS-Indication is optional and sent to all affected mobile stations after an HLR outage. The subscriber is requested to synchronize its SS data with the network.
2B	checkIMEI	F	This local operation code is used to convey an IMEI (international mobile equipment identity) between MSC/VLR and EIR.
2D	sendRoutingInfo-ForSM	C	This local operation code is used by the SMS-Gateway-MSC during the MT-SMS procedure (mobile terminating SMS) in order to deliver a short message to the MSC as to which area the subscriber roams. This request for routing information from the SMS Gateway MSC contains the MSISDN of the subscriber, while the result contains the ISDN number (routing address) of the destination MSC. This address is used by the SCCP to forward the short message in a forwardSM message.

Table 11.4 (continued)

Op.-Code (Hex)	Name	Interface	Description
2E	forwardSM	E	The MO-SMS procedure (mobile originating SMS) as well as the MT-SMS procedure (mobile terminating SMS) is used in both cases to carry a short message between the MSC where the subscriber roams and the MSC, which has a connection to the SMS Service Center (= SMS Interworking MSC).
2F	reportSM-DeliveryStatus	C	When the transmission of a short message from the SMS Service Center to the MS was unsuccessful, (e.g., because the subscriber was not reachable) then the MSC returns a negative response to the SMS Gateway MSC. In this case, the SMS Gateway MSC sends a reportSM-DeliveryStatus to the HLR to allow for a later delivery of the short message. The HLR sets a message waiting flag in the subscriber data of the subscriber, sends an alertServiceCentre message (as an information about the negative result of the short message transfer) to the SMS Interworking MSC, and waits until the subscriber is reachable again. When the VLR, which is also aware of the unsuccessful SM delivery, detects that the subscriber is reachable again it sends a readyforSM message. When the HLR receives this message it reacts with an alertServiceCentre message to the SMS Interworking MSC, which in turn informs the SMS Service Center. Now the delivery process to the MS can start again with a forwardSM message.
32	activateTrace-Mode	D	Is used by the HLR to activate the trace mode for a particular subscriber (IMSI). Note that the request for subscriber tracking is not originated by the HLR but the OMC. After receiving an activateTraceMode request, the VLR waits until that particular MS becomes active. When this is the case, the VLR sends an internal request to the MSC to trace the MS. In contrast to most other MAP operation codes, no acknowledgment is expected in case of activateTraceMode. The results are directly passed from the BSS/MSC to the OMC.
33	deactivateTrace-Mode	D	When the HLR receives this operation code it turns the active trace mode off (see activateTraceMode).

Table 11.4 (continued)

Op.-Code (Hex)	Name	Interface	Description
37	sendIdentification	G	When an MS changes the VLR area the new VLR queries the old VLR with sendIdentification for the currently valid authentication data. If the new VLR is unable to identify the old VLR, e.g., when the PLMN is changed as well, then this information can also be retrieved from the HLR, in this case by means of sendAuthenticationInfo.
38	sendAuthenticationInfo	D	Please refer to sendIdentification.
39	restoreData	D	When a VLR receives a provideRoamingNumber request from the HLR for a) an IMSI, unknown in the VLR or b) an IMSI, where the VLR entry is unreliable after an HLR outage, then the VLR sends a restoreData request to the HLR, in order to synchronize the data between VLR and HLR.
3A	SendIMSI	D	When the VLR receives a request from the OMC to identify a subscriber, based on his MSISDN (directory number) then this request is handled by the exchange of sendIMSI operation codes between VLR and HLR.
3B	processUnstructuredSS Request	B/D	This operation code is used to provide means for the handling of additional, non-GSM standardized supplementary services within a PLMN (the unstructured supplementary services). Unlike unstructuredSS-Request, processUnstructuredSS Request is used by both sides, the MS and the addressed NSS entity, if the MS has initiated the transaction.
3C	unstructuredSS-Request	B/D	This operation code is used to provide means for the handling of additional, non-GSM standardized supplementary services within a PLMN (the so-called unstructured supplementary services). unstructuredSSRequest is used by both sides, if the request was initiated by the NSS.
3D	unstructuredSS-Notify	B/D	Unlike processUnstructuredSSRequest and unstructuredSSRequest, unstructuredSSNotify is used when an additional feature in the NSS needs to transport USSD (unstructured supplementary services data) to the MS, without expecting an acknowledgment from the subscriber. The MS, however, confirms receipt of the corresponding data by returning an empty unstructuredSSNotify (FACILITY message on the Air-interface).

Table 11.4 (continued)

Op.-Code (Hex)	Name	Interface	Description
3F	informService-Centre	C	The HLR sends this operation code to the SMS Gateway MSC, when a sendRoutingInfoForSM was received for a subscriber who is currently not available.
40	AlertService-Centre	C	Please refer to reportSM-DeliveryStatus
42	readyForSM	D	Please refer to reportSM-DeliveryStatus
43	purgeMS	D	If a MS was inactive for an extended period of time, that is, no call or location update was performed, then the VLR sends a purgeMS request to the HLR. This indicates that the VLR has deleted the data for that particular MS. The HLR sets the "MS Purged" flag and no longer attempts to reach the MS in case of an incoming call.
44	prepareHandover	E	At the beginning of a inter-MSC handover (MSC A MSC B) a prepareHandover request and response is sent between both MSCs in order to exchange BSSAP messages and to trigger the activation of a TCH in MSC B. The prepareHandover message is used in particular to transport the handover number and the two BSSMAP messages: HND_REQ and HND_REQ_ACK.
45	prepareSubsequent Handover	E	If after an inter-MSC handover another inter-MSC handover should become necessary, either back to MSC A or to a third MSC (MSC C), then MSC B sends a prepareSubsequentHandover message to MSC A. This message contains all necessary information for MSC A to send a prepareHandover message to MSC C.

11.2.4 Communication Between Application, MAP, and TCAP

An application communicates with MAP by means of common MAP services and special MAP services. But how does MAP pass these services to TCAP? And how does TCAP pass information it receives, commands, and responses to MAP? This section provides answers to those questions.

The term *dialog* stems from the vocabulary of TCAP and addresses the exchange of data between two TCAP users. GSM uses only the services of the so-called structured dialog, which is used when, upon delivery of data, a reaction, an acknowledgment, or an answer is expected from the recipient.

With respect to data transmission between MAP, TCAP, and application, this restriction simplifies the situation, since a dialog between MAP applications always has to be structured. That requires, from the perspective of TCAP, that it starts with a BEGIN message and, in case of no errors, terminates with an END message. A special case is the abortion of a dialog with an ABORT message, which can be sent by either MAP or TCAP.

Figure 11.21 illustrates, by means of the example of the cancelLocation service, how the MAP services are applied internally. Note that the primitives between MAP and TCAP are not shown. The cancelLocation service is required after a location update if a MS has changed the VLR area and the subscriber data in the old VLR need to be deleted.

- The application, in this case, the HLR, transfers a MAP-OPEN service REQ to MAP. It contains the ISDN addresses of VLR and HLR which are required for addressing by the SCCP. Furthermore, the MAP-OPEN service REQ contains the requested application context name for the dialog, in this case, [LocationCancel.version2] = [2.2]. This application context is required for the TCAP dialog portion.
- The message in the frame with double lines shows the special MAP cancelLocation service REQ which carries the actual signaling data, which in this case is the invoke ID, IMSI, and the local mobile subscriber identity (LMSI). These data are transported in the component portion of the subsequent TCAP message.
- The application requests MAP, by means of the MAP-DELIMITER service REQ, to pass all the information to TCAP.
- In this situation, TCAP will send a BEG message to the requested address that includes the corresponding dialog and component portions.
- The TCAP entity on the side of the VLR receives a BEG message after SS7 and SCCP have properly routed that message to the VLR, and passes the information in a primitive to MAP. If MAP does not know this specific application context, it sends an ABORT primitive back to TCAP. In such cases, the application in the VLR does not receive any indication.
- In the positive case, if the VLR supports the application context then MAP passes the address information and the application context in a MAP-OPEN IND to the application, in this case, to the VLR. The application context allows the VLR to conclude how the received data have to be processed. At this stage, the VLR does not yet know the identity of the subscriber whose entry is to be deleted.

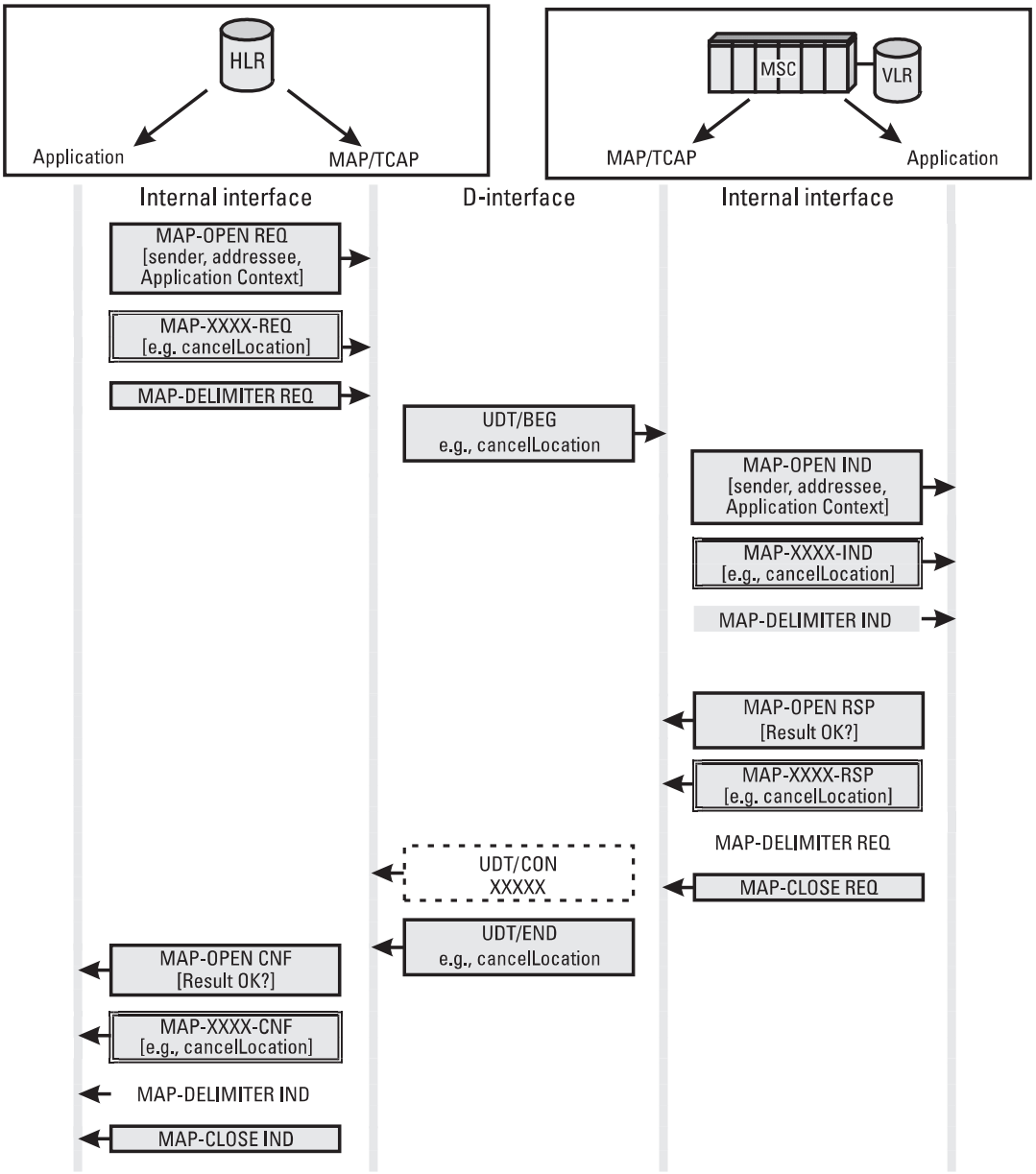


Figure 11.21 Interaction of application, MAP, and TCAP during cancelLocation.

- Exactly this information is provided by the MAP cancelLocation service IND, which corresponds to the content of the component portion of the TCAP BEG message. In Figure 11.21, the primitive is presented in a double-lined frame.
- When the VLR has received and evaluated all necessary information, it deletes the corresponding subscriber data, including the LMSI. Then the VLR responds to MAP in a MAP-OPEN RSP, which contains the information as to whether the result was positive

or negative but not the address information previously received in MAP-OPEN IND.

- The invoke ID is included in the MAP cancelLocation service RSP, sent to MAP.
- In the scenario in Figure 11.21, the next message sent to MAP is the MAP-DELIMITER REQ. This message is sent, however, only when a dialog should not be closed but continued. A MAP-CLOSE REQ is sent in the case of the cancelLocation process. Thus, the MAP-DELIMITER REQ is marked as optional.
- Now, the difference between closing and continuing a dialog becomes more obvious. TCAP would use a CON message, to respond to the VLR in case the dialog needs to be continued (if MAP-DELIMITER REQ was received). In case of cancelLocation or as a reaction or response to the MAP-CLOSE REQ, TCAP sends an END message back to the HLR.
- You might wonder at this point if the confirmation for the opening of the dialog is still pending in the HLR. That is taken care of by sending the MAP-OPEN CNF from MAP to the HLR, after the TCAP-END message is received. The same applies for the special MAP service cancelLocation.
- Receipt of MAP-CLOSE IND terminates the dialog on both sides.

12

Scenarios

This chapter applies the acquired knowledge base of the previous chapters to describe the various GSM subsystems via signaling protocols. Every presented scenario is explained in detail.

Before presenting those details, however, the commonality, or "red thread" of the scenarios should be emphasized. For that purpose, the block diagram in Figure 12.1 applies to all: MOC (mobile originating call), MTC (mobile terminating call), and LU (location update). The following is an explanation of the individual blocks in Figure 12.1:

- Only in a MTC does the network search for a particular subscriber (paging).
- When the MS is located or when the MS initiates a call, a control channel between MS and BSC has to be established.
- The MS uses the control channel for identification and indicates to the BSC in detail which service is requested.
- The BSC passes the service request of the MS to the NSS. For that purpose, the BSS has to request an SCCP connection from the MSC.
- The NSS reacts on a connection request of any kind with a request for authentication (except for an emergency call). Additionally, the IMEI may be checked.
- Ciphering between BTS and MS is activated in successful authentication. Ciphering prevents tapping into the Air-interface.
- Additional information between MS and NSS are exchanged after activation of ciphering. The additional information either terminates

Samsung Ex. 1032, Page 229 of 417

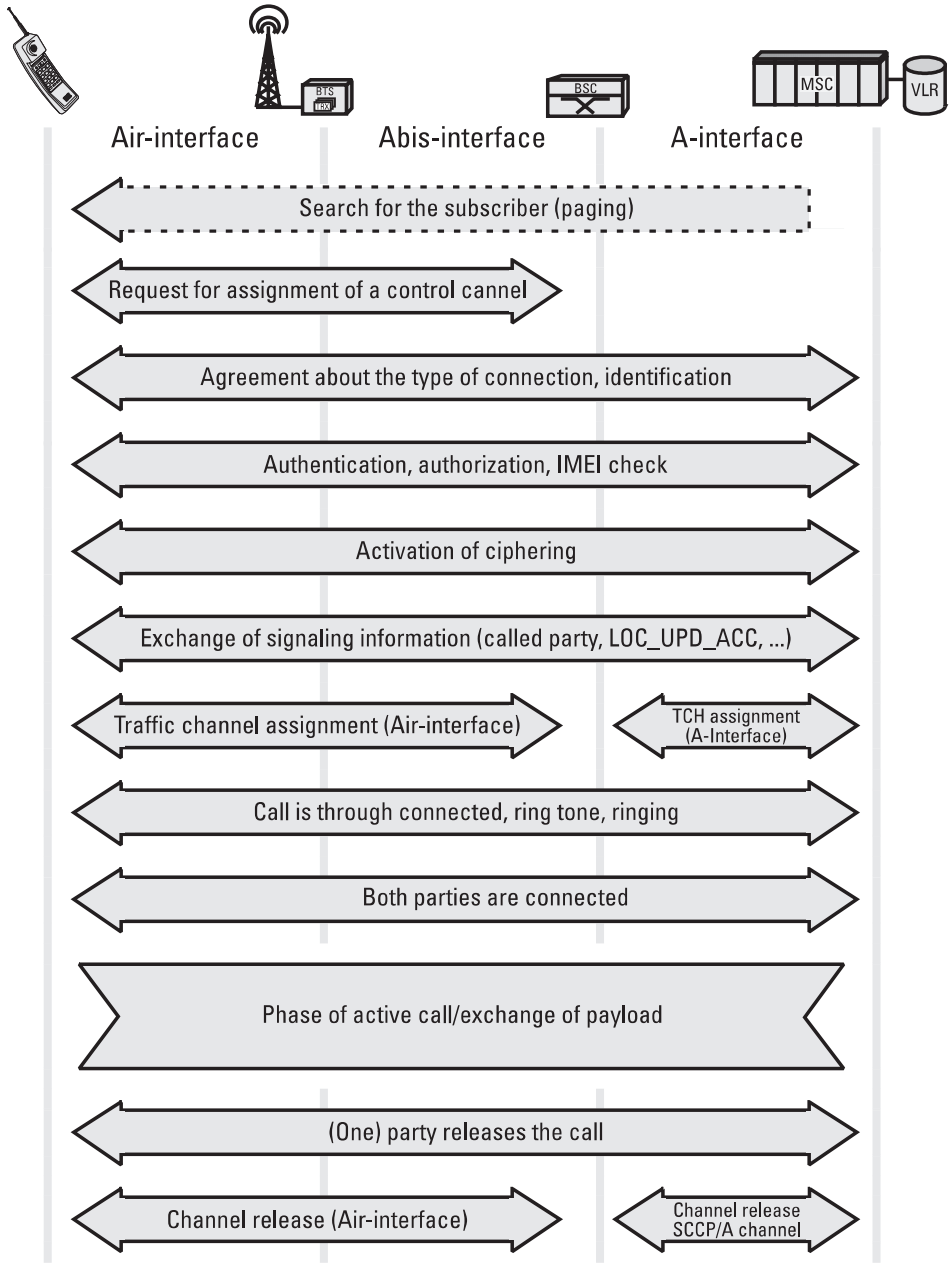


Figure 12.1 Block diagram of the base scenarios.

a successful LU, or, in case of a connection request, defines the details of that connection (e.g., directory number of the called subscriber, required technical capabilities of the network and the MS). The process is synchronized between MS and NSS.

- The assignment of the TCH on the A-interface and Air-interface is done separately, except in the case of off-air call setup (OACSU). Up to this point, the communication has been done via a control channel.

- The system waits, after assignment of the traffic channel, until an end-to-end connection is in place. At the end of this phase, the telephone on one side rings, and the other side hears the ring-back tone.
- When the called subscriber takes the call, the actual conversation begins and charges apply from then on.
- Both ends terminate the call after the conversation has ended. This is the trigger for the MSC, as well as for the MS, to release all the occupied channels and resources.

12.1 Location Update

12.1.1 Location Update in the BSS

An MS performs LU on several occasions: every time it changes the location area, periodically, when a periodic location update is active, or with IMSI attach/detach switched on at the time when it is subsequently turned on again. The only subsystems shown in Figure 12.2 are the MSC/VLR, BSC, BTS, and MS. Nevertheless, if the VLR area changes, the HLR, as well as the old VLR, are involved, too. Furthermore, if the equipment-check is active, the EIR is also involved. Figure 12.3 shows LU from the perspective of the NSS.

12.1.2 Location Update in the NSS

Figure 12.3 shows a LU in which the VLR changes. In this case, the HLR is particularly involved in the overall process. When the LU involves no VLR change, the HLR does not need to be accessed. The HLR only has information about the VLR area of a subscriber; it has no information about the details of the location area. If the equipment check is turned on, the EIR is checked with every activity of an MS.

12.2 Equipment Check

The GSM standard enables a network operator to not only verify the identity of a subscriber by means of authentication but also to check the mobile equipment (ME) as such, which is identified by a unique number, the IMEI. This targets particularly the theft of mobile equipment.

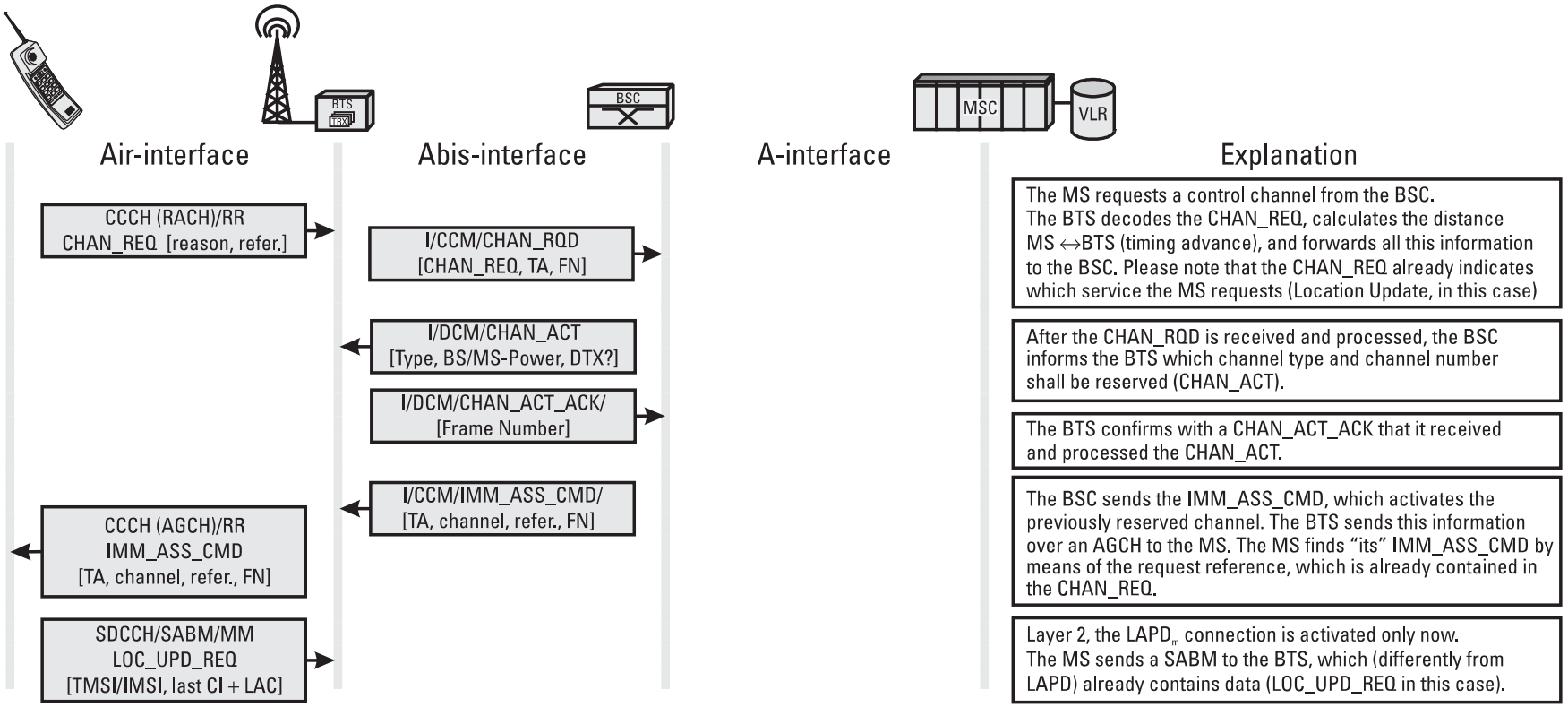


Figure 12.2 Location update on the BSS interfaces.

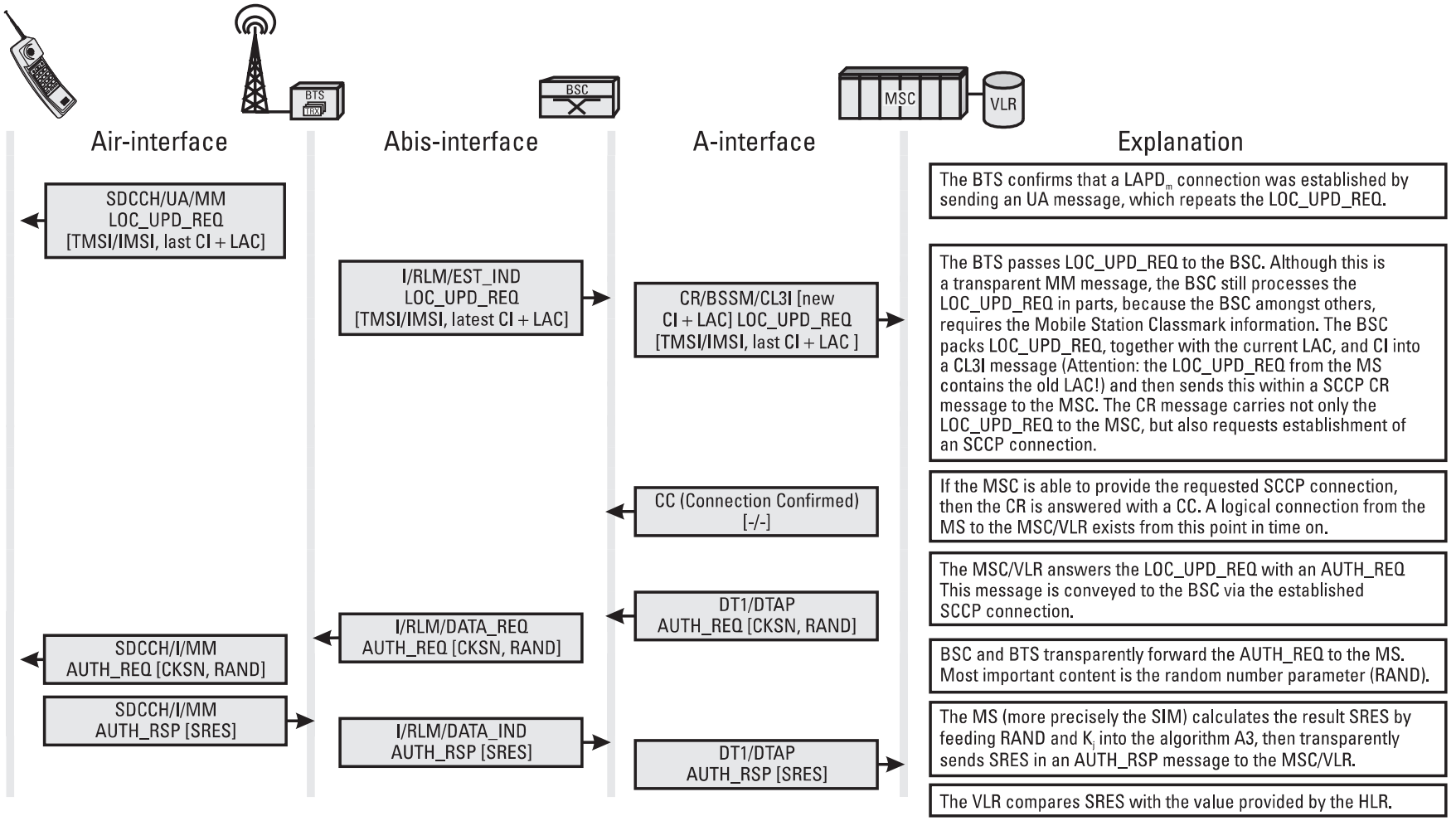


Figure 12.2 (continued)

Samsung Ex. 1032, Page 233 of 417

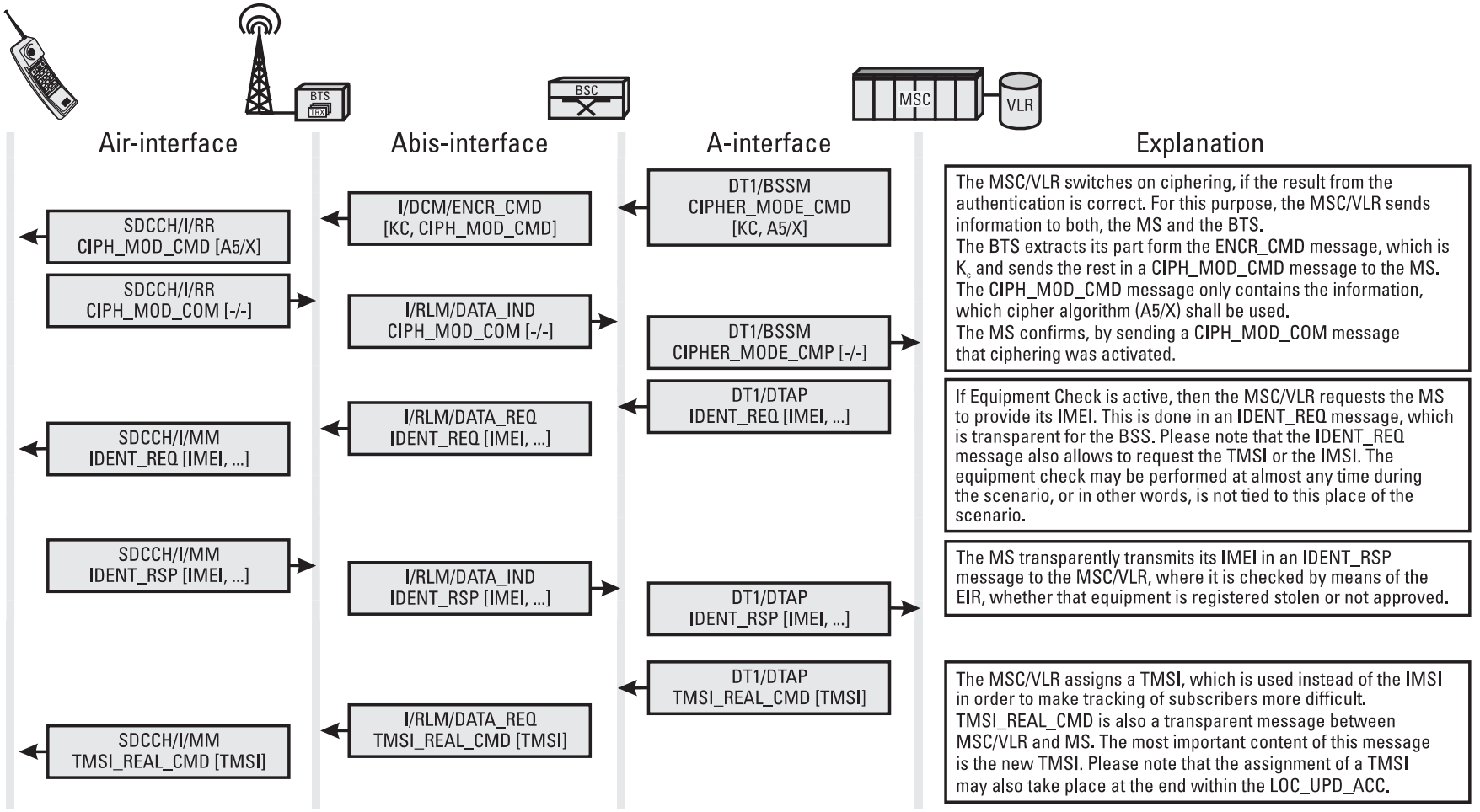


Figure 12.2 (continued)

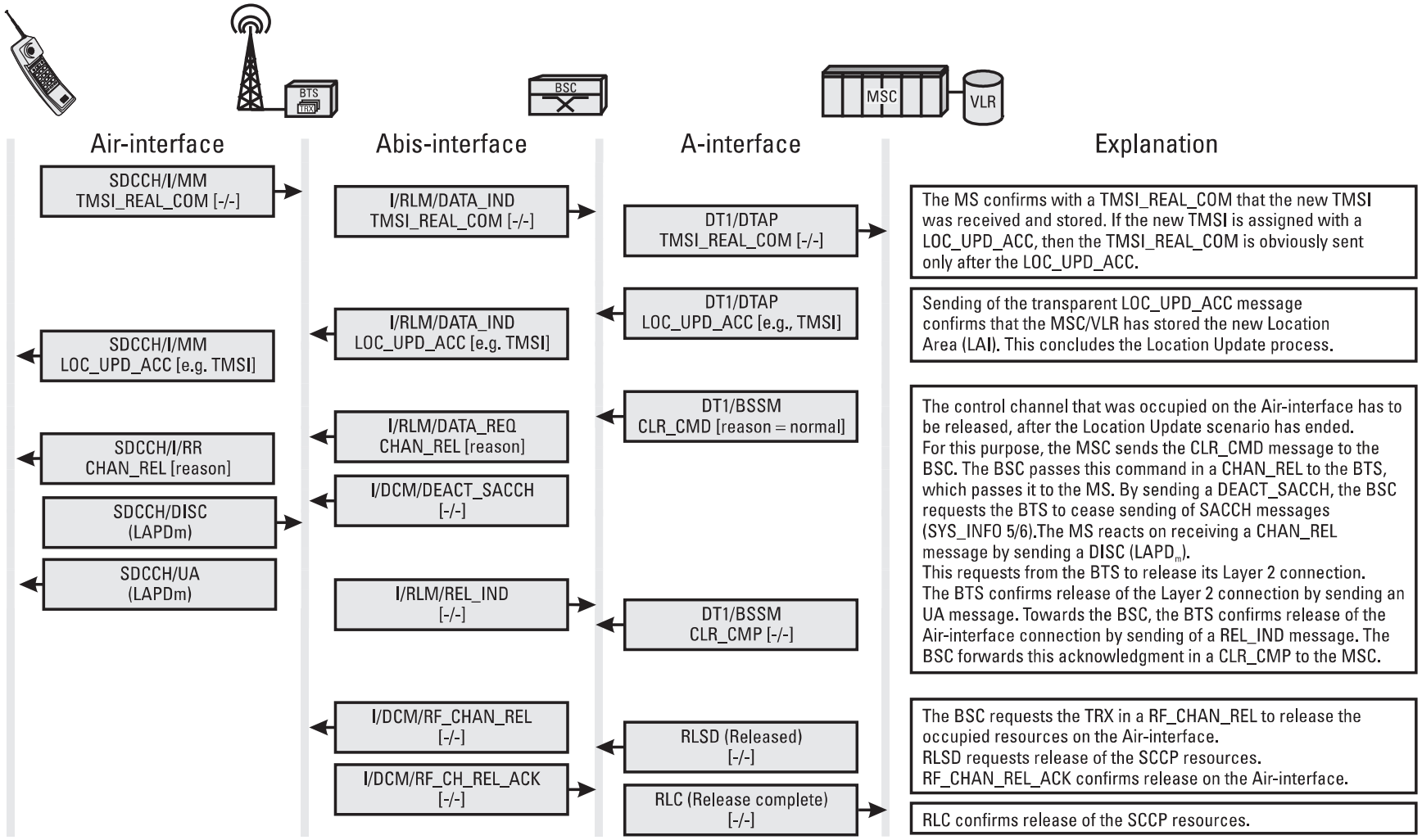


Figure 12.2 (continued)

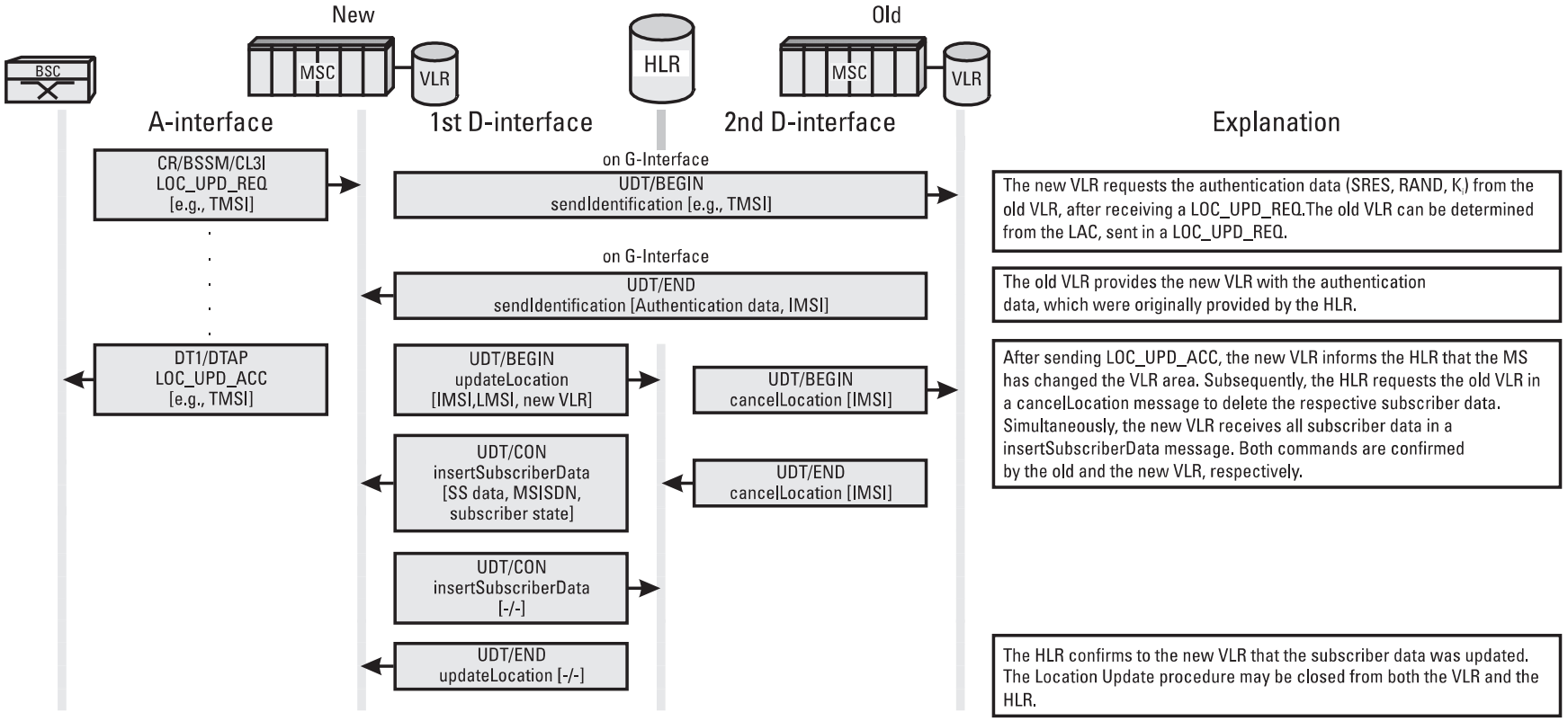


Figure 12.3 Location update on the NSS interfaces.

For that purpose, the NSS includes a database, the EIR, that contains information such as the serial numbers of barred mobile equipment. Figure 12.4 illustrates the process of an equipment check between MSC/VLR and EIR.

12.3 Mobile Originating Call

12.3.1 Mobile Originating Call in the BSS

The MS initiates a network access with a MOC. The network access is specified in more detail in the first message that the MS sends (CM_SERV_REQ) on the SDCCH. The reasons for such a request could be a regular telephone call, transfer of MO-SMS, activation of a supplementary service, or an emergency call. The CM_SERV_ACC message, shown in Figure 12.5 as a confirmation of a CM_SERV_REQ, is used only when ciphering is not active. If ciphering is active, the MS, when receiving the CIPH_MOD_CMD message, interprets it as a positive acknowledgment from the network for the service request. Figure 12.5 illustrates the MOC on the BSS interfaces. In addition, Figure 12.6 explains which signaling is taking place during an active connection.

12.3.2 Mobile Originating Call in the NSS

From the perspective of the NSS, a connection request of a subscriber can be directed as follows:

1. To the same PLMN (MS-to-MS call);
2. To another PLMN (MS-to-MS call);
3. To the ISDN (digital);
4. To the PSTN (analog).

In case 1, ISUP signaling is used between both MSCs, after the HLR of the called subscriber has provided the necessary routing information. ISUP is also used in cases 2 and 3. There is no principle difference between a call to another PLMN and to an ISDN.

Figure 12.7 shows signaling for the MOC, which applies to cases 1, 2, and 3. (Query of the routing information is discussed in Section 12.4.2.) In case 4 (PSTN), the gateway MSC has to provide the necessary conversion between digital and analog signaling.

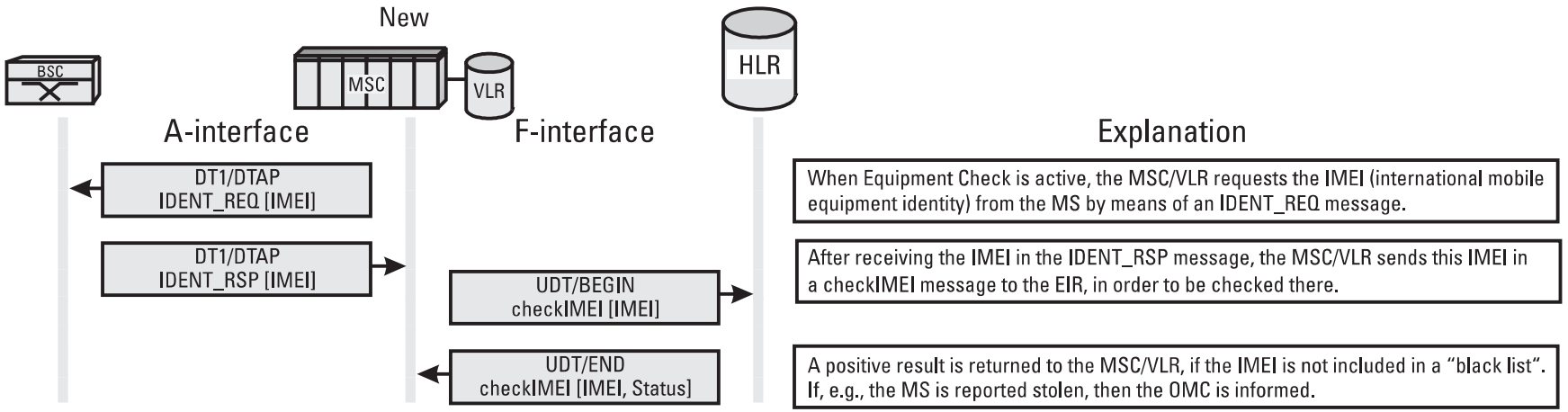


Figure 12.4 Scenario of checking the IMEI.

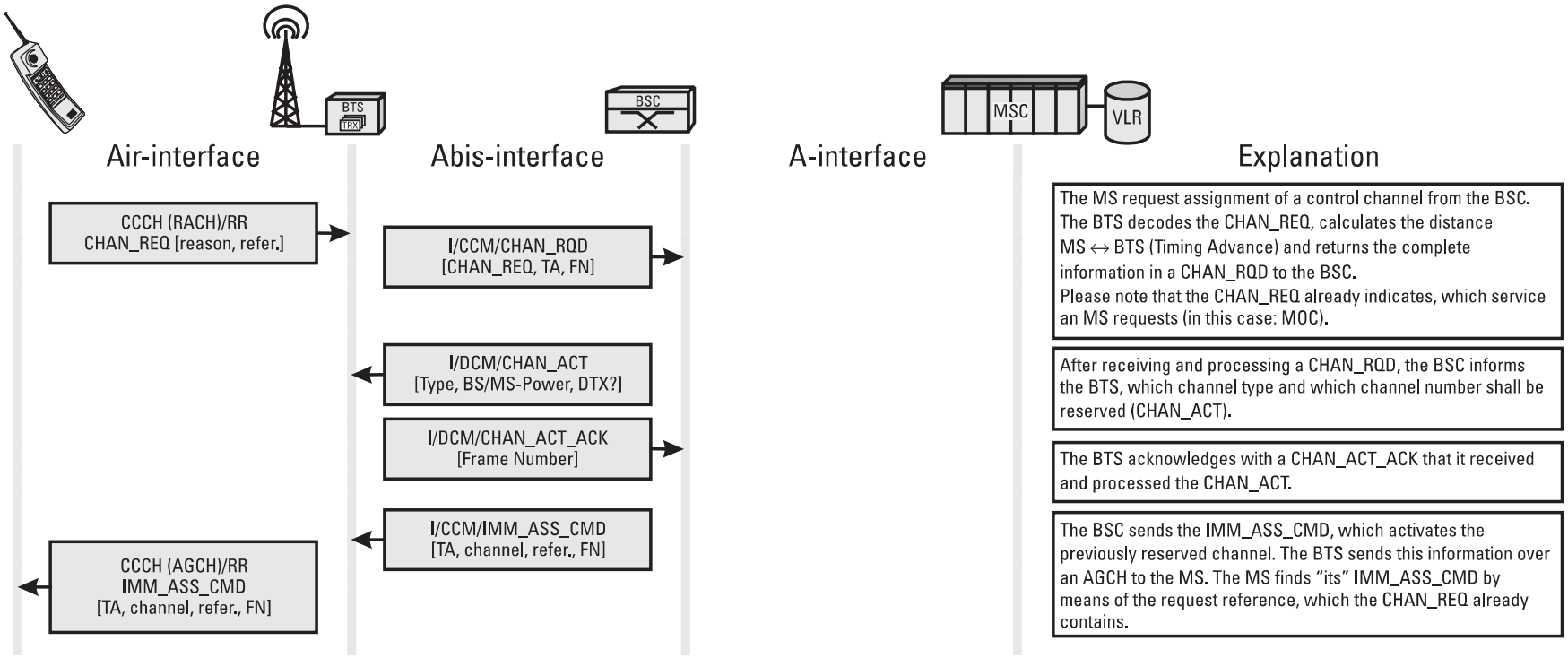


Figure 12.5 Mobile originating call in the BSS.

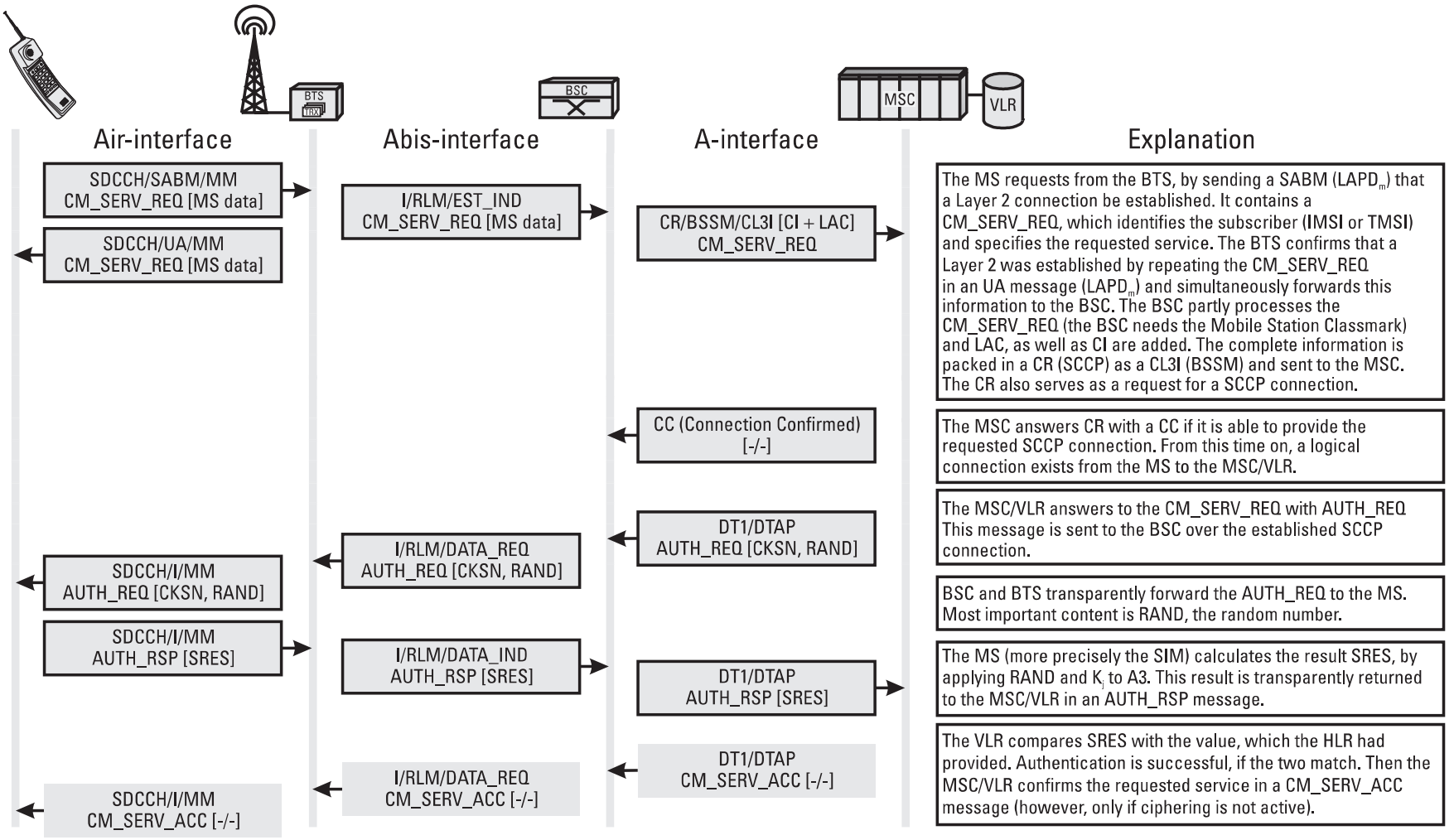


Figure 12.5 (continued)

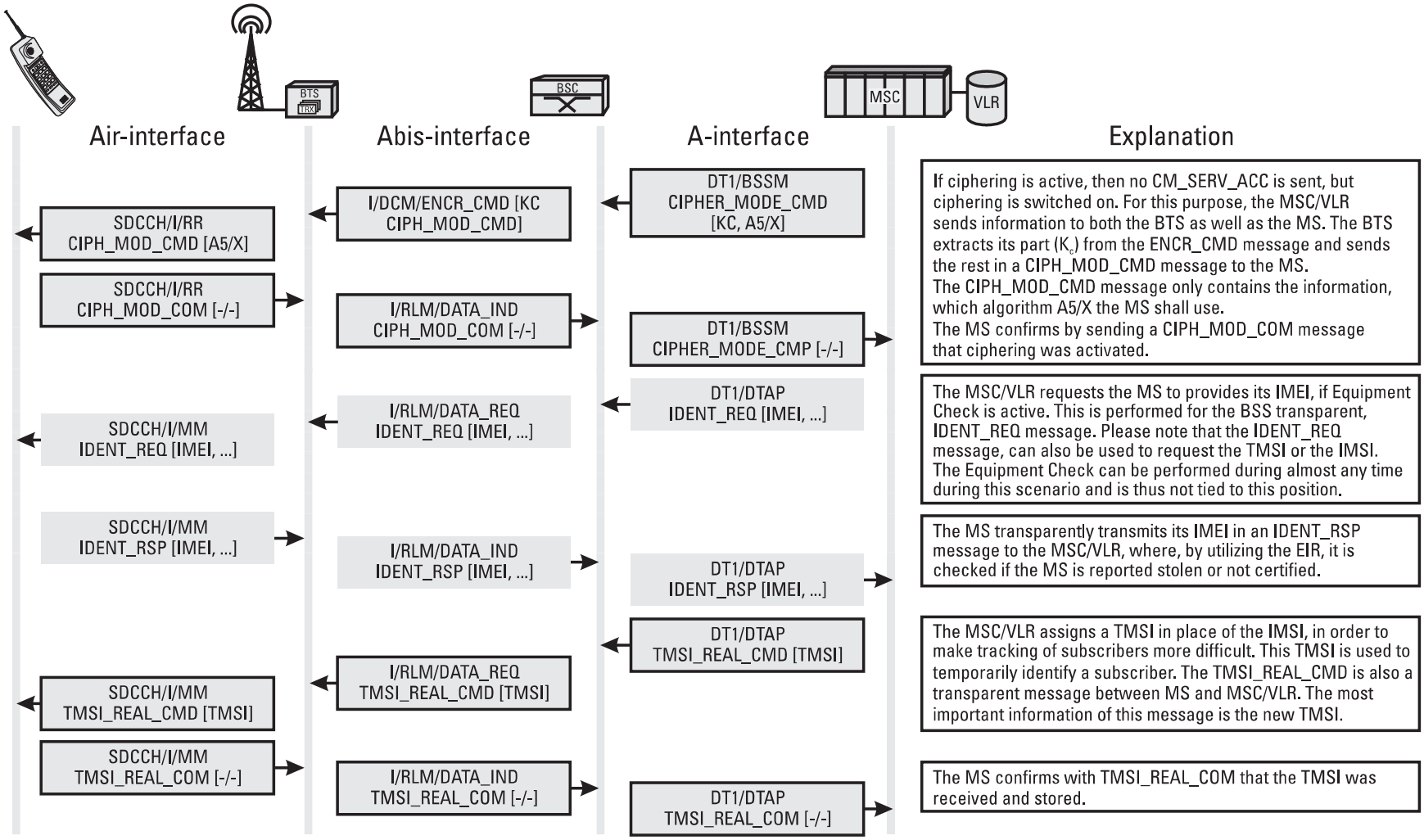


Figure 12.5 (continued)

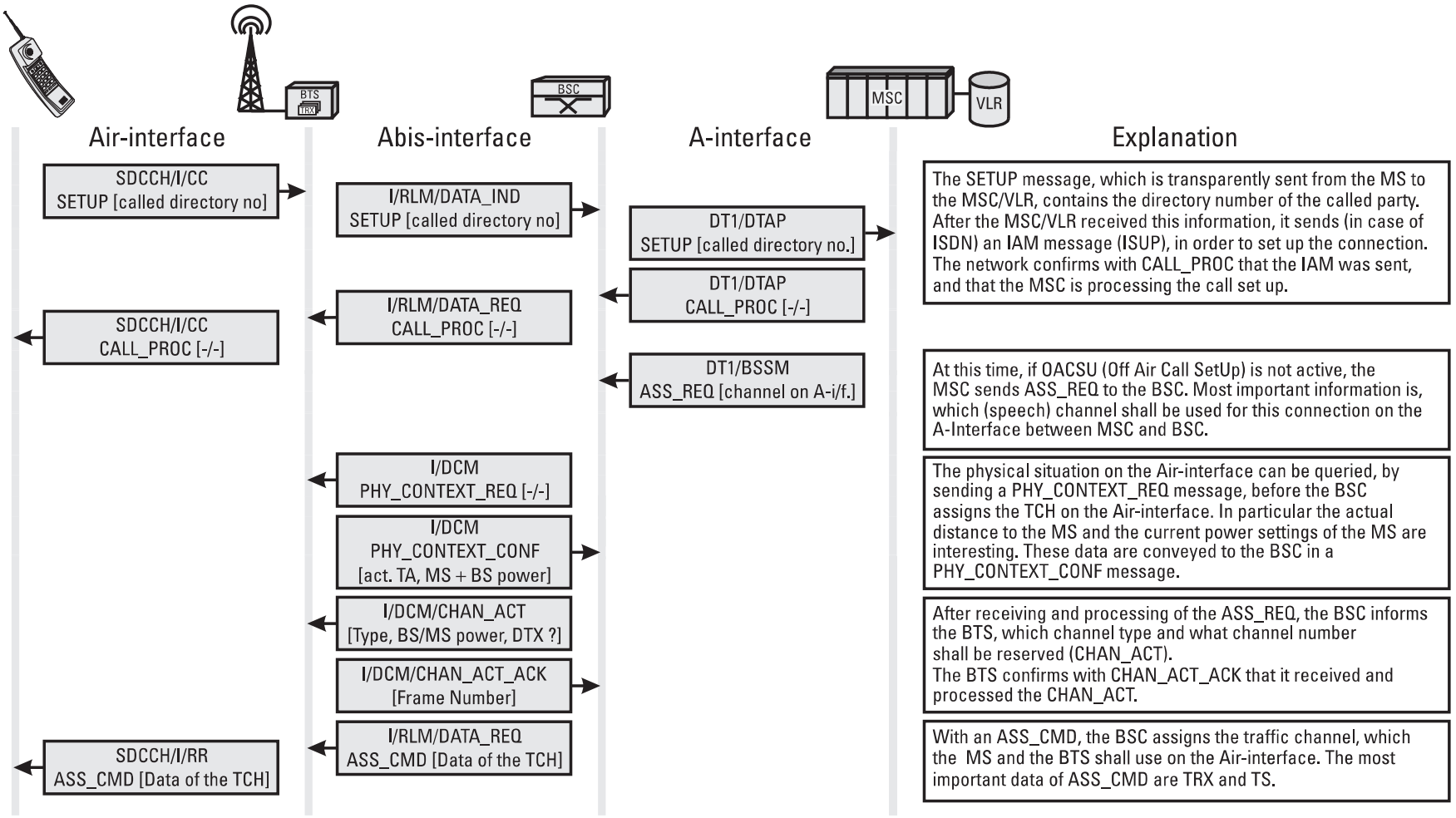


Figure 12.5 (continued)

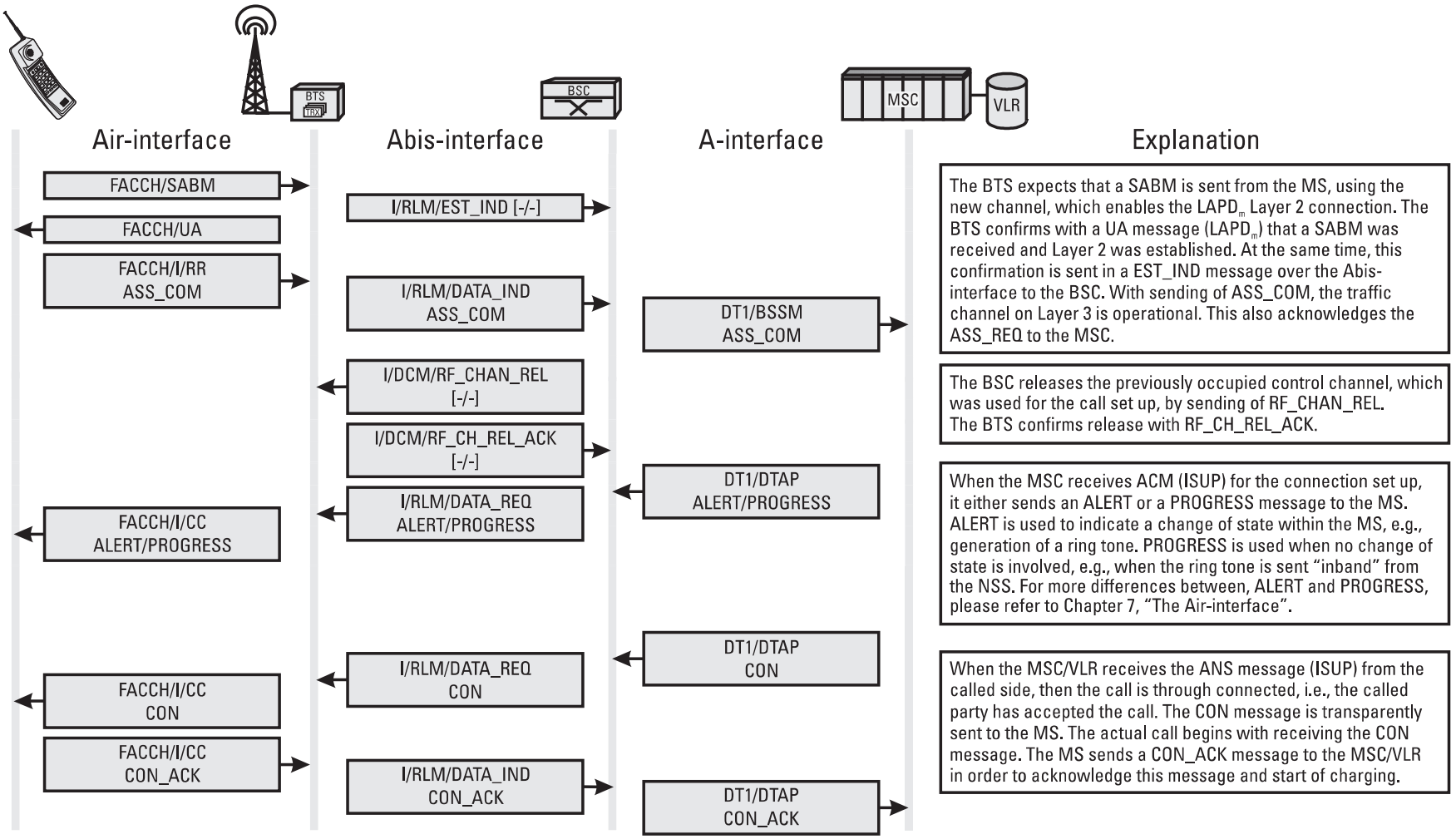


Figure 12.5 (continued)

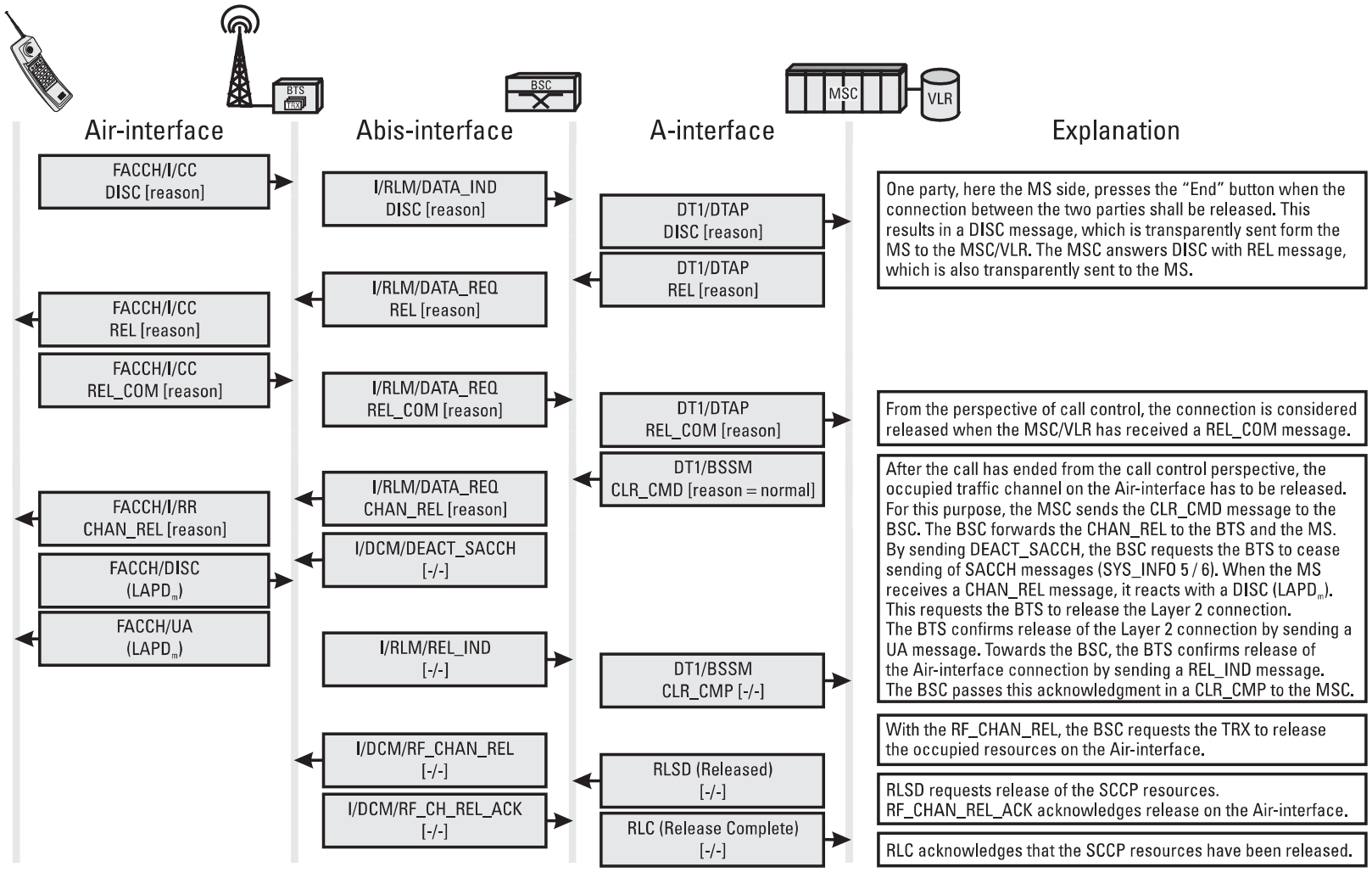


Figure 12.5 (continued)

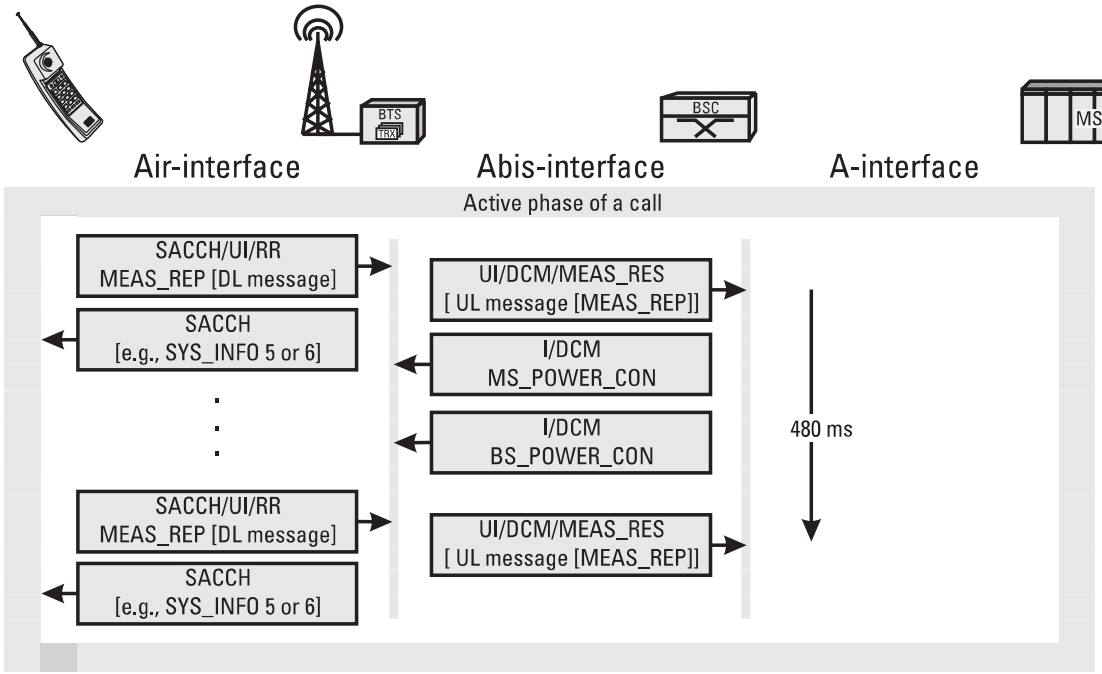


Figure 12.6 Signaling traffic during a connection.

Samsung Ex. 1032, Page 245 of 417

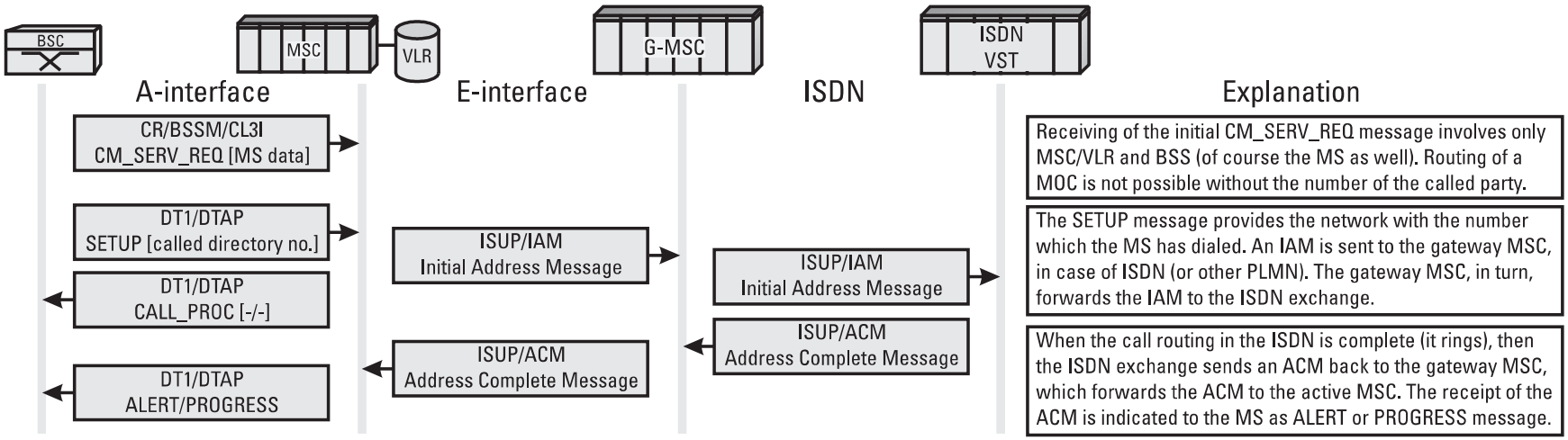


Figure 12.7 Mobile originating call in the NSS.

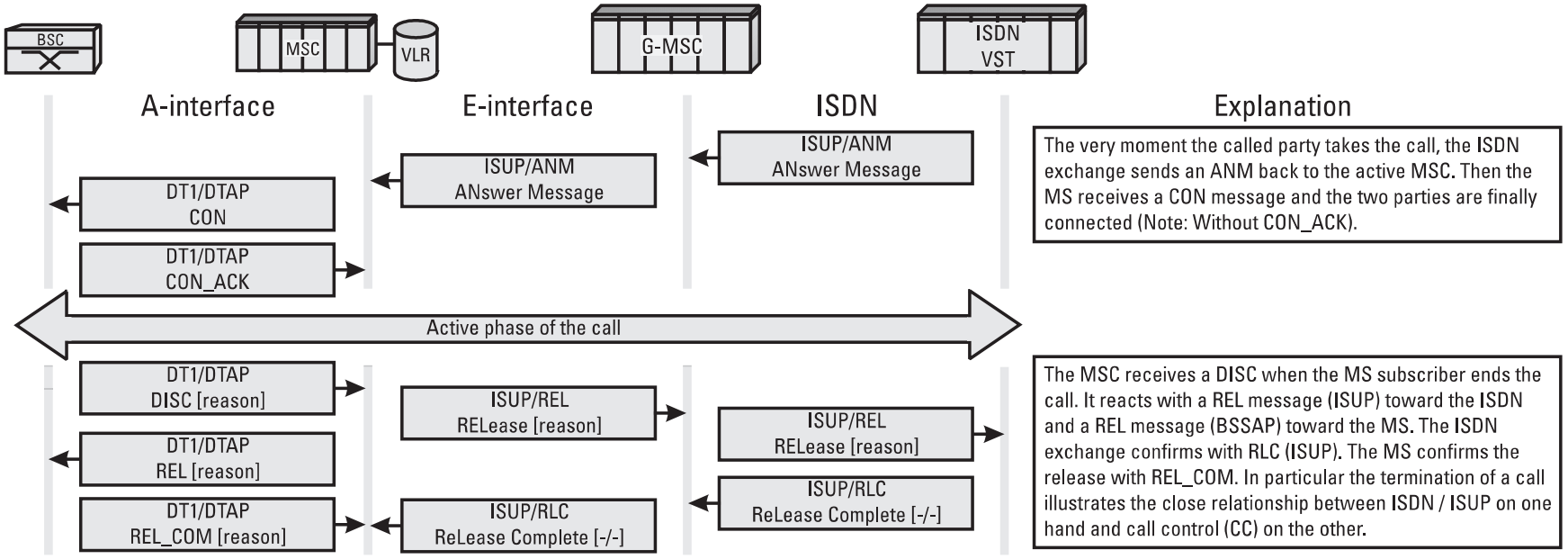


Figure 12.7 (continued)

Samsung Ex. 1032, Page 247 of 417

12.4 Mobile Terminating Call

12.4.1 Mobile Terminating Call in the BSS

In the case of a MTC, a subscriber (PLMN internal or from external) tries to reach a mobile subscriber. Although the connection request in a MTC is not originated by the MS, there are some similarities between the MOC and the MTC, particularly for the network access on the BSS interfaces. The following differences, however, need to be pointed out:

- The CHAN_REQ of the MS in an MTC is the answer to PAGING_REQ.
- The first message sent over the new SDCCH is not a CM_SERV_REQ but a PAG_RSP.
- The SETUP message in an MTC is initiated by the MSC/VLR, not by the MS.

In the example of a MTC shown in Figure 12.8, the call is terminated by the "other" side. Thus, this example is the exact opposite of the example in Section 12.3. Of course, in real life, either side may end the call.

12.4.2 Mobile Terminating Call in the NSS

From the perspective of the NSS, finding a mobile subscriber is one of the most important tasks during an MTC. What is the scenario for this search? How is the further cooperation with BSS and ISDN performed? This section focuses on answering those questions.

In the case of a MTC, any subscriber from within or outside the PLMN dials the MSISDN of a subscriber. The ISDN routes the call to the PLMN or, more precisely, to the gateway MSC, based on the information contained in the MSISDN, national destination code (NDC), and the country code. This step is not necessary in case of a PLMN internal MS-to-MS call. After reception by the gateway MSC the HLR of the subscriber has to be identified, based on the MSISDN, to retrieve information, in particular the VLR area where the subscriber currently roams (the HLR does not know the location area). The HLR, in turn, queries the VLR, which assigns an MSRN for routing purposes and provides that number to the HLR. The HLR only forwards the MSRN to the gateway MSC, which uses the address to finally route the call to the destination MSC/VLR. After a radio connection to the MS is established, the NSS or, more precisely, the MSC mainly provides interfacing functionality between the

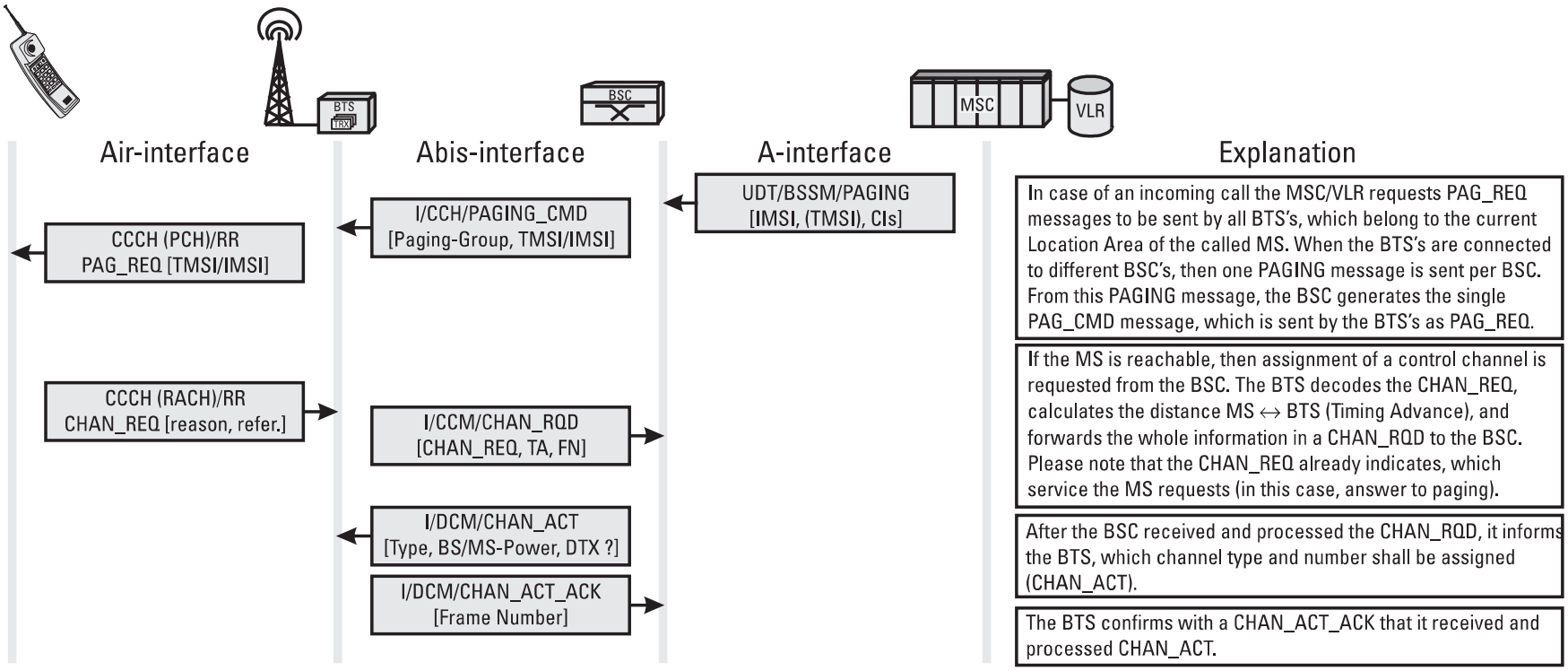


Figure 12.8 Mobile terminating call in the BSS.

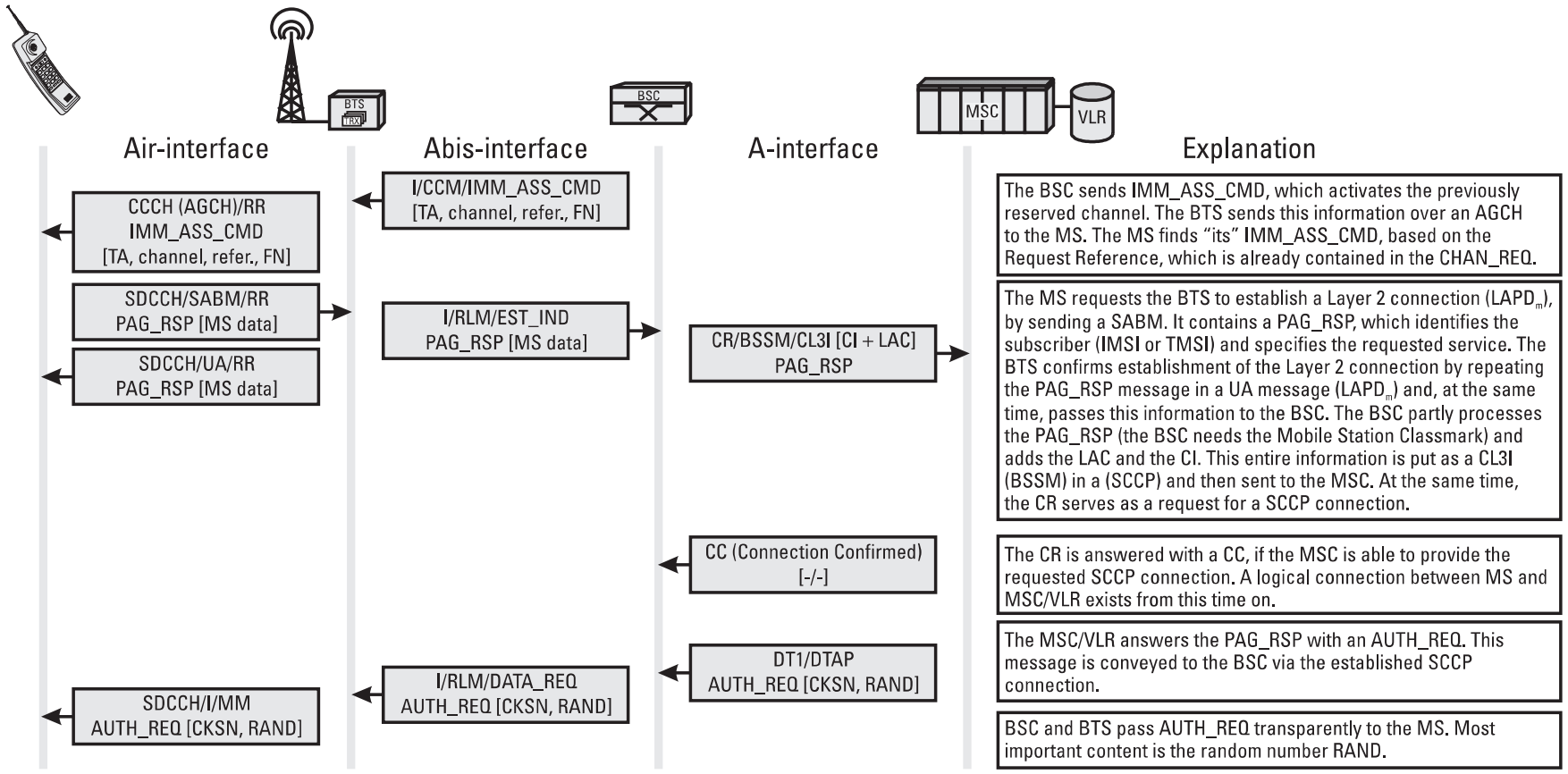


Figure 12.8 (continued)

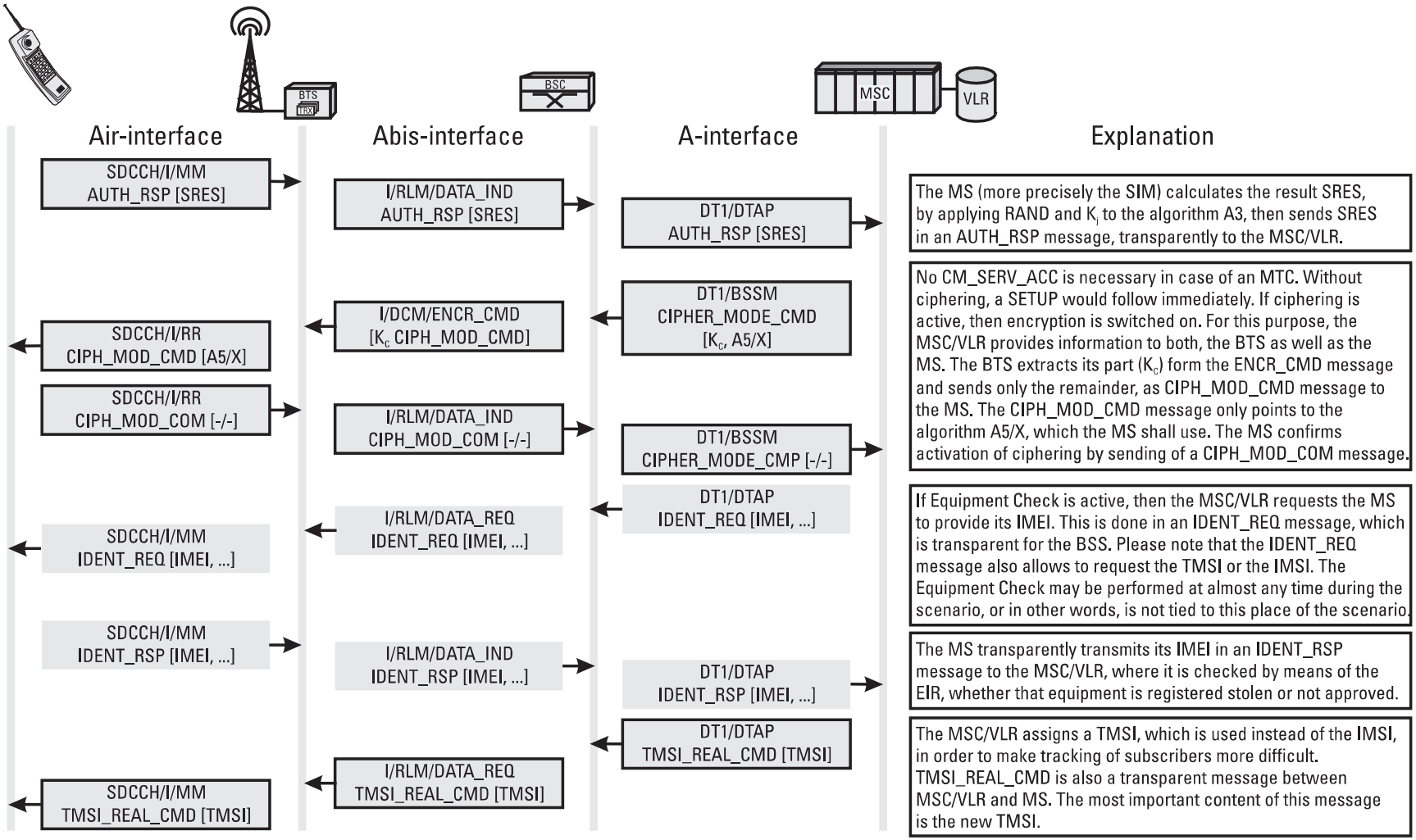


Figure 12.8 (continued)

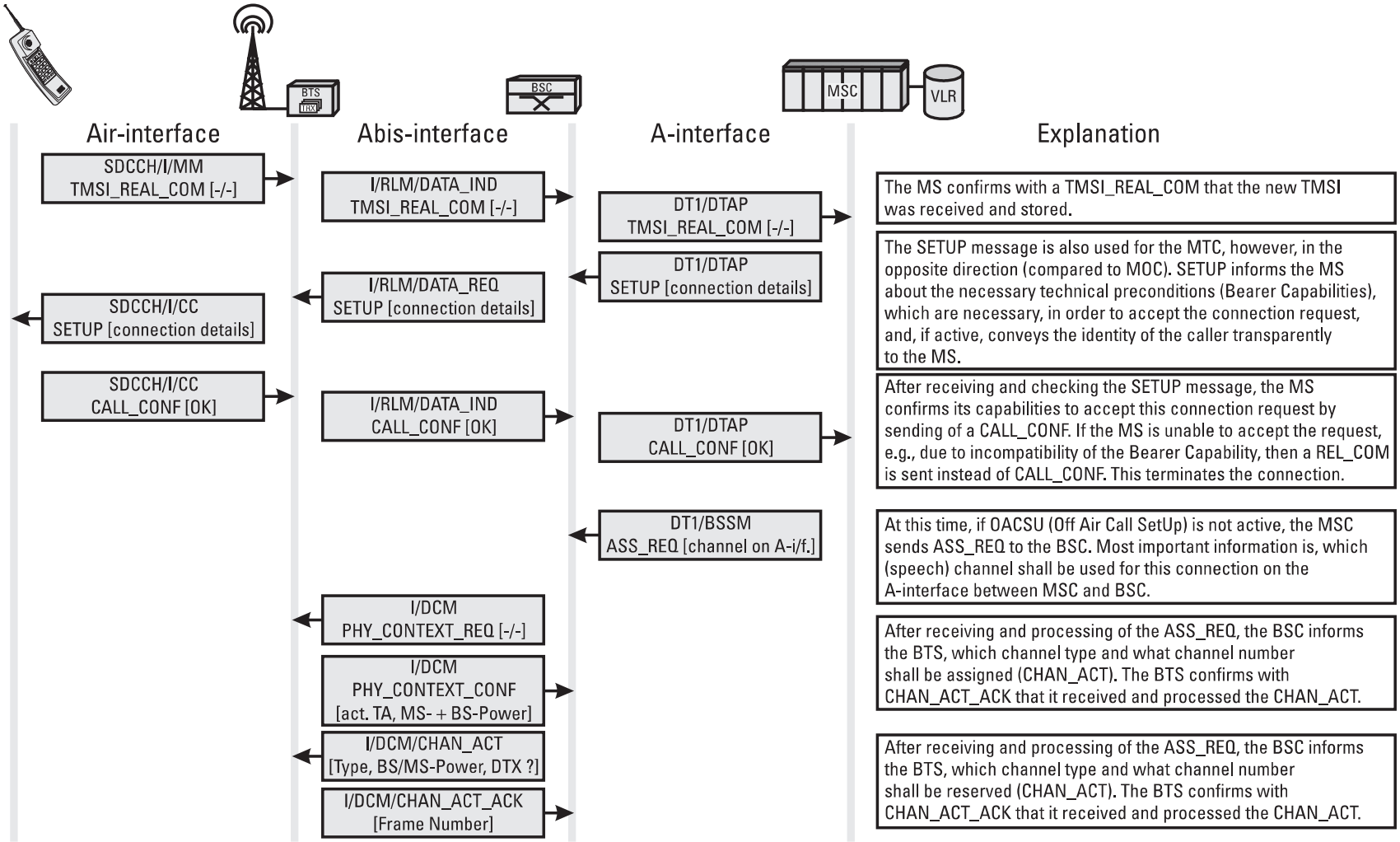


Figure 12.8 (continued)

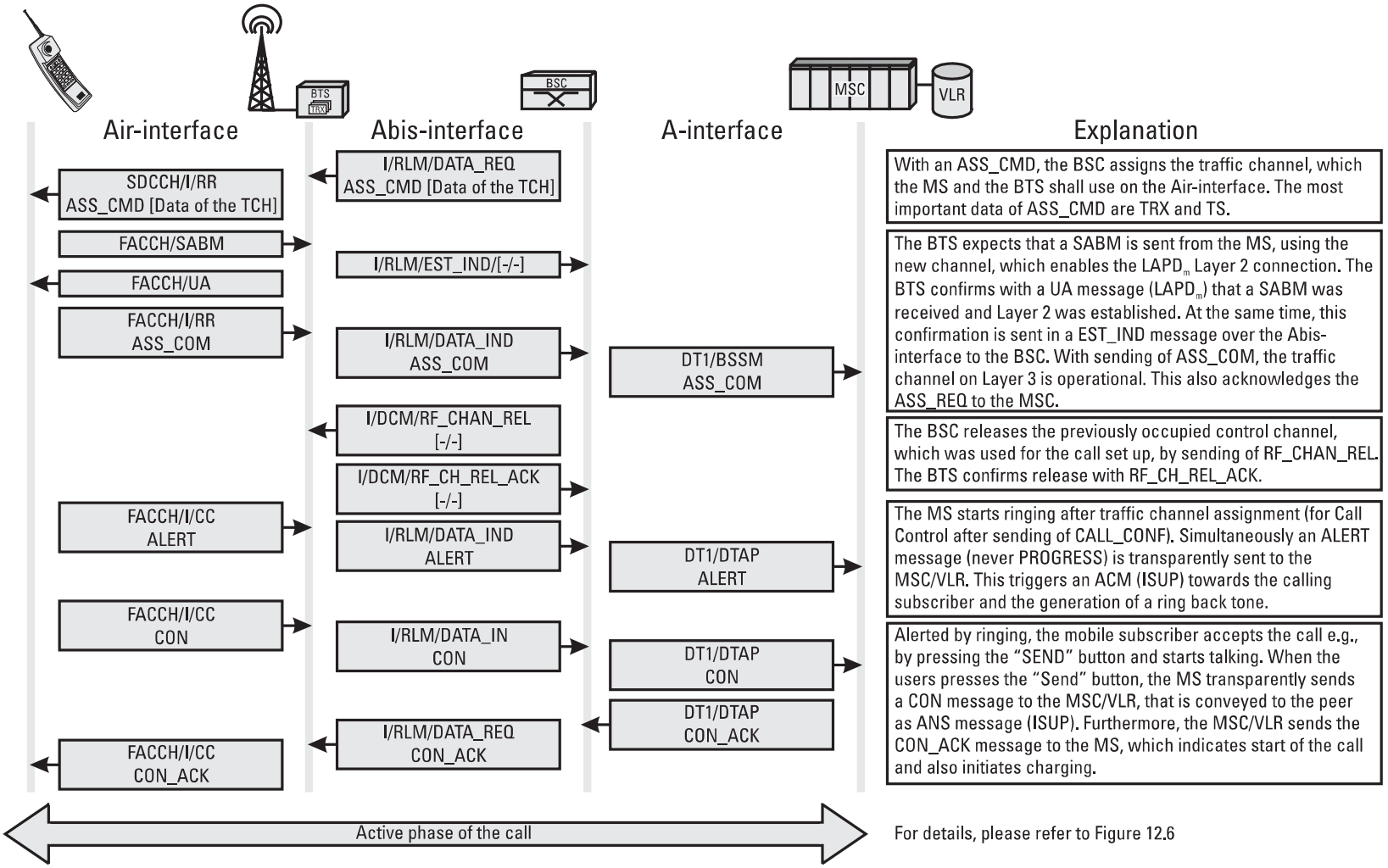


Figure 12.8 (continued)

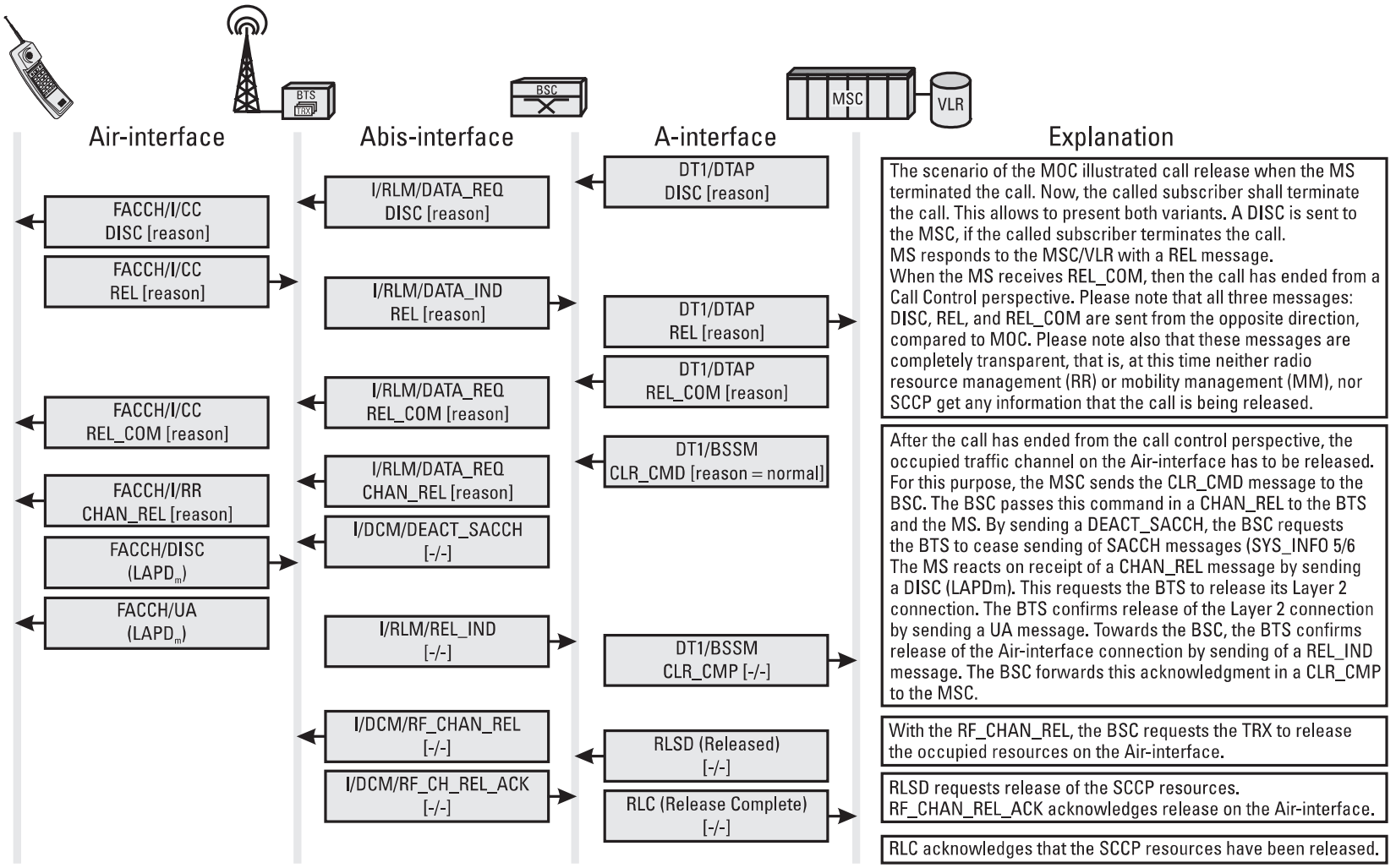


Figure 12.8 (continued)

NSS and the ISDN. For a call from the analog PSTN, the gateway MSC has to convert the analog signaling into digital SS7 ISUP signaling. (The reverse applies similarly, of course, in the opposite direction.) The process is illustrated in Figure 12.9.

12.5 Handover

The capability of a handover and its execution are some of the more interesting characteristics of a modern wireless service. Note that the GSM-specific term *handover* corresponds to the same concept as *handoff,* which is used in cellular networks in the United States. A handover is defined as the change of the currently used radio channel (SDCCH or TCH) to another radio channel during an existing and active connection between MS and BTS. The requirement for an already existing and active radio connection distinguishes the handover from the SDCCH assignment in the idle state. The differences relative to frequency redefinition, channel modify, and TCH assignment are, however, fuzzy. For the intra-BTS handover, it is even an option to use the TCH assignment procedure for handover. GSM has defined several handover types that can be activated by the network operator and executed when necessary. (The handover types are described in Section 12.5.3.) The decisions of whether a handover should be performed and if so the type of handover chosen lie with the BSC, based on the measurement results of the BTS and the MS (MEAS_RES/MEAS_REP), taking into account the parameter and criteria set by the OMC. A detailed explanation of these criteria and the possible parameters is beyond the scope of this presentation and provides enough material for another book. What is presented here are the starting points and values for a decision on handover by the BSC as the controlling instance, based on the measurement results sent to the BSC once per multiframe.

12.5.1 Measurement Results of BTS and MS

The example in Section 12.5.2 analyzes a MEAS_RES message in more detail. The reader is asked to duplicate the following values by means of that example. Table 12.1 provides an overview of the power control and most important parameters, which can be separated into two groups:

- The measurement results of the MS, which can be separated into the results related to the active BTS and those related to the neighbor cells;
- The measurement results of the BTS.

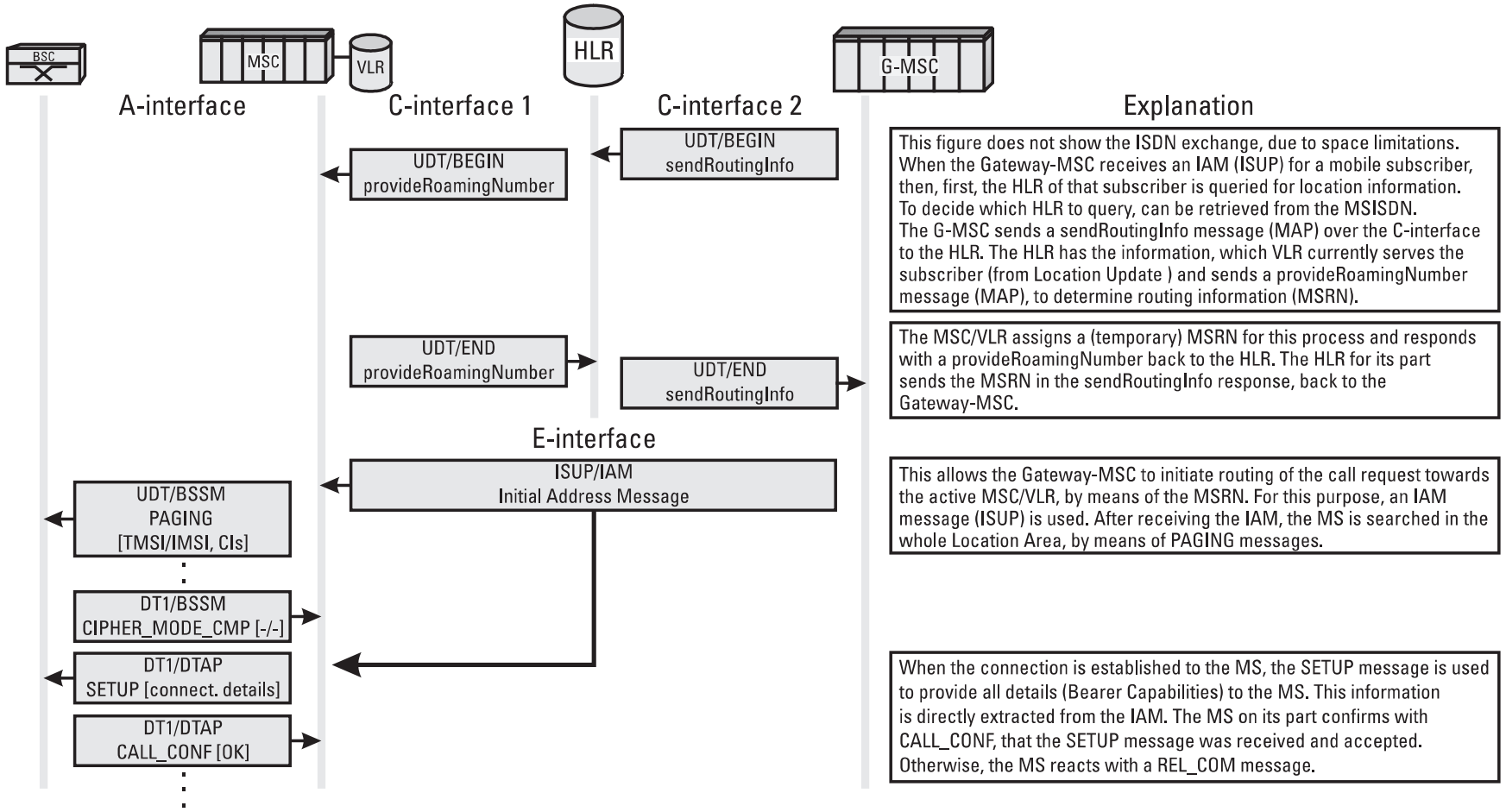


Figure 12.9 Mobile terminating call in the NSS.

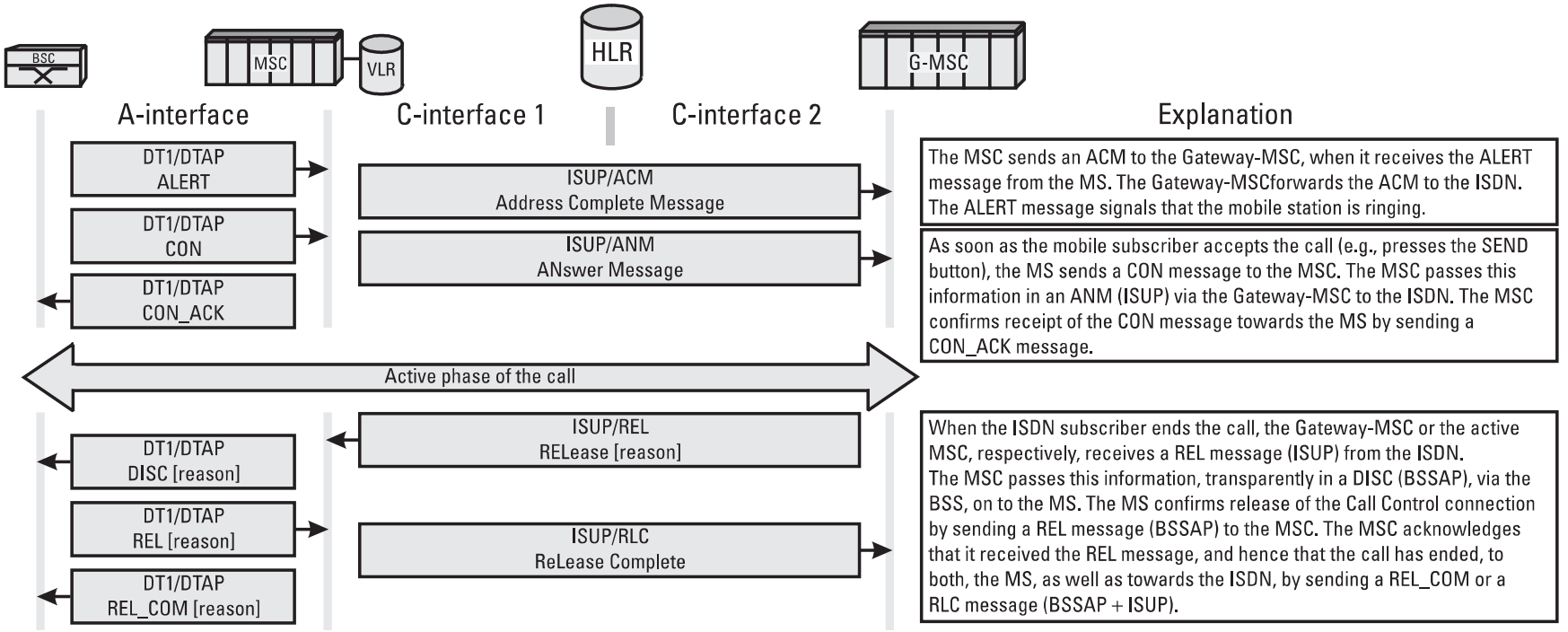


Figure 12.9 (continued)

Samsung Ex. 1032, Page 257 of 417

The values for the receiving level (= RXLEV) and the receiving quality (= RXQUAL) are provided for both cases. Obviously, in the case of neighbor cell measurements, only the receiving level measurements are available, since the MS does not have an active connection.

Table 12.1
Input Parameters for Power Control and Handover Decision

Measured Value	Object to be Measured	Explanation
RXLEV-FULL-SERVING-CELL (6 bit $0 \equiv 63_{dec}$)	BTS	With what level does the MS receive the active BTS? This value is always provided but only relevant if no DTX is active in the downlink direction.
RXLEV-SUB-SERVING-CELL (6 bit $0 \equiv 63_{dec}$)	BTS	With what level does the MS receive the active BTS? This value is always provided but only relevant if DTX is active in the downlink direction.
RXQUAL-FULL-SERVING-CELL (3 bit $0 \equiv 7_{dec}$)	BTS	How well (BER) does the MS receive the active BTS? The BER is determined by means of the Training Sequence Code. This value is always present but only relevant if no DTX is active in the downlink direction.
RXQUAL-SUB-SERVING-CELL (3 bit $0 \equiv 7_{dec}$)	BTS	How well (BER) does the MS receive the active BTS? The BER is determined by means of the Training Sequence Code. This value is always present but only relevant if DTX is active in the downlink direction
RXLEV-NCELL 1 - N (6 bit $0 \equiv 63_{dec}$)	BTS	With what level does the MS receive the neighbor cells (as indicated in SYS_INFO 2)?
RXLEV-FULL-up (6 bit $0 \equiv 63_{dec}$)	MS	With what level does the BTS receive the MS? This value is always provided but only relevant if no DTX is active in the uplink direction.
RXLEV-SUB-up (6 bit $0 \equiv 63_{dec}$)	MS	With what level does the BTS receive the MS? This value is always provided but only relevant if DTX is active in the uplink direction.
RXQUAL-FULL-up (3 bit $0 \equiv 7$dec)	MS	How well (BER) does the BTS receive the MS? The BER is determined by means of the Training Sequence Code. This value is always present but only relevant if no DTX is active in the uplink direction.
RXQUAL-SUB-up (3 bit $0 \equiv 7$dec)	MS	How well (BER) does the BTS receive the MS? The BER is determined by means of the Training Sequence Code. This value is always present but only relevant if DTX is active in the uplink direction.
Timing Advance (6 bit $0 \equiv 63$dec)	MS	How far is the MS away from the BTS?

12.5.2 Analysis of a MEAS_RES/MEAS_REP

This example (Figure 12.10) analyzes a MEAS_RES in more detail (including a MEAS_REP) that was captured with a protocol tester on the Abis-interface of a GSM900 PLMN. Note, when looking at the values for RXQUAL or RXLEV, respectively, that the following applies: The qualifier "FULL" or "ALL" refers to the case with *inactive* DTX, while the qualifier "SUBSET" refers to the case with *active* DTX.255

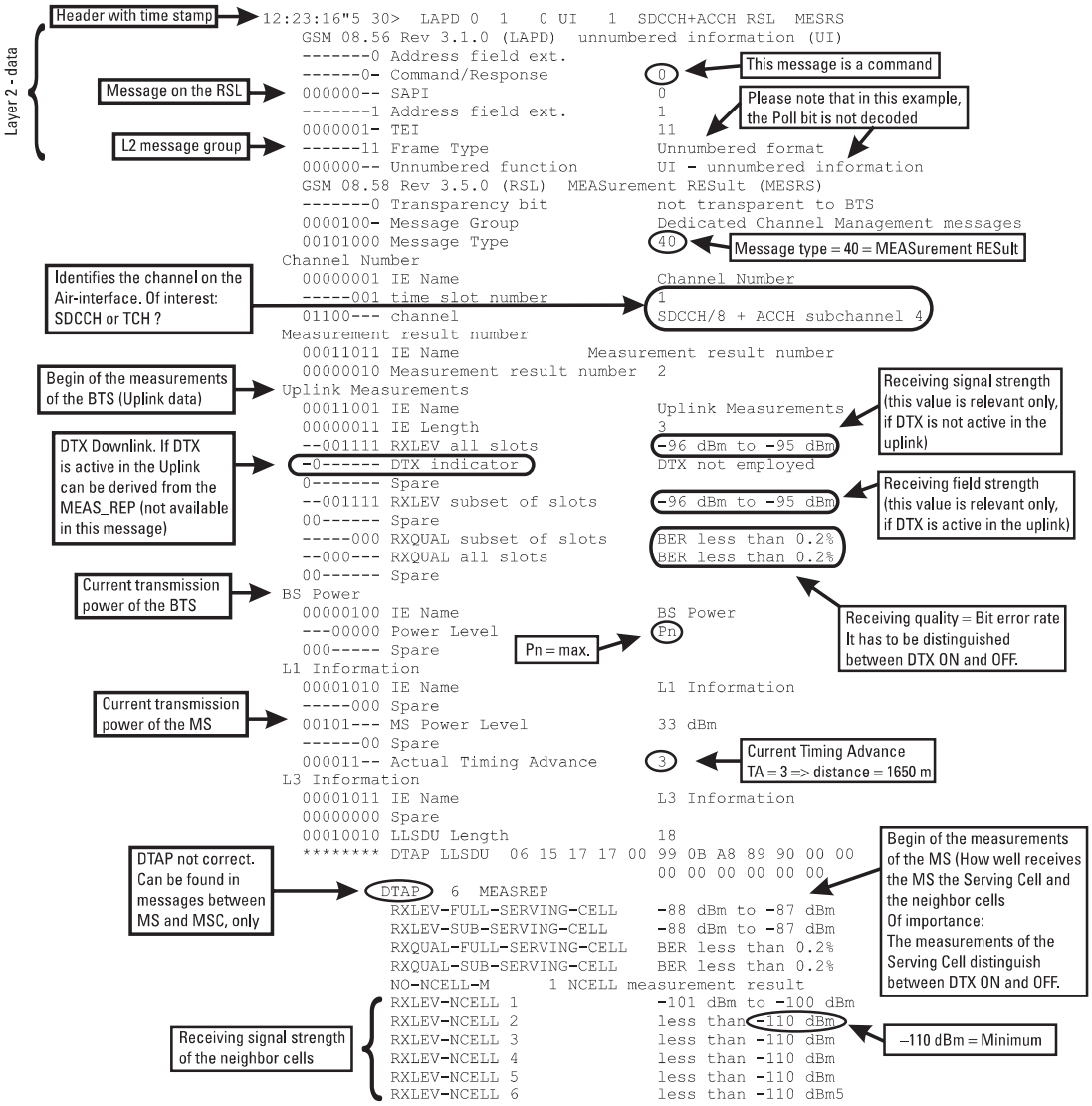


Figure 12.10 Analysis of a MEAS_RES message.

Whether DTX is active in the *uplink* direction can be derived from the *downlink* measurements (MEAS_REP). Whether DTX is active in the *downlink* direction can be derived from the *uplink* measurements (MEAS_RES).

When tracing a call protocol, one occasionally sees MEAS_RES messages, which do not contain a MEAS_REP. That is the case if the BTS is unable to decode the uplink SACCH, because of problems in the area of radio transmission. In that case, typically, the connection breaks down shortly due to radio link timeout. This type of call drop cannot be prevented completely. A closer investigation is necessary, however, if such failure rate is relatively high or is increasing dramatically.

12.5.3 Handover Scenarios

When categorizing the various handover scenarios, two criteria or perspectives have to be considered:

- What entity is executing the handover? In other words, which BTS is the source and which BTS is the destination of a handover? This category covers expressions like intra-BTS and inter-MSC. We will return to this issue, because the location of the executing functionality is important for the handover scenario. Note that the BSC always decides whether a handover needs to be executed. However, for the execution itself, either the BSC or the MSC might be in charge.
- Are the system clocks of the origination cell and the destination cell of a handover finely synchronized? This criterion affects the handover scenario on the Air-interface.

Regarding the second criterion: it has to be added that GSM, regarding synchronization, distinguishes among four different levels: *nonsynchronized*, *synchronized*, *presynchronized*, and *pseudo-synchronized*. Details and differences of these concepts are provided in the Glossary.

The protocol scenario is the same for synchronized, presynchronized, and pseudo-synchronized handover. Only the nonsynchronized handover has to be regarded separately.

12.5.3.1 Synchronized Versus Nonsynchronized Handover

In practical operation, synchronized and nonsynchronized handover are mainly used, where nonsynchronized handover has the advantage of shorter dead time during the handover process. Synchronized handover, on the other hand, requires that the clock of all involved cells be finely synchronized. Therefore,

the synchronized handover can be used only in intra-BTS handover or inter-BTS handover when the BTSs are sectorized or collocated, in which case the equipment is located closely enough together to allow for fine synchronization in an inexpensive way. However, the majority of the handovers performed in commercial systems are nonsynchronized.

12.5.3.2 Intra-BTS Handover

In intra-BTS handover, a new channel in the same BTS is assigned to the MS. The intra-BTS handover does not distinguish whether the new channel is just on another timeslot in the same TRX (frequency) or whether the TRX changes as well. An intra-BTS handover is performed particularly when the RXQUAL values in uplink or downlink are relatively bad, while the RXLEV values stay good (interference). Figure 12.11 illustrates the intra-BTS handover. The procedure usually is executed autonomously by the BSC, but the MSC also may be in charge. It is worth pointing out that an intra-BTS handover is always synchronized, since all TRXs of a BTS have to use the same clock. Figure 12.12 presents the corresponding scenario. Note that for an intra-BTS handover both the ASS_CMD message and the HND_CMD message may be applied.

12.5.3.3 Intra-BSC Handover

In the intra-BSC handover, an MS changes the BTS but not the BSC, as illustrated in Figure 12.13. Like the intra-BTS handover, the intra-BSC handover may be carried out autonomously by the BSC, without support from the MSC. It is an option by the network operator, however, to decide that the MSC supervises the process. For intra-BSC handover, depending on the circumstances, both handovers are possible, synchronized as well as nonsynchronized. Figure 12.14 presents the scenario for a nonsynchronized intra-BSC handover. The difference from the synchronized intra-BSC handover is simply that the PHYS_INFO messages from the BTS would not have to be sent.

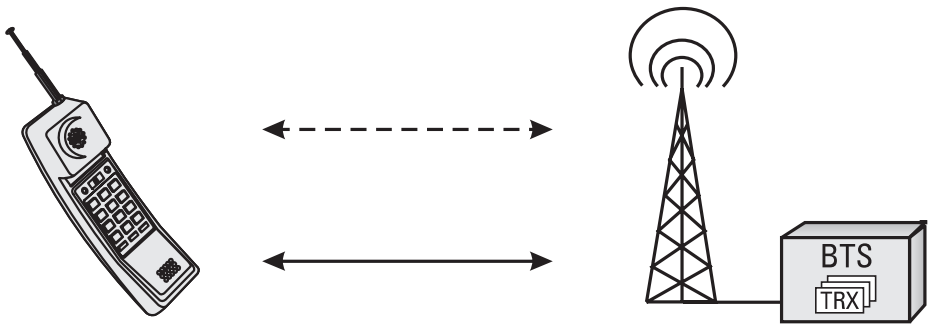


Figure 12.11 The intra-BTS handover.

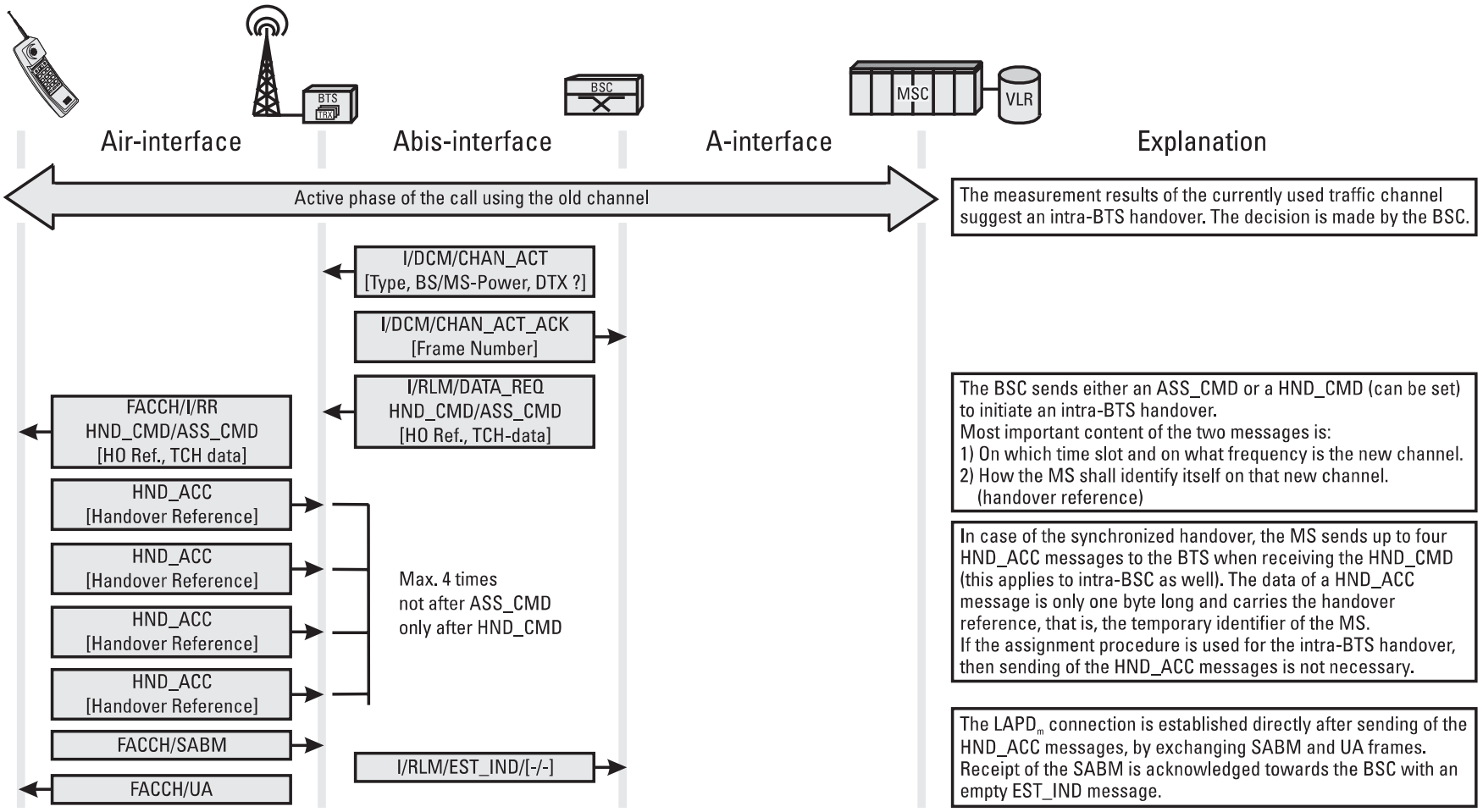


Figure 12.12 The synchronized intra-BTS handover.

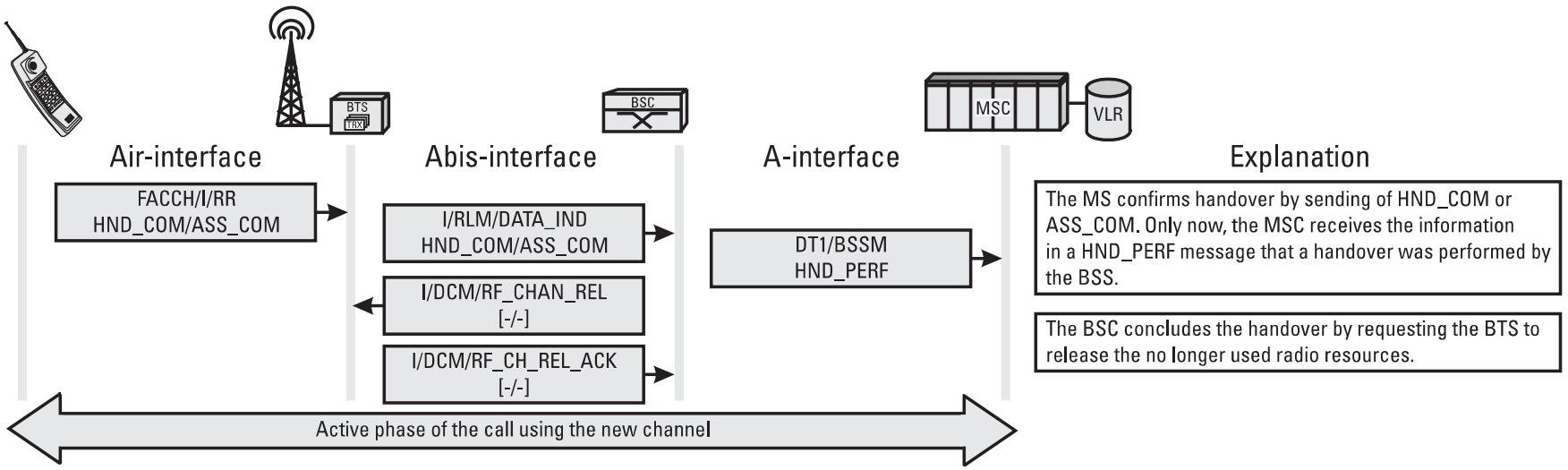


Figure 12.12 (continued)

Samsung Ex. 1032, Page 263 of 417

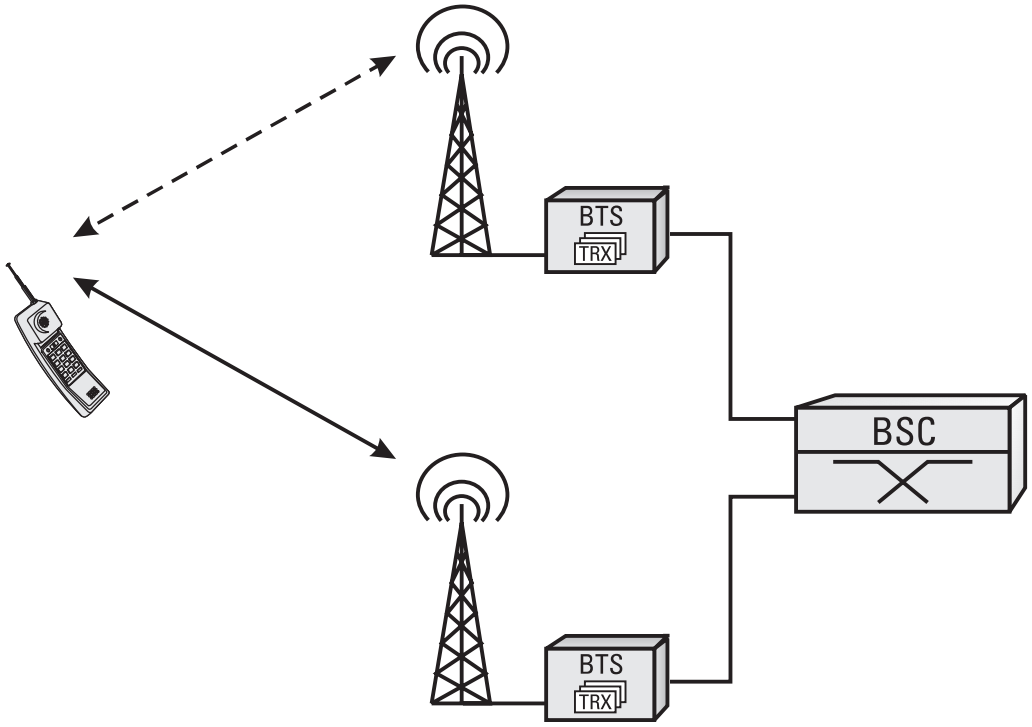


Figure 12.13 The intra-BSC handover.

12.5.3.4 Intra-MSC Handover

In an intra-MSC handover, the MS changes not only the BTS, but the BSC as well (Figure 12.15). Therefore, external handover is another term for this type of handover. In contrast to the intra-BTS handover and the intra-BSC handover, the MSC mandatorily is in charge for the execution of the intra-MSC handover. The responsibility for the MSC does not, however, include processing the measurements of the BTS or the MS or to conclude that a handover is necessary. These functions always remain with the BSC. (Note: How should the BSC know in advance what type of handover will be needed, or, in other words, where the destination cell of a handover will be?) After the BSC has decided that a handover to a BTS controlled by another BSC has to be performed, it informs the MSC and waits for instructions. The MSC requests the target or new BSC to reserve the necessary radio resources for the new connection. If the new BSC is able to process the request, it returns a complete HND_CMD message to the MSC, which will pass it on to the first BSC. The old BSC, after receiving the response from the target BSC, passes the HND_CMD to the MS and releases the radio resources after confirmation by the MSC. Figure 12.16 describes this scenario. In Figure 12.16, the distinction between messages to and from the old and new BSC is made by the different arrow styles (old BSC = small arrows, new BSC = large arrows).

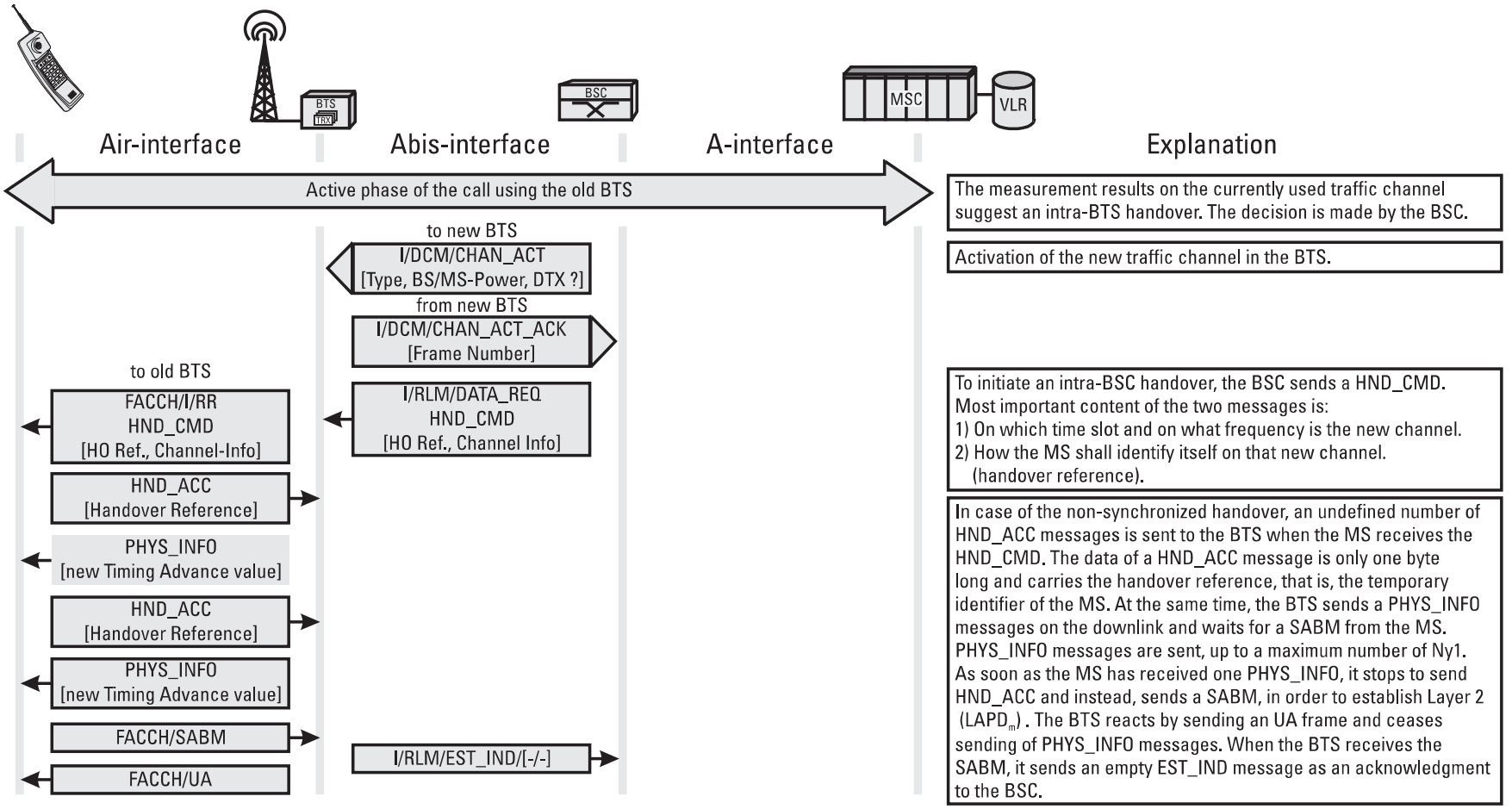


Figure 12.14 The nonsynchronized intra-BSC handover.

Samsung Ex. 1032, Page 265 of 417

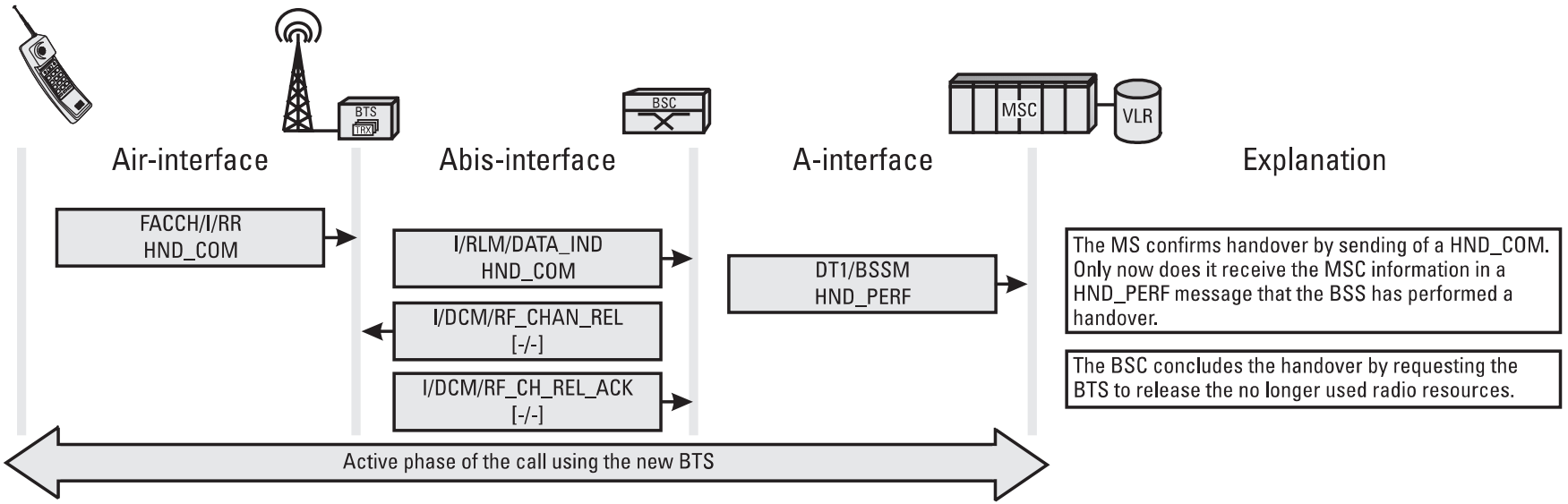


Figure 12.14 (continued)

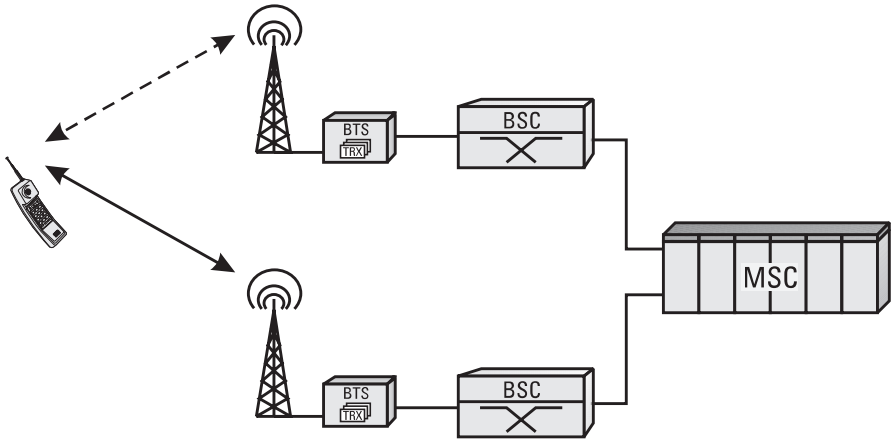


Figure 12.15 The intra-MSC handover.

12.5.3.5 Inter-MSC Handover and Subsequent Handover

Inter-MSC Handover

The handover cases described so far have involved increasingly more and more subsystems that were affected every time the next higher level in the hierarchy took over control of the execution of the handover process. However, which part of the system will take the control task when even the MSC is changed during a handover? This scenario is referred to as inter-MSC handover.

The answer is simple but requires some explanation. The control of the inter-MSC handover stays with the old MSC (MSC A in Figure 12.17).

Furthermore, even the CC functions for a connection handed over to MSC B stay with MSC A *after* the inter-MSC handover, that is, MSC A stays in full control of that connection.

Consider this example. If a GSM call toward an ISDN subscriber is originally set up in city A (with MSC A), that call is controlled by MSC A in city A. If the mobile subscriber drives into another MSC area, let's say city B (with MSC B), the call needs to be handed over by an inter-MSC handover procedure from MSC A to MSC B. However, because the ISDN does not provide any handover capabilities, the outgoing connection stays somewhat tied to MSC A. Therefore, MSC A remains in charge for all CC functions and, by means of the inter-MSC handover, just relays its RR functions toward MSC B. This rule is not restricted to calls toward the ISDN but is applicable for all calls. Figure 12.18 shows the scenario for an inter-MSC handover.

If in an inter-MSC handover, the original MSC always maintains the CC functionality, what then are the tasks of MSC B, and what happens if another inter-MSC handover is performed, either back to MSC A or to a third MSC, MSC C? As before, these answers are simple but require some explanation.

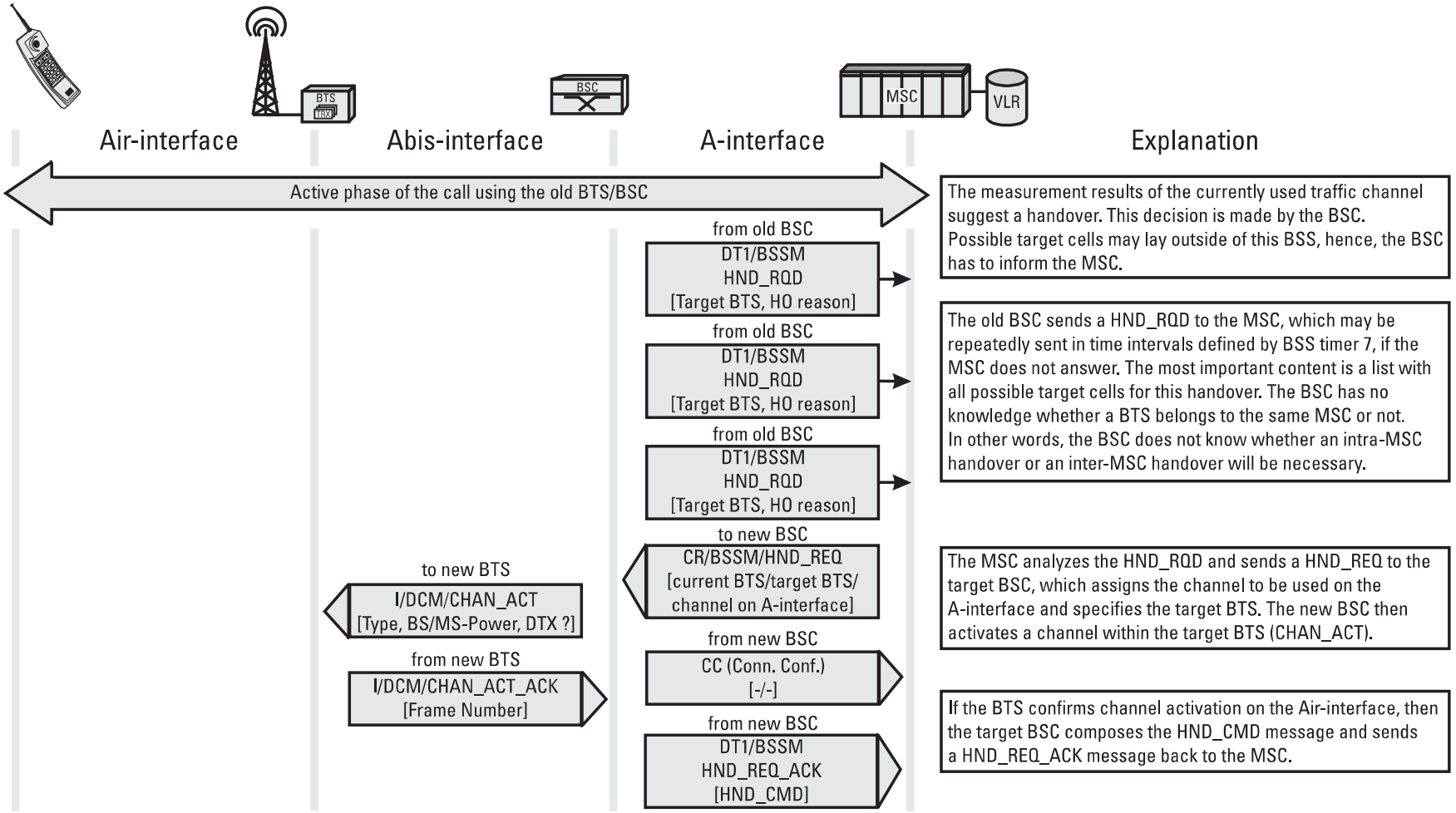


Figure 12.16 Scenario of intra-MSC handover.

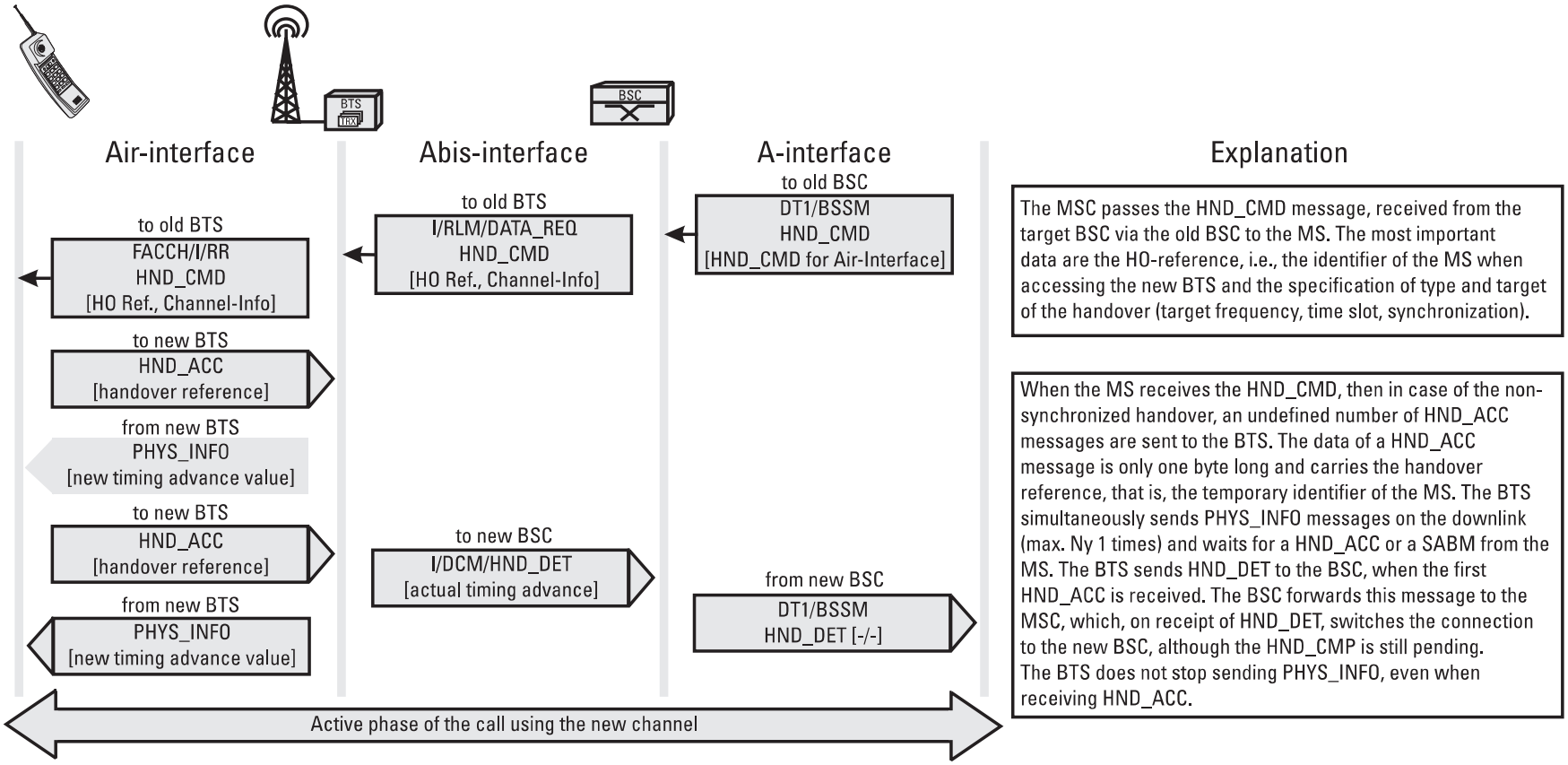


Figure 12.16 (continued)

Samsung Ex. 1032, Page 269 of 417

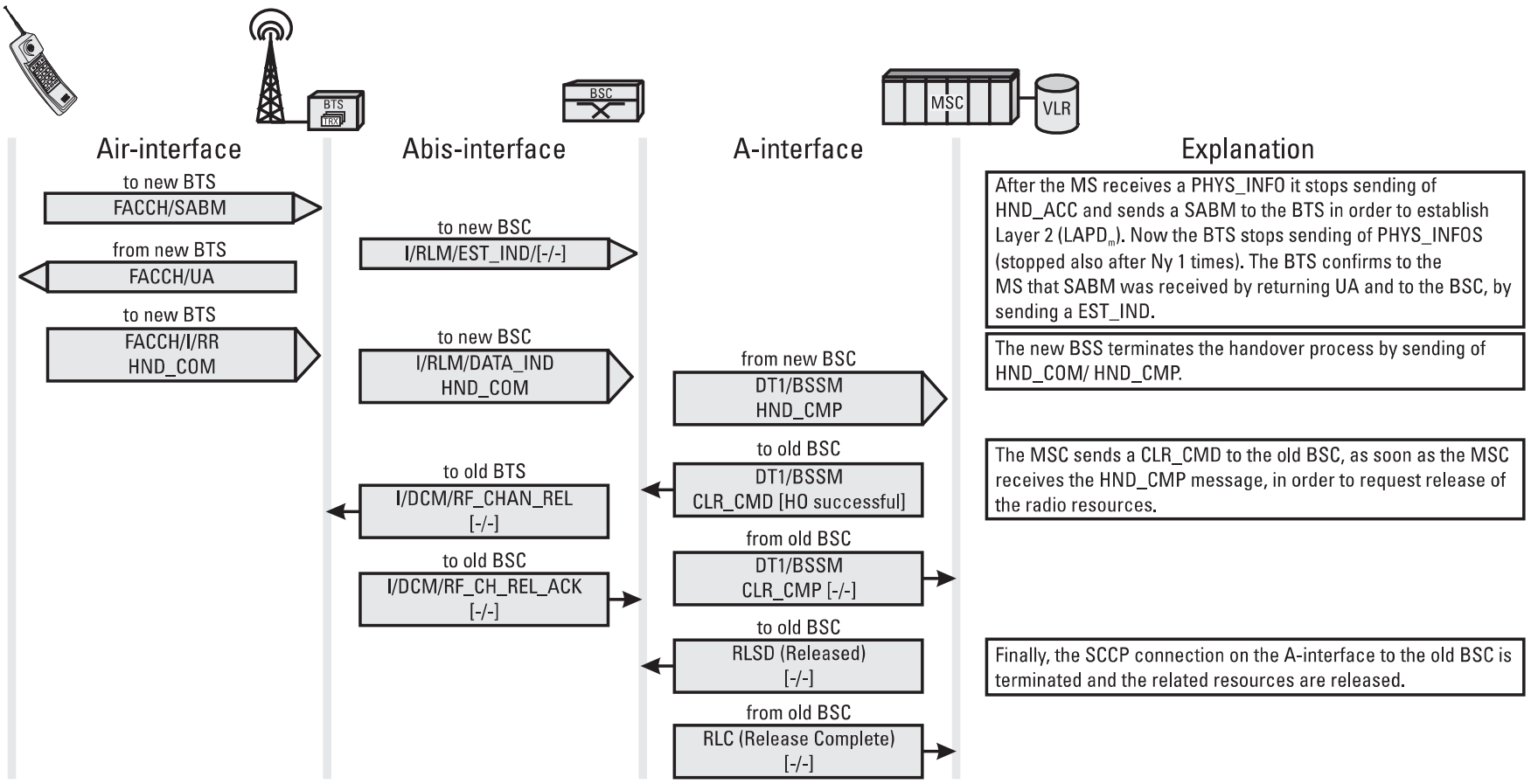


Figure 12.16 (continued)

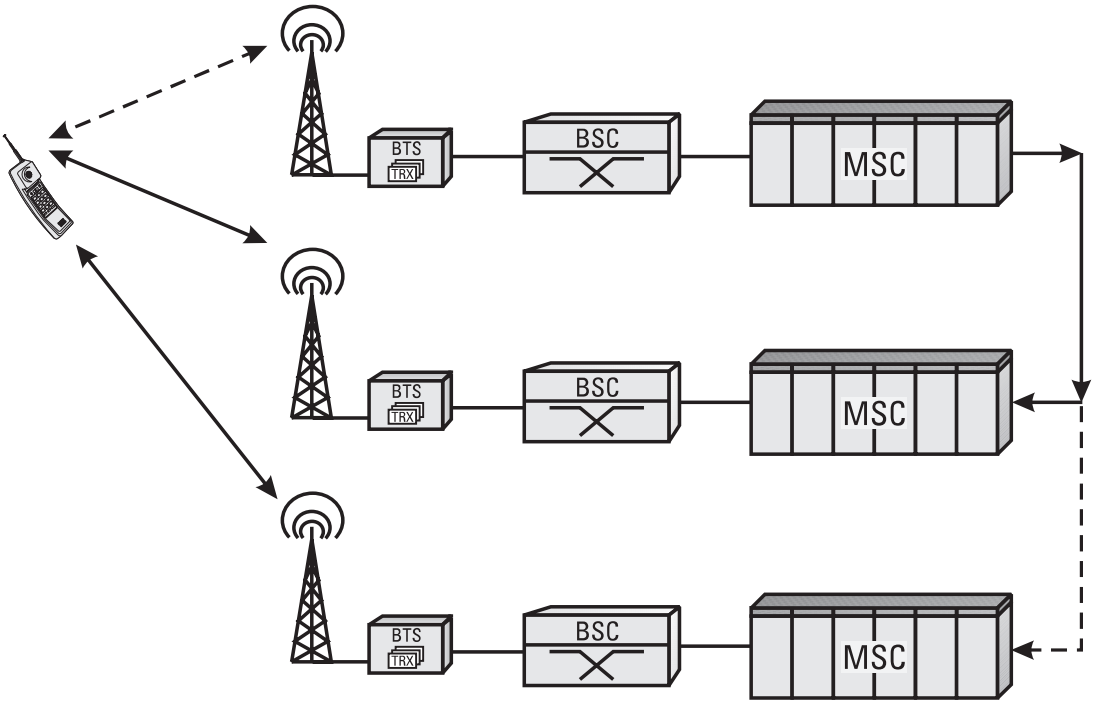


Figure 12.17 Inter-MSC and subsequent handover.

As already mentioned, MSC B, as the receiving MSC, takes control over all RR tasks, which are internal to the MSC. These are in particular intra-MSC handover-related tasks.

The subsequent handover scenario is applied in case of such a second inter-MSC handover, described next.

Subsequent Handover

Two cases have to be distinguished for the subsequent handover:

- A handover from MSC B back to the original MSC (MSC A);
- A handover into a third MSC area (MSC C).

Although MSC B initiates a subsequent handover, MSC A still maintains overall control of the call, during and even after a subsequent handover. Overall control means that, in any case, independent of whether the target of the handover is MSC A or a third MSC, the CC functionality always remains with MSC A. Figure 12.19 provides the scenario and the messages for a subsequent handover back to MSC A. Figure 12.20 provides the scenario and the messages for a subsequent handover to a third MSC (MSC C).

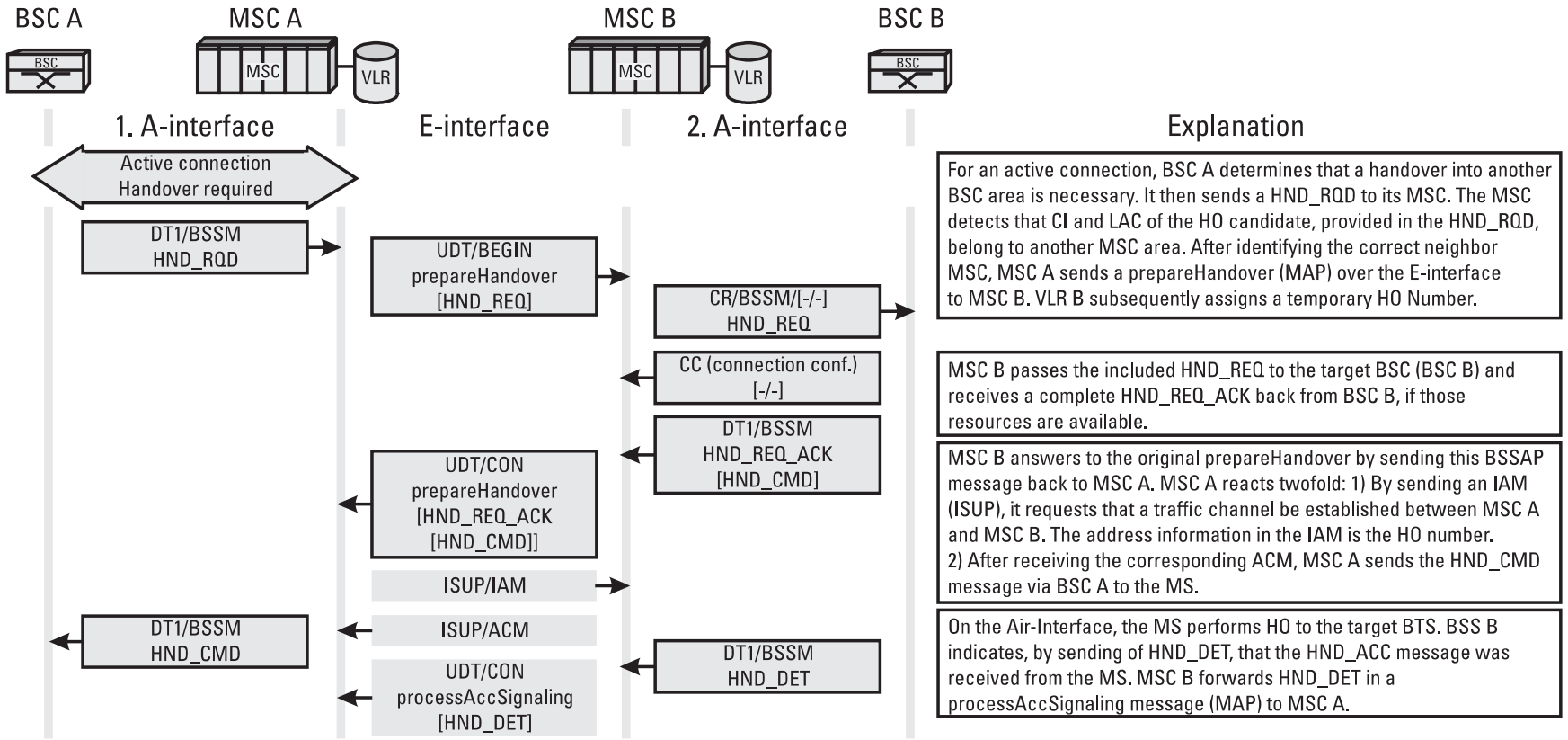


Figure 12.18 Scenario for inter-MSC handover.

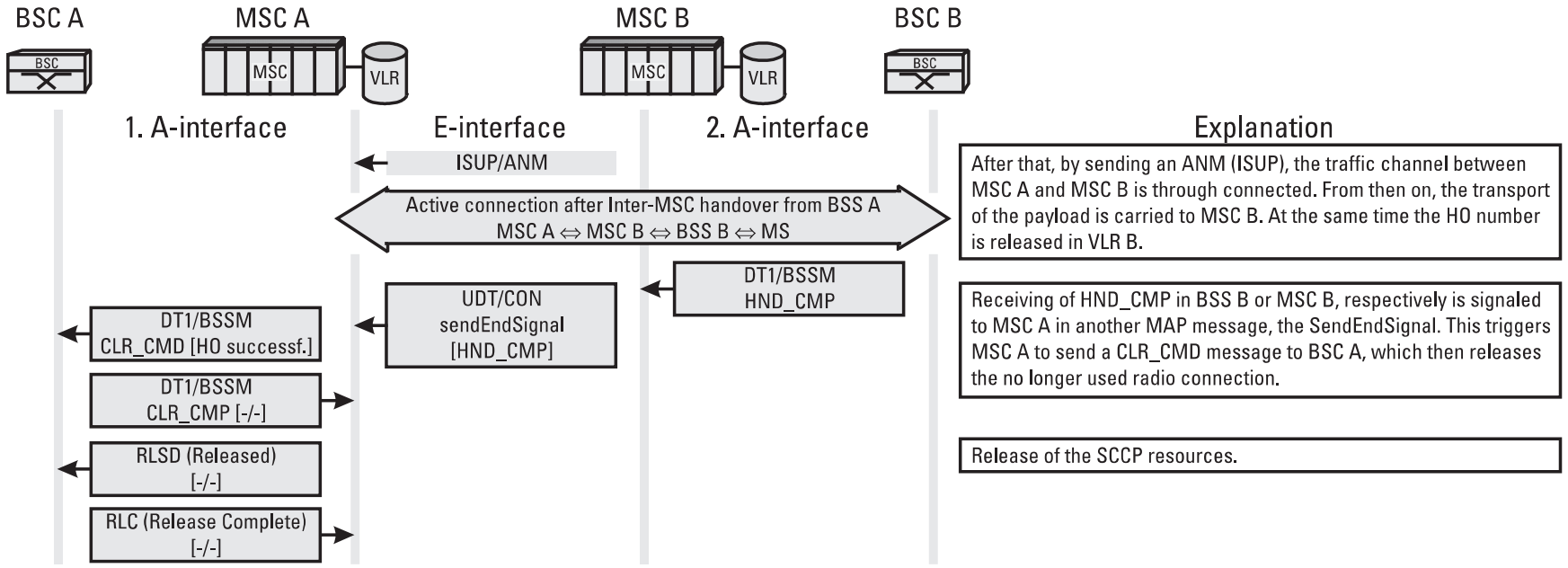


Figure 12.18 (continued)

Samsung Ex. 1032, Page 273 of 417

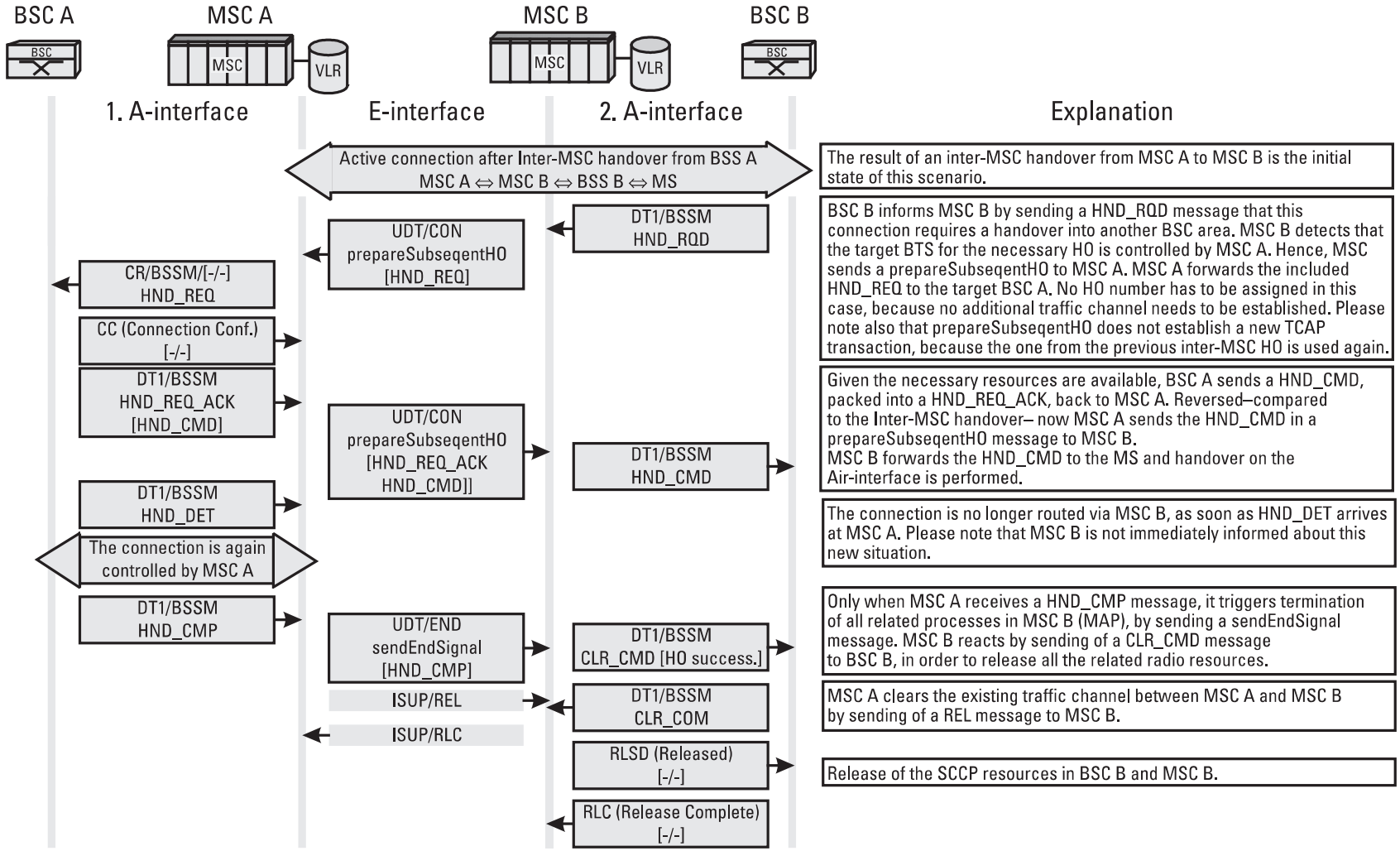


Figure 12.19 Senario for subsequent handover back to MSC A.

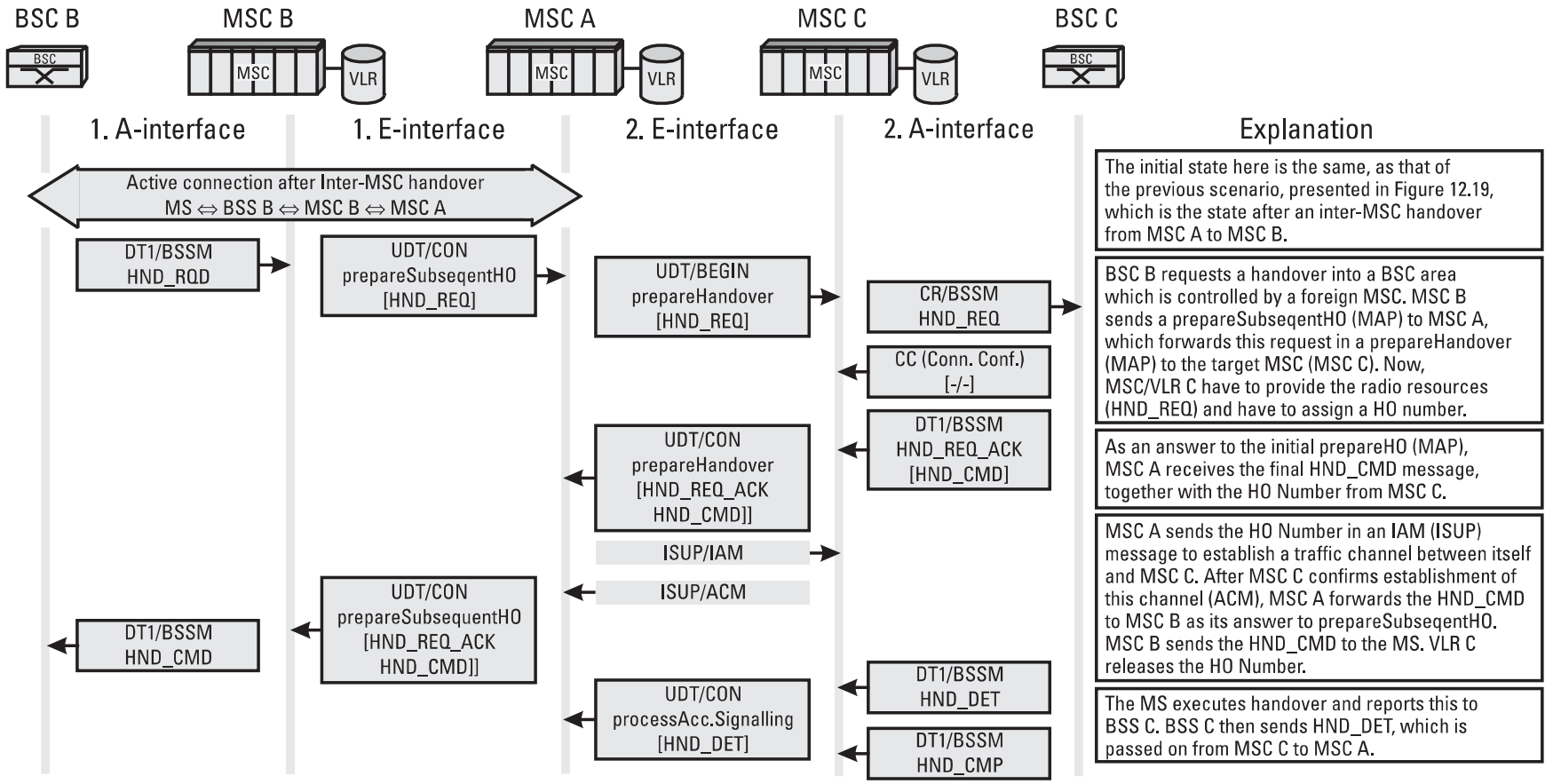


Figure 12.20 Senario for subsequent handover to MSC C.

Samsung Ex. 1032, Page 275 of 417

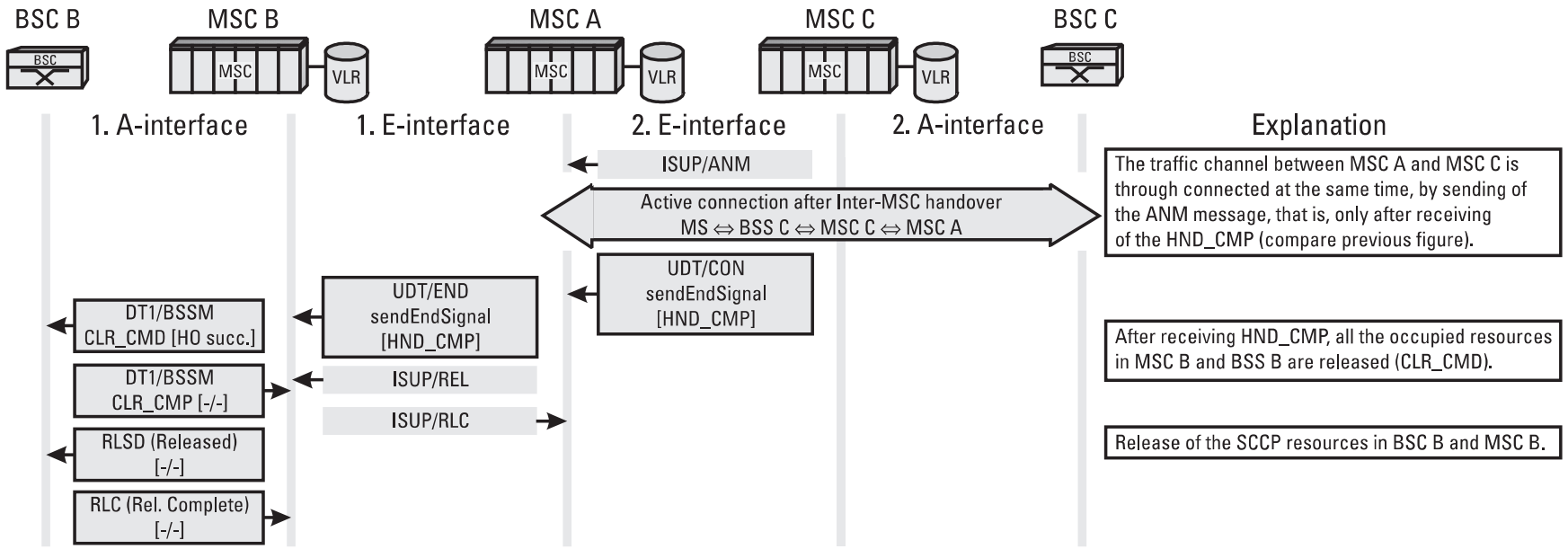


Figure 12.20 (continued).

Message Transport Over the E-Interface

MSCs have to relay BSSAP-related data that is coming from the A-interface, over the E-interface during inter-MSC handover, during subsequent handover, and thereafter. For that reason, the MAP protocol includes two messages specifically defined to perform that task, that is, to transparently transmit messages between MSCs. The two messages are the forwardAccessSignaling message and the processAccessSignaling message. As illustrated in Figure 12.21, the forwardAccessSignaling message is used to transport BSSAP messages in the downlink, that is, to the MS, while the processAccessSignaling message is used in the opposite direction.

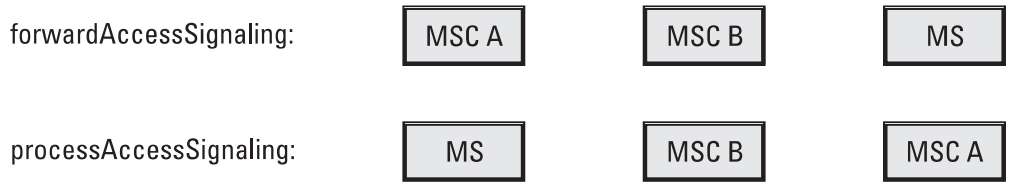


Figure 12.21 Transfer of BSSAP signaling over the E-Interface after Inter-MSC handover.

13

Quality of Service

The term quality of service (QOS) has a specific meaning in telecommunications. It refers to the usability and reliability of a network and its services. This chapter highlights possible applications of protocol analyzers for the supervision and analysis of network quality and presents the problems that GSM network operators most frequently face.

How can protocol test equipment be used to improve network quality? What errors occur most frequently in GSM and what are the root causes of those errors? How can reliable and comparable routines for statistical analysis be developed? This chapter focuses on answering those questions.

13.1 Tools for Protocol Measurements

In general, there are three ways to determine the QOS of a GSM network:

- Drive tests. Teams, paid by the network operator, drive on predefined routes in the network and periodically initiate calls. The results (e.g., unsuccessful handover, low-quality audio, dropped calls, signal strength) are transferred from the MSs to a dedicated PC, where the respective data are available for postprocessing. This kind of measurement represents most closely the network quality as real subscribers experience it. The disadvantage, however, is that only a limited area and a small time window can be tested and the testing is extremely expensive. Real-time measurement tools for call quality like QVOICE

Samsung Ex. 1032, Page 278 of 417

belong to the same category but allow for a more objective judgment on the call quality.

- Protocol analyzers. Preferably at a central place, protocol analyzers are connected to BTSs, BSCs, and MSCs over a period of time. Frequently, these devices come with remote access capabilities, which eases most configuration changes. Captured trace files can be uploaded to a central office for statistic evaluation. When problems are detected, the trace file needs to be analyzed manually and more thoroughly. Measurements with protocol analyzers have the advantage that all captured events are available for later, detailed analysis. The disadvantage is that it is not commercially feasible to have them in such great numbers that an entire GSM network could be observed permanently. (Of course, vendors of protocol analyzers might have a different opinion.)
- OMC. Several counters can be activated in the BSS and in the NSS from the OMC to provide the central office with the most important data about network quality. Various counters for all kinds of events permanently provide the network operator with information about the state and quality of the network. Examples are counters for the number of incoming or outgoing handovers; call drops before, during, and after assignment; and dropped calls due to missing network or radio resources. The major advantage of measurements via the OMC is that it provides results about the quality of the entire network rather than single BTSs or BSCs. On the other hand, this method is the most abstract one and the one that least relates to what the subscribers are encountering. Furthermore, it hardly allows for a detailed postmortem analysis.

Only the combination of the measurement results of OMC, protocol test equipment, and the–most expensive–drive tests, allows to make a qualified and objective statement about the real Quality of Service.

The focus of the following explanation is put on measurements with protocol analyzers, whereas this information can be translated, fairly easily to OMC measurements.

13.1.1 OMC Versus Protocol Analyzers

QOS involves the permanent observation, supervision, and adjustment of the various network parameters in a telecommunication system. GSM makes no exception. One of the most important functions of the OMC is to provide

feedback about network quality in real-time (more or less). For that purpose, a network operator can choose from a large selection of measurable events that may occur in the BSS or NSS, to be gathered in a predefined time period and then displayed at the OMC. It is a typical task of the network operator to determine the network quality from the available data and to decide on eventual corrective measures.

The time period that a single TS is occupied, the rate of ASS_FAI, separated for MOC and MTC, and the number of handovers, based on DL_QUALITY, are more examples of such counters, to name only a few.

The OMC has some advantages in detecting existing and potential network problems, compared to protocol analyzers:

- The OMC is part of the standard delivery of a GSM system and as such requires no extra procurement.
- The OMC plays a central part in its function as an O&M platform. If network quality is monitored by the OMC, countermeasures can be taken immediately when problems arise.
- Although protocol analyzers allow the capture of data on the A-interface, other important data have to be gathered on the BTS level, that is, on the Abis-interface. A complete analysis of data related to the entire coverage area by protocol analyzers, including data from the Abis-interface (e.g., idle channel measurements on the Air-interface) is not possible, due to logistical and financial limitations. That is where the OMC appears as the optimal tool.
- The OMC measures events and provides the results of respective counters to the network operator. Those values later can be processed and evaluated. For that reason, the OMC is the optimal aid for statistics tasks.

The protocol analyzers, on the other hand, can also claim a number of advantages as follows:

- A protocol analyzer is not part of the standard delivery of the infrastructure but an *independent* tool. To analyze the OMC counters, the field engineer needs system-specific know-how for the measurement. For the protocol analyzer system-independent know-how is necessary.
- The OMC is of little help for problem analysis during the process of bringing a network or single network elements into service (without subscriber traffic). That is different for protocol analyzers.

- Protocol analyzers allow the network operator and the system supplier to conduct measurements on the lowest level; it allows capture of complete call traces.
- Protocol analyzers typically come with additional software that provides for excellent statistical analysis. That enables the field engineer to evaluate a situation quickly. Technologically advanced software makes a manual analysis of data unnecessary in most cases.

In summary, both OMC and protocol analyzers are necessary tools for the network operator as well as for the system supplier. That is particularly true for the supervision of QOS. OMC and protocol analyzers perfectly supplement each other in this area, to ensure optimal network quality for both the network operator and subscribers. For those reasons, network operators use the OMC to monitor a GSM network on a broad scale, while they still have specialists with protocol analyzers for the bottom-down analysis of specific network problems. If the OMC detects a problem but is not able to identify the cause of the problem, the specialist goes on site, usually with a protocol analyzer, to narrow the problem down.

In the laboratory of a system provider or for product development and integration, the protocol analyzer plays a much more important role than the OMC.

13.1.2 Protocol Analyzer

A protocol analyzer is a measurement tool with a high impedance that can be connected between two system devices to intercept the digital data traffic between the devices (Figure 13.1). The focus here is on the analysis of signaling, that is, the control information between the devices. For that purpose and to simplify its operation, a state-of-the-art protocol analyzer needs the following:

- The complete hardware and software necessary to detect and adapt to the settings of the various interface configurations and time slots;
- Software that allows decoding of the binary PCM-code in plain text;
- A screen to display the measurement results;
- Facilities for remote access;
- Storage capacity of an appropriate size to store the measurement results for postprocessing;

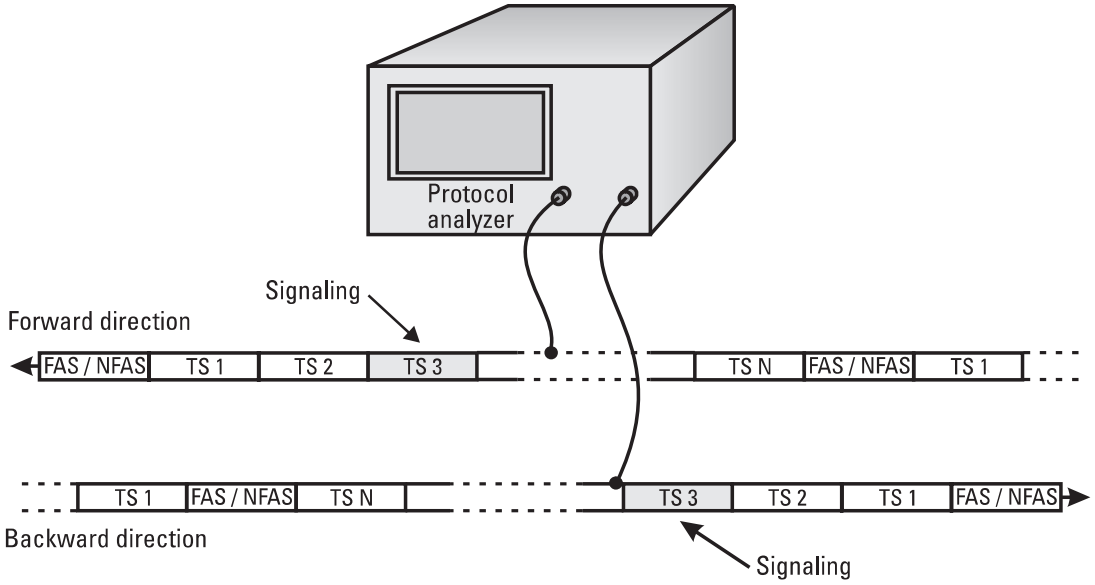


Figure 13.1 Setup of a protocol analyzer.

- Software tools to filter or search for specific data and parameters;
- A software interface to regular PC editor to be able to export data, for example, for reports;
- Flexible and easy-to-use statistic functionality.

The majority of the protocol analyzers available today meet those requirements reasonably well. Operation is fairly simple, because most of the devices are PC-based and offer additional hardware in form of expansion boards.

The protocol analyzer of the late 1990s consists of a mechanically robust PC expansion board loaded with software and offers the above listed functionality and additional features. Built into a laptop computer or desktop PC, protocol analyzers are portable or can be used in versatile ways in the laboratory.

It is worthwhile to point out what enormous progress has been made in recent years by the manufacturers of such equipment. While there was hardly any choice in the beginning of GSM (1991), system manufacturers and network operators quickly reacted to the increased need. Today, a multiplicity of protocol analyzers are available from many European and U.S. vendors. With GSM, a new era has started in this area. High-frequency (radio) measurements clearly have lost importance, compared to protocol measurements. GSM, as a digital standard, carries the analog problems on the Air-interface (e.g., interference), digitally coded into the BSS. Most radio-specific problems are well suited for analyzing and narrowing down the problem with a protocol analyzer.

13.2 Signaling Analysis in GSM

Most of the signaling measurements in GSM are performed on the interfaces in the BSS for two reasons:

- The majority of the subsystems and interfaces of a wireless network are part of the BSS. Simply from the sheer number of Abis-interfaces and A-interfaces, BSCs, and BTSs, it is obvious that more need for error analysis exists in this area.
- The critical area of a wireless system, however, is the Air-interface. Interference and handover problems are only two examples for mobile-specific error scenarios that can best be investigated in the BSS.

Measurement of signaling is, of course, also important in the NSS. Note that there is an interesting difference between measurements in the BSS and the NSS:

Measurements of signaling in the NSS more often are performed manually, that is, individual messages have to be analyzed. The reason is that the problems in the NSS typically are not hardware related but are concerned with interworking of protocol implementations of different manufacturers or related to software errors after major or minor software updates.

The majority of the problems that occur in the BSS, on the other hand, are hardware related or caused by deficiencies in network tuning. These types of errors typically can be detected only after a statistical, that is, an automatic, analysis.

13.2.1 Automatic Analysis of Protocol Traces

In most cases, it is important to localize the source of error or first to get an overview. For this application, a number of manufacturers have developed extensive software packages that illustrate a summary or interpretation of the most important results of such measurements graphically or in tabular form.

One example is the software package developed by a group of people from DeTeMobil, headed by Mr. Hochscherff. Their software package illustrates in tabular form error rates, quality data, and load parameter for various GSM interfaces. For the time being, it allows processing of measurement results captured with a SIEMENS K1103 or Wandel & Goltermann MA-10. Figures 13.2a, 13.2b, and 13.3 show parts of such analysis on the A-interface and the Abis-interface, which are presented here with the permission of DeTeMobil. Note the extensive amount of detailed information that the

```
******************** A-Interface Statistic ***-1.9.6d-**********************
Copyright by M.Dicks, W.Ditzer /DeTeMobil GmbH
Starttime: 06/06/1997 10:07                 Stoptime : 06/06/1997 21:18
MSC: Entenhausen(A)  1.BSC spc: 12345 Own-BTSs: 33 LAs: 2 TotalBTSs: 43
Z  0   1.0 MOC-Analysis (no EC/SS/SMS)       Incoming
Z  1   Cm Serv Req     :  26543     100.0%   HO Request      :      0   100.0%
Z  2   Cm Serv Acc     :     49       0.2%   HO Request Ack  :      0     0.0%
Z  3   Cm Serv Rej     :    143       0.5%   HO Complete     :      0     0.0%
Z  4   Setup           :  25539      96.2%
Z  5   Alerting        :  21183      79.8%   6.0 Other messages
Z  6   Connect         :  14875      56.0%   Auth Request    :  87192   100.0%
Z  7   Connect Ack     :  14778      55.7%   Auth Response   :  85715    98.3%
Z  8                                         Auth Reject     :      2     0.0%
Z  9   2.0  MTC-Analysis                     Cipher Cmd      :  84712
Z 10   Pagings         :  60415              Cipher Complete :  84328
Z 11   Paging Response :  13615     100.0%   Ident Request   :   4388
Z 12   Setup           :  13125      96.4%   Ident Response  :   4280
Z 13   Alerting        :  12721      93.4%   TMSI Command    :  39704
Z 14   Connect         :   8305      61.0%   TMSI Complete   :  83969
Z 15   Connect Ack     :   8266      60.7%   MM-Status       :     20
Z 16                                         Block           :     32
Z 17   3.0 Location Update-Analysis          Block Ack       :     32
Z 18   LU Request      :  46598     100.0%   UnBlock         :     30
Z 19   davon Normal    :  32802              UnBlock Ack     :     35
Z 20         Periodic  :   4139              Reset           :      0
Z 21         IMSI att  :   9657              Reset Ack       :      0
Z 22   LU Reject       :   1182       2.5%   Reset CIC       :    169
Z 23   LU Accept       :  44733      96.0%   Overload        :      0
Z 24                                         HoRqd SDCCH-OWN :    252
Z 25   4.0  Assignment Analysis              HO Failure      :   1026
Z 26   Assignment Cmd  :  37809     100.0%   HO Performed    :    160
Z 27   Assignment Cmp  :  37173      98.3%   Clear Command   : 115487   100.0%
Z 28   Assignment Fail :    612       1.6%   Clear Complete  : 115481   100.0%
Z 29                                         Clear Request   :   3571     3.1%
Z 30   5.0  HO Analysis                      Pagings         :  60415
Z 31   5.1 Intra-BSC                         Paging Repeat   :  26039
Z 32   HO Required(TCH):  18876     100.0%   2.Pag & No Resp :  26045
Z 33   HO Request      :  18814      99.7%   SCCP-UDT        :  60882
Z 34   HO Request Ack  :  18753      99.3%   SCCP-CREQ       : 115701
Z 35   HO Command      :  18445      97.7%   SCCP-CC         : 115694
Z 36   HO Complete     :  17554      93.0%   SCCP-DT1        : 1241708
Z 37   5.2 Inter-BSC                         SCCP-RLSD       : 115686
Z 38   Outgoing                             SCCP-RLC        : 115570
Z 39   HO Required(TCH):   2463     100.0%   SCCP-CREF       :      1
Z 40   HO Command      :   2406      97.7%   SCCP-IT         :    774
Z 41   HO Success      :   2299      93.3%   SCCP-lost(BSC)  :     17
Z 42   Incoming                             SCCP-lost(MSC)  :     55
Z 43   HO Request      :   2595     100.0%   MTP-TFA         :      0
Z 44 .....
Z 45 ...
Z 46 .
Z 47 .
```

Figure 13.2(a) Result of a measurement on the A-interface (BSC related).

```
Copyright  M. Dicks, W. Ditzer / DeTeMobil GmbH

Z 76   Cell Individuell Statistics Subpage:   1

Z 77 BSC Index      :       1      1      1      1      1      1      1      1      1      1
Z 78 Cell Id        :     123    234    345    456    567    678    789    890    901   4321
Z 79 LUs            :    7276    756   1635   2250   1915   1165   1386   2102   1619   1519
Z 80 MOCs           :    2763    251   1377    827   2642   1006   1768   1846   1662   2721
Z 81 MTCs           :    1416    114    560    450   1389    470   1047    905    802   1321
Z 82 AssReq         :    3864    340   1821   1192   3703   1333   2608   2572   2324   3748
Z 83 AssCmpl        :    97.3%  98.2%  98.5%  98.2%  98.6%  98.3%  99.3%  98.8%  99.4%  97.8%
Z 84 AsFailCause 10 :    33.7%  33.3%  53.8%  57.9%  36.5%  64.7%  37.5%  68.6%  57.1%  27.7%
Z 84 AsFailCause  0 :    22.4%  66.7%  46.2%  31.6%  40.4%  35.3%  56.2%  25.7%  28.6%  18.1%
Z 84 AsFailCause 33 :    41.8%                        23.1%          6.2%   5.7%   7.1%  53.0%
Z 84 AsFailCaus.oth.:    3.1%                 25.0%                                16.7%   1.7%
Z 85 .....
Z 86 ...
Z 87 ..
Z 88 .
```

Figure 13.2(b) Result of a measurement on the A-interface (BTS related).

```
                ------------ Analysis TCHCHECK 1.3 (DTC PDM F14) ------------
File: Entenh_1.rec
Begin of recording 03.09.1993 at 17:17h,
Duration 18.7 hours
Link 1-2; Channels: |  33 |  92  |
Assignments         | 176 |  86  |

1:   act| assg| acpl|  ho| hcpl|  cf|  02|  1f|  28|  ei|  Tall|  Dlev|  Ulev| Dqul| Uqul|  SACCH%
       0|    0|   0%|   0|   0%|   0|   0|   0|   0|   0|     0|     0|     0| 0  0| 0  0|    0.00
       0|    0|   0%|   0|   0%|   0|   0|   0|   0|   1|     0|     0|     0| 0  0| 0  0|    0.00
      35|   15| 100%|  20| 100%|   0|   0|   0|   0|   0| 18.27|    34|    21| 0  2| 0  2|    2.60
      70|   23|  96%|  47|  83%|   6|   4|   1|   0|   0| 44.58|    36|    22| 0  2| 0  2|    2.40
      69|   37| 100%|  32|  72%|   2|   1|   1|   0|   0| 33.94|    33|    20| 0  3| 0  2|    1.83
      70|   33| 100%|  37|  89%|   3|   2|   1|   0|   0| 38.89|    31|    20| 0  2| 0  3|    2.33
      74|   36|  97%|  38|  89%|  16|   2|   5|   4|   0| 23.54|    33|    20| 0  3| 1  6|    7.13
      74|   31| 100%|  43|  84%|   6|   2|   1|   2|   0| 32.22|    35|    22| 0  2| 0  2|    3.77

2:   act| assg| acpl|  ho| hcpl|  cf|  02|  1f|  28|  ei|  Tall|  Dlev|  Ulev| Dqul| Uqul|  SACCH%
      26|   12|   0%|  14|   0%|  13|   5|   0|   8|   0|  0.05|     3|    18| 7 49| 3 17|   45.45
      26|    9|   0%|  17|   0%|  12|   6|   0|   6|   0|  0.03|     0|    23| 7 49| 4 26|   60.00
      27|   12|   0%|  15|   0%|  14|   6|   0|   8|   0|  0.02|     0|    25| 7 49| 3 15|   72.73
      26|    9|   0%|  17|   0%|  15|   9|   1|   4|   0|  0.03|     2|     8| 7 49| 5 40|   86.21
      26|    8|   0%|  18|   0%|  10|   4|   0|   6|   0|  0.02|     4|    13| 7 49| 5 33|   75.00
      25|   11|   0%|  14|   0%|  12|   2|   0|  10|   0|  0.06|     2|    25| 7 49| 2 13|   46.15
      25|   12|   0%|  13|   0%|  14|   5|   0|   9|   0|  0.05|     1|    24| 7 49| 3 20|   72.73
      26|   13|   0%|  13|   0%|  11|   3|   1|   6|   0|  0.02|     5|    10| 7 49| 5 39|   87.88
```

Figure 13.3 Result of detailed measurement on the Abis-interface.

automatic analysis already contains. Figure 13.2a presents the data from the perspective of the BSC, while Figure 13.2b presents the data for the BTSs of that BSC. Figure 13.3 presents a measurement example for the Abis-interface. Table 13.1 explains Figure 13.3.

Table 13.1
Explanation of Figure 13.3

Parameter	Explanation
act	The total number of CHAN_ACT messages per time slot.
assg	The total number of ASS_CMD messages per time slot.
acpl	The success rate for TCH assignment ((ASS_CMP) / (ASS_CMD)).
ho	The total number of HND_CMD messages per time slot.
hcpl	The success rate for TCH assignment ((HND_COM) / (HND_CMD)).
cf	The total number of all CONN_FAIL messages per time slot (all *causes*).
02	The total number of all CONN_FAIL messages per time slot with cause value 02 = *Handover Access Failure.*
1f	The total number of all CONN_FAIL messages per time slot with cause value $1F_{hex}$ = *Radio Link Failure (RLF) Warning.*
28	The total number of all CONN_FAIL messages per time slot with cause value 28 = *Remote Transcoder Failure*.
ei	The total number of ERROR_IND messages per time slot (all *causes*).
Tall	Indicates the average channel occupation time.
Dlev	The average level, with which the MS has received the BTS [dB_m].
Ulev	The average level, with which the BTS has received the MS [dB_m].
Dqul	The average receiving quality on the side of the MS (smaller numbers indicate a better quality).
Uqul	The average receiving quality on the side of the BTS (smaller numbers indicate a better quality).
SACCH%	Fraction of the MEAS_RES messages without MEAS_REP (that is, without measurement results from the MS). The smaller the number, the better.

The company Wandel & Goltermann takes a similar approach with its protocol analyzer MA-10. All the measurement results can be postprocessed, using commercial PC spreadsheet software. Creation of all kinds of statistics and graphical presentations is greatly simplified.

Figure 13.4 presents, as an example, the graphical analysis of an MA-10 trace file captured on the Abis-interface. It shows the graph of the RXLEV value over time for a single call, whereby the measurements for neighboring cells also are shown. The values are taken from MEAS_RES messages. Compare this

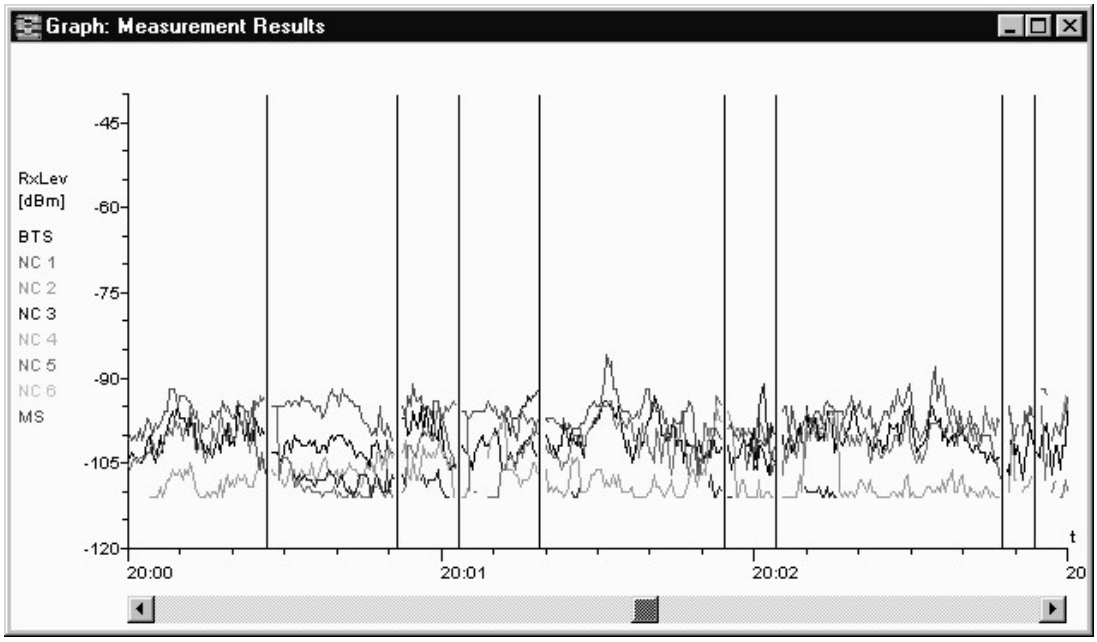


Figure 13.4 Graphical evaluation by means of the protocol analyzer MA-10.

form of analysis with the time-consuming analysis of single messages, for example, when interference needs to be analyzed in the uplink or the downlink of individual TRXs or TSs.

13.2.2 Manual Analysis of Protocol Traces

During the manual analysis of captured signaling data, experienced technicians investigate problems by searching specifically for error messages or inconsistencies, which allows them to draw conclusions on the possible reasons for an unknown problem. The result of such an investigation depends largely on the experience and the ability of the technicians to operate the equipment well.

In contrast to the automatic analysis of measurements on signaling, which also can be used for statistical purposes, the manual approach is more time consuming and hence used only in concrete error situations. Such cases typically are related to errors that cannot be solved by automatic analysis. Protocol errors and timer problems are two examples of such problems.

First of all, it is important during manual analysis to know whether the data are coded in hexadecimal or as normal text. It is much more difficult and

more time consuming to analyze hexadecimal data. To make the task easier, previous chapters provided a detailed description of the binary and hexadecimal formats of OSI Layers 2 and 3. That makes those chapters a practical reference. If protocol test equipment is available, the task of decoding is not necessary and interpretation of the data can start immediately. But even in that case, the task of the field engineer still is not easy. By taking advantage of all filter capabilities and search functionality, the essential information has to be extracted. Besides, a thorough understanding of the various scenarios and protocols is mandatory.

13.3 Tips and Tricks

During manual analysis of signaling data, some questions come up repeatedly. This section is intended to provide some help for such questions.

13.3.1 Identification of a Single Connection

13.3.1.1 Connection-Oriented SCCP Mode

The A-interface uses the connection-oriented SCCP mode for all major scenarios. The various messages between BSC and MSC, which are related to an individual connection, can be extracted by using SLR and DLR as a filter. Figure 13.5 illustrates that relationship. The SPC of SCCP network elements (the MSC and BSC, in the A-interface) are not suited, since this value is the same for all messages.

13.3.1.2 Connectionless SCCP Mode

The connectionless SCCP mode is used on the A-interface, for example, to administer the A-interface resources and for paging. There exists hardly any need for filtering connectionless messages. If, however, that should become necessary, the best approach is to use the BSSAP message type as the filter criterion.

Furthermore, the complete MAP communication of the NSS is performed via the connectionless SCCP mode. Because of the fact that MAP scenarios positively are dialogs between subsystems, there is a need to identify all messages of a single dialog. As shown in Figure 13.6, the originating transaction identifier and the destination transaction identifier of the TCAP protocol are well suited for that task.

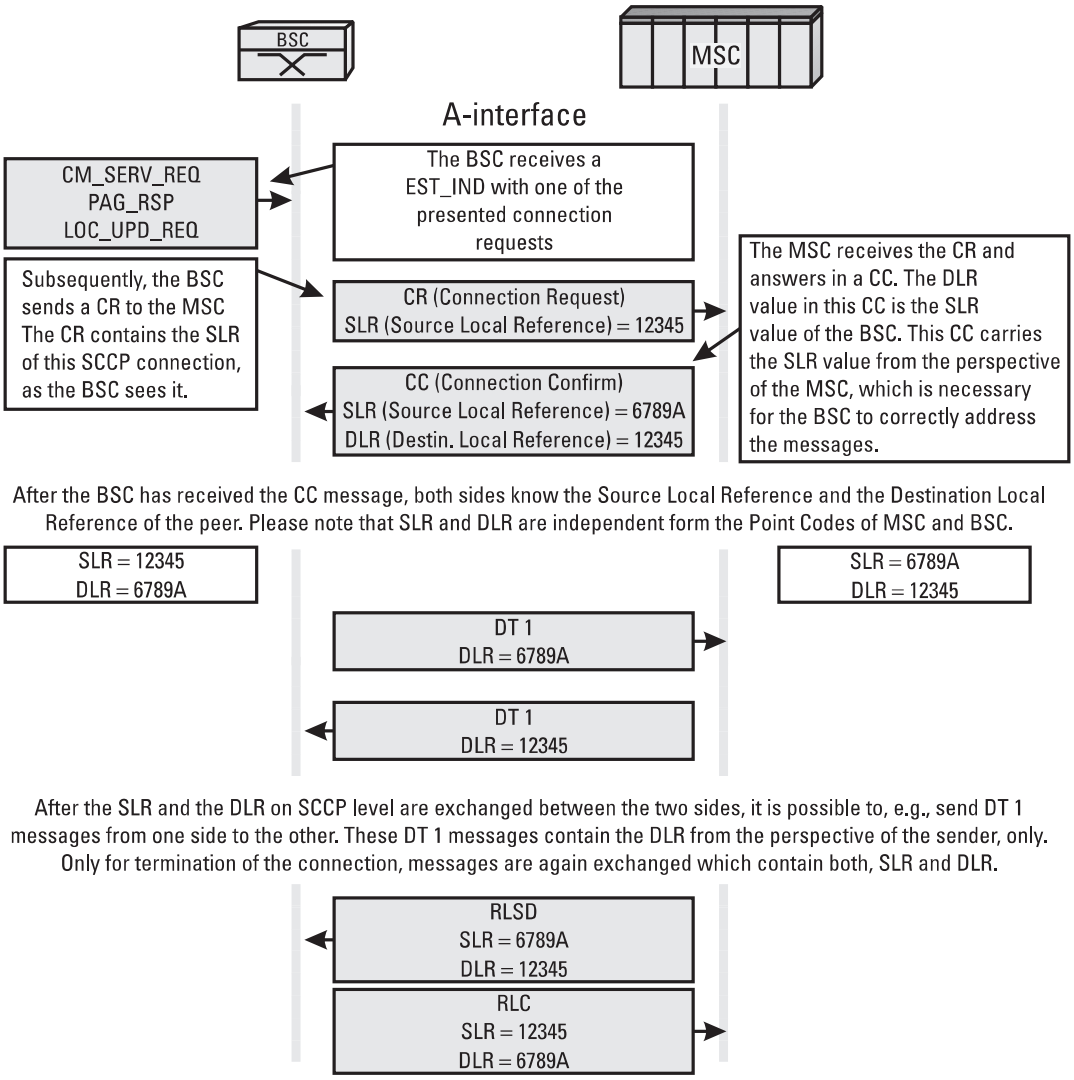


Figure 13.5 Identification of a connection by source local reference and destination local reference.

13.3.1.3 On the Abis-Interface

Before taking measurements on the link between BTS and BSC, the channel configuration has to be determined, since every TRX communicates with the BSC over another TS on the Abis-interface. Otherwise, the risk of capturing the wrong data exists.

A single connection on the Abis-interface can be determined by analyzing the parameter channel number, where a distinction has to be made between CCHs and TCHs (see Chapter 6).

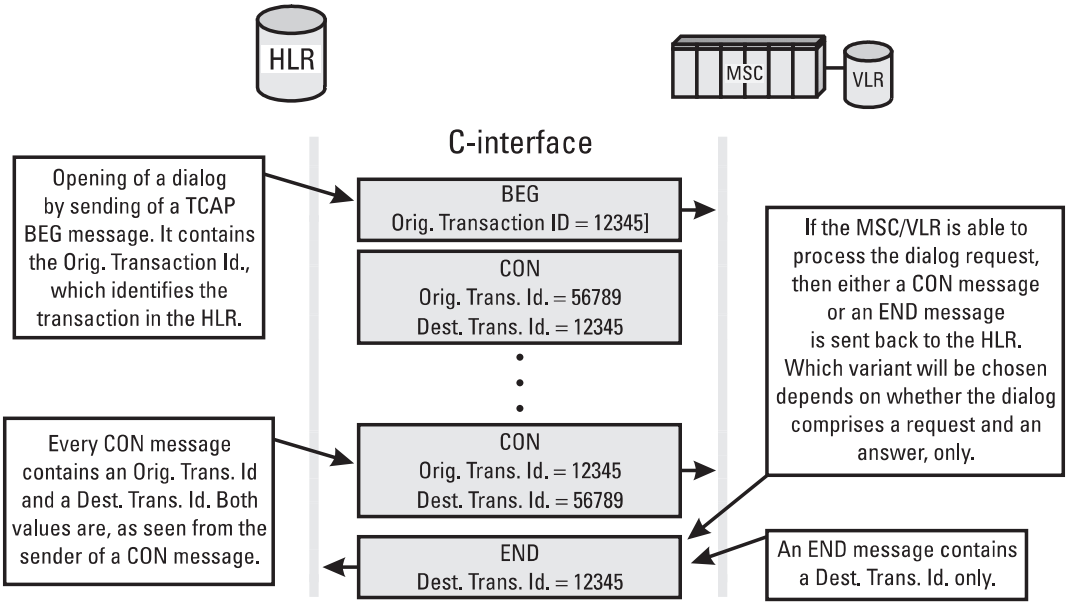


Figure 13.6 Identification of a single MAP connection.

13.4 Where in the Trace File to Find What Parameter?

In which messages and what parameters can the key information be found, and how can the dependencies be detected rapidly? Table 13.2 provides some hints, while Table 13.3 lists statistical information.

13.5 Detailed Analysis of Errors on Abis-Interface and A-Interface

Protocol analyzers are preferably used on the A-interface where it is possible to observe the quality of an entire BSS. The disadvantage of this approach is that it frequently requires additional measurements on the Abis-interface, because the root cause of an error cannot be localized just by looking at the messages on the A-interface.

It is frequently possible, however, because of an unambiguous relationship between error messages on the A-interface and the Abis-interface, to narrow a problem down to a few possible causes within the BSS by analyzing an A-interface trace only. The same applies to an even greater extent to the Abis-interface and the Air-interface. Because the BTS can be regarded as a transparent node for messages between BSC and MS, every error message on the

Table 13.2
General Information

Wanted Information	Interface, Protocol	Parameter, Message Type
Identity of the BTS	A, Abis	Cell Identity (CI) in CM_SERV_REQ, PAG_RSP, LOC_UPD_REQ.
Subscriber identity	A, Abis	IMSI/TMSI in CM_SERV_REQ, PAG_RSP, LOC_UPD_REQ.
Actual LAC during LU	A only	LAI parameter in the *Complete Layer 3* Information message (CL3I).
Former LAC during LU	A, Abis	LAI parameter in the LOC_UPD_REQ message.
Sender/receiver of a SCCP message	SCCP	*Called/Calling Party Address parameter* (Cd/CgPA) in the header of a SCCP message. The Cd/CgPA consists of a combination of a point code, a subsystem number (HLR, VLR, MSC, etc.), and a Global title.
Are there any SCCP problems?	SCCP	Look for CREF messages and UDTS messages. If either message can be found, problems are certain (overload?). Check also if all CR's (Connection Request) are answered with CC (Connection Confirm).
Are there any SS7 problems?	SS7	Look for LSSU's and COO's (change over orders). If LSSU's (SIPO or SIB) are detected, then severe SS7 problems on one of the two ends of the SS7 link exist.
Are there any SS7 problems because of high bit error rates?	SS7, OMC	Check if there have been frequent link failures recently. If so, find out if the cause SUERM threshold exceeded is indicated. Look for LSSU's (SIO and SIOS) in the trace file.
Are there any problems in the VLR/HLR?	A, Abis	Look for LOC_UPD_REJ, CM_SERV_REJ, and AUTH_REJ messages. Suspicious causes are: IMSI unknown in HLR, IMSI unknown in VLR, and LAC not allowed. If this occurs frequently, then data errors in the NSS database are likely.
Is there any MS activity in a BSC or a BTS?	A, Abis	Look for CM_SERV_REQ, PAG_RSP, and LOC_UPD_REQ. Detection of CHAN_RQD or IMM_ASS_CMD is not sufficient.

Table 13.2 (continued)

Wanted Information	Interface, Protocol	Parameter, Message Type
Are there Layer 1 problems on the Air-interface?	Abis	Look for CONN_FAIL messages (cause: '1' = Radio Interface Failure). If this occurs frequently, then further investigation is necessary (e.g., identify affected TRX).
Are there Layer 2 problems on the Air-interface?	Abis	Look for ERR_IND messages (frequent cause: '1' = timer T200 expired (N200 + 1) times; 'C_{hex}' = frame not implemented).
Is there interference in the uplink or downlink?	Abis	The RX_QUAL values are poor despite good or acceptable RX_LEV values in the uplink/downlink, frequent intra-BTS handover. Check assignment rate.
Are there problems when sending TRAU frames between transcoder, BTS, and MS	A, Abis	Abis-interface: Look for CONN_FAIL messages (cause: '28hex' = Remote Transcoder Alarm). A-interface: Look for CLR_REQ messages (cause: '20' = Equipment Failure).
Are there problems during incoming handover?	A, Abis	Abis-interface: Look for CONN_FAIL messages (cause: '2' = Handover Access Failure). A-interface: Look for CLR_REQ messages (cause: '0' = Radio Interface Failure).
Are there problems during outgoing handover?	A, Abis	A-interface: Look for HND_FAIL messages. Abis-interface: Look for HND_FAI messages.
Errors in the neighborhood relations? Poor coverage?	A, Abis	Check if there is hardly any outgoing handover. Check if the number of CLR_REQ cause: '1' = Radio Interface Failure (A) and CONN_FAIL (cause: '1' = Radio Link Failure (Abis)) is higher than normal (location dependent).
Are there problems related to interworking between MSC and BSC?	A	High ASS_FAI rate. Causes: Requested Terrestrial Resource unavailable, Terrestrial Circuit already allocated, Protocol Error BSC/MSC. Check trunk assignment and other settings in MSC and BSC. Were the BLO messages, possibly after a reset procedure, not repeated?
Are there any PLMN interworking problems?	MAP	Many ABT messages from the affected PLMN (cause: Application Context Name not supported).

Table 13.2 (continued)

Wanted Information	Interface, Protocol	Parameter, Message Type
Are there any BSC problems?	A	Though the related BTS's do not suffer overload, there are many ASS_FAI messages cause: '33' = Radio Resource unavailable.
Is a BTS blocked?	Abis	Check the RACH control parameters in the SYS_INFOS BCCH_INFOS 1–4. Is the Cell Barr Access bit = 1 or the Access Control Class not equal 0?
MSISDN /IMSI combination of a subscriber	MAP	The BEG/provideRoamingNumber message possibly contains both parameters. Another possibility is the BEG/sendRoutingInformation message contains the MSISDN and the END/sendRoutingInformation message contains the IMSI.
IMSI /TMSI combination of a subscriber	A only	PAGING message (works on the A-interface, only)
Signaling Point Codes	SS7	Routing Label in every message signal unit (MSU)
Distance between MS and BTS	Abis	Access delay in CHAN_RQD, timing advance (TA) in CHAN_ACT and all MES_RES. For a conversion from TA to distance refer to the Glossary.
Target cell during handover	A	Cell Identity in HND_RQD messages
MS power class (Handy, …)	A, Abis	Mobile Station Classmark X (RF Power Capability) parameter in CM_SERV_REQ, PAG_RSP, LOC_UPD_REQ
Called directory number in case of a MOC	A, Abis	Parameter Called Party BCD Number in SETUP message
Is DTX active?	Abis	DTX (uplink): downlink measurements (MEAS_REP) DTX (downlink): uplink measurements (MEAS_RES)

Air-interface translates uniquely into an error message on the Abis-interface; hence, for the majority of the applications, a protocol analysis on the Air-interface is not required.

Table 13.3
Statistical Information

Wanted Information	Interface, Protocol	Parameter, Message Type
Total of all moc attempts (bts/bsc)	Abis, A	$\sum$(CM_SERV_REQ)
Total of all mtc attempts (bts/bsc)	A, Abis	$\sum$(PAG_RSP)
Total of the successful incoming handover	A only	$\sum$(HND_CMP)
Total of the successful outgoing handover	A only	$\sum$(CLR_CMD [cause: '0B' = Handover successful])
Success rate for MOC's (BSS/BTS)	A, Abis	$\frac{\sum(\text{ALERT [from MSC} \rightarrow \text{MS]}) + \sum(\text{PROGRESS})}{\sum(\text{CM\_SERV\_REQ [Establishment cause} = \text{MOC]})}$
Error rate for MOC's (BSS/BTS)	A, Abis	$1 - \frac{\sum(\text{ALERT [from MSC} \rightarrow \text{MS]}) + \sum(\text{PROGRESS})}{\sum\text{CM\_SERV\_REQ [Establishment cause} = \text{MOC]})}$
Success rate for MTC's (BSS/BTS)	A, Abis	$\frac{\sum(\text{ALERT [from MS} \rightarrow \text{MSC]})}{\sum(\text{PAG\_RSP})}$
Error rate for MTC's (BSS/BTS)	A, Abis	$1 - \frac{\sum(\text{ALERT [from MS} \rightarrow \text{MSC]})}{\sum(\text{PAG\_RSP})}$
Success rate for incoming handover	A only	$\frac{\sum(\text{HND\_CMP})}{\sum(\text{HND\_REQ})}$
Error rate for incoming handover	A only	$1 - \frac{\sum(\text{HND\_CMP})}{\sum(\text{HND\_REQ})}$
Success rate for outgoing handover	A only	$\frac{\sum(\text{CLR\_CMD [cause: '0B'} = \text{handover successful]})}{\sum(\text{HND\_CMD})}$
Error rate for outgoing handover	A only	$1 - \frac{\sum(\text{CLR\_CMD [cause: '0B'} = \text{handover successful]})}{\sum(\text{HND\_CMD})}$

13.5.1 Most Important Error Messages

13.5.1.1 Clear Request (CLR_REQ) on the A-Interface

A CLR_REQ indicates a connection error detected in the BSS and mandates an abnormal termination. Except for error indications during the assignment

procedure, the CLR_REQ message is used for various error scenarios, including incoming and outgoing handover, as well as radio link failures in Layers 1 and 2.

In particular, CLR_REQ messages with cause '0' = radio interface message failure and cause '1' = radio interface failure frequently can be found in trace files.

The difference between the causes is that a *radio interface message failure* is reported when, during a Layer 3 scenario, signaling messages from the MS are not received on time. For example, during a mobile originating call setup, the SETUP message from the mobile station is not received. The connection is torn down by the BSS with CLR_REQ and cause '0' = radio interface message failure. On the other hand, CLR_REQ with cause '1' = radio interface failure is indicated, when problems in Layers 1 and 2 were detected on the Air-interface that require abnormal termination of a connection. Note that a *radio interface message failure* occurs most likely during connection setup, when Layer 3 signaling data need to be exchanged, while a *radio interface failure* can happen at any time during an active connection. In both cases, radio interface problems are the actual problem source.

As presented in Figure 13.7, the MSC reacts on receiving a CLR_REQ message by sending a CLR_CMD message to release the still seized radio resources.

13.5.1.2 Assignment Failure on the A-, Abis- , and Air-Interfaces

In contrast to the CLR_REQ, which can be sent any time during an active connection, the ASS_FAIL indication can frequently be sent only as a reaction to

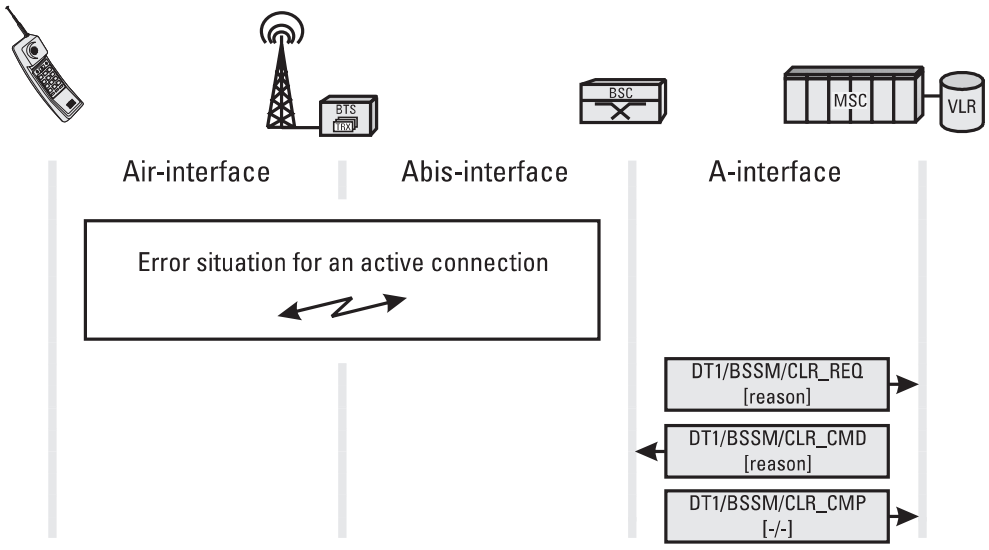


Figure 13.7 Use of the CLR_REQ message.

a faulty traffic channel assignment during call establishment. In that case, one has to distinguish between ASS_FAI on the Air-interface and Abis-interface, as defined in GSM 04.08, and the ASS_FAIL on the A-interface, as defined in GSM 08.08. The ASS_FAI is used on the Air-interface and the Abis-interface as a negative response for an ASS_CMD message, while ASS_FAIL is used as a reaction for an ASS_REQ message on the A-interface. Note that every ASS_FAI/ASS_FAIL message indicates an aborted connection setup. For that reason, network operators react sensitively on an increasing ASS_FAI/ASS_FAIL rate.

Another reason to use the ASS_FAI/ASS_FAIL rate as a rough indicator for the network quality lies in the fact that for the BSS and the radio interface, the assignment procedure is the most critical phase during call establishment. Any radio or BSS related problems most likely will become visible during the assignment procedure.

If the assignment procedure is unsuccessful, one of the following scenarios applies (see Figure 13.8):

- The BSC may reject an ASS_REQ, for instance, if the MSC tries to assign a channel on the A-interface that the BSC regards as not available or that is already in use. In such cases, ASS_FAIL with the respective cause is returned to the MSC, without the BSC sending a ASS_CMD message to the MS. Such an error cannot be investigated on the Abis-interface.
- When the BSC is able to process the ASS_REQ, it assigns a free traffic channel on the Air-interface and forwards the corresponding information in an ASS_CMD message (via the BTS) to the MS. The BSC then

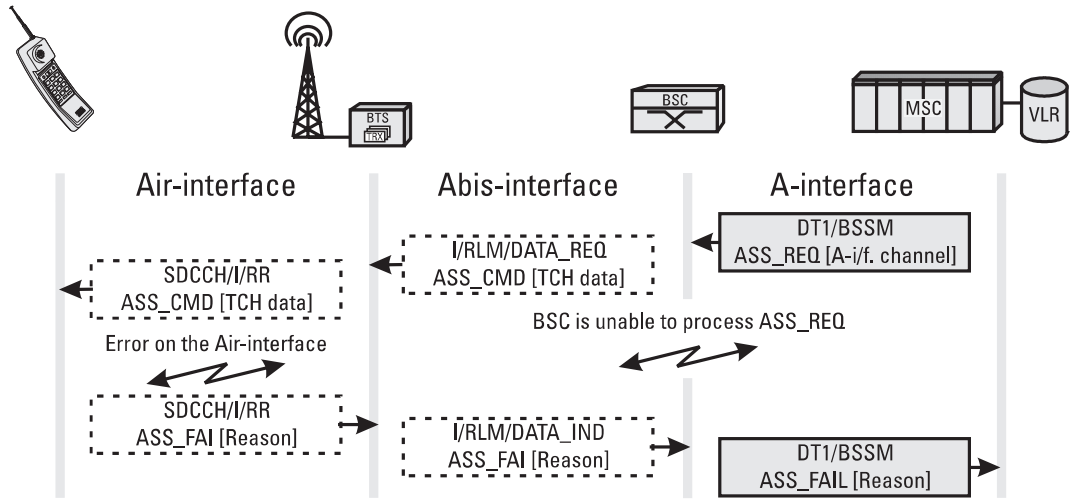


Figure 13.8 ASS_FAIL/ASS_FAI on A-, Abis-, and Air-interface.

waits for a defined time period, as specified by BSS timer T10, for a response from the MS.

- If the MS is unable to seize that traffic channel, it tries to send an ASS_FAI message with the appropriate RR cause over the SDCCH. Only in those cases will the ASS_FAIL message on the A-interface contain an RR cause.
- If the MS, because of an interrupted radio connection, is unable to send either an ASS_COM or an ASS_FAI to the BSC, the BSS timer T10 expires and an ASS_FAIL message with cause '0' = radio interface message failure is sent over the A-interface to the MSC.

13.5.1.3 Connection Failure (CONN_FAIL)

CONN_FAIL is an error message on the Abis-interface that indicates a Layer 1 error on the Air-interface. The most frequent reasons for a CONN_FAIL message are the following:

- The radio connection is lost on the uplink or downlink. In GSM, this kind of error is referred to as radio link failure (see Figure 13.9). After the BTS detects that the connection is lost, it sends a CONN_FAIL with cause 451' = radio link failure to the BSC. Radio link failures occur frequently on the SDCCH (particularly between AUTH_REQ and AUTH_RSP, since there is a fairly long time between the two), because a poor radio connection could just be established but not stay stable. For that reason, during a statistical analysis, it is advised that there be a distinction between errors on the SDCCH and errors on the TCH.
- Errors during incoming handover (cause '2' = handover access failure) (see Figure 13.10). The access on the new channel does not work and the BTS informs the BSC by sending a CONN_FAIL message. The occupied resources are released.
- Error during the TRAU frame synchronization in the uplink or the downlink after assignment of a traffic channel. In most cases, the problems are in the uplink direction, for example, because the wrong channel type was assigned (halfrate instead of fullrate, DTX on/off). When this error is detected in the TRX, the BTS sends a CONN_FAIL with cause '28_{hex}' = remote transcoder failure to the BSC (see Figure 13.11). Note that sporadic CONN_FAIL (remote transcoder failure) may occur, even without systematic errors. The rate should, however, not exceed 1.0% of all call attempts.

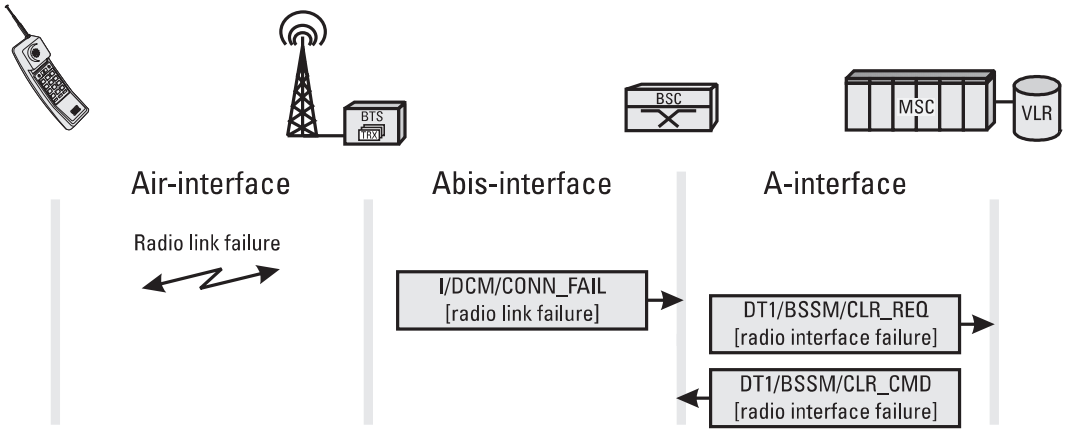


Figure 13.9 CONN_FAIL (cause '1' = radio link failure).

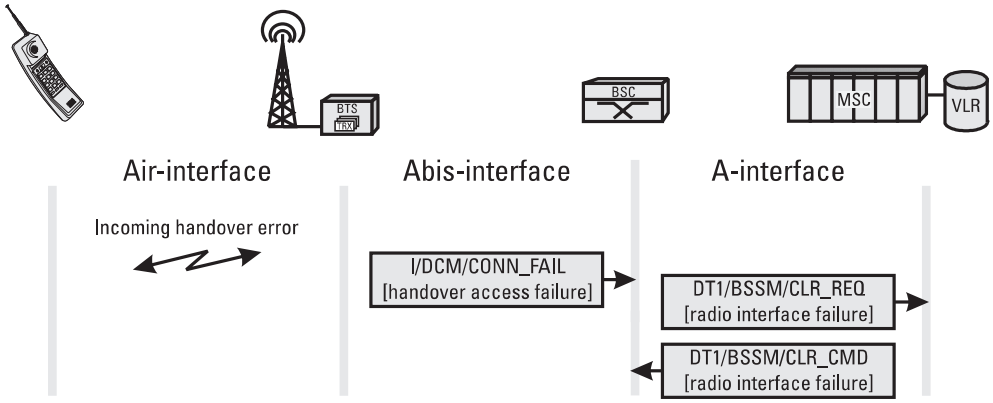


Figure 13.10 CONN_FAIL (cause '2' = handover access failure).

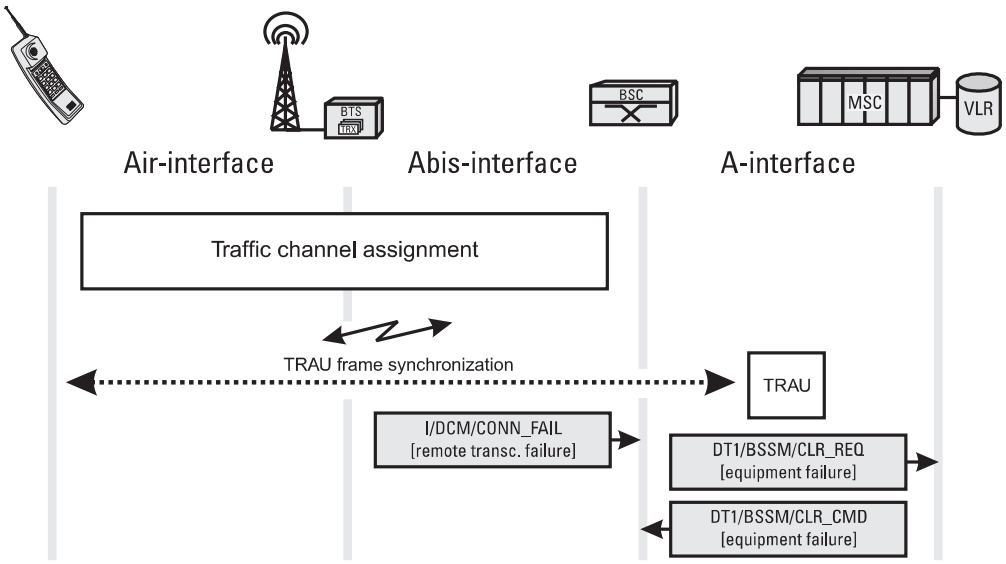


Figure 13.11 CONN_FAIL (cause '28_{hex}' = remote transcoder failure).

13.5.1.4 Error Indication (ERR_IND)

The ERR_IND message indicates a protocol error in Layer 2 on the Abis-interface, which occurred on the Air-interface. The reason, however, typically is not a protocol error but problems with the transmission as a consequence of a poor radio connection. Consequences of a poor radio connection may be the following:

- An increased bit error rate, which in turn can affect the $LAPD_m$ protocol. Examples include wrong frame type and P/F bit or C/R bit set wrong. In many of those cases, an ERR_IND with cause '$0C_{hex}$' = frame not implemented is sent to the BSC. When the BSC receives an ERR_IND message with this cause, it takes no special action, in particular, it does not tear down the connection (Figure 13.12).
- Repeated sending of $LAPD_m$ frames, for which the peer expects an acknowledgment, which it does not receive (Figure 13.13). If a Layer 2 message was repeated without acknowledgment as many times as indicated by the parameter N200, then an ERR_IND with cause '1' = timer T200 expired (N200 + 1) times is sent to the BSC. The BSC will then try to release the Layer 2 and Layer 1 resources, which in turn mainly results in a radio link failure in Layer 1, because the MS is not there anymore (see *Radio Link Failure* and the values for N200 in the Glossary).

13.5.2 Error Analysis in the BSS

This section presents hints on how to investigate the most frequent errors in a GSM network. The general approach is the exclusion method, that is, eliminating possible causes one by one, which is applied by many "cookbooks" that deal with this subject. Note that the explanation provides a good help to solving

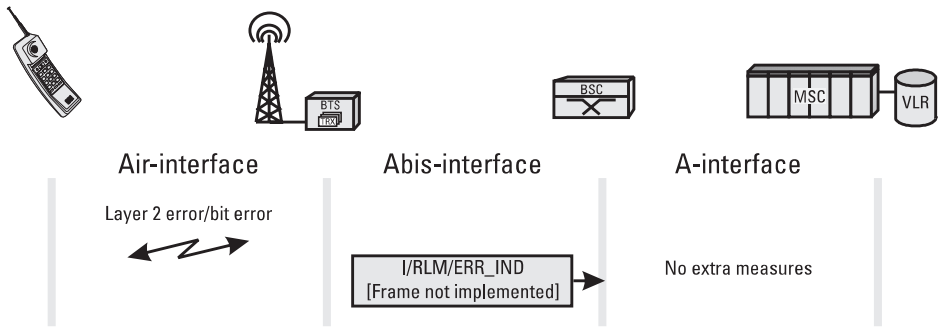


Figure 13.12 ERR_IND / Cause '$0C_{hex}$' = Frame not implemented.

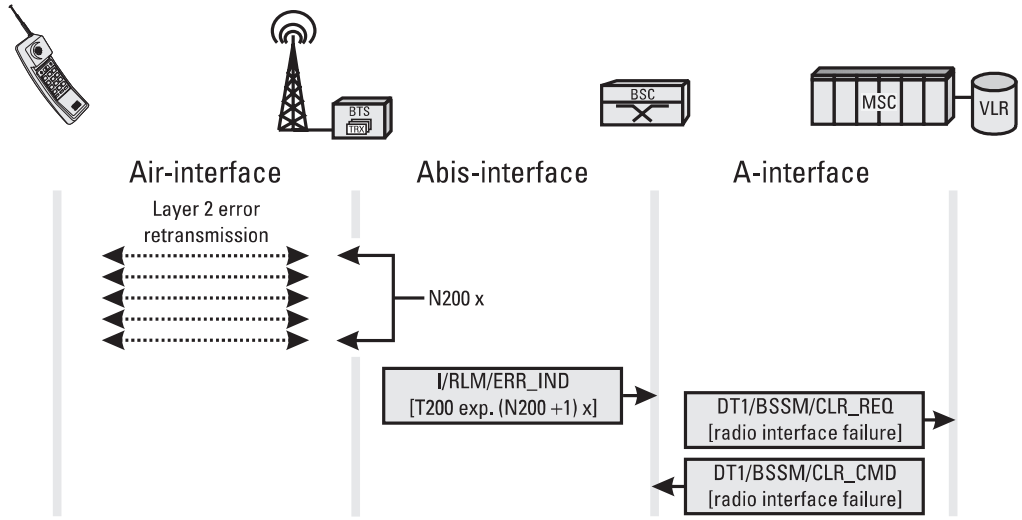


Figure 13.13 ERR_IND (cause '01' = timer T200 expired (N200 + 1) times).

many problems, but it is by no means the universal approach that always leads to success. Most times, field engineers need only an initial hint to be brought on the right track; from there, they are able to narrow the problem down on their own.

Also note that some of the proposed actions may be performed only during low traffic hours and only with the agreement of the network operator.

13.5.2.1 CLeaR REQuest (cause value: '0' = Normal Event—Radio Interface Message Failure)

An increased number of CLR_REQs point to problems during outgoing intra-MSC handover and during inter-MSC handover. In case of such a scenario, after sending a HND_CMD message, the old BSC expects a CLR_CMD message from the MSC within the time period defined by the BSS timer T8, to release the still occupied radio resources (Figure 13.14). If the old BSC receives no CLR_CMD or no HND_FAIL from the MS/BTS, it sends a CLR_REQ with the cause, radio interface message failure, to the MSC to trigger the release the occupied resources.

13.5.2.2 CLeaR REQuest (Cause Value: '1' = Normal Event—Radio Interface Failure)

A higher number of this CLR_REQ points toward problems during connection setup, during a connection, or during incoming handover. The cause for this error typically is related to the BTS or the radio link. Frequently, a CLR_REQ with cause '1' is the reaction for a radio link failure on the Air-interface (CONN_FAIL with cause '1' = radio link failure on the Abis-interface) or

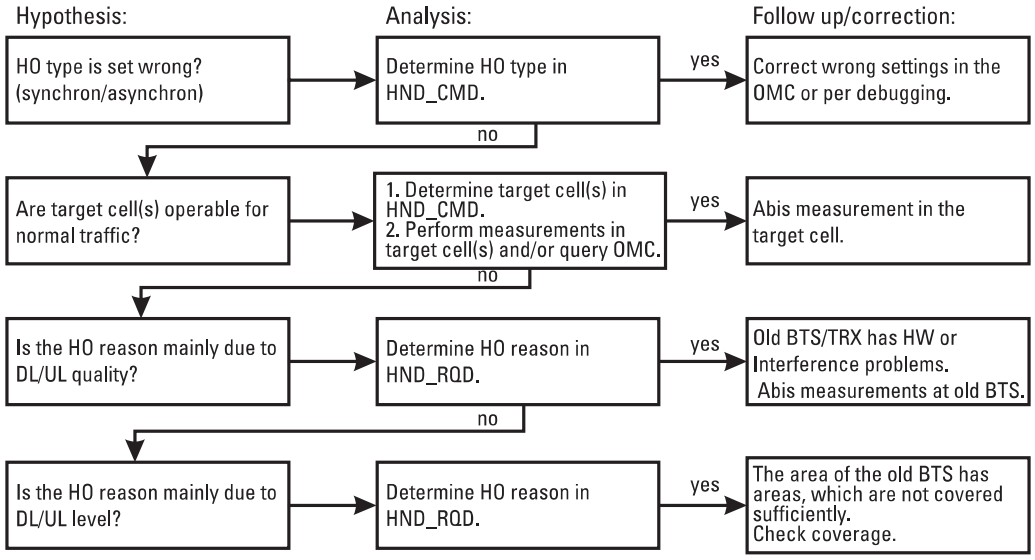


Figure 13.14 Investigation of CLR_REQ/cause value: '0' = Normal event-Radio Interface Message Failure.

a reaction for errors during channel seizure during an incoming handover (CONN_FAIL with cause '2' = handover access failure on the Abis-interface)(Figure 13.15).

13.5.2.3 CLeaR REQuest (Cause Value: '20'hex = Resources Unavailable—Equipment Failure)

CLR_REQs with this cause, if they occur in a higher number, to problems with the connection between transcoder and the BTS (Figure 13.16). A CLR_REQ with the cause of equipment failure on the A-interface frequently is the result of a CONN_FAIL with cause '28'hex = remote transcoder alarm on the Abis-interface.

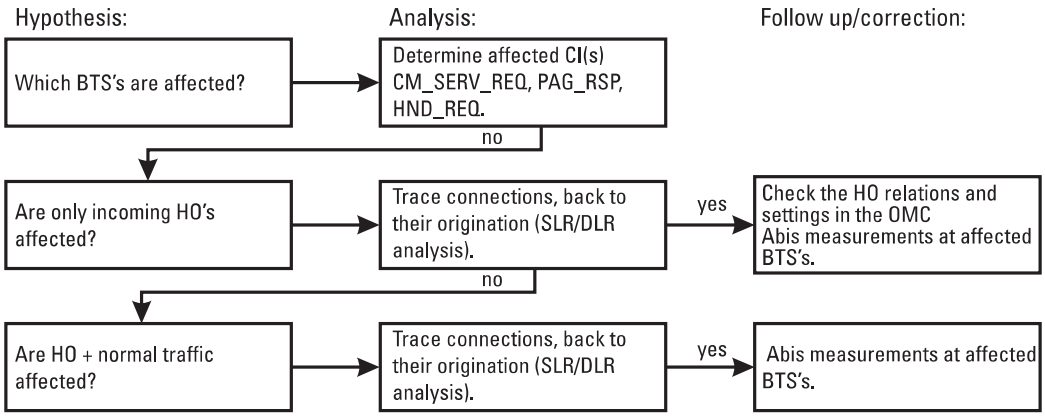


Figure 13.15 Investigation of CLR_REQ/cause value: '1' = Normal event-Radio Interface Failure.

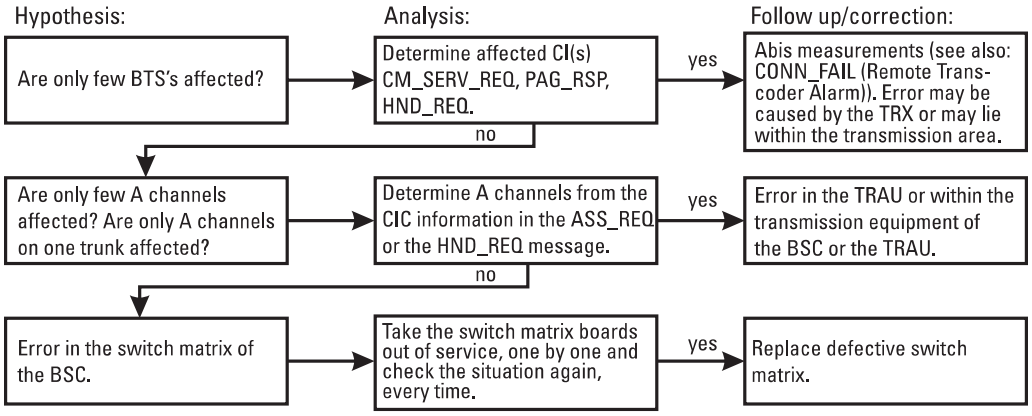


Figure 13.16 Investigation of CLR_REQ/cause value: '20'$_{hex}$ = Resources unavailable-Equipment Failure.

13.5.2.4 ASSignment FAILure (Cause Value: '50'hex Invalid Message—Terrestrial Circuit Already Allocated)

This case of ASS_FAIL should be taken seriously, even in case of a few occurrences. This cause is sent when inconsistencies exist between BSC and MSC about the state of A channels. Different from the ASS_FAIL (Resources Unavailable—Requested Terrestrial Resource Unavailable), this case of ASS_FAI (Invalid Message—Terrestrial Circuit Already Allocated) is sent if the BSC determines that the channel the MSC has requested is—although generally available for traffic—already occupied (Figure 13.17).

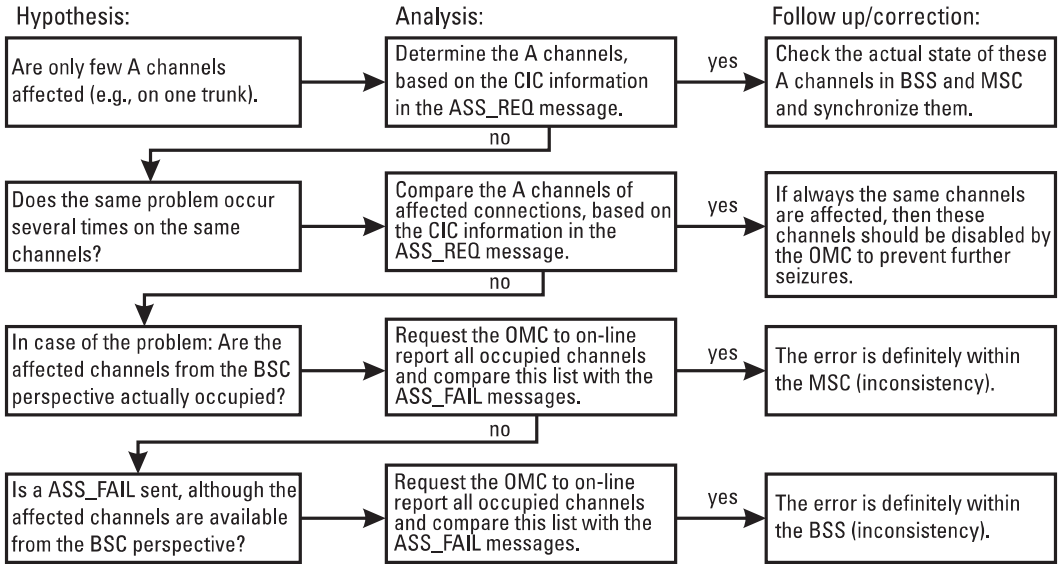


Figure 13.17 Investigation of ASS_FAIL/cause value: '50'$_{hex}$ = Invalid Message-Terrestrial Circuit already allocated.

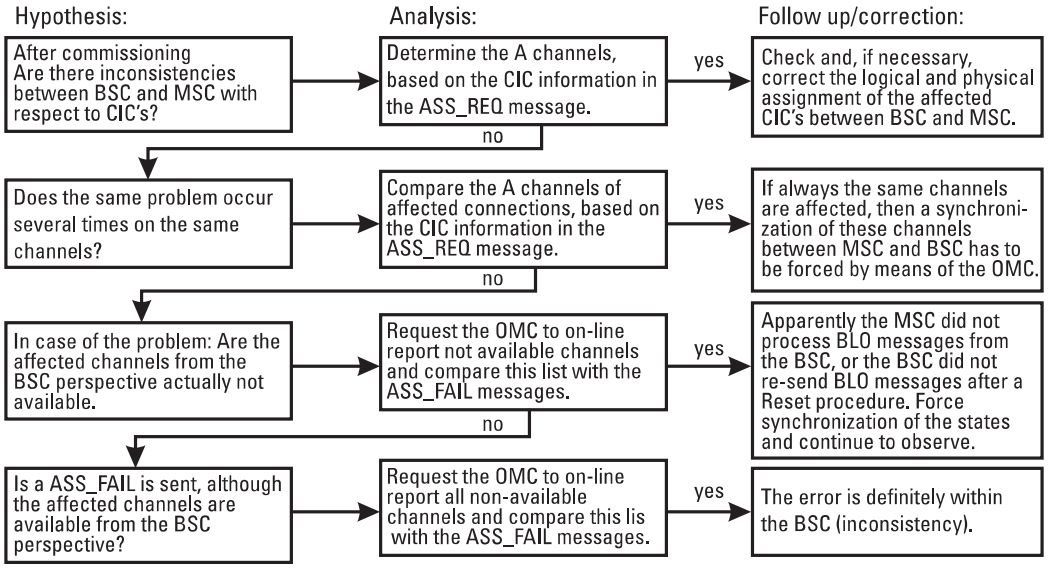


Figure 13.18 Investigation of ASS_FAIL/cause value: '22'$_{hex}$ = Resources unavailable-Requested terrestrial resource unavailable.

13.5.2.5 ASSignment FAILure (Cause Value: '22'hex Resources Unavailable—Requested Terrestrial Resource Unavailable)

This case of ASS_FAIL should be taken seriously, even in case of only a few occurrences. This cause is sent when inconsistencies occur between BSC and MSC about the state of A channels (Figure 13.18). Different from the ASS_FAIL (Invalid Message—Terrestrial Circuit Already Allocated), this ASS_FAIL is sent if the BSC determines that the channel the MSC has selected is not already occupied by another connection but generally is not available for traffic.

13.5.2.6 Infrequent SRES Mismatch Error Messages at the OMC

Description of the Error

One of our customers filed a complaint that the OMC receives an increased number of SRES mismatch error messages. Such error messages are not unusual. They are indicated, for instance, if someone tries to make a phone call with an invalid SIM card.The difference in this case was that all SRES mismatches originated in only one BSC area.55

It could not be completely ruled out that someone used a faulty SIM card in this BSC area only. However, a more detailed analysis showed that even perfect SIM cards were affected by this phenomenon. It could easily be told that the SIM cards were perfect, because they worked flawlessly immediately after

the problem occurred. Therefore, a technical defect was suspected, with a high probability of being located in the BSS.

Error Analysis

The analysis was performed on site with a protocol analyzer. For that purpose, all the SS7 connections between MSC and BSC were monitored for several hours, and the signaling data were captured and later analyzed. The tracing period was long enough that several errors could be recorded. The investigation revealed the situation on the A-interface and is illustrated in Figure 13.19.
Affected MSs almost simultaneously (Δt = 20 ms) sent two identical CM_SERV_REQ messages on the A-interface to the MSC, with a normal establishment cause. The values for SLR and signaling link selection (SLS) were, however, different for the two connection requests. The MSC/VLR responded to the first request with an AUTH_REQ and to the second one with a CM_SERV_REJ with the cause congestion. In line with the protocol, the MS then aborted the connection. Further investigations, carried out simultaneously on the A-interface and various Abis-interfaces revealed that the CM_SERV_REQ message, which was duplicated on the A-interface, was actually only a single message on the Abis-interface. Therefore, the error had to be located in the BSC. It appeared as if the BSC forwarded some messages with

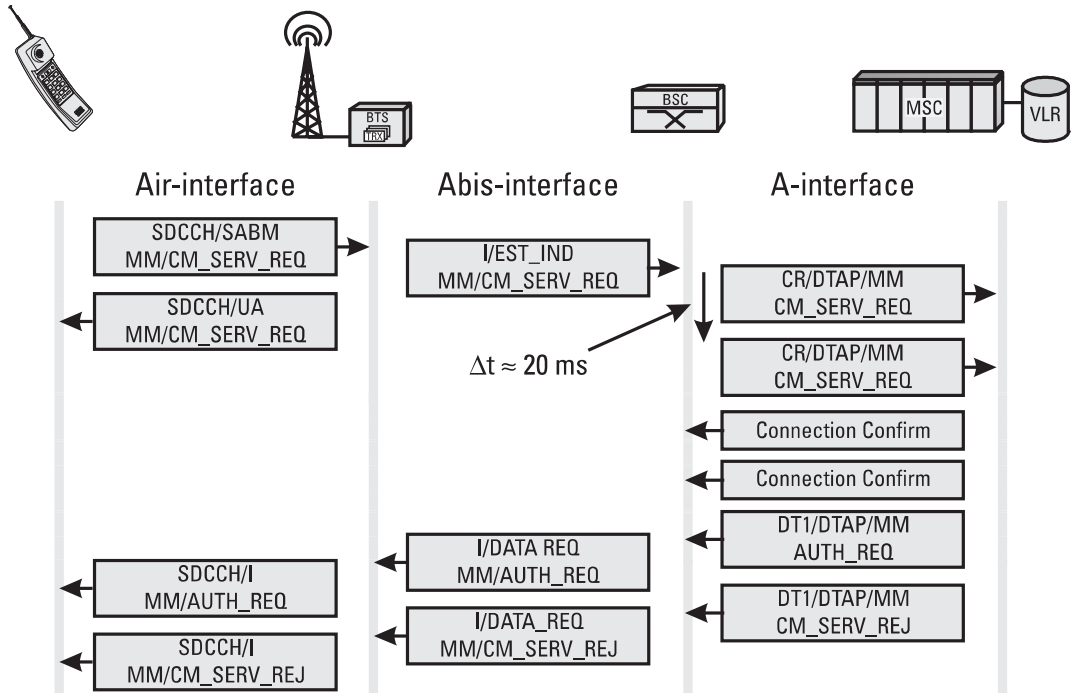


Figure 13.19 SRES mismatches caused by duplicate CM_SERV_REQs.

echo. A detailed analysis of the trace file revealed also that this problem was not restricted to CM_SERV_REQ messages, but other messages were also duplicated.

Error Correction

BSC internal protocol measurements performed by utilizing low-level measurement tools helped to detect a faulty board in the switch matrix, which was exchanged.

13.5.2.7 All TRXs Perform Restarts When Brought Into Service

Description of the Error

During the commissioning of a BSC massive problems occurred. All TRXs in all connected BTSs did not start their service but were continually restarting. A hardware problem was extremely unlikely and could be ruled out. For that reason, an affected Abis-interface was more closely monitored by means of a protocol analyzer.

Error Analysis

The investigation with the protocol analyzer quickly revealed the cause of the error. As Figure 13.20 shows, the RF_RES_IND were not sent in intervals of TX = 120s, as mandated, but with the wrong interval of TX = 0s.

Error Correction

The settings of TX were changed in the BTS-related software in the BSC. All BTSs were loaded again, and the problem was fixed.

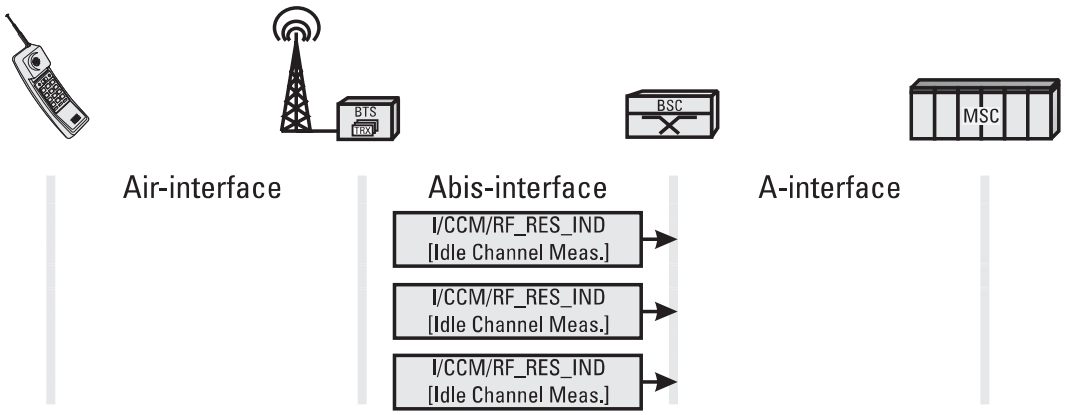


Figure 13.20 TRX restarts caused by permanently repeated RF_RES_IND messages.

Glossary

Anyone who works on GSM issues will encounter many terms and parameters that have specific meanings in the telecommunications environment. This glossary provides an alphabetically ordered description of a significant number of these terms. Many of the descriptions are supplemented with references to GSM and ITU Recommendations, shown in brackets […].

26-Multiframe *See 51 multiframe.*

51-Multiframe Time slots for transport of information in a GSM system are organized in frames. One TDMA frame consists of 8 time slots, each 0.577 ms long. TDMA frames are organized in multiframes. Two such multiframes are defined, one with 26 TDMA frames (26-multiframe) and one with 51 TDMA frames (51 multiframe). Multiframes are organized in superframes, and superframes are organized in hyperframes. For more details, see Chapter 7.

A-interface [GSM 04.08, 08.06, 08.08] The interface between BSC and MSC. For more details, see Chapters 8, 9, and 10.

A-law [G.711] Spoken language generally is not linear in its dynamics, and the human ear is rather sensitive to soft sounds, but difference in amplitude for loud sounds cannot be distinguished so easily. When digitizing speech, one can take advantage of this situation and code a sufficient-quality sound with relatively few bits. In particular, the relative error that is made when quantizing needs to be minimized. The relative error is $\Delta x/x$ or dx/x. To minimize that value for all cases, it has to be constant. Since the integral of 1 over x equals the

Samsung Ex. 1032, Page 306 of 417

natural logarithmic function (as in the equation $\int \frac{dx}{x} = 1n(x) + C$, a logarithmic function best suits that objective. For this purpose, the A-law and the μ-law were invented. Both are approximations of the natural logarithmic function, and both were standardized by ITU for transmission of digital speech on PCM transmission lines, as shown in Figure G.1(a).

Both methods are used on a per-country basis. The μ-law is used only in the United States and Japan. All other countries use the A-law. The international standard G.711 deals with the case of an international connection that involves two countries where different methods are used. The standard requires that, independent of the origination, a possibly necessary transformation be carried out in the country that uses the μ-law.

The first step is the same for both methods, that is, to sample the analog signal with a sampling rate of 8 kHz. The sample then is quantized according to the respective law and coded in 8-bit code words. That results in the transmission rate of 64 Kbps, used on PCM channels. Both methods differ only in a slight variation of the no-linear quantization of the sample.

Figure G.1(b) is a graphic representation of the A-law, and Figure G.1(c) provides the representation of the μ-law. The first bit indicates whether the value is positive or negative, the following 3 bits define the segments, while the bits marked with "x" represent values within that segment.

A3, A5/X, A8 [GSM 03.20] Names of three algorithms used in GSM for authentication and ciphering (Figure G.2). All the algorithms used in GSM are highly confidential and therefore not published in any standard.

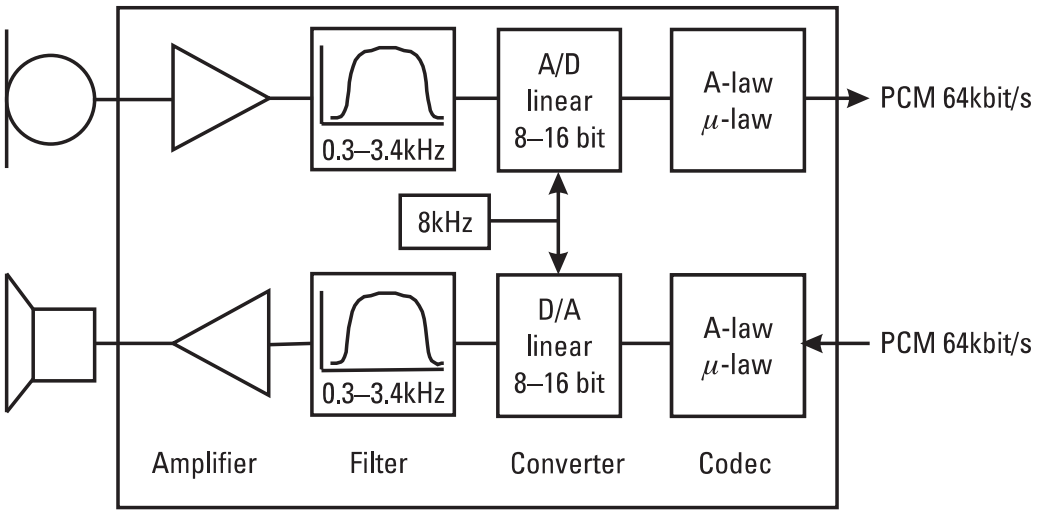


Figure G.1(a) A-law and μ-law for digitalization of speech.

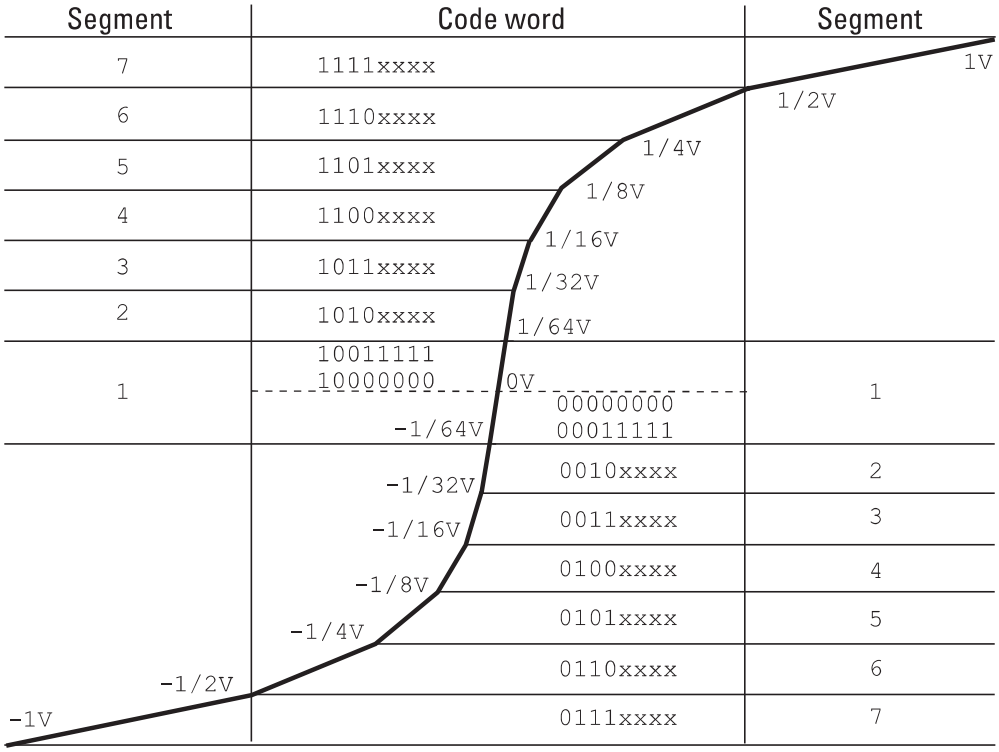


Figure G.1(b) Graph for the A-law.

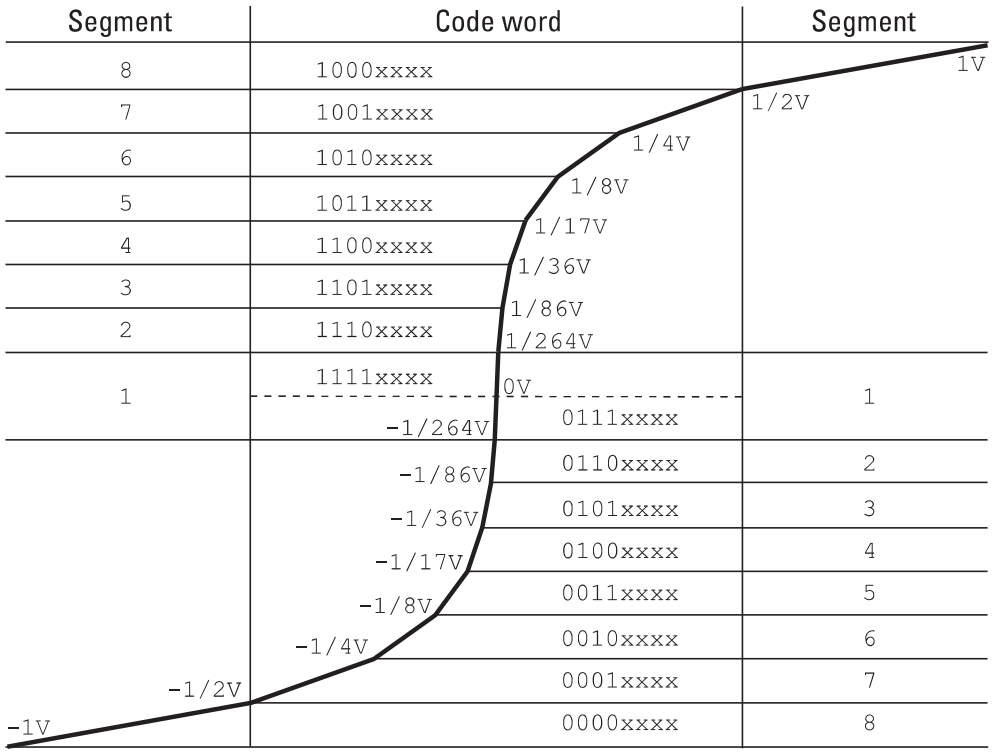


Figure G.1(c) Graph for the μ-law.

The "X" in A5/X indicates that there are several A5 algorithms. The network and the mobile station (MS) have to agree on one of these algorithms before ciphering can be used. The MS does not necessarily "know" every algorithm. Originally, GSM had only one algorithm, A5, but due to export restrictions of security codes, more less-secure algorithms were defined. The algorithm A5 is built into the MS, not into the SIM. GSM has defined A5/1 through A5/7, and the MS uses an information element, the mobile station classmark, to inform the network during connection setup which algorithms it actually supports.

Abis-interface [GSM 04.08, 08.58] The interface between BTS and BSC. For more details, refer to Chapter 6.

Access class GSM recognizes 16 different access classes. This parameter is stored on the SIM module and allows the network operator to specifically bar certain types of subscribers. A typical application is to set up an access class exclusively for the operator personnel for test purposes during installation and testing. In that case, the system can be on the air but ordinary users do not recieve access. Another application is to define access classes for emergency personnel only. This can prevent overload during an emergency and allows rescue workers to be reachable via mobile phone.

The BTS broadcasts the admitted access classes within the RACH control parameters, which are part of the information that the BTS permanently broadcasts in its broadcast control channel (BCCH). The MS reads the information and compares it with the access classes on the SIM. The MS attempts to access the system only if it finds a matching access class. That prevents signaling overload because an unauthorized MS does not even try to access the system.

Table G.1
Application of the GSM Algorithms A3, A5/X, and A8

Algorithm	Dependency	Remark
A3	SRES = f(A3, K_i , RAND)	The MS calculates the SRES by using the RAND as a parameter for the A3 algorithm.
A5/X	CS = f(A5/X, K_c , FN)	MS and BTS both need the ciphering sequence for the ciphering process.
A8	K_c = f(A8, K_i , RAND)	K_c is calculated from A8, K_i, and RAND. It is then used as an input parameter for ciphering.

The access classes in GSM use values from 0 to 15. The numbers do not indicate any priority as such, that is, a higher number does not imply a higher priority or vice versa. Table G.2 shows the use of the access classes. "Ordinary" subscribers receive values from 0 through 9 on a random basis. Only the access classes 11 through 15 were predefined. Note that one SIM module is capable of storing several access classes, which allows one subscriber to belong to several subscriber groups.

Access delay Synonym for timing advance (TA).

ACCH [GSM 05.01, 05.02] Associated control channel. Two types are defined: slow associated control channel (SACCH) and fast associated control channel (FACCH). An ACCH is assigned for traffic channels (TCHs) as well as for SDCCHs.

Adjacent cells See *Neighbor cell.*

AE [GSM 09.02, X.200–X.209] The term application entity (AE) is used by the OSI Reference Model in which it refers to a physical entity in Layer 7, the application layer. The different protocols for the GSM network elements HLR, VLR, and EIR are examples of AEs. Refer to Chapter 11 for more details about AEs.

AGCH [GSM 05.01, 05.02] Access grant channel. A common control channel (CCCH) that is used only in the downlink direction of even-numbered

Table G.2
Access Classes in GSM

Access Class (Decimal)	Subscriber Group
15	Network operator personnel
14	Emergency service
13	Public services (utilities)
12	Security service
11	To be assigned by the operator
10	Not used
0–9	"Ordinary" subscribers

time slots (typically solely in time slot 0) of the BCCH-TRX. It is used to assign a SDCCH to the MS, and it transports the IMM_ASS (IMMediate ASSign) message. Depending on the chosen channel configuration, the AGCH shares the available downlink CCCHs with the paging channel (PCH) and the SDCCH. The transmission rate per AGCH block is 782 bps. (See Chapter 7.)

Air-interface [GSM 04.XX, GSM 05.XX] The interface between MS and BTS. In an analogy to the fixed network, this interface is also referred to as the U_m interface. Chapter 7 provides more details.

AIS [G.703] Alarm indication signal. An alarm known from the transmission systems. A terminal shows the alarm when the Layer 1 connection to the next entity is working properly, but the peer entity still is not reachable because somewhere down the line the connection is broken. For example, consider a BTS that has a connection to a BSC. The connection is composed of two links connected in serial, as shown in Figure G.2. If one of the two connections fails, for example, the one next to the BSC, the BTS shows an AIS.

AoC/AoCI/AoCC Three terms relative to the GSM charging type of supplementary services (SS). Advice of charge (AoC) (the generic term for the two specific SSs), advice of charge indication (AoCI), and advice of charge charging (AoCC). The difference lies in the level of accuracy. For more details, see Supplementary services.

APDU See *PDU.*

Application context name [GSM 09.02, X.208, X.209] An identifier used by the transaction capabilities application part (TCAP) that identifies which protocol an application has to use. Optional information element of the dialog part in a TCAP message.

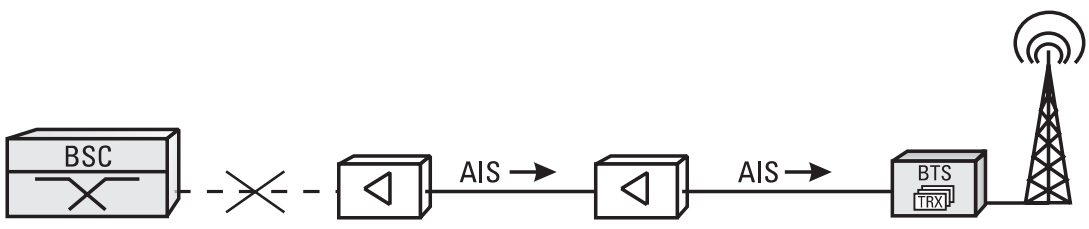


Figure G.2 Use of the alarm indication signal (AIS).

The application context in the GSM-MAP identifies the application to be used for execution of a MAP dialog in the HLR, VLR, MSC, or EIR. More details are provided in Chapter 11.

Application entity See *AE.*

ARFCN [GSM 05.01] Absolute radio frequency channel number. An identifier or number of a channel used on the Air-interface. From the ARFCN, it is possible to calculate the frequency of the uplink and the downlink that the channel uses. How to perform this calculation is shown under downlink.

ASE [GSM 09.02, X.200–X.209] Application service element. Single-user protocol of OSI Layer 6. For example, the whole GSM MAP (Layer 7) is an ASE of the transaction capabilities application part (TCAP), while individual parts of MAP (e.g., HLR, VLR) are referred to as application entities (AEs).

ASN.1 [Q.771, Q.772, Q.773, X.208, X.209] Abstract Syntax Notation number 1 (ASN.1) is the first—and so far only—standardized means to describe operations of interfaces and their parameters. ITU has standardized this notation in its Recommendations X.208 and X.209, based on the OSI Reference Model (X.200 through X.207).

The interfaces of the mobile application part (MAP) of GSM are specified with the use of ASN.1.

An important part of ASN.1 is the definition of how to assign parameter identifiers, depending on their category and the type of application. A parameter identifier is called TAG.

Table G.3 shows the encoding of the various parameter types defined in X.208. Encoding of those bits, indicated by X, are determined by the type of application. For more details, see Chapter 11.

ATT See *IMSI attach, IMSI detach; BCCH_INFO SYS_INFO 1–4.*

AuC [GSM 03.02, 03.20] Authentication center. Part of the network switching subsystem (NSS). It is a physical part of the HLR. For more details, see Chapter 4.

Authentication [GSM 03.20] Getting access to telecommunication services by cloning of a valid user identifier is a common problem in many mobile networks. GSM anticipated that problem and defined an authentication procedure: an operation that prevents unauthorized use of service by challenging a user to provide proof of the claimed identity. After the user requests access to

Table G.3
Parameter Types in ASN.1

Encoding								Parameter Type
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**Bit**
X	X	0	0	0	0	0	1	Boolean
X	X	0	0	0	0	1	0	Integer
X	X	X	0	0	0	1	1	Bitstring
X	X	X	0	0	1	0	0	Octetstring
X	X	X	0	0	1	0	1	Null
X	X	X	0	0	1	1	0	Object identifier
X	X	X	0	0	1	1	1	Object descriptor
X	X	X	0	1	0	0	0	External
X	X	X	0	1	0	0	1	Real
X	X	X	0	1	0	1	0	Enumerated
X	X	X	1	0	0	0	0	Sequence/sequence of
X	X	X	1	0	0	0	1	Set/set of
X	X	X	1	0	0	1	0	Character string
X	X	X	1	0	0	1	1	Character string
X	X	X	1	0	1	0	0	Character string
X	X	X	1	0	1	0	1	Character string
X	X	X	1	0	1	1	0	Character string
X	X	X	1	1	0	0	1	Character string
X	X	X	1	1	0	1	0	Character string
X	X	X	1	1	0	1	1	Character string
X	X	X	1	0	1	1	1	Time
X	X	X	1	1	0	0	0	Time

the network and provides the user identifier, the network sends a random number (RAND) to the MS. The input is used, together with some secret information on the SIM and a secret algorithm, to provide a response (SRES). More details can be found under ciphering.

B-interface [GSM 09.02] The interface between MSC and VLR. Since the time when GSM Phase 2 was specified, this interface is no longer part of

the external interfaces, and SMG provides no detailed specifications. For more details, see Chapter 4.

BAIC, BAOC, BIC Roam, BOIC, BOICexHC Supplementary services (SS) that bar certain types of calls: Barring of all incoming calls (BAIC), barring of all outgoing calls (BAOC), barring of incoming calls while roaming (BIC-Roam), barring of outgoing international calls (BOIC), barring of outgoing international calls except those to the home country (BOICexHC). For more details, see SS.

Bbis [GSM 04.06] Frame format used on the Air-interface for the $LAPD_m$ protocol exclusively to transmit the BCCH, PCH, and AGCH. It is different from the regular $LAPD_m$ frame format in that Bbis utilizes neither address or control fields nor length indicators. For more details, refer to Chapter 7.

BCC [GSM 03.03] Base station color code. A 3-bit-long parameter that is part of the BSIC. Used to distinguish among the eight different training sequence codes (TSCs) that one BTS may use on the CCCHs and to distinguish between neighbor BTSs without the need for the MS to register on any other BTS.

BCCH [GSM 04.08, 05.01, 05.02] Broadcast common control channel. The "beacon" of every BTS. Per BTS, there is always exactly one BCCH, which is transmitted in time slot 0 of the BCCH frequency. The transmission rate is 782 bps.

BCCH / SYS_INFO 1–4 [GSM 04.08] Message sent on the BCCH for radio resource management purposes. Several types of this message exist. Types 1 through 4 are explained in more detail.

A BTS uses the SYS_INFO 1–4 on the BCCH to provide all cell-specific data to every MS that receives the signal. That includes accessibility, available services, neighbor cells, radio frequencies, and so on. The BSC provides the relevant BCCH information to each BTS individually. An example captured from a GSM system in East Asia illustrates the content of the BCCH information (Figures G.3 through G.6). Note that the number of neighbor cells, and hence frequencies in DCS1800 and PCS1900 is large and, therefore, exceeds the capacity of SYS_INFO 2. This large number of frequencies is required to define and broadcast a SYS_INFO 2bis and SYS_INFO 2ter, in addition.

The following description shows that SYS_INFO 4 only provides repetition of the already sent parameters. Only with active cell broadcast (CB) does

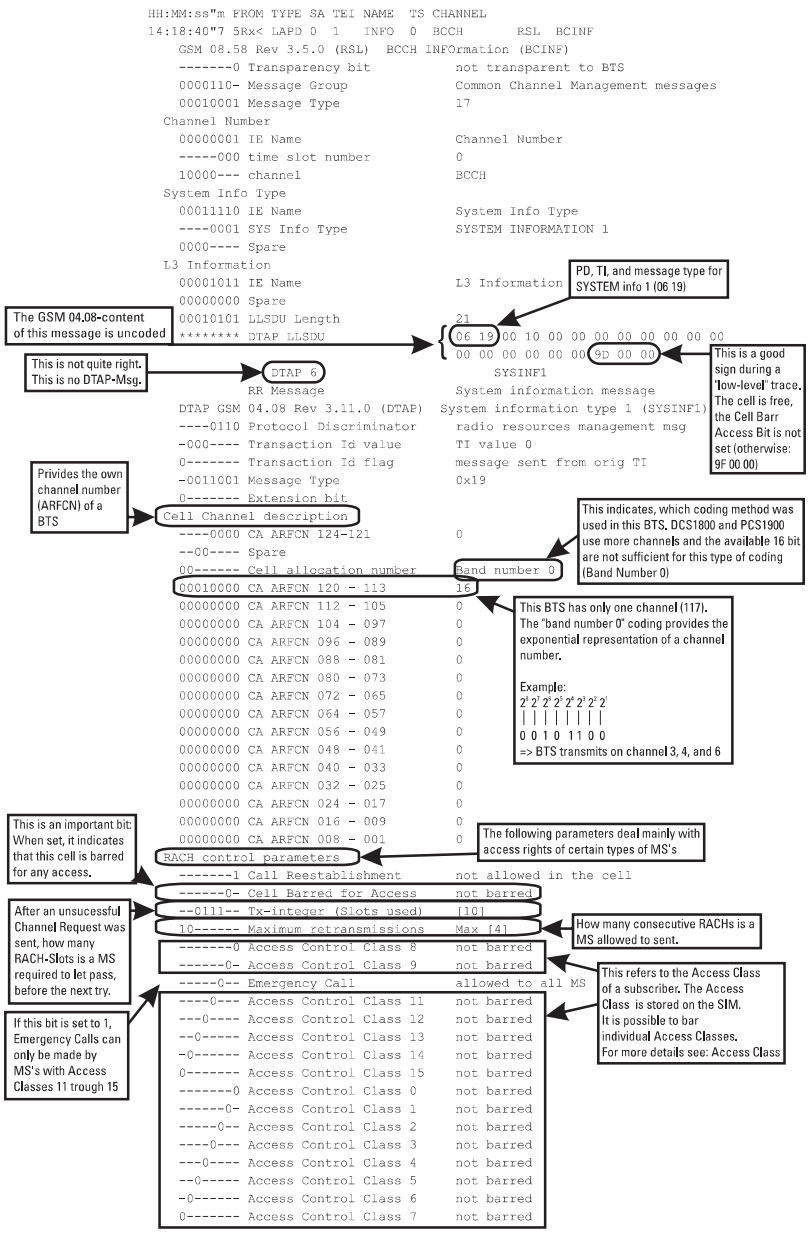


Figure G.3 Example of a BCCH SYS_INFO 1 message.

SYS_INFO 4 provide new information by describing the cell broadcast channel.

SYS_INFO 5 and 6 [GSM 04.08] In contrast to BCCH/SYS_INFO 1–4, which broadcasts all BTS-specific data to the mobile stations in the idle case, the SYS_INFO 5 and 6 perform that task when there is an active connection either on a SDCCH or on a TCH. Note that in DCS 1800 and PCS 1900 the

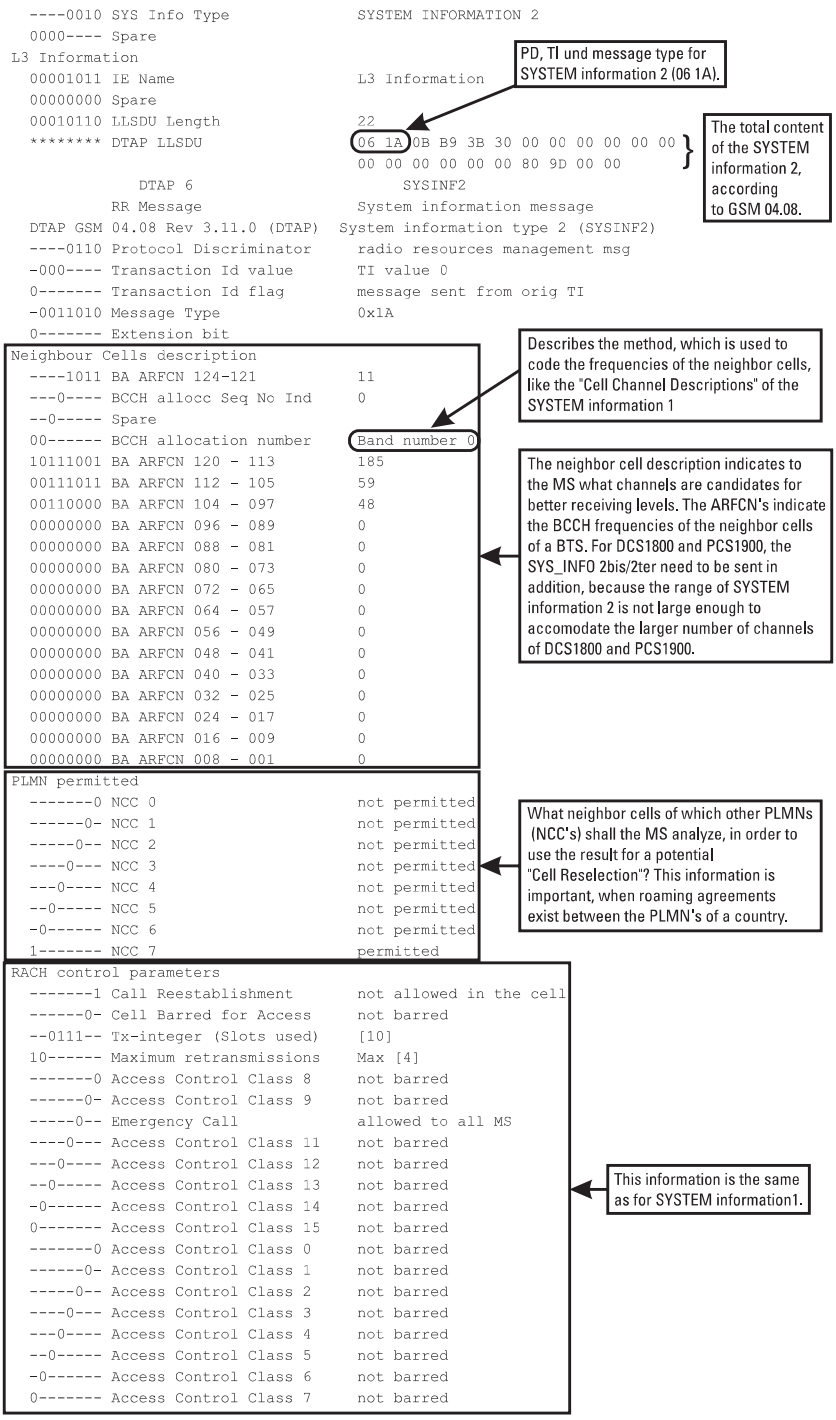


Figure G.4 Example of a BCCH SYS_INFO 2 message.

SYS_INFO 5 was expanded by SYS_INFO 5bis and 5ter, to accommodate the greater number of available frequencies of neighbor cells. More details on the use of SYS_INFO 5 and 6 can be found in Chapter 12.

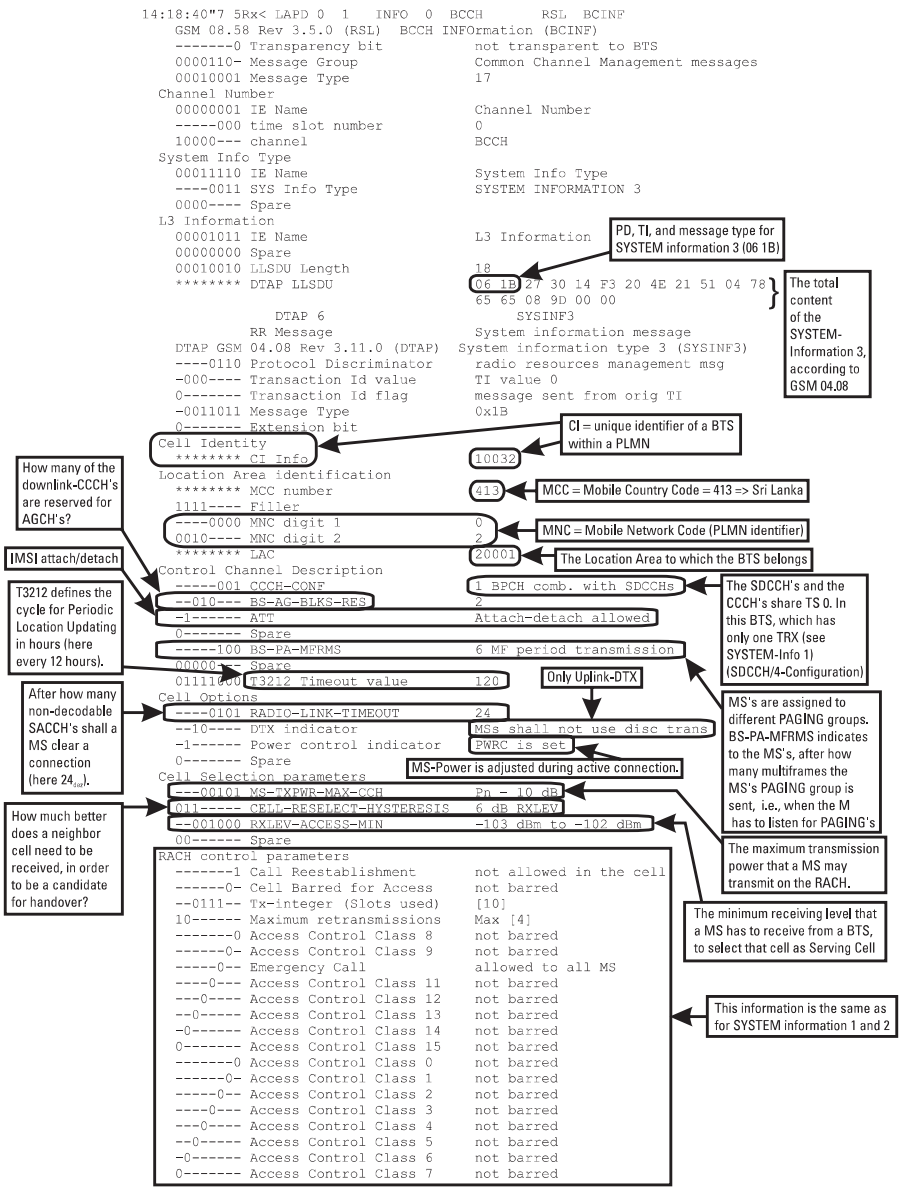


Figure G.5 Example of a BCCH SYS_INFO 3 message.

BCCH SYS_INFO 7 and 8 Specific messages for DCS 1800 and PCS 1900. They share a logical channel with BCCH SYS_INFO 4.

BCD Binary coded decimal. A method to code a decimal digit with four binary bits. If the decimal number has several digits (i.e., because it is greater than 9), each digit is coded individually, for example, 79_{dez} = '0111 1001'$_{bin}$.

Bearer services [GSM 02.01, 02.02] Different transmission capabilities that GSM provides, as listed in Table G.4. Note that bearer services need to be

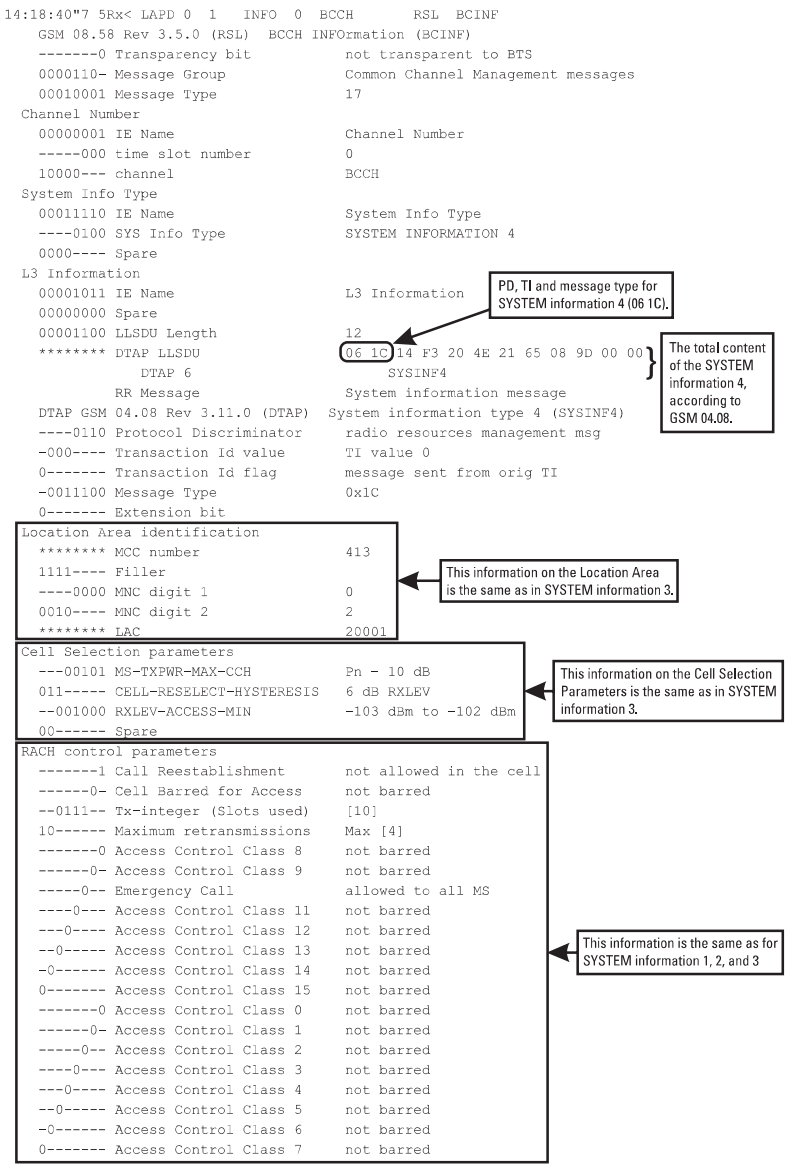


Figure G.6 Example of a BCCH SYS_INFO 4 message.

distinguished from teleservices, which include possibly required terminal equipment.

BER Bit error rate on the Air-interface. Determined by the value of RXQUAL.

BERT Bit error rate test. A measurement of bit error rates.

BFI [GSM 05.05, 06.31, 08.60] Bad frame indicator. A parameter within the TRAU frame. The value of the BFI indicates to the voice decoder if a

Table G.4
Bearer Services in GSM

Bearer Service		Remarks
No.	Name	
21	Asynchron/300 baud	-/-
22	Asynchron/1200 baud	-/-
23	Asynchron/1200 baud/75 baud	Only for mobile originating call. 1200 Baud for downlink and 75 baud for uplink.
24	Asynchron/2400 baud	-/-
25	Asynchron/4800 baud	-/-
26	Asynchron/9600 baud	-/-
31	Synchron/1200 baud	-/-
32	Synchron/2400 baud	-/-
33	Synchron/4800 baud	-/-
34	Synchron/9600 baud	-/-
41	Asynchron over PAD 300 baud	Only mobile originating call.
42	Asynchron over PAD 1200 baud	Only mobile originating call.
43	Asynchron over PAD 1200 baud /75 baud	Only mobile originating call. 1200 baud on downlink and 75 baud on uplink.
44	Asynchron over PAD/2400 baud	Only mobile originating call.
45	Asynchron over PAD/4800 baud	Only mobile originating call.
46	Asynchron over PAD/9600 baud	Only mobile originating call.
51	Synchron/packet access/2400 baud	Only mobile originating call.
52	Synchron/packet access/4800 baud	Only mobile originating call.
53	Synchron/packet access/9600 baud	Only mobile originating call.
61	Speech and data	This allows to switch back and forth between speech and data. During the data phase bearer services 21–26 are used.
81	Speech followed by data	After the switch to data transmission, it is not possible to switch back to speech. Bearer services 21–26 are used during the data phase.

TRAU frame contains valid data (BFI = 0) or not (BFI = 1). Depending on that information, the voice decoder uses or discards a TRAU frame. Note: For FACCH frames, BFI always equals 1, because they contain signaling data.

BIB [Q.700–Q.704] Backward indicator bit. Used to detect transmission errors in SS7 messages. Other related indicators are the BSN, FSN, and FIB. BIB is the most significant bit (MSB) of the first byte of an SS7 message (FISU, MSU, LSSU). For more details, see Chapter 8.

B_m channel [GSM 04.03] Another term for the GSM fullrate channel. It allows transmission of speech at a rate of 13 Kbps.

BS Bearer service.

BS_AG_BLKS_RES [GSM 05.02] Parameter transmitted with the BCCH SYS_INFO 3 message. BS_AG_BLKS_RES is 3 bits long and hence can take on the values 0 through 7. The value of this parameter indicates to all mobile stations in a cell how many of the CCCH blocks of a 51 multiframe on a BCCH-TS 0 are reserved for access grant channels (AGCHs). The number of available paging channels (PCHs) is reduced accordingly. Note that during operation in the combined mode of SDCCH and CCCH the number of CCCH blocks per time slot is four rather than eight, compared to the non-combined mode. The complete picture is illustrated in Figure G.7. (See also CCCH_CONF).

BS_PA_MFRMS [GSM 05.02] Mobile stations are organized into paging groups based on their IMSI. A mobile station that belongs to a certain paging group needs to check for a paging message only once in a number of 51 multiframes. In between, the mobile station may switch over to an energy-saving mode, discontinuous reception (DRX).

The 3-bit-wide parameter BS_PA_MFRMS is part of the BCCH SYS_INFO 3 and tells the mobile station after how many multiframes the content of the paging channel (PCH) has to be analyzed by the MS. In other words, this parameter indicates how often a particular paging group is repeated. Figure G.8 provides an example of how this parameter is used.

BS_CC_CHANS [GSM 05.02] Parameter that indicates how many time slots on the BCCH frequency are reserved for common control channels

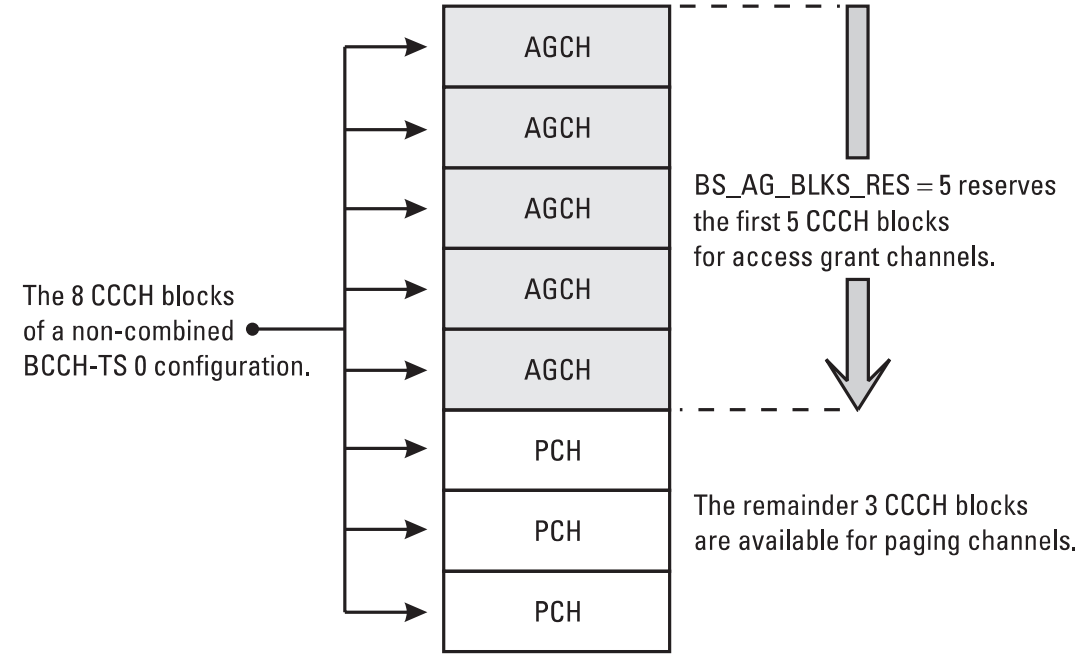


Figure G.7 The meaning of BS_AG_BLKS_RES.

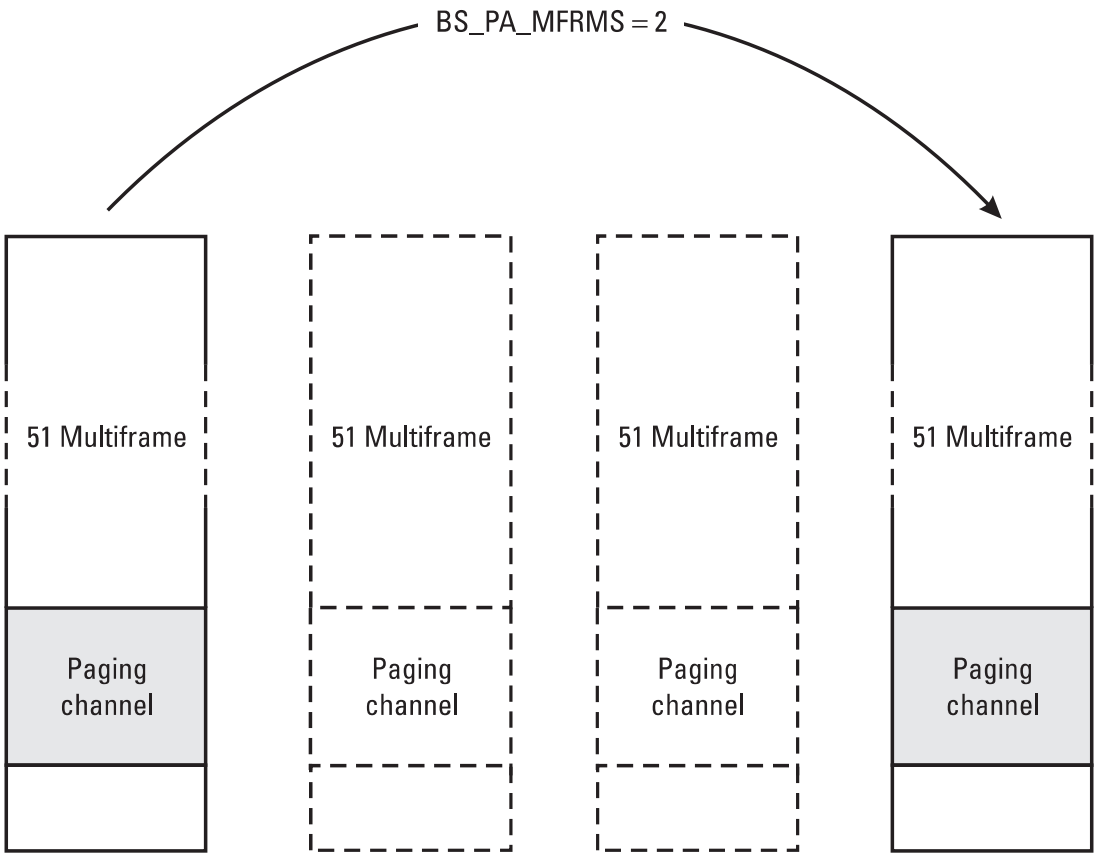


Figure G.8 The task of the BS_PA_MFRMS.

(CCCHs). This parameter is not transmitted but is derived from another parameter, CCCH_CONF.

BS_CCCH_SDCCH_COMB [GSM 05.02] Parameter that indicates whether the dedicated control channels (SDCCHs) and the common control channels (CCCHs) share a given time slot. Such a combined configuration is described in Chapter 7. This parameter is not transmitted but is derived from another parameter, CCCH_CONF.

BSC [GSM 03.02] Base station controller. Details are presented in Chapter 3.

BSIC [GSM 03.03] Base station identity code. An identifier for a BTS, although the BSIC does not uniquely identify a single BTS, since it has to be reused several times per PLMN. The purpose of the BSIC is to allow the mobile station to identify and distinguish among neighbor cells, even when neighbor cells use the same BCCH frequency. Because the BSIC is broadcast within the synchronization channel (SCH) of a BTS, the mobile station does not even have to establish a connection to a BTS to retrieve the BSIC. Figure G.9 shows the format of the BSIC. It consists of the network color code (NCC), which identifies the PLMN, and the base station color code (BCC).

BSN [Q.700–Q.704] Backward sequence number (7 bits). Used to acknowledge to the sender of a message (MSUs in SS7) that certain messages have been received. Chapter 8 presents more details.

BSS [GSM 03.02] Base station subsystem. Used to address all network elements belonging to the radio part of a GSM system. Parts of the BSS are the base transceiver station (BTS), the base station controller (BSC), and the transcoding rate and adaptation unit (TRAU). For more details, see Chapter 3.

BSSAP See *BSSMAP*.

BSSMAP [GSM 08.06, 08.08] Base station subsystem mobile application part. Both the BSSMAP and the direct transfer application part (DTAP) are

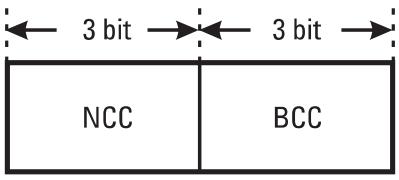


Figure G.9 Format of the BSIC.

users of the SCCP protocol of SS7 on the A-interface. BSSMAP and DTAP together form the BSSAP. The difference between the two is as follows:

- The BSSMAP is responsible for transmitting messages that the BSC has to process. This applies generally to all messages to and from the MSC where the MSC participates in radio resource management, for example, handover. The BSSMAP contains, furthermore, all messages for the administration of the A-interface itself.
- In contrast, the DTAP transports messages between the MS and the MSC, in which the BSC has just the relaying function, that is, it is transparent for these messages. These are all messages dealing with mobility management (MM) and call control (CC).

BTS [GSM 03.02] Base transceiver station. Described in more detail in Chapter 3.

Burst [GSM 05.01, 05.02] The nature of TDMA transmission is that radio energy is emitted in a pulsed manner rather than continuously. Mobile stations and BTSs send bursts periodically. Figure G.10 illustrates this for a GSM system in a power-over-time presentation. The actual data transmission is happening during the time period represented in Figure G.10 as a horizontal line. This time period is 148 bits, or 542.8 μs, long. Because GMSK—at least in theory—does not contain an amplitude modulated signal, the effective transmission power is constant over the entire transmission period. Figure G.10 also shows the specified corridor for the allowed power level of the signal over time. In total, a burst has a window of 577 μs, or 156.25 bit, before the next time slot starts. Physically speaking, the power level has to be reduced by 70 dB after 577 μs. These restrictions apply to the uplink as well as the downlink and determine the maximum number of bits an MS can send or receive at one time. The net bit rate is only 114 bits per burst, not 156.25. This reduced number of bits results from the mapping of a physical burst to a logical burst. The physical burst needs bits for administrative purposes that reduce the space available for signaling or user data. Note that all burst types specified for GSM follow a similar pattern:

- Each burst always begins with tail bits, which are necessary to synchronize the recipient. Tail bits are, except for the access burst, always coded as '000'.
- The tail bits are followed by 148 data bits, which differ in format for the various burst types.

- Each burst is terminated by another set of tail bits and the so-called guard period. This guard period is required for the sender to physically reduce the transmission power. The guard period is particularly long for the access burst, to allow mobile stations that are far from a BTS and hence experience propagation delays to also access the BTS (see *TA*).

The functional differences between the five logical bursts, defined for GSM, are as follows:

- Normal burst. The normal burst is used for almost every kind of data transmission on all channel types. The only exceptions to that rule are the initial channel request from the mobile station (CHAN_REQ/HND_ACC) sent in an access burst and the transmission of the synchronization data of a BTS that is done via the synchronization burst. All other data transfer on all traffic channels, dedicated control channels (DCCHs) and common control channels (CCHs) in uplink and downlink directions are done in normal bursts.

  Every normal burst contains 114 bits of useful data that are sent in two packets of 57 bits each. The so-called training sequence (TSC) is placed between the two packets. Note that the term *useful data* is not entirely accurate in this context, since the 114 bits are already channel coded and therefore contain some overhead (channel coding). Last but

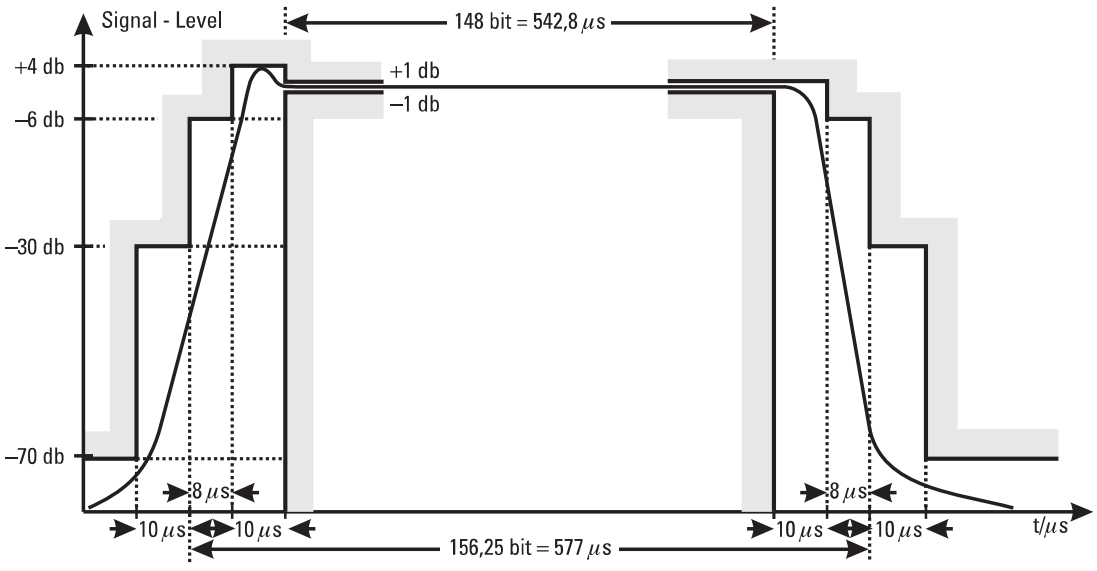


Figure G.10 The burst in the power-over-time presentation.

not least, there is a stealing flag between the training sequence and each data packet, which indicates to the recipient whether a 57-bit packet actually contains user data or FCCH information.

- Synchronization burst. The synchronization burst is used to transmit synchronization channel information (SCH) The synchronization burst uses a format similar to that of the normal burst (Figure G.12). In both cases, there are two data packets, left and right, from the training sequence. However, for the synchronization burst, each packet contains only a 39-bit payload, because the training sequence is 64 bits long. Note that the training sequence for the synchronization channel is identical for all BTSs and therefore allows a mobile station to easily distinguish an accessible GSM-BTS from any other radio system that accidentally works at the same frequency. Therefore, the training sequence in the synchronization channel serves two purposes: (1) It allows the mobile station to determine if there might have been transmission errors, and (2) it allows the mobile station to distinguish a GSM source from other transmission systems on the same frequency.
- Access burst. In contrast to the bursts described so far, the access burst comes in a rather unique format because of its special tasks (Figure G.12). A mobile station uses the access burst only for the initial access to a BTS, which applies in two cases: (1) for a connection setup starting from the idle state and (2) for handover (see under synchronized handover). In the first case, the MS sends the CHAN_REQ message in an access burst to the BTS. In the second case, the MS sends HND_ACC messages that also are mapped on access bursts.

  In both cases the MS does not know the current distance to the BTS and, hence, the propagation delay for the signal (see *TA*). As long as the propagation delay is not known to the MS, the MS assumes it is zero. Therefore, it generally is uncertain if the access burst arrives within the receiver window of a BTS and how big the overlap is (Figure G.11). That is the reason for the lesser length of an access burst and the longer duration of the guard period. To ensure that an access burst arrives at the BTS during the proper time period the number of bits for the access burst was set to only 88 bits. The maximum distance between BTS and MS is, with this timing, about 35 km.

  The normal burst would not fit into the receiver window if the unknown propagation delay was greater than zero. That is the reason why the normal burst is used only after the distance of the MS from the BTS is determined, and the MS is able to adjust its transmission accordingly. The adjustment parameter is called offset time and is

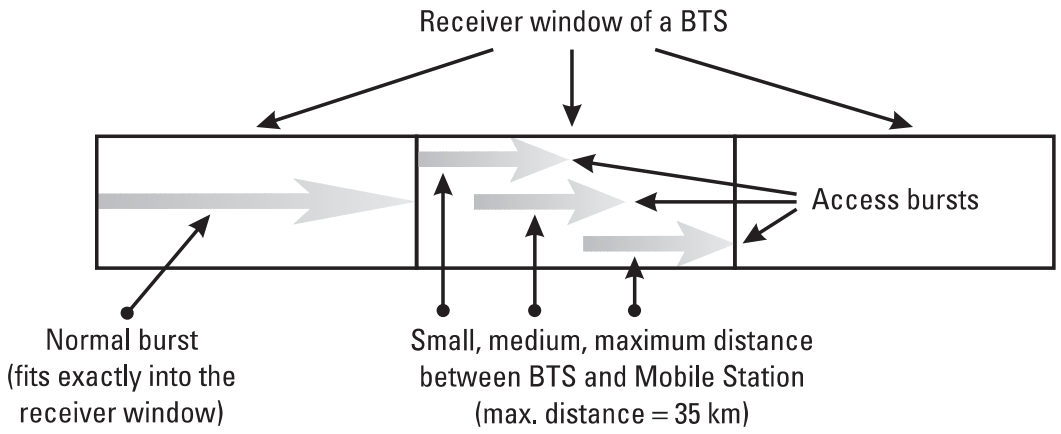


Figure G.11 The lesser length of an access burst.

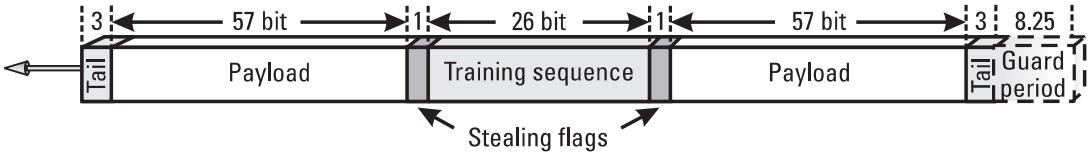
calculated fairly simply. The BTS knows format and length of an access burst and is able to determine the actual propagation delay from when the signal arrives back at the BTS after being relayed by the MS. That also allows calculation of the distance of an MS from the BTS. The BTS provides the offset time to the MS, which in turn transmits its signal earlier, exactly by that time period (see *TA*).

The format of an access burst is also different from the other bursts. The access burst begins with 8 tail bits, rather than 3 as in the case of the other bursts, and the access burst always starts with the bit sequence 0011 1010_{bin}. The tail bits, together with the following 41-bit synchronization sequence which also always carries the same value, allows the BTS to distinguish the access burst from error signals or interfering signals. Hence, the access burst serves on the uplink a similar purpose as the synchronization burst does on the downlink. Nevertheless, in practice, it is common that the BTS determines background noise to be a CHAN_RQD message, as presented in Chapter 6.

The data field of an access burst is only 36 bits long and contains either a CHAN_RQD or an HND_ACC message. Note that both messages actually contain only 8 bits of "useful data."

- Frequency correction burst. The most simple format of all the bursts is used for the frequency correction burst, which is transmitted only in the frequency correction channel (FCCH) (Figure G.12). All 148 bits (142 bits + 6 tail bits) are coded with 0. A sequence of zeros at the input of a GMSK modulator produces, because of the peculiarities of the GMSK modulation, a constant transmitter frequency which is exactly 67.7 kHz above the BCCH median frequency. Therefore, the frequency of the FCCH is always 67.7 kHz above the frequency that is

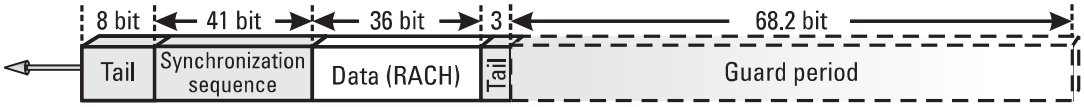
Normal burst:



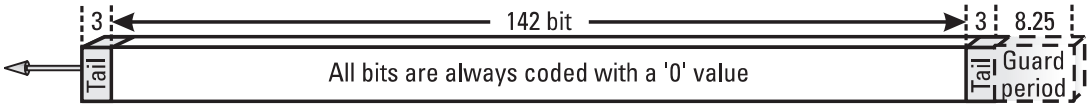
Synchronization burst:



Access burst:



Frequency correction burst:



Dummy burst:

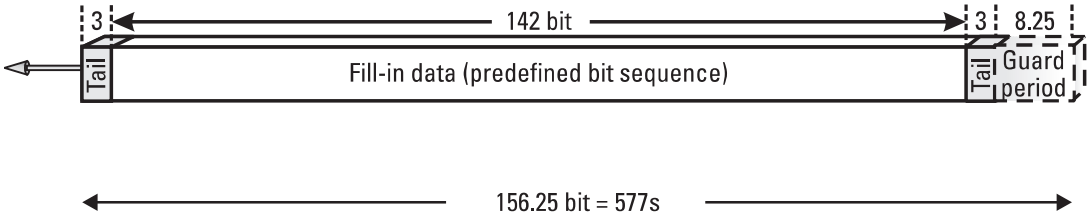


Figure G.12 The logical burst types.

advertised as the downlink frequency. This constant transmission frequency allows an MS to fine-tune its frequency to the BCCH frequency, to subsequently be able to read the data within the synchronization burst.

- Dummy burst. When the MS powers up, it checks the power level of the BCCH frequencies of the cells (BTSs) nearby to determine which BTS to use as a serving cell (Figure G.12). Similarly, when the MS is active, that is, involved in a call, the power level of the BCCH frequencies of the neighbor cells serve as basis for a possible handover decision.

To be useful as a reference, the BCCH frequency has to be transmitted with a constant power level. Thus, all time slots have to be occupied, and it is not allowed to apply power control on the downlink. For this purpose, the dummy burst was defined. These dummy bursts are inserted into otherwise empty time slots on the BCCH frequency. To prevent accidental confusion with frequency correction bursts, the dummy burst is coded with a pseudo-random bit sequence predefined by GSM.

C-Interface [GSM 09.02] The interface between the HLR and the MSC. More details are presented in Chapter 4.

Call reestablishment [GSM 04.08] A GSM functionality that currently is not used. Call reestablishment is applicable for speech connections only. In the case of an interruption of the radio connection during an ongoing conversation, the radio link failure procedure is invoked and the existing connection drops. With call reestablishment enabled, it is possible to prevent the disconnection of the conversation by establishing a connection to a suitable neighbor cell. Therefore, the mobile station will transmit a CHAN_REQ to this neighbor cell (cause: call reestablishment) that after SDCCH-assignment is followed by a CM_RES_REQ message (see Chapter 7) which is sent to the MSC for reconnecting the former MM and the CC connection. Since the GSM handover is a lengthy procedure with respect to time, it is possible that when the quality of the radio connection degrades rapidly the handover process could not be completed before the connection to that cell is lost completely. The call reestablishment functionality is addressing that behavior and allows a call to be maintained, even when the radio contact to the serving cell drops.

CB [GSM 03.41, 07.05] Cell broadcast. Synonymous with short message service cell broadcast (SMSCB). It allows a cell broadcast center (CBC) to send cell broadcast services (CBS), that is, text messages to all MSs in the entire

PLMN or parts thereof. Example applications of CB are traffic reports, weather forecasts, and stock quotes. In contrast to "regular" SMS, CB requires no confirmation from the mobile station. Another difference from SMS is that the CBC forwards broadcast messages directly to the BSC, bypassing the entire NSS. Figure G.13 illustrates this configuration. The BSC forwards the broadcast message over the Abis-interface to the BTS by facilitating an SMS_BC_REQ message or an SMS_BC_CMD message. The BTS, in turn, periodically transmits that information on the (cell broadcast channel (CBCH). When a BSS supports SMSCB, the CBCH is configured instead of the SDCCH/2.

A single CBS message may contain up to 82 bytes. In addition, it is possible to combine up to 15 CBS messages to form a so-called hypermessage.

CBC [GSM 03.41, 07.05] Cell broadcast center. See *CB*.

CBCH [GSM 03.41, 07.05] Cell broadcast channel. Used to transmit broadcast messages to mobile stations. The transmission rate of this optional channel is 782 bps. Network operators may choose to equip a CBCH instead of a SDCCH

CBS [GSM 03.41, 07.05] Cell broadcast services. See *CB*.

CC Call control. Application protocol between MS and MSC. See Chapter 7. Also, connection confirm message type of the SCCP (see Chapter 9.)

CCCH [GSM 05.01/05.02] Common control channel. Generic term for all point-to-multipoint channels on the Air-interface. CCCHs are in the downlink

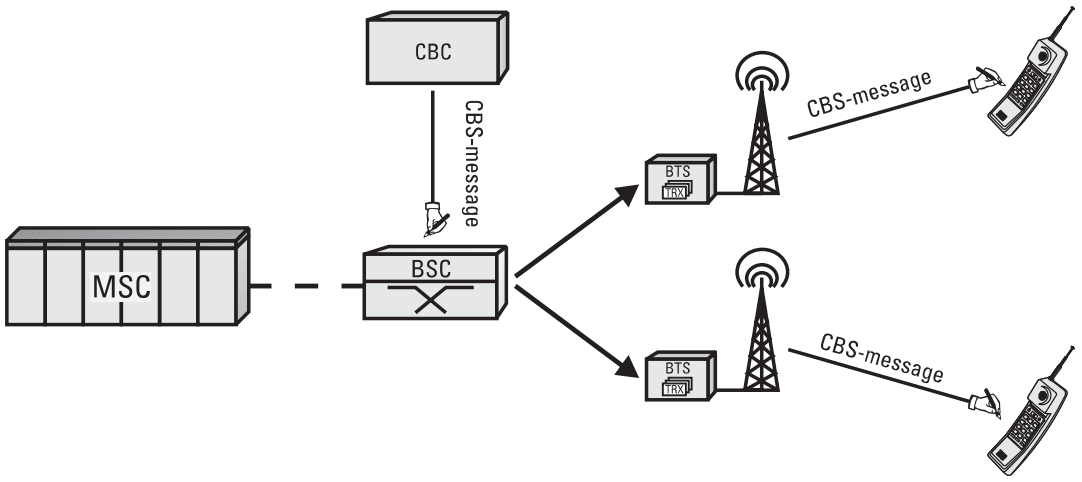


Figure G.13 Function of the CB/SMSCB.

direction, in particular the BCCH, the PCH, the CBCH , the AGCH . The only CCCH in the uplink direction is the random access channel (RACH). Network operators may configure the BCCH frequency to carry CCCHs in all even-numbered time slots (0, 2, 4, 6).

CCCH_CONF [GSM 05.02] Parameter of the BCCH/SYS_INFO 3 message that informs the MS about the actual configuration of the CCCHs in a cell. This information contains, in particular, whether a BTS uses a shared SDCCH/CCCH time slot (typically time slot 0) (BS_CCCH_SDCCH_COMB) and how many time slots are reserved for CCCHs (BS_CC_CHANS). Table G.5 lists all possible combinations.

CCITT Comité Consultatif International Télégraphique et Téléphonique. Organization that used to be responsible for international standardization of telecommunications-related issues. In 1993, CCITT was merged into International Telecommunication Union–Telecommunication Standardization Sector (ITU-T).

CDR Call drop rate. Indicator for the quality of service in a network. There is, however, no consistent understanding on how the CDR is to be determined. Some CDRs count dropped calls only if the drop occurs after the connection was already established; others also count unsuccessful call attempts.

For that reason, one has to be careful when comparing two systems based on the CDR. To properly determine the CDR, it is suggested to sum up all errors that are visible to the subscriber, that is, drops during outgoing handover, drops during mobile originating call setup, drops during mobile terminating call setup, and dropped calls during the stable phase of a call (without handover).Typically, the OMC measures the CDR by activating counters in the NSS or the BSS. (See Chapter 13.)

Table G.5
Relation Between CCCH_CONF, BS_CC_CHANS and BS_CCCH_SDCCH_COMB

CCCH_CONF	BS_CC_CHANS	BS_CCCH_SDCCH_COMB
0	1	No
1	1	Yes
2	2	No
4	3	No
6	4	No

CEPT Conférence Européenne des Postes et Télécommunications or Conference of European Postal and Telecommunications Administrations. Members are public administrations from European countries.

CFB, CFNRe, CFNRy, CFU, CUG, CW See *SS*.

CGI [GSM 03.03] Cell global identification. Identification composed of the location area identity (LAI) and the cell identity (CI). GSM allows use of both the CGI and the CI to identify a cell. Figure G.14 illustrates the format of the CGI.

Channel coding [GSM 05.03] Generic term that summarizes the different methods to protect data transmitted on the Air-interface from interference and transmission errors. In GSM, the fire code and the convolutional code are applied for that purpose. The devices performing channel coding are the mobile station and the TRX in the BTS. Channel coding adds information to the actual data, which allows the recipient to detect and sometimes even correct transmission errors. Figures G.15 and G.16 show the principles of channel coding for signaling and traffic channels (fullrate) respectively.

Figure G.16 shows that for channel coding the data in a TRAU frame (260 bits for fullrate) are separated into 182 class-1 bits (very important) and 78 class-2 bits (less important). Channel coding protects the two classes with different priorities. After channel coding is performed, the original data packet of 260 bits (user data) or 184 bits (signaling data) is extended to a length of 456 bits. The packet is then mapped on various bursts for the actual transmission. (see *Interleaving**).

Channel configuration Process of mapping signaling channels and traffic channels onto physical interfaces, for example, PCM 30. For the Air-interface, refer to Chapter 7; for the Abis-interface, Chapter 6; for the A-interface, Chapter 10.

Channel decoding [GSM 05.03] Reverse operation of channel coding. The received data are checked for errors; when errors are detected they are corrected

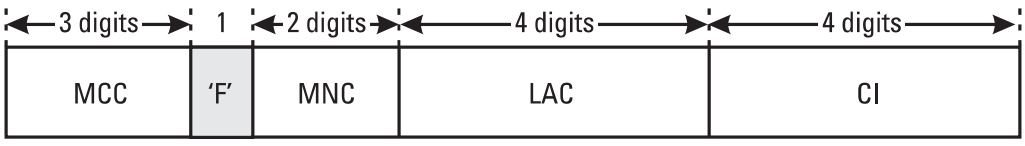


Figure G.14 Format of the CGI.

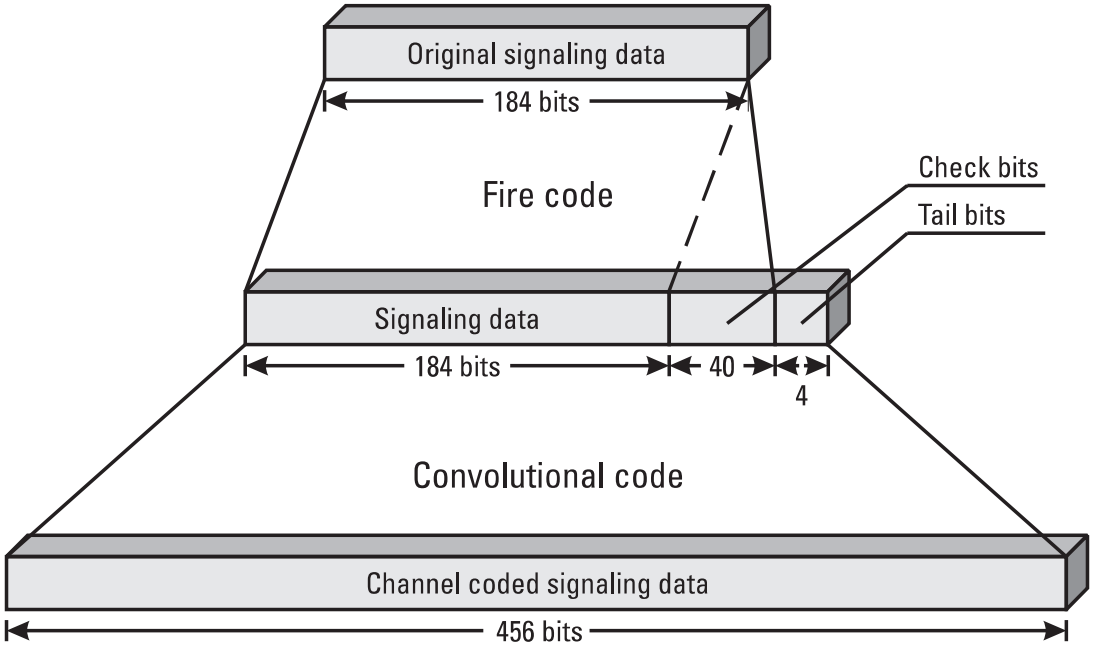


Figure G.15 Channel coding for signaling data.

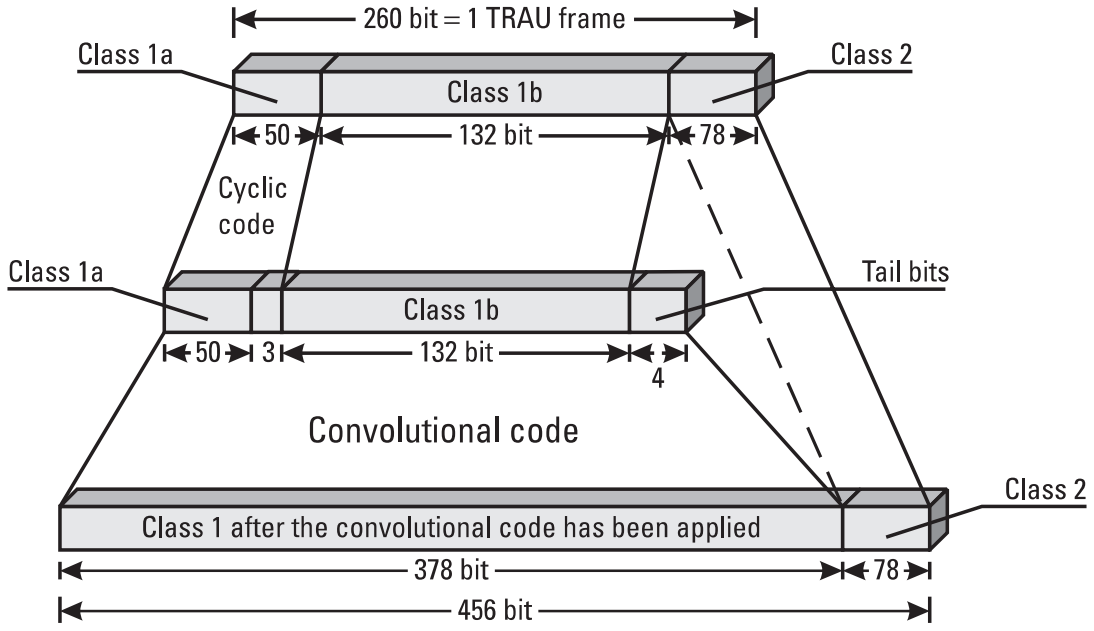


Figure G.16 Channel coding for user data (fullrate).

if possible. If the received data are found to be correct, the information that was added by channel coding has to be removed.

CI [GSM 03.03] Cell identity. A 2-byte-long hexadecimal identifier that, together with the location area (LAI) (see *CGI*), uniquely identifies a cell within a PLMN.

Ciphering [GSM 03.20] Used in GSM to encrypt data on the Air-interface between the mobile station and the BTS. Encryption applies only to the Air-interface. Therefore, tapping of a call still is possible on the terrestrial part of the connection. Precondition for ciphering is successful authentication. The process of authentication and activation of ciphering is performed in the following steps:

1. For each mobile station, the VLR stores up to five different authentication triplets (Figure G.17). Such a triplet consists of SRES, RAND, and K_c, and was originally calculated and provided by the HLR/AuC.
2. At first, the MS is sending a connection request to the network (e.g., LOC_UPD_REQ). Among others, this request contains the ciphering key sequence number (CKSN) and the mobile station classmark, which indicates what ciphering algorithms (A5/X) are available in the mobile station.
3. The NSS (more precisely, the VLR) examines the CKSN and decides whether authentication is necessary (see *CKSN*). Particularly to establish a second connection while another connection already exists (e.g., for a multiparty call), it is obvious that authentication is not required a second time during the same network access. A message is sent to the MS in case authentication is necessary. This DTAP message (AUTH_REQ) contains the random number, RAND, received from the HLR/AuC. The MS—more precisely, the SIM—uses the RAND and the value K_i as well as the algorithm A3 to calculate SRES (authentication procedure), as shown in Figure G.18.
4. The MS sends the result of this calculation, the SRES, to the VLR. The VLR compares the SRES that the MS has sent with the one that the HLR/AuC had sent earlier. The authentication is successful if both values are identical.
5. Immediately after calculating SRES, the MS uses RAND and K_i to calculate the ciphering key K_c via the algorithm A8.
6. To activate ciphering, the VLR sends the value K_c that the AuC has calculated and a reference to the chosen A5/X algorithm via the MSC and the BSC to the BTS.

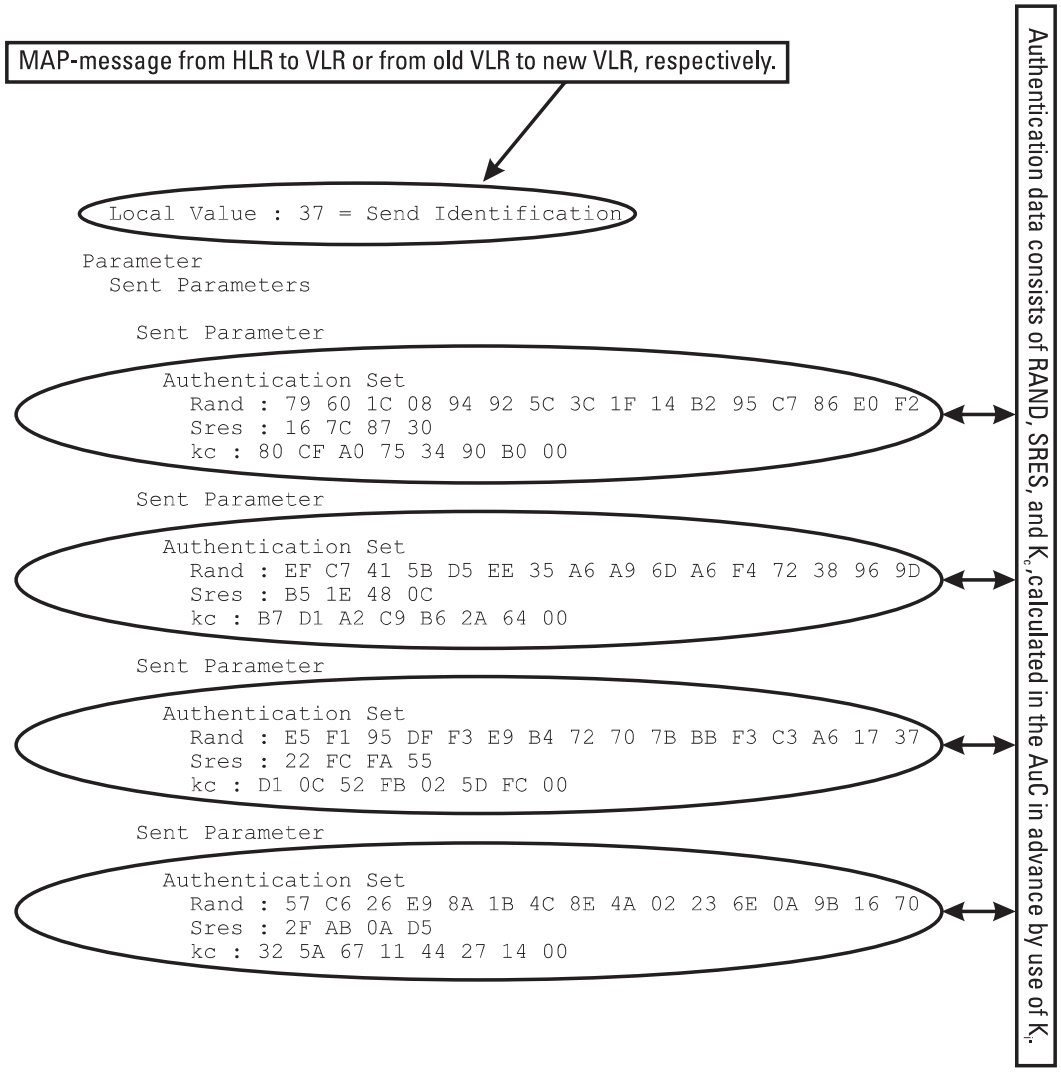


Figure G.17 Example of a (MAP) sendIdentification message, which, in this case, sends four authentication triplets for a mobile station to the VLR.

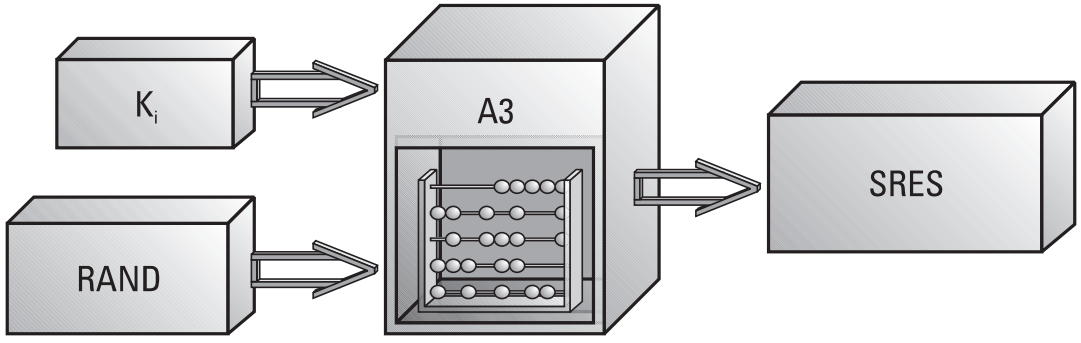


Figure G.18 Calculation of SRES from K_i and RAND by use of A3.