

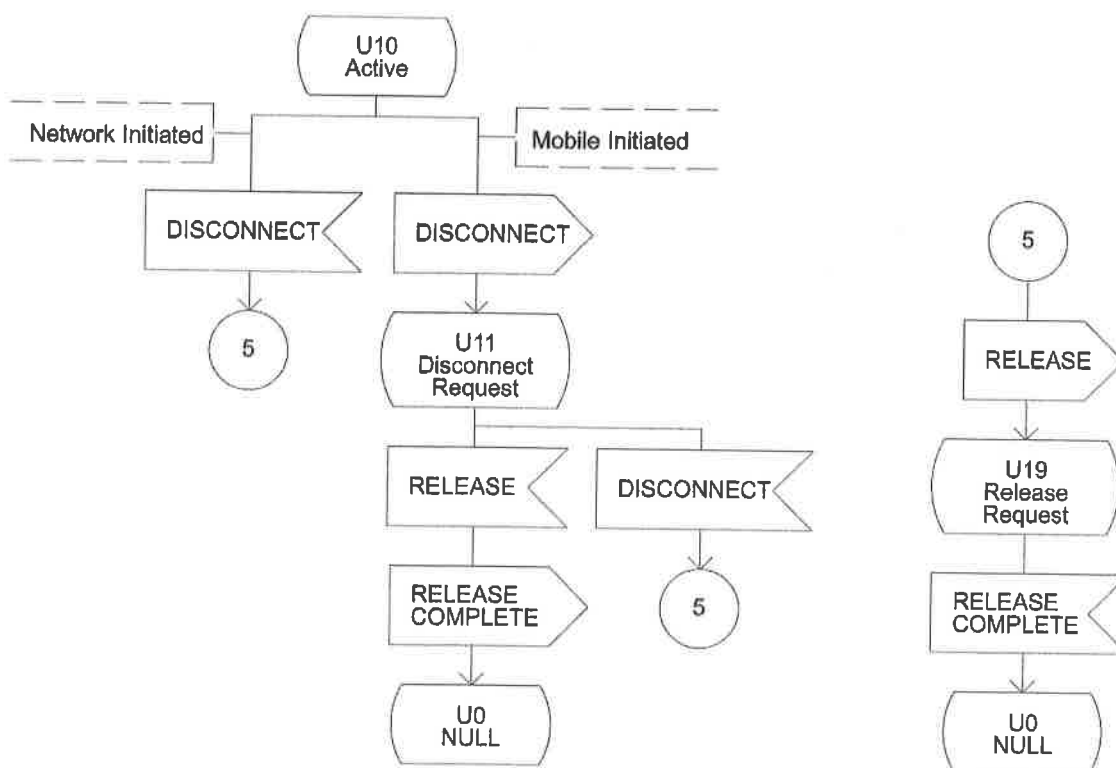


Figure 5.29 Call termination at the MS: mobile-initiated and network-initiated.

first requests a MM connection from the local MM entity, also indicating whether it is a normal or emergency call (MMCC ESTABLISHMENT REQUEST; Figure 5.28). The call to be established on this MM connection requires a special service quality of the MM sublayer.

For a simple call, the MS must be registered with the network, whereas this is only optionally required with an emergency call, i.e. an emergency call can also be established on an unenciphered RR connection from a MS that is not registered.

After successful establishment of this MM connection and activation of the user data encryption, the service-requesting CC entity is informed (further interactions with the MM entity are not shown in Figure 5.28 for call establishment). The MS signals on this connection the desire to connect to the CC entity in the MSC (SETUP). An emergency call is initiated with the message EMERGENCY SETUP; the remaining call setup is identical to that used for single calls.

The MSC can respond to this connection request in several ways: it can indicate with a message CALL PROCEEDING that the call request has been accepted and that all of the necessary information for the setup of the call is available. Otherwise the call request is declined with RELEASE COMPLETE. As soon as the called party is being signaled, the MS receives an ALERTING message; once the called party accepts the call, a CONNECT message is returned which is acknowledged with a CONNECT ACKNOWLEDGE message, thus switching through the call and the associated user data connection. If the call request need not be signaled to the called party and the call can be accepted directly, the ALERT message is omitted. CC signaling in GSM corresponds essentially to the call setup according

to Q.931 in ISDN. In addition, CC in GSM has a number of peculiarities, especially to account for the limited resources and properties of the radio channel. In particular, the call request of the MS can be entered into a queue (call queuing), if there is no immediately free traffic channel (TCH) for the establishment of the call. The maximum waiting time a call may have to wait for assignment of a traffic channel can be adjusted according to operator needs. Furthermore, the point at which the traffic channel is actually assigned can be chosen. For example, the traffic channel can be assigned immediately after acknowledging the call request (CALL PROCEEDING); this is early assignment. On the other hand, the call can be first processed completely and the assignment occurs only after the targeted subscriber is being called; this is late assignment or Off-Air Call Setup (OACSU). The variant OACSU avoids unnecessary allocation of a traffic channel if the called subscriber is not available. The blocking probability for call arrivals at the air interface can be reduced this way. On the other hand, there is the probability that after a successful call request signaling procedure, no traffic channel can be allocated for the calling party before the called party accepts the call, and thus the call cannot be completely switched through and must be broken off.

If a call arrives at the MS (mobile-terminating call), a RR connection with the MS is established within the MM connection setup (inclusive of paging). Once the MM connection is successfully completed and the encryption is activated, the call request is signaled to the MS with a SETUP message. This message includes information about the requested service, and the MS examines first whether it can satisfy the requested service profile (compatibility check). If affirmative, it accepts the call request and signals this to the local subscriber (local generation of call signal). This is finally communicated to the MSC with a CALL CONFIRMED message and an ALERTING message. If the mobile subscriber eventually accepts the call, the call is switched through completely with handshake messages CONNECT and CONNECT ACKNOWLEDGE. If, because of the selected service, there is no necessity for call request signaling to the called subscriber and the call can be switched through immediately (e.g. with a fax call), the MS signals the call acceptance (CONNECT) immediately after the message CALL CONFIRMED. Call queuing and OACSU can also be used for mobile-terminating calls. The OACSU variant for mobile-terminating calls allocates a traffic channel only after the call has been accepted by the mobile subscriber with a CONNECT message.

The release of a connection is started with a DISCONNECT message either from the mobile or the network side (mobile-/network-initiated) and is completed with handshake messages RELEASE and RELEASE COMPLETE. If there is a collision of DISCONNECT messages, i.e. if both CC entities send a DISCONNECT simultaneously, they also answer it with a RELEASE so that a secure termination is ensured.

During an established call, two more CC procedures can be employed: DTMF signaling and in-call modification. DTMF signaling is an inband signaling procedure, which allows terminals (here MSs) to communicate with the respective other side, e.g. answering machines, or configuring special network services, e.g. voice mailboxes in the network. In GSM, DTMF can only be used during a voice connection. With a message START DTMF on the FACCH, the network is told that a key has been pressed, and the release of the key is signaled with a STOP DTMF message (Figure 5.30). Each of these messages is acknowledged by the network (MSC). A minimum interval must be maintained between the START/STOP messages ($T_{\text{press_min}}$, $T_{\text{release_min}}$). While a key is depressed at the MS, the MSC generates a DTMF tone corresponding to the key code signaled with the START DTMF

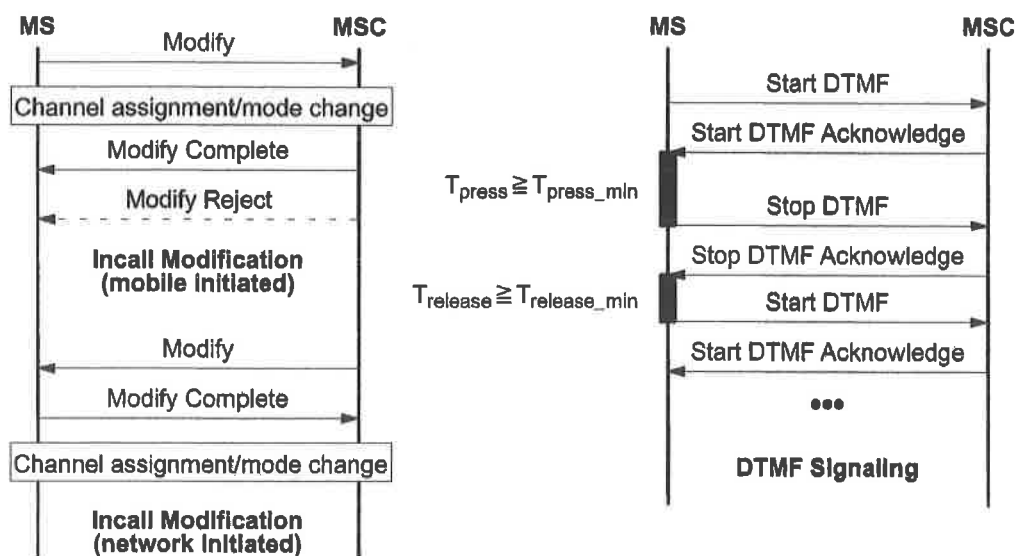


Figure 5.30 DTMF signaling and service change.

command. The DTMF tones must be generated within the MSC, since the speech coding in the GSM codec does not permit the pure transmission of DTMF tones in the voice band, and thus DTMF tones generated by the MS would arrive at the other side in distorted form.

Using the in-call modification procedure, a service change can be performed, e.g. when speech and fax data are sent in sequence and are alternating during a call. A service change is started either from the MS or from the network by sending a MODIFY request. This request contains the service and kind of change (returning or nonreturning). After sending the MODIFY request, the transmission of user data is halted. If the service change can be performed, this is signaled with a MODIFY COMPLETE message; otherwise the request is denied with a MODIFY REJECT. The service change may necessitate a change in the current physical channel configuration or operating mode. For this purpose, the MSC will use the respective channel assignment (ASSIGNMENT COMMAND; Figure 5.24).

5.4.6 Structured signaling procedures

The preceding sections have presented the basic signaling procedures of the three sublayers RR, MM and CM. These procedures have to cooperate in the form of structured procedures for the different transactions. The elements of a structured signaling procedure are as follows.

- Phase 1: paging, channel request, assignment of a signaling channel.
- Phase 2: service request and collision resolution.
- Phase 3: authentication.
- Phase 4: activation of user data encryption.
- Phase 5: transaction phase.
- Phase 6: release and deallocation of the channel.

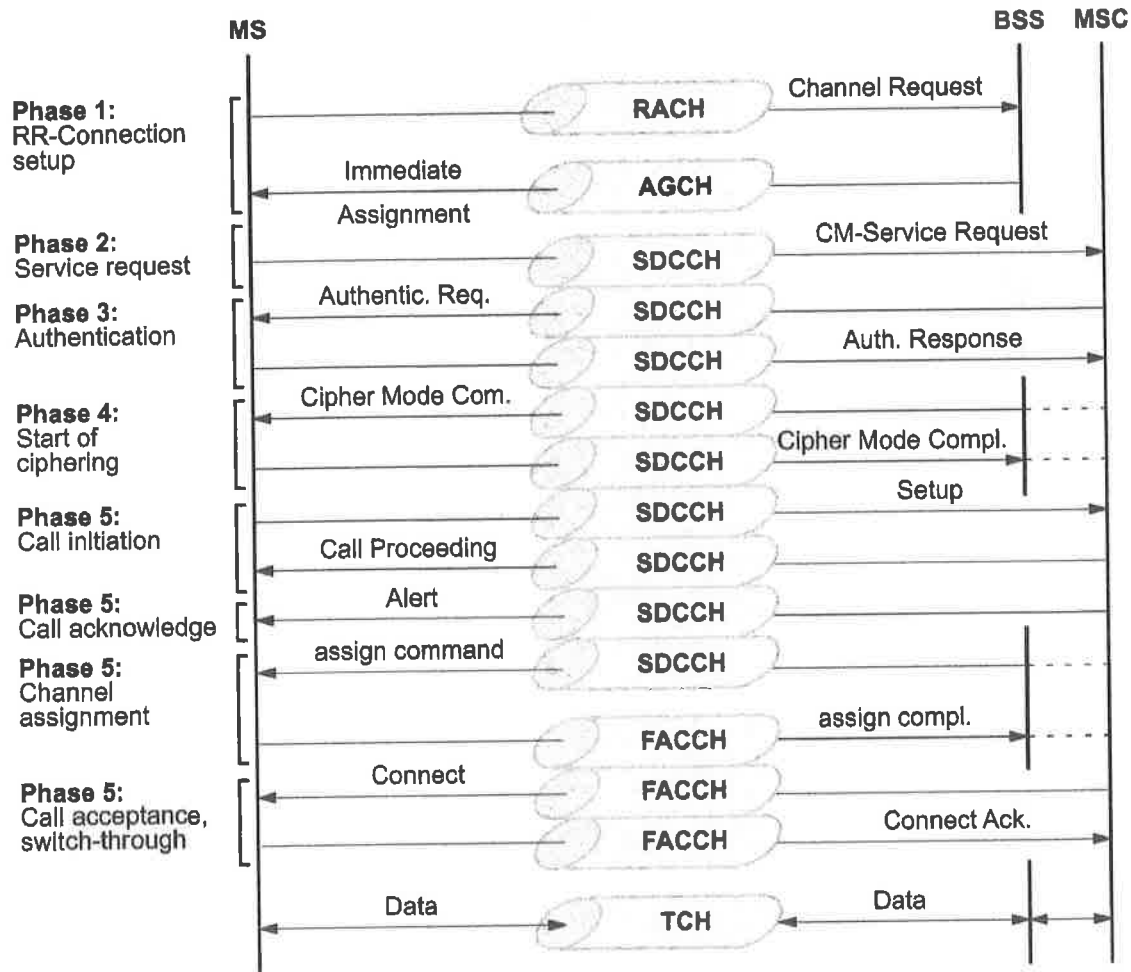


Figure 5.31 Mobile-initiated call setup with OACSU (late assignment).

Two examples of structured signaling procedures are presented in Figures 5.31 and 5.32. They show the phases executed for the structured transaction, the terminating entities (MS, BSS, MSC), the respective message and the logical channel used for the transport of the message. The first example (Figure 5.31) is a mobile-initiated call setup with OACSU – a traffic channel is only assigned after the subscriber of the called station is presented with the call request (ALERTING). The second example (Figure 5.32) shows a service change from voice to data and the modification of the selected data service. Such a modification could, for example, be the change of transmission rate. Finally, the call is released and the traffic channel is deallocated.

5.4.7 Signaling procedures for supplementary services

As can be seen in Figure 5.21, signaling messages to control SS are coded with special protocol discriminators: 0011 for call related; 1011 for noncall related. A special set of signaling messages has been defined for their control (Table 5.7). The category CC

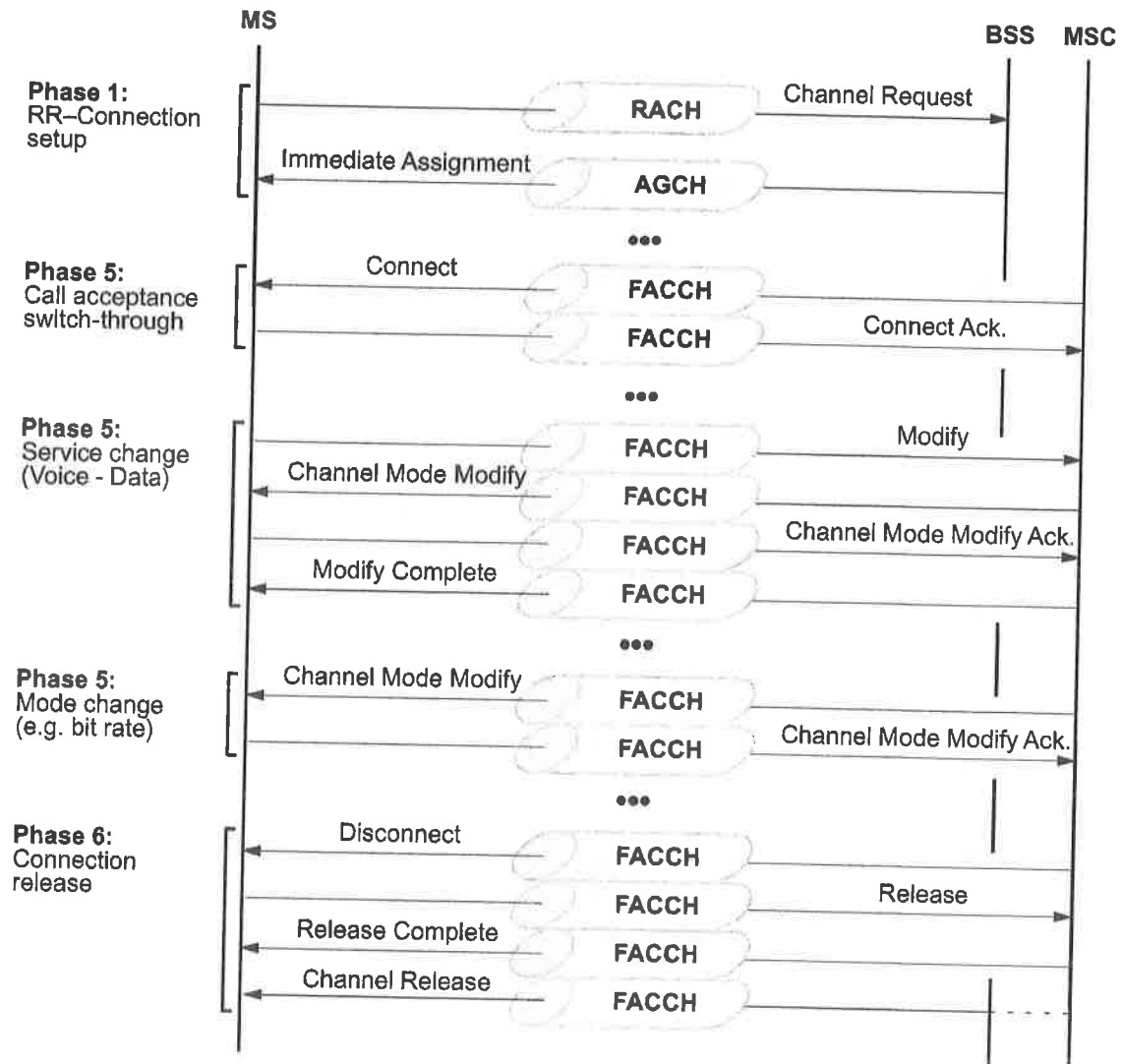


Figure 5.32 In-call modification and call release.

Messages (Table 5.6) consists of the subcategories call information phase (message type MT=0x01tttt) and Miscellaneous (message type MT=0x11tttt). These two message categories are used in two categories of SS procedures: the separate message approach and the common information element procedure. Whereas the separate message approach uses its own messages (HOLD/RETRIEVE; Table 5.7) to activate specific functions, the functions of the common information element procedure are handled with a generic FACILITY message. Functions of the first category need synchronization between network and MS. The FACILITY category, however, is only used for SS which do not require synchronization. This distinction becomes obvious in the examples of realized SS, which is presented in the following.

The messages of the separate message approach can be used during the call information phase to realize supplementary services like hold, callback or call waiting. Figure 5.33 shows

Table 5.7 CC messages for SS.

Category	Message	Direction	MT
Call information phase	Hold	N ↔ MS	0x011000
	Hold acknowledge	N ↔ MS	0x011001
	Hold reject	N ↔ MS	0x011010
	Retrieve	N ↔ MS	0x011100
	Retrieve acknowledge	N ↔ MS	0x011101
	Retrieve reject	N ↔ MS	0x011110
Miscellaneous	Facility	N ↔ MS	0x111010
	Register	N ↔ MS	0x111011

examples. A completely established call (call reference CR: 1 in Figure 5.33) can be put into the hold state from either one of the two partner entities.

To perform this SS, it is initiated with a HOLD message. The MSC interrupts the connection and indicates with a HOLD message to the partner entity that the call is in the hold state. On each call segment this fact is acknowledged with a HOLD ACKNOWLEDGE message, which leads both the requesting MS and the MSC to cut the traffic channel. The MS which caused the hold state to be entered can now establish another call (CR: 2 in Figure 5.33) or accept a call that may be coming in. Using another handshake HOLD/HOLD ACKNOWLEDGE, this call could also be put into the hold state and there could be switching between both held calls (brokering). For this purpose, a held call (CR: 1 in Figure 5.33) can be reactivated with a RETRIEVE message and reconnected to the call at each side of the traffic channel after the reactivation of the call has been acknowledged with a RETRIEVE ACKNOWLEDGE message.

These call-related signaling procedures modify the call state and define an extended state diagram with an auxiliary state. The participating calls all remain in the active state whereas the auxiliary state changes between hold and idle. In a two-dimensional state space, for example, call CR: 1 changes from (active, idle) through the state (active, hold request) into the state (active, call held) and back through the state (active, retrieve request).

If outgoing or incoming calls are barred (Figure 5.34), a call request is immediately refused by giving a RELEASE COMPLETE message with a reason in a FACILITY information element (Barring Of Outgoing Calls (BAOC), Barring Of Incoming Calls (BAIC)). A state change of the call in the extended state space does not occur. The assumption is, of course, that the calling or called subscriber has activated call barring. The MSC receiving the call request from the calling subscriber must verify the activation of this supplementary service. This requires an inquiry of the HLR of the calling subscriber (for BAOB) or the called subscriber (for BAIC), since the HLRs store the service profiles of the respective subscribers. In this case the HLR acts not only as a database but also as a participant in controlling intelligent network services.

Another call-related supplementary service uses the FACILITY message of the common information element procedure: Call Forwarding Unconditional (CFU); see Figure 5.34. With this supplementary service, a regular call setup is performed, however, not to the

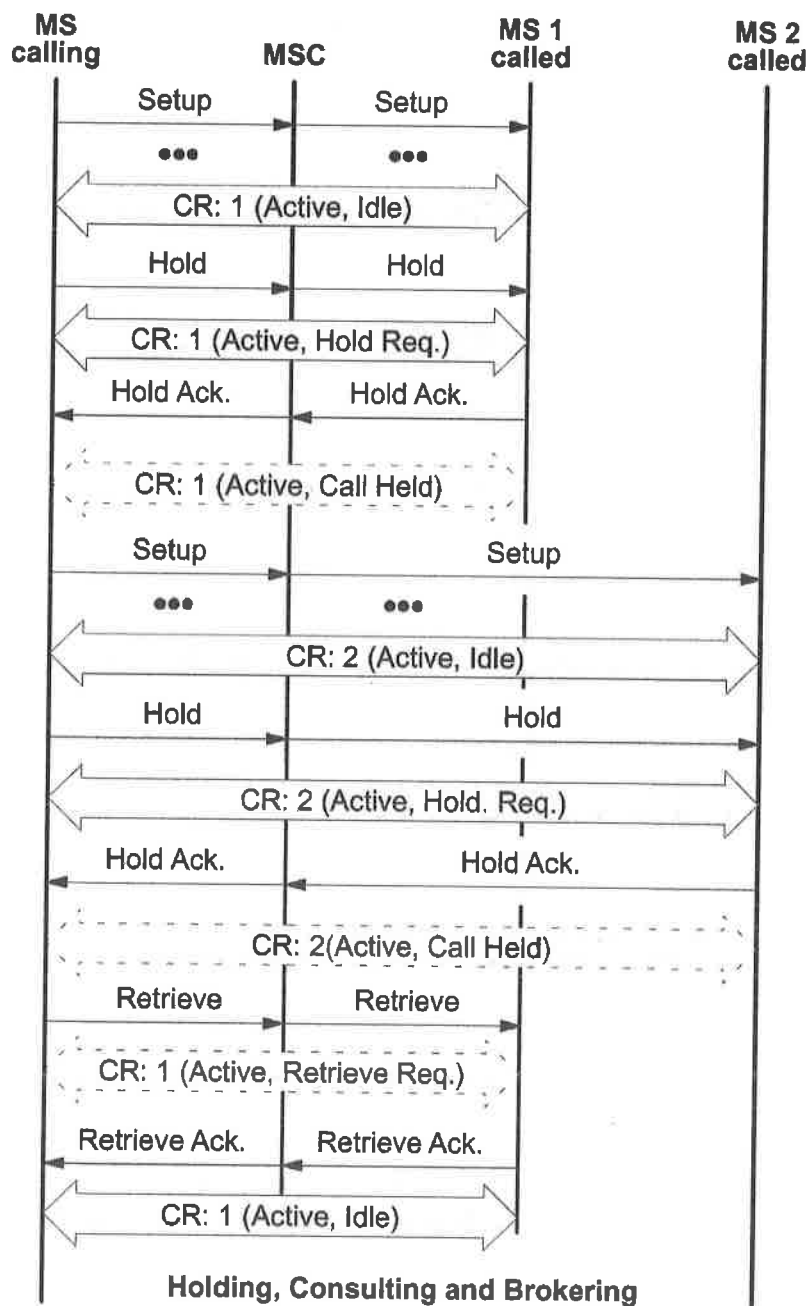


Figure 5.33 Call holding and associated procedures.

called subscriber but to the forwarding target selected when the service was activated (in Figure 5.34 it is another MS). The calling subscriber is informed about the change of the called number with a FACILITY message. Likewise the target of the forwarding is informed with a FACILITY message that the incoming call is a forwarded call. In this case, there is no necessity for a change in the extended state diagram nor is synchronization between network and MS required. It is only necessary that the involved MSs are informed about the occurrence of forwarding. In this case, the target of the call forwarding is also stored in

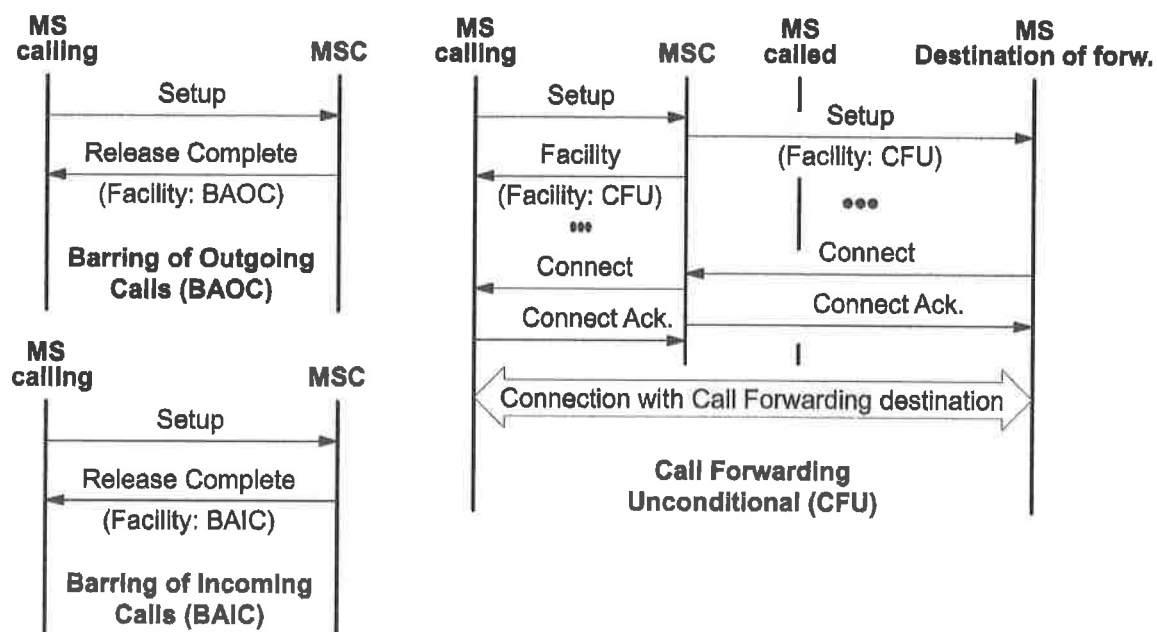


Figure 5.34 Barring and forwarding of calls.

the HLR of the subscriber who activated the service (the called MS in Figure 5.34). Thus, the call processing in the MSC of the called subscriber must be interrupted and the HLR must be informed about the call request. If the called subscriber has activated unconditional call forwarding, the HLR returns the new call target to the MSC, which can continue call processing with the changed target number.

5.4.8 Realization of SMS

The procedures for the transport of point-to-point short messages reside in the CM sublayer, also called the Short Message Control Layer (SM-CL) and in the Short Message Relay Layer (SM-RL) directly above. Accordingly, the protocol entities are called the Short Message Control (SMC) entity and the Short Message Relay (SMR) entity. A complete established MM connection is needed for the transport of short messages, which again presumes an existing RR connection with LAPDm protection on a SDCCH or SACCH channel. To distinguish among these packet-switched user data connections, SMS messages are transported across SAPI = 3 of the LAPDm entity.

A SMS transport PDU (SMS-SUBMIT or SMS-DELIVER; Figure 5.35) is transmitted with an RP-DATA message between MSC and MS using the SM-RP; section 5.3.2. Correct reception is acknowledged with an RP-ACK message either from the SMS-SC (mobile-initiated SMS transfer) or from the MS (mobile-terminated SMS transfer).

For the transfer of short messages between SMR entities in MS and MSC, the CM sublayer provides a service to the SM-RL layer above. The SMR entity requests this service for the transfer of RP-DATA or RP-ACK (MNSMS-ESTABLISH-REQUEST; Figure 5.36). Following the SMR service request, the SMC entity itself requests a MM connection on which it then transfers the short message inside a CP-DATA message. The appropriate

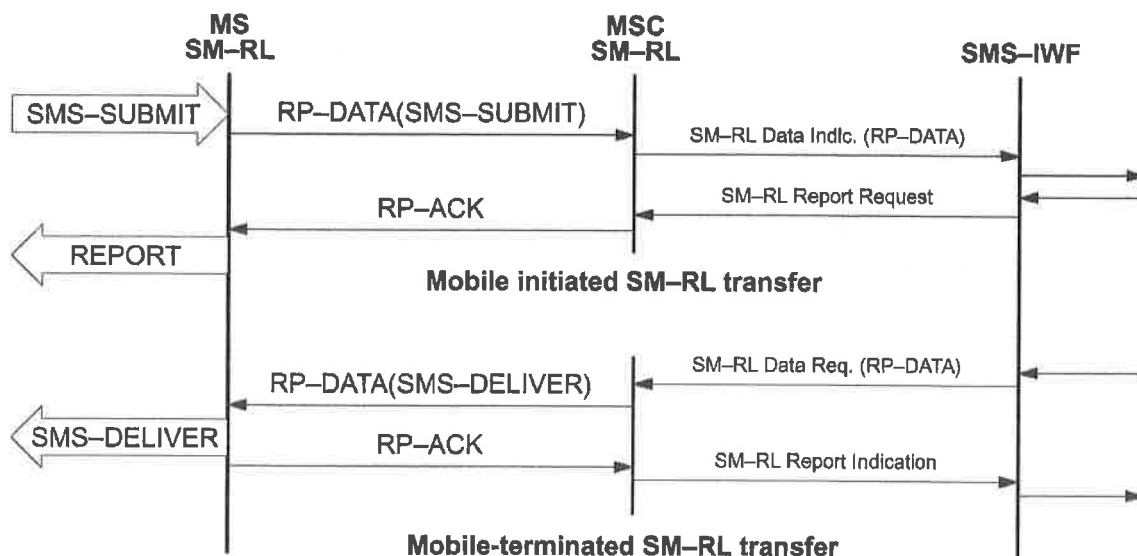


Figure 5.35 Short message transfer between SMR entities.

service primitives between protocol layers are also illustrated in Figure 5.36. The correct reception of CP-DATA is acknowledged with CP-ACK. In these SMC messages, one PDU transports a SDU from the SMR sublayer above. This SMC-SDU is the SMS relay message RP-DATA and its acknowledgement RP-ACK which are used to signal the transfer of short messages. The Short Message Transport Layer (SM-TL) above the SM-RL provides end-to-end transport of short messages between the MS and SMS-SC.

5.5 Signaling at the A and Abis interfaces

Whereas the transport of user data between MSC and BSC occurs across standard connections of the fixed network with 64 or 2048 kbit/s (or 1544 kbit/s), the transport of signaling messages between MSC and BSC runs over the SS#7 network. The MTP and SCCP parts of SS#7 are used for this purpose. A protocol function using the services of the SCCP is defined at the A interface. This is the BSSAP, which is further subdivided into DTAP and BSSMAP; see Figure 5.37. In addition, the Base Station System Operation and Maintenance Part (BSSOMAP) was introduced, which is needed for the transport of network management information from OMC via the MSC to the BSC.

At the A interface, one can distinguish between two signaling message streams: one between MSC and MS and another between MSC and BSS. The messages to the MS (CM, MM) are passed on transparently through the BSS using the DTAP protocol part of SS#7. BSC and BTS do not interpret them. The SCCP protocol part provides a connection-oriented and a connectionless transfer service for signaling messages. For DTAP messages, only a connection-oriented service is offered. The DTAP of the BSSAP uses one signaling connection for each active MS with one or more transactions per connection. A new connection is established each time when messages of a new transaction with a MS are to be transported between MSC and BSS.

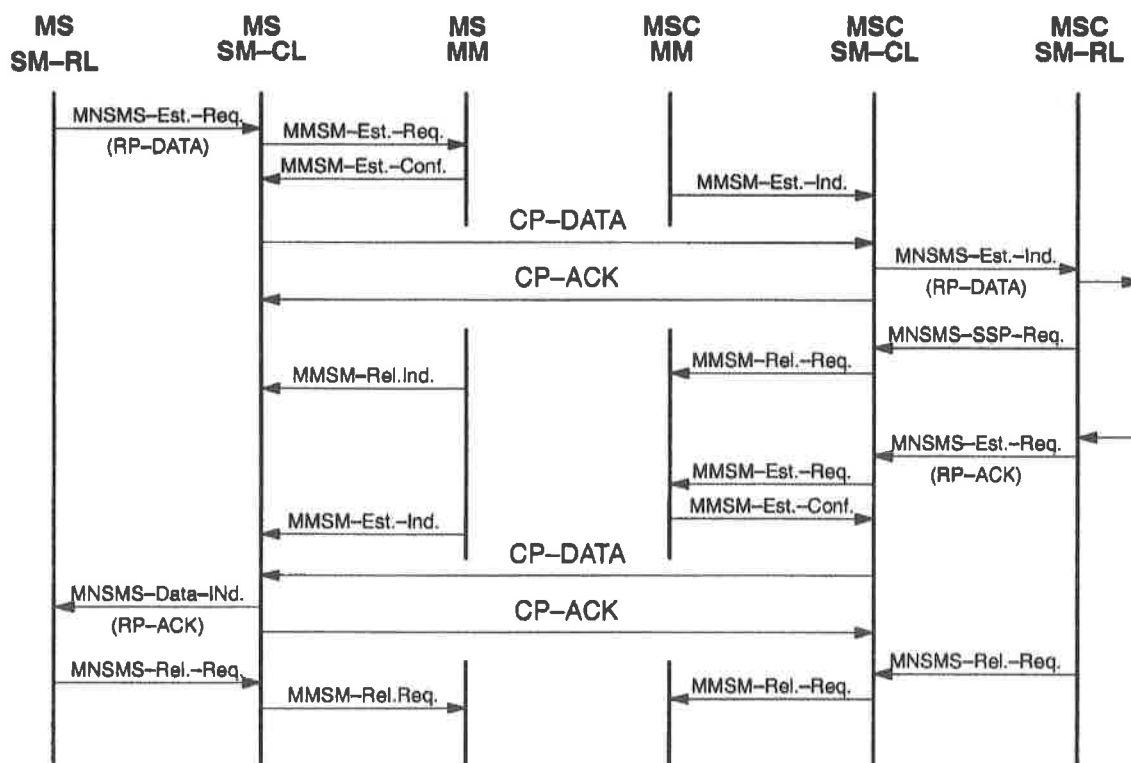


Figure 5.36 Short message transfer on the CM plane between MS and MSC.

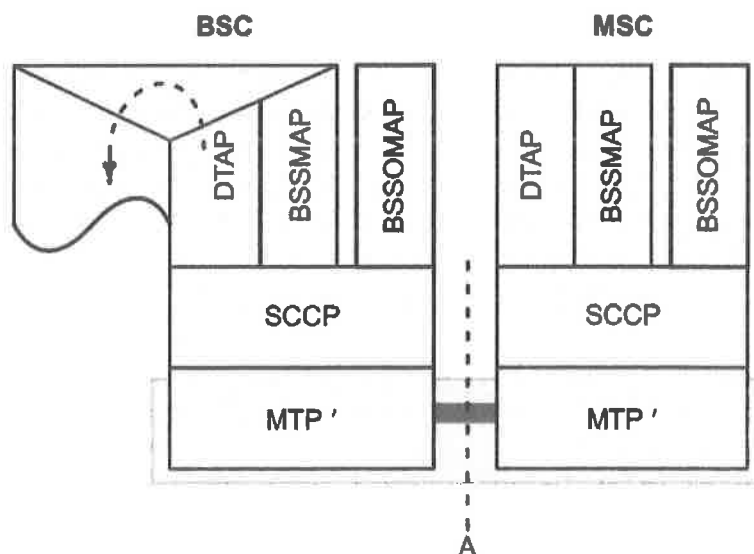


Figure 5.37 Protocols at the A interface between MSC and BSS.

Two cases of setting up a new SCCP connection are distinguished. First, in the case of location update and connection setup (outgoing or incoming), the BSS requests an SCCP

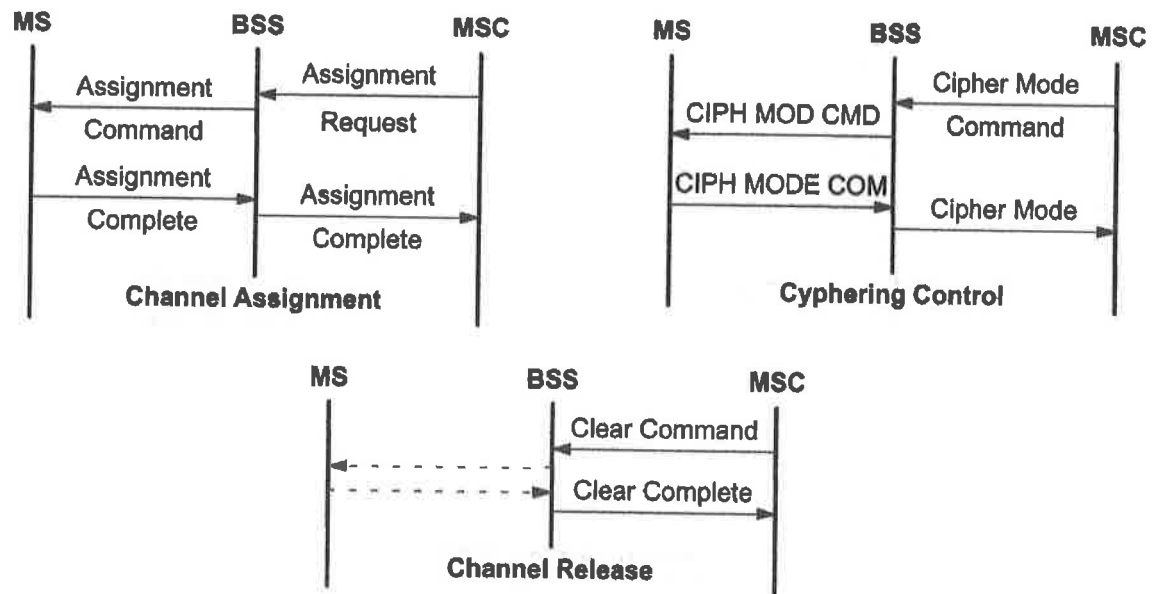


Figure 5.38 Examples of dedicated BSSMAP procedures.

connection after the channel request (access burst on RACH) from the MS has been satisfied with a SDCCH or TCH and after an LAPDm connection has been set up on the SDCCH or FACCH. The second situation for setting up an SCCP connection is a handover to another BSS, in which case the MSC initiates the connection setup. Most of the signaling messages at the air interface (CM and MM; Tables 5.5 and 5.6) are passed transparently through the BSS and packaged into DTAP-PDUs at the A interface, with the exception of some RR messages.

The BSSMAP implements two more kinds of signaling procedure between MSC and BSS: first those concerning one MS or single physical channels at the air interface; and, second, global procedures for the control of all of the resources of a BSS or cell. In the first case, the BSSMAP also uses connection-oriented SCCP services, whereas, in the second case, global procedures are performed with connectionless SCCP services. Among the BSSMAP procedures for a dedicated resource of the air interface are functions of resource management (channel assignment and release, start of cyphering) and of handover control (Figures 5.38 and 5.39).

Among the global procedures of BSSMAP are paging, flow control to prevent overloading protocol processors or CCCH channels, closing and opening of channels, and parts of handover control (Figure 5.40).

The transmission layer at the Abis interface between BTS and BSC is usually realized as a primary multiplexed line with 2048 kbit/s (1544 kbit/s in North America) or 64 kbit/s. This may include one physical connection per BTS or one for each connection between a TRX/BCF module and the BTS (Figure 5.5). On these digital paths, traffic or signaling channels of 16 or 64 kbit/s are established. The Layer 2 protocol at the Abis interface is LAPDm, whose Terminal Equipment Identifier (TEI) is used to address the TRX and/or BCF of a BTS (Figure 5.41).

Several LAPDm connections are established for each TEI: the Radio Signaling Link (RSL), SAPI = 0; the Operation and Maintenance Link (OML), SAPI = 62; and the Layer 2

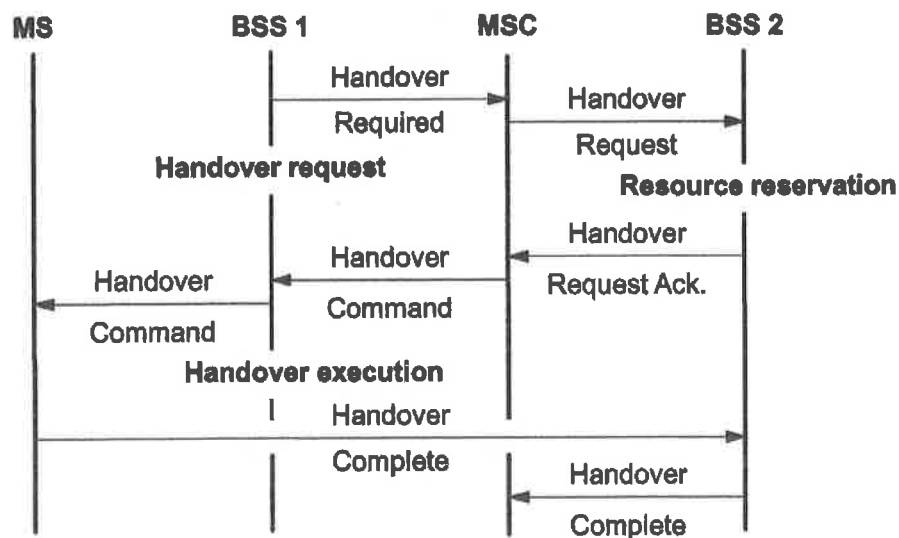


Figure 5.39 Dedicated BSSMAP procedures for internal handover.

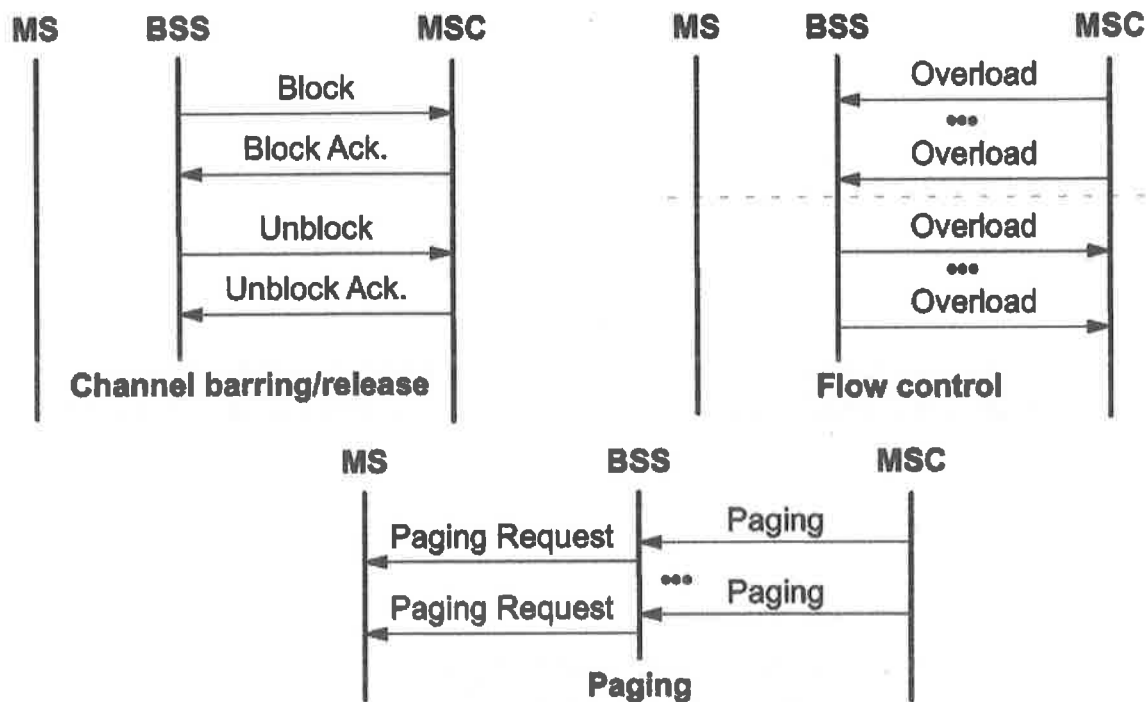


Figure 5.40 Examples of global BSSMAP procedures.

Management Link (L2ML), SAPI = 63. Traffic management is handled on the RSL, operation and maintenance on the OML, and management messages of Layer 2 are sent on the L2ML to the TRX or BCF. The RSL is the most important of these three links for the control of radio resources and connections for communication between MS and

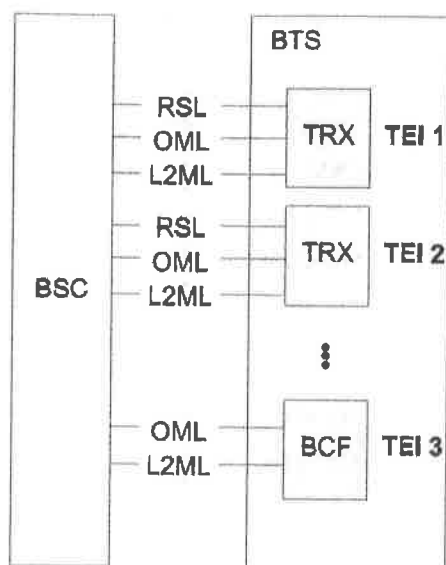


Figure 5.41 Logical connections at Layer 2 of the Abis interface.

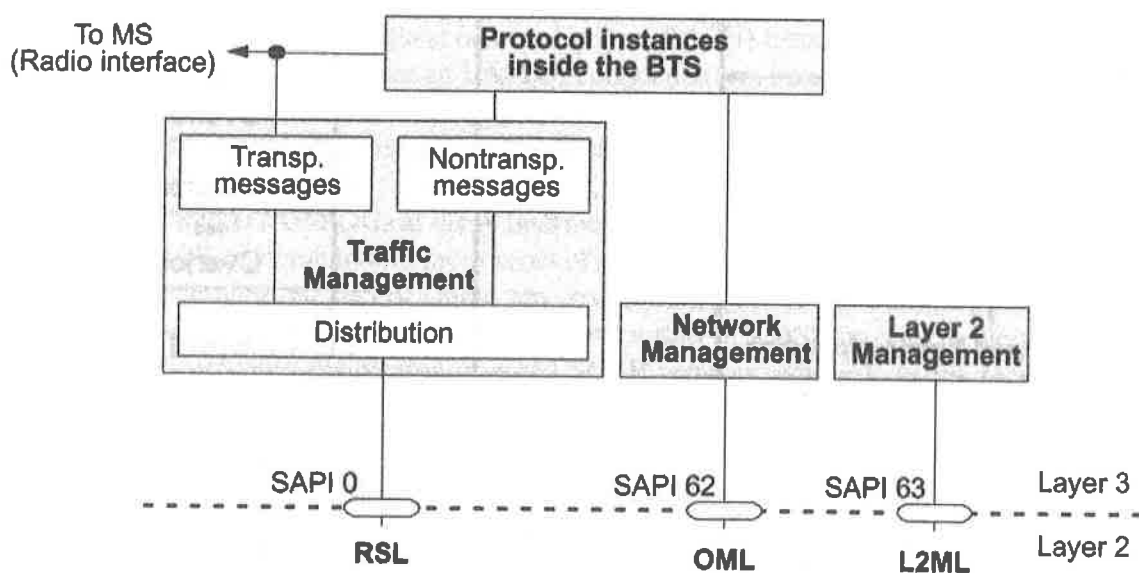


Figure 5.42 Protocol Layer 3 of the BTS at the Abis interface (BTSM).

network. Two types of messages are distinguished on this signaling link: transparent and nontransparent messages (Figure 5.42). Whereas the BTS passes on transparent messages from/to the LAPDm entity of a MS without interpreting or changing them, nontransparent messages are exchanged between BTS and BSC.

In addition, one distinguishes between four groups of traffic management messages of the BTS.



Figure 5.43 Transfer of transparent signaling messages.

- *Radio link layer management*: procedures to establish, modify and release connections of the link layer (LAPDm) to the MS at the air interface Um.
- *Dedicated channel management*: procedures to start ciphering, transfer of channel measurement reports of a MS, transmitter power control of MS and BTS, handover detection and modification of a dedicated channel of the BTS for a specific MS which can then receive the channel in another message (assign, handover command).
- *Common channel management*: procedures for transferring channel requests from MS (received on RACH), start of paging calls, measurement and transfer of CCCH traffic load measurements, modification of BCCH broadcast information, channel assignments to the MS (on the AGCH) and transmission of SMSCBs.
- *TRX management*: procedures for the transfer of measurements of free traffic channels of a TRX to the BSC or for flow control. In the case of overloaded TRX processors or overload on the downlink CCCH/ACCH.

In this way, all of the RR functions in the BTS can be controlled. The majority of RR messages (Table 5.4) are passed on transparently and do not terminate in the BTS. These messages are transported between BTS and BSC (Figure 5.43) in special messages (DATA REQUEST/INDICATION) packaged into LAPDm frames (Layer 2 at the radio interface).

All protocol messages received by the BTS on the uplink from the MS in LAPDm I/UI frames, except for channel measurement reports of the MS, are passed on as transparent messages in a DATA INDICATION.

Except for the link protocol LAPDm which is completely implemented in the BTS, there are some functions which are also handled by the BTS, and the pertinent messages from or to the MS are transformed by the BTS into the appropriate RR messages. This includes channel assignment, ciphering, assembly of channel measurements from MS and TRX and their transfer to the BSC (possibly with processing in the BTS), power control commands from the BTS for the MS, and channel requests from the MS (on the RACH) as well as channel assignments (Figure 5.44). Thus, four of the RR messages on the downlink direction to the MS (Table 5.4) cannot be treated as transparent messages: CIPHERING MODE COMMAND, PAGING REQUEST, SYSTEM INFORMATION and the three IMMEDIATE ASSIGN messages. All of the other RR messages to the MS are sent transparently within a DATA REQUEST to the BTS.

Figure 5.45 shows the format of a BTSM message (Layer 3 between BSC and BTS). Transparent and nontransparent messages are distinguished between with a message discriminator in the first octet. For this purpose, the T-bit (bit 1 of octet 1) is set to logical 1 for messages which the BTS is supposed to handle transparently or has recognized as transparent.

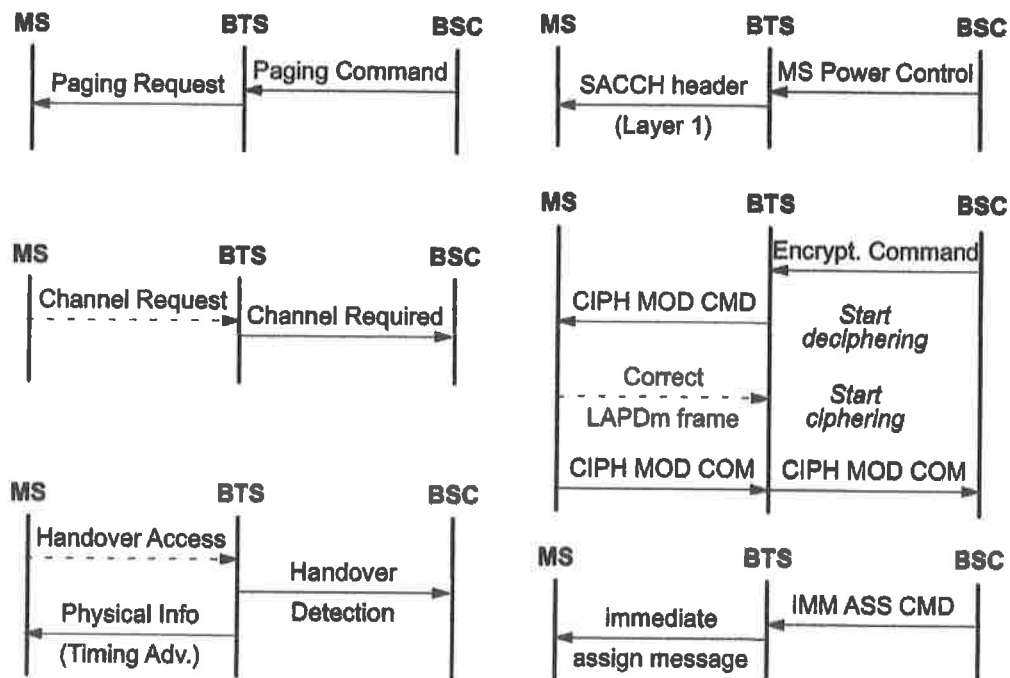


Figure 5.44 Examples of nontransparent signaling between BTS and BSC.

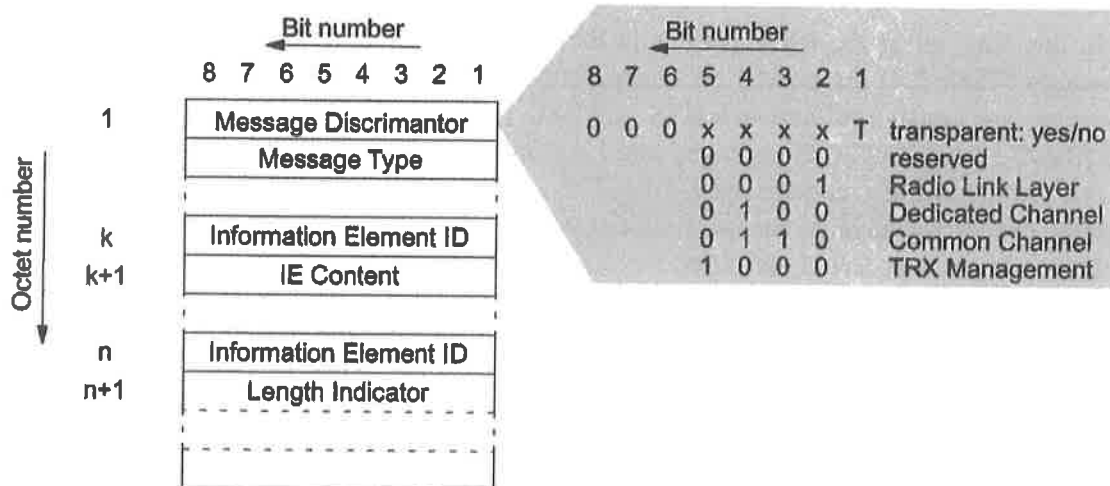


Figure 5.45 Format of BTSM-RSL protocol messages.

Bits 2 to 5 serve to assign the messages to one of the four groups defined on the RSL. Including the MT defines the message completely (Figure 5.45). The remainder of the BTSM message contains mandatory and optional IEs which have a fixed length of mostly two octets or which contain an additional length indicator in the case of variable length.

5.6 Security-related network functions: authentication and encryption

Methods of encryption for user data and for the authentication of subscribers, like all techniques for data security and data protection, are gaining enormous importance in modern digital systems (Eberspächer, 1999). GSM therefore introduced powerful algorithms and encryption techniques. The various services and functions concerned with security in a GSM PLMN are categorized in the following way:

- subscriber identity confidentiality;
- subscriber identity authentication;
- signaling information element confidentiality;
- data confidentiality for physical connections.

In the following, the security functions concerning the subscriber are presented.

5.6.1 Protection of subscriber identity

This function is intended to prevent the disclosure of which subscriber is using which resources in the network, by listening to the signaling traffic on the radio channel. On the one hand, this should ensure the confidentiality of user data and signaling traffic; on the other hand, it should also prevent the localization and tracking of a MS. This means above all that the IMSI should not be transmitted as clear text, i.e. unencrypted.

Instead of the IMSI, one uses a TMSI on the radio channel for identification of subscribers. The TMSI is temporary and has only local validity, which means that a subscriber can only be uniquely identified by TMSI and the LAI. The association between IMSI and TMSI is stored in the VLR.

The TMSI is issued by the VLR, at the latest, when the MS changes from one LA into another (location updating). When a new location area is entered, this is noticed by the MS (section 3.3.5) which reports to the new VLR with the old LAI and TMSI (*LAI_{old}* and *TMSI_{old}*; Figure 5.46). The VLR then issues a new TMSI for the MS. This TMSI is transmitted in encrypted form.

The subscriber identity is thus protected against eavesdropping in two ways: first, the TMSI is used on the radio channel instead of the IMSI; second, each new TMSI is transmitted in encrypted form.

In the case of database failures, if the VLR database is partially lost or no correct subscriber data are available (loss of TMSI, TMSI unknown at VLR, etc.), the GSM standard provides for a positive acknowledgement of the subscriber identity. For this subscriber identification, the IMSI must be transmitted as clear text (Figure 5.47) before encryption is turned on. Once the IMSI is known, encryption can be restarted and a new TMSI can be assigned.

5.6.2 Verification of subscriber identity

When a subscriber is added to a home network for the first time, a subscriber authentication key (*K_i*) is assigned in addition to the IMSI to enable the verification of the subscriber identity

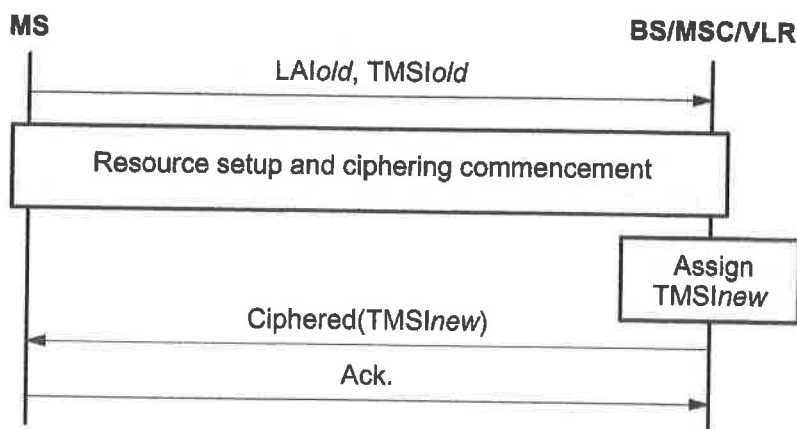


Figure 5.46 Encrypted transmission of the temporary subscriber identity.

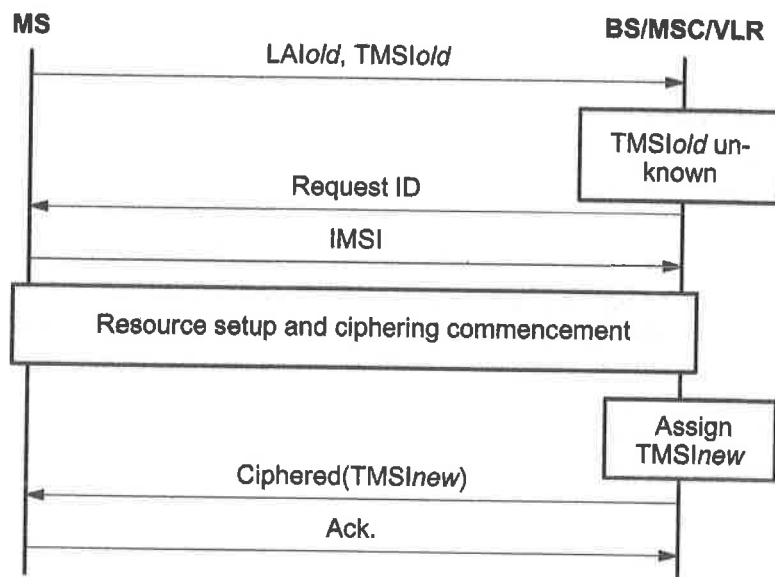


Figure 5.47 Clear text transmission of the IMSI when the TMSI is unknown.

(also known as authentication). All security functions are based on the secrecy of this key. At the network side, the key K_i is stored in the Authentication Center (AUC) of the home PLMN. At the subscriber side, it is stored on the SIM card of the subscriber.

The process of authenticating a subscriber is essentially based on the A3 algorithm, which is performed at the network side as well as at the subscriber side (Figure 5.48). This algorithm calculates independently on both sides (MS and network) the Signature Response (SRES) from the authentication key K_i and a Random Number (RAND) offered by the network. The MS transmits its SRES value to the network which compares it with its calculated value. If both values agree, the authentication was successful. Each execution of the algorithm A3 is performed with a new value of the random number RAND which cannot be predetermined;

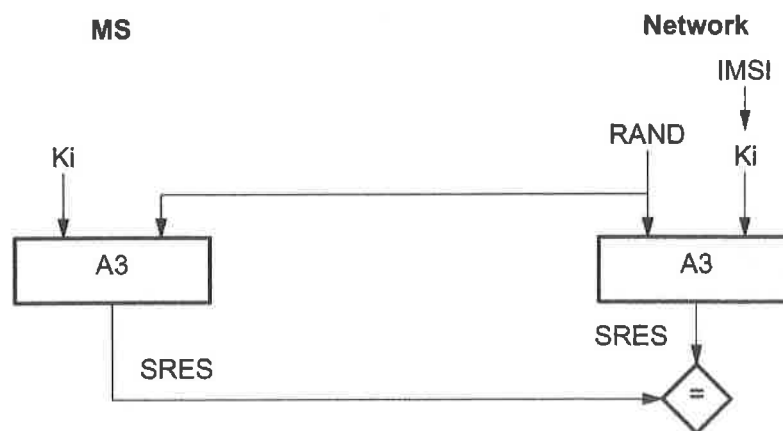


Figure 5.48 Principle of subscriber authentication.

in this way recording the channel transmission and playing it back cannot be used to fake an identity.

5.6.3 Generating security data

At the network side, the 2-tuple (RAND, SRES) need not be calculated each time when authentication has to be done. Rather the AUC can calculate a set of (RAND, SRES) 2-tuples in advance, store them in the HLR, and send them on demand to the requesting VLR. The VLR stores this set (RAND[n], SRES[n]) and uses a new 2-tuple from this set for each authentication procedure. Each 2-tuple is used only once; so new 2-tuples continue to be requested from the HLR/AUC.

This procedure, which lets the security data (Kc, RAND, SRES) be calculated in advance by the AUC, has the advantage that the secret authentication key Ki of a subscriber can be kept exclusively within the AUC, which ensures a higher level of confidentiality. A somewhat less secure variant is to supply the currently needed key Ki to the local VLR which then generates the security data locally.

If the key Ki is kept exclusively in the AUC, the AUC has to generate a set of security data for a specific IMSI on demand from the HLR (Figure 5.49): the random number RAND is generated and the pertinent signature SRES is calculated with the A3 algorithm, whereas the A8 algorithm generates the encryption key Kc.

The set of security data, a 3-tuple consisting of Kc, RAND, and SRES, is sent to the HLR and stored there. In most cases, the HLR keeps a supply of security data (e.g. 5), which can then be transmitted to the local VLR, so that one does not have to wait for the AUC to generate and transmit a new key. When there is a change of LA into one belonging to a new VLR, the sets of security data can be passed on to the new VLR. This ensures that the subscriber identity IMSI is transmitted only once through the air, namely when no TMSI has yet been assigned (see registration) or when these data have been lost. Afterwards the (encrypted) TMSI can be used for communicating with the MS.

If the IMSI is stored on the network side only in the AUC, all authentication procedures can be performed with the 2-tuples (RAND, SRES) which were precalculated by the AUC.

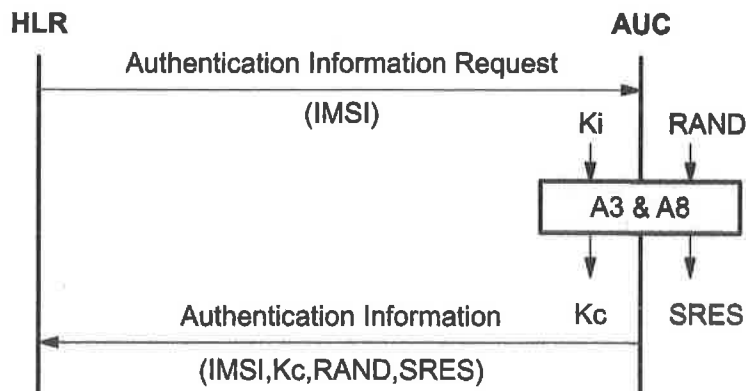


Figure 5.49 Generation of a set of security data for the HLR.

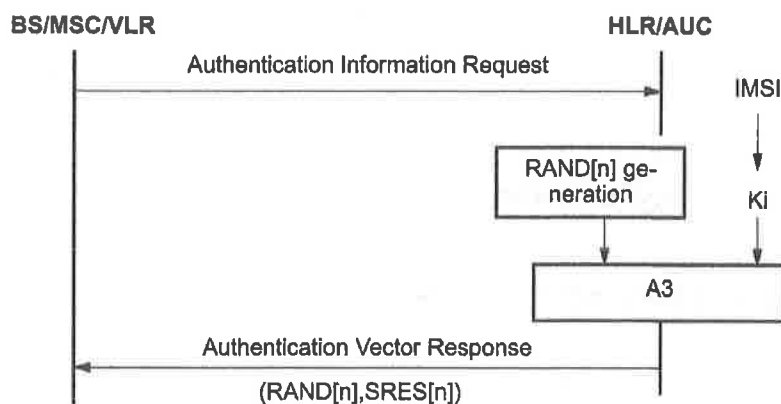


Figure 5.50 Highly secure authentication (no transmission of Ki).

In addition to relieving the load on the VLR (no execution of the A3 algorithm), this kind of subscriber identification (Figure 5.50) has the other advantage of being particularly secure, because confidential data, especially K_i , need not be transmitted over the air. It should be used, in particular, when the subscriber is roaming in a network of a foreign operator, since it avoids passing of security-critical data over the network boundary.

The less secure variant (Figure 5.51) should only be used within a PLMN. In this case, the secret (security-critical) key K_i is transmitted each time from the HLR/AUC to the current VLR, which executes the algorithm A3 for each authentication.

5.6.4 Encryption of signaling and payload data

The encryption of transmitted data is a special characteristic of GSM networks that distinguishes the offered service from analog cellular and fixed ISDN networks. This encryption is performed at the transmitting side after channel coding and interleaving and immediately preceding modulation (Figure 5.52). On the receiving side, decryption directly follows the demodulation of the data stream.

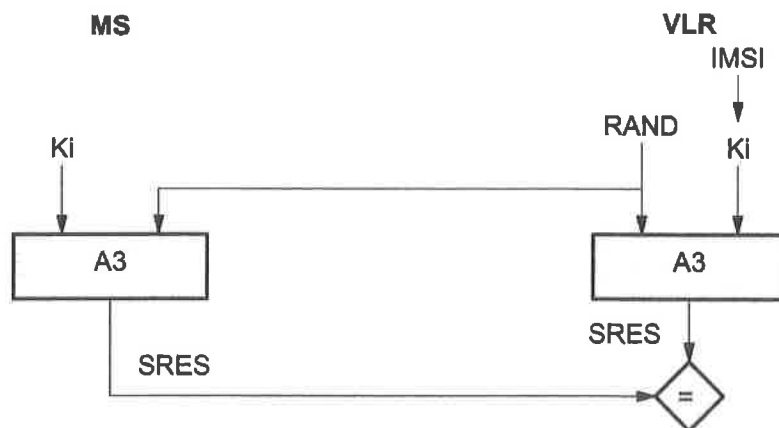


Figure 5.51 Weakly secure authentication (transmission of K_i to VLR).

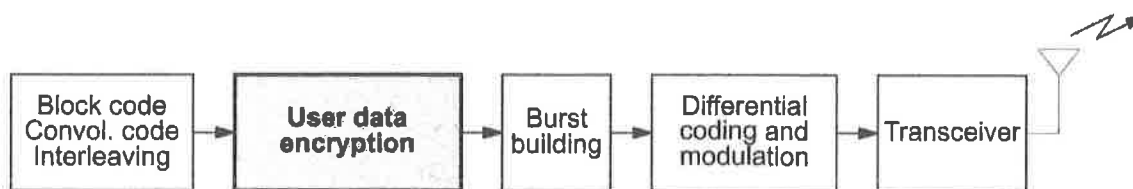


Figure 5.52 Encryption of payload data in the GSM transport chain.

A Cipher Key (K_c) for the encryption of user data is generated at each side using the generator algorithm A8 and the random number RAND of the authentication process (Figure 5.53). This key K_c is then used in the encryption algorithm A5 for the symmetric encryption of user data. At the network side, the values of K_c are calculated in the AUC/HLR simultaneously with the values for SRES. The keys K_c are combined with the 2-tuples (RAND, SRES) to produce 3-tuples, which are stored at the HLR/AUC and supplied on demand, in case the subscriber identification key K_i is only known to the HLR (section 5.6.2). In the case of the VLR having access to the key K_i , the VLR can calculate K_c directly.

The encryption of signaling and user data is performed at the MS as well as at the base station (Figure 5.54). This is a case of symmetric encryption, i.e. ciphering and deciphering are performed with the same key K_c and the A5 algorithm.

Based on the secret key K_i stored in the network, the cipher key K_c for a connection or signaling transaction can be generated at both sides, and the BTS and MS can decipher each other's data. Signaling and user data are encrypted together (TCH/SACCH/FACCH); for dedicated signaling channels (SDCCH) the same method is used as for traffic channels. This process is also called a *stream cipher*, i.e. ciphering uses a bit stream which is added bitwise to the data to be enciphered (Figure 5.55).

Deciphering consists of performing an additional EXCLUSIVE OR operation of the enciphered data stream with the ciphering stream. The FN of the current TDMA frame within a hyperframe (section 4.3.1) is another input for the A5 algorithm besides the key

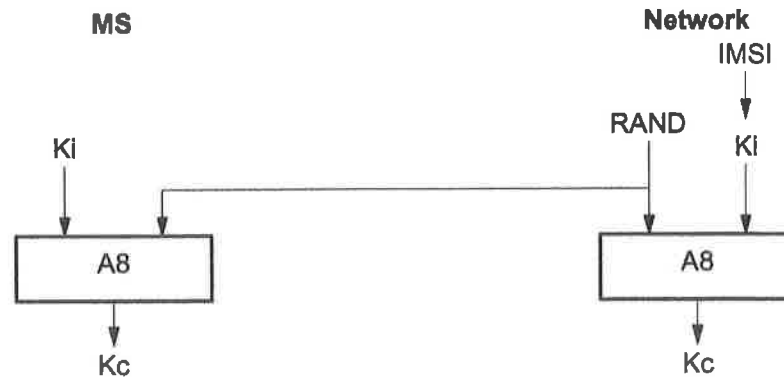
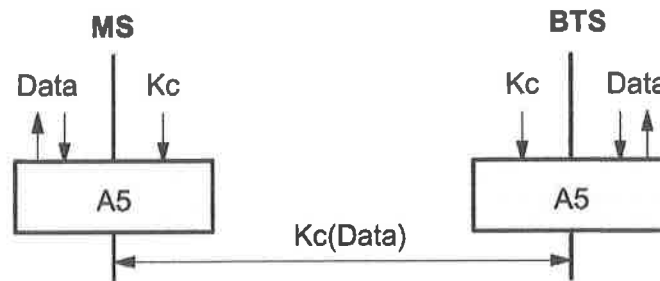
Figure 5.53 Generation of the cipher key K_c .

Figure 5.54 Principle of symmetric encryption of user data.

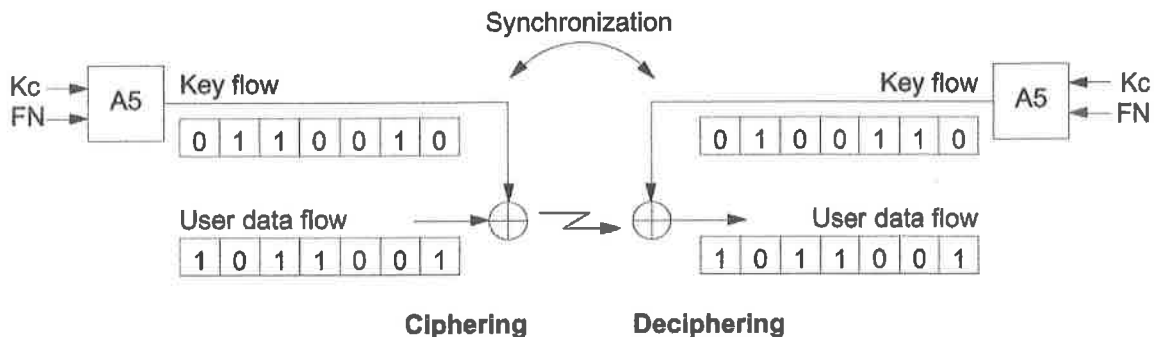


Figure 5.55 Combining payload data stream and ciphering stream.

K_c , which is generated anew for each connection or transaction. The current frame number is broadcast on the SCH and is thus available any time to all mobile stations currently in the cell. Synchronization between ciphering and deciphering processes is thus performed through FN.

However, the problem of synchronizing the activation of the ciphering mode has to be solved first: the deciphering mechanism on one side has to be started at precisely the correct moment. This process is started under network control, immediately after the authentication procedure is complete or when the key K_c has been supplied to the base station; Figure 5.56.

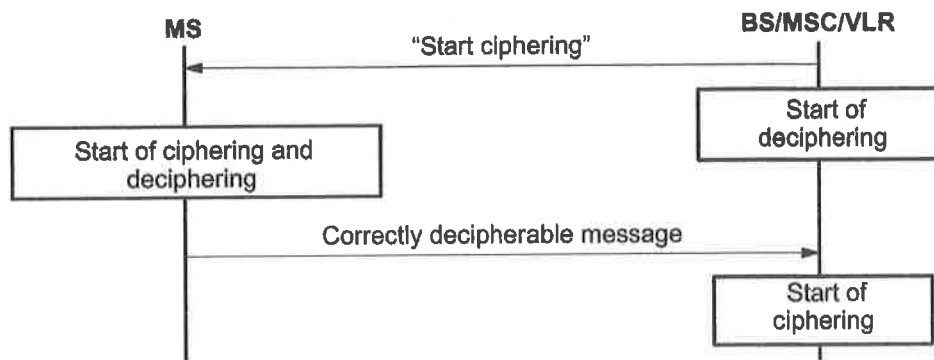


Figure 5.56 Synchronized start of the ciphering process.

The network, i.e. the BTS, transmits to the MS the request to start its (de)ciphering process, and it starts its own deciphering process. The MS then starts its ciphering and deciphering. The first ciphered message from the MS which reaches the network and is correctly deciphered leads to the start of the ciphering process on the network side.

5.7 Signaling at the user interface

Another often neglected but nevertheless very important interface in a mobile system is the user interface of the MS equipment. This Man-Machine Interface (MMI) can be realized freely and therefore in many different ways by the mobile equipment manufacturers. In order to keep a set of standardized service control functions in spite of this variety, the MMI commands have been introduced. These MMI commands define procedures mainly for the control of basic services and SS. The control procedures are constructed around the input of command token strings which are delineated and formatted with the tokens * and #. In order to avoid a user having to learn and memorize a certain number of service control procedures before being able to use the mobile phone, a small set of basic required commands for the MMI interface has been defined; this is the basic public MMI which must be satisfied by all MSs.

The specification basic public MMI outlines the basic functions which must be implemented as a minimum at the MMI of a MS. This includes the arrangement of a 12-key keyboard with the numbers 0 through 9 and the keys for * and # as well as SEND and END keys, which also serve to initiate a desired call or accept or terminate a call.

Some basic operational sequences for making or taking a call are also defined. These requirements are so general that they can be easily satisfied by all mobile equipment.

The MMI commands for the control of SS and the enquiry and configuration of parameters are much more extensive. Using a set of MMI commands which are uniform for all MSs allows control functions to be performed which are often hidden in equipment-specific user guidance menus. For certain functional areas, a MS can thus be operated in a manufacturer-independent way, if one forgoes the sometimes very comfortable possibilities of user-guiding menus and instead learns the control sequences for the respective functions. These sequences are mapped onto the respective signaling procedures within the MS.

Table 5.8 Input format of some MMI commands.

Function	MMI procedure
Activate	*nn(n)*Si#
Deactivate	#nn(n)*Si#
Status enquiry	*#nn(n)*Si#
Registration	**nn(n)*Si#
Delete	##nn(n)*Si#

A MMI command is always constructed according to the same pattern. Five basic formats are distinguished (Table 5.8), which all start with a combination of the tokens * and #: activation (*), deactivation (#), status inquiry (*#), registration (***) and cancellation (##).

In addition, the MMI command must contain a MMI service code of two or three tokens, which selects the function to be performed. In certain cases, the MMI procedure requires additional arguments or parameters, which are separated by *, as Supplementary Information (Si). The MMI command is always terminated with # and may also require the SEND key to be depressed, if the command is not executed locally within the MS but must be transmitted to the network. Table 5.9 contains some basic examples of MMI commands, e.g. the inquiry for the IMEI of the MS (*#06#) or the change of the PIN (**04*old_PIN*new_PIN*new_PIN#) used to protect the SIM card against misuse. This example also shows how supplementary information is embedded in the command.

Table 5.9 Some basic MMI commands.

Function	MMI procedure
Mobile phone IMEI enquiry	*#06#
Change password for call barring	**03*330*old_PWD*new_PWD*new_PWD#
Change PIN in SIM	**04*old_PIN*new_PIN*new_PIN#
Select SIM number storage	n(n)(n)#

With MMI commands, it is also possible to configure and use SS. For this purpose, each SS is designated with a two- or three-digit MMI service code to select the respective SS (Table 5.10). In some cases, supplementary information is mandatory for the activation of the service, e.g. one needs the target Destination Number (DN) for the call forwarding functions, or the Activation Password (PW) for the SS of barring incoming or outgoing calls (Sia in Table 5.10).

The example of unconditional call forwarding also illustrates the difference between registration and activation of a service. With the command **21*call_number# the forwarding function is registered, the target number configured, and the unconditional forwarding activated. Later, the unconditional forwarding can be deactivated any time with #21# and

Table 5.10 MMI service codes for SS.

Abbreviation	Service	MMI code	Sia	Sib
	All call forwarding, only for (de)activation	2	—	—
	All conditional call forwarding (not CFU), only for (de)activation	4	—	—
CFU	Call forwarding unconditional	21	DN	BS
CFB	Call forwarding on mobile subscriber busy	67	DN	BS
CFNRy	Call forwarding on no reply	61	DN	BS
CFNRc	Call forwarding on mobile subscriber not reachable	62	DN	BS
	All call barring (only for deactivation)	330	PW	BS
BAOC	Barring of all outgoing calls	33	PW	BS
BOI	Barring of outgoing international calls	331	PW	BS
BOIC-exHC	Barring of outgoing international calls except those to home PLMN	332	PW	BS
BAIC	Barring of all incoming calls	35	PW	BS
BIC-Roam	Barring of incoming calls when roaming outside the home PLMN	351	PW	BS
CLIP	Calling line identification presentation	30	—	BS
CLIR	Calling line identification restriction	31	—	BS
CW	Call waiting	43	—	BS
COLP	Connected line identification presentation	76	—	BS
COLR	Connected line identification restriction	77	—	BS

reactivated with *21#. The target number call_number remains stored, unless it is cancelled with the command ##21#. After cancellation, if call forwarding is desired again, it must first be registered again using the **21... command. For some basic services, characteristics can also be activated selectively. The MMI command can contain a second parameter field

Table 5.11 MMI codes for basic services.

Category	Service	MMI code BS
Telematic service	All telematic services	10
	Telephone	11
	All data services	12
	Facsimile	13
	Videotex	14
	Teletext	15
	SMS	16
	All data services except SMS	18
	All telematic services except SMS	19
Bearer service	All bearer services	20
	All asynchronous services	21
	All synchronous services	22
	All connection-oriented synchronous data services	24
	All connection-oriented asynchronous data services	25
	All packet-oriented synchronous data services	26
	All PAD-access services	27

with supplementary information (Sib, Table 5.10) which is again delineated with *. This field contains the service code BS of the basic service for which the SS is to become effective.

An overview of MMI codes for basic services is given in Table 5.11. For example, one can bar incoming calls except short messages with the command `**35*PW*18#`, or one can forward incoming fax calls to the number fax_number with the command `**21*fax_number*13#` (the other teleservices remain unaffected).

Roaming and handover

6.1 Mobile application part interfaces

The main benefit for the mobile subscribers that the international standardization of GSM has brought is that they can move freely not only within their home networks but also in international GSM networks and that at the same time they can even gain access to the special services they subscribed to at home provided that there are agreements between the operators. The functions needed for this free roaming are called roaming or mobility functions. They rely mostly on the GSM-specific extension of the SS#7. The MAP procedures relevant for roaming are first the location registration/update, IMSI attach/detach, requesting subscriber data for call setup and paging. In addition, the MAP contains functions and procedures for the control of SS and handover, for subscriber management, for IMEI management, for authentication and identification management, as well as for the user data transport of the SMS. MAP entities for roaming services reside in the MSC, HLR and VLR. The corresponding MAP interfaces are defined as B (MSC-VLR), C (MSC-HLR), D (HLR-VLR), E (MSC-MSC) and G (VLR-VLR) (Figure 3.6). At the subscriber interface, the MAP functions correspond to the functions of MM, i.e. the MM messages and procedures of the Um interface are translated into the MAP protocols in the MSC.

The most important functions of GSM MM are location registration with the PLMN and location updating to report the current location of a MS, as well as the identification and authentication of subscribers. These actions are closely interrelated. During registration into a GSM network, during the location updating procedure, and also during the setup of a connection, the identity of a mobile subscriber must be determined and verified (authentication).

The MM data are the foundation for creating the functions needed for routing and switching of user connections and for the associated services. For example, they are requested for routing an incoming call to the current MSC or for localizing a MS before paging is started. In addition to mobility data management, information about the configuration of SS is requested or changed, e.g. the currently valid target number for unconditional call forwarding in the HLR or VLR registers.

6.2 Location registration and location update

Before a MS can be called or gain access to services, the subscriber has to register with the mobile network (PLMN). This is usually the home network where the subscriber has a service contract. However, the subscriber can equally register with a foreign network provider in whose service area they are currently visiting, provided that there is a roaming agreement between the two network operators. Registration is only required if there is a change of networks, and therefore a VLR of the current network has not yet issued a TMSI to the subscriber. This means the subscriber has to report to the current network with their IMSI and receives a new TMSI by executing a location registration procedure. This TMSI is stored by the MS in its nonvolatile SIM storage, such that even after a powerdown and subsequent power-up only a normal location updating procedure is required.

The sequence of operations for registration is presented schematically in Figure 6.1. After a subscriber has requested registration at their current location by sending a LOCATION UPDATE REQUEST with their IMSI and the current location area (LAI), first the MSC instructs the VLR with a MAP message UPDATE LOCATION AREA to register the MS with its current LAI. In order for this registration to be valid, the identity of the subscriber has to be checked first, i.e. the authentication procedure is executed. For this purpose, the authentication parameters have to be requested from the AUC through the HLR. The precalculated sets of security parameters (Kc, RAND, SRES) are not usually transmitted individually to the respective VLR. In most cases, several complete sets are kept at hand for several authentications. Each set of parameters, however, can only be used once, i.e. the VLR must continually update its supply of security parameters (AUTHENTICATION PARAMETER REQUEST).

After successful authentication (section 5.6.2), the subscriber is assigned a new MSRN, which is stored with the LAI in the HLR, and a new TMSI is also reserved for this subscriber; this is TMSI reallocation (Figure 5.25). To encrypt the user data, the base station needs the ciphering key Kc, which it receives from the VLR by way of the MSC with the command START CIPHERING. After ciphering of the user data has begun, the TMSI is sent in encrypted form to the MS. Simultaneously with the TMSI assignment, the correct and successful registration into the PLMN is acknowledged (LOCAPDATE ACCEPT). Finally, the MS acknowledges the correct reception of the TMSI (TMSI REALLOCATION COMPLETE; Figure 5.26).

While the location information is being updated, the VLR is obtaining additional information about the subscriber, e.g. the MS category or configuration parameters for SS. For this purpose, the insert subscriber data procedure is defined (INSERT SUBSCRIBER DATA message in Figure 6.1). It is used for registration or location updating in the HLR to transmit the current data of the subscriber profile to the VLR. In general, this MAP procedure can always be used when the profile parameters are changed, e.g. if the subscriber reconfigures a SS such as unconditional forwarding. The changes are communicated immediately to the VLR with the insert subscriber data procedure.

The location update procedure is executed if the MS recognizes (by reading the LAI broadcast on the BCCH) that it is in a new location area, which leads to updating the location information in the HLR record. Alternatively, the location update can also occur periodically, independent of the current location. For this purpose, a time interval value is broadcast on the BCCH, which prescribes the time between location updates. The main objective of this

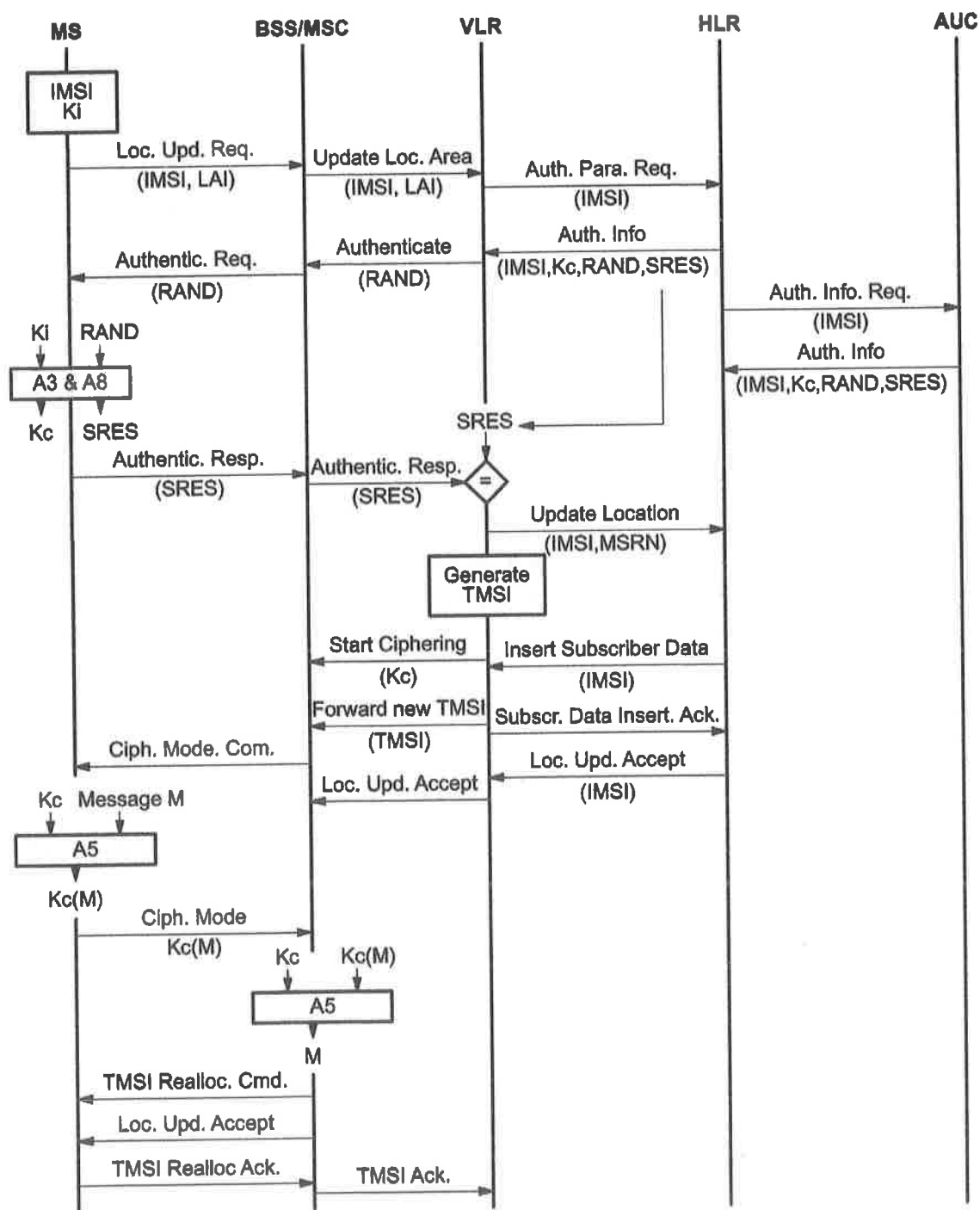


Figure 6.1 Overview of the location registration procedure.

location update is to know the current location for incoming calls or short messages, so that the call or message can be directed to the current location of the MS. The difference between the location update procedure and the location registration procedure is that in the first case

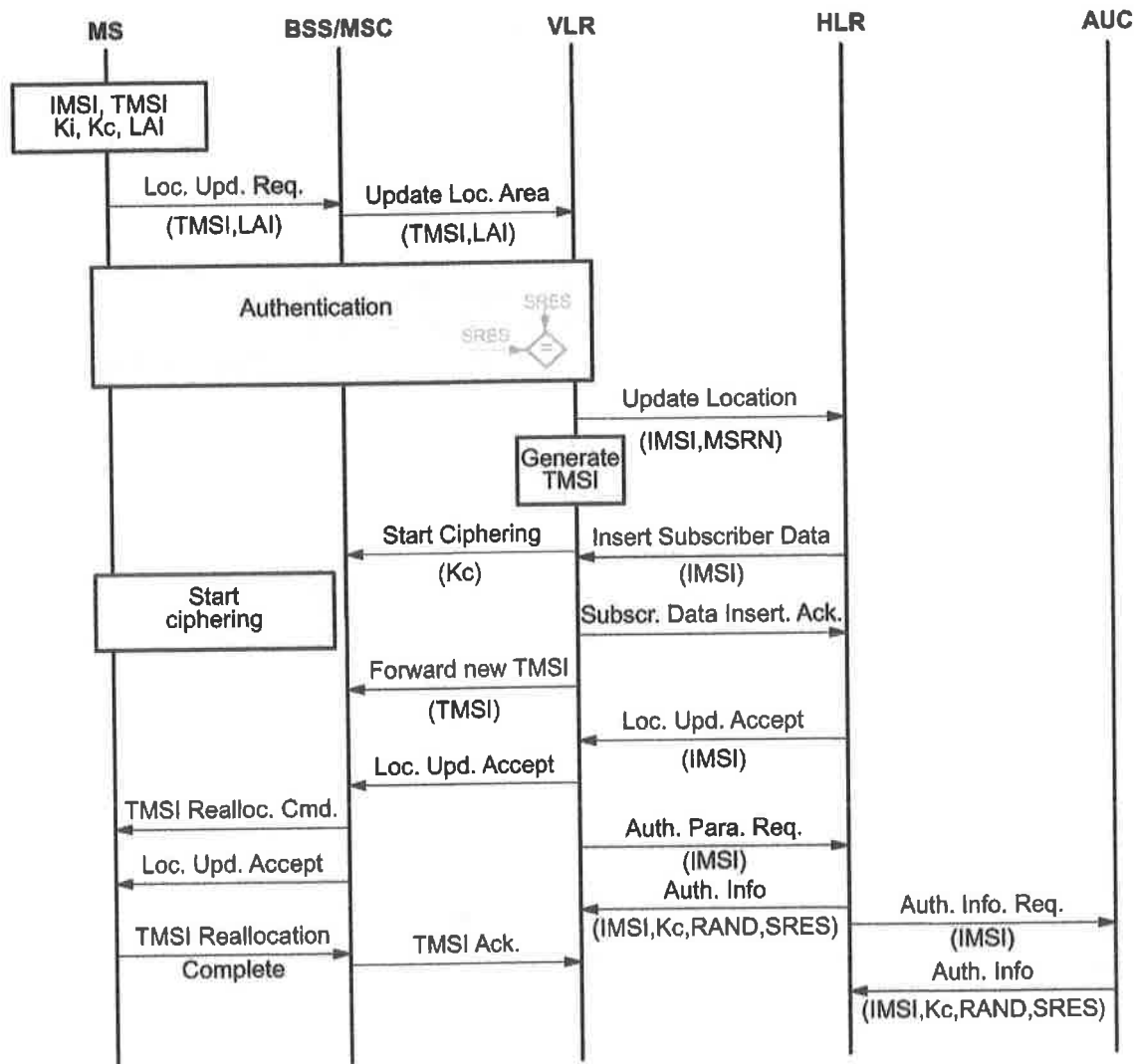


Figure 6.2 Overview of the location updating procedure.

the MS has already been assigned a TMSI. The TMSI is unique only in connection with an LAI, and both are kept together in the nonvolatile storage of the SIM card. With a valid TMSI, the MS also keeps a current ciphering key K_c for encryption of user data (Figure 6.2), although this key is renewed during the location update procedure. This key is recalculated by the MS based on the random number RAND used for authentication, whereas on the network side it is calculated in the AUC and made available in the VLR.

Corresponding to the location update procedure, there is a MM procedure at the air interface of the MM category 'specific'. In addition to the location updating proper, it contains three blocks which are realized at the air interface by three procedures of the category 'common' (Figure 5.26): the identification of the subscriber, the authentication and the start of ciphering on the radio channel. In the course of location updating, the MS also receives a new TMSI, and the current location is updated in the HLR. Figure 6.2 illustrates the standard case of a location update. The MS has entered a new LA, or the timer for periodic

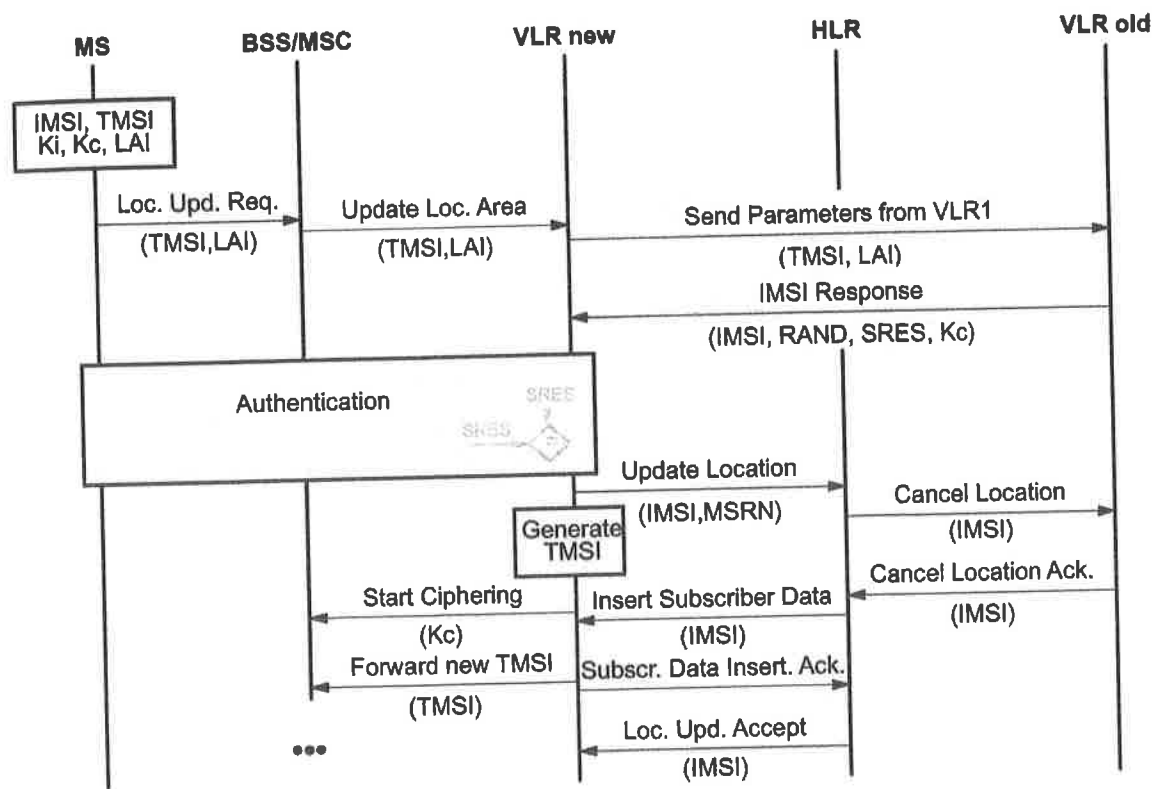


Figure 6.3 Location update after changing the VLR area.

location updating has expired, and the MS requests to update its location information. It is assumed that the new LA still belongs to the same VLR as the previous LA, so only a new TMSI needs to be assigned. This is the most frequent case. However, if it is not quite so crucial to keep the subscriber identity confidential, it is possible to avoid assigning a new TMSI. In this case, only the location information is updated in the HLR/VLR.

The new TMSI is transmitted to the MS in enciphered form together with the acknowledgement of the successful location update. The location update is complete after acknowledgement by the MS. After execution of the authentication, the VLR can complete its database and replace the 'consumed' 3-tuple (RAND, SRES, Kc) by another one requested from the HLR/AUC.

If location change involves both LA and VLR, the location update procedure is somewhat more complicated (Figure 6.3). In this case, the new VLR has to request the identification and security data for the MS from the old VLR and store them locally. Only in emergency cases, if the old VLR cannot be determined from the old LAI or if the old TMSI is not known in the VLR, the new VLR may request the IMSI directly from the MS (identification procedure). Only after a MS has been identified through the IMSI from the old VLR and after the security parameters are available in the new VLR, is it possible for the MS to be authenticated and registered in the new VLR, for a new TMSI to be assigned, and for the location information in the HLR to be actualized. After successful registration in the new VLR (LOCATION UPDATE ACCEPT) the HLR instructs the old VLR to cancel the invalid location data in the old VLR (CANCEL LOCATION).

In the examples shown (Figures 6.1–6.3), the location information is stored as a MSRN in the HLR. The MSRN contains the routing information for incoming calls and this information is used to route incoming calls to the current MSC. In this case, the HLR receives the routing information already at the time of the location update. Alternatively, at location update time, the HLR may just store the current MSC and/or VLR number in connection with an LMSI, such that routing information is only determined at the time of an incoming call.

6.3 Connection establishment and termination

6.3.1 Routing calls to MSs

The number dialed to reach a mobile subscriber (MSISDN) contains no information at all about the current location of the subscriber. In order to establish a complete connection to a mobile subscriber, however, one must determine the current location and the locally responsible switch (MSC). In order to be able to route the call to this switch, the routing address to this subscriber (MSRN) has to be obtained. This routing address is assigned temporarily to a subscriber by its currently associated VLR. At the arrival of a call at the GMSC, the HLR is the only entity in the GSM network which can supply this information, and therefore it must be interrogated for each connection setup to a mobile subscriber. The principal sequence of operations for routing to a mobile subscriber is shown in Figure 6.4. An ISDN switch recognizes from the MSISDN that the called subscriber is a mobile subscriber, and therefore can forward the call to the GMSC of the subscriber's home PLMN based on the CC and NDC in the MSISDN (1). This GMSC can now request the current routing address (MSRN) for the mobile subscriber from the HLR using the MAP (2,3). By way of the MSRN the call is forwarded to the local MSC (4), which determines the TMSI of the subscriber (5,6) and initiates the paging procedure in the relevant location area (7). After the MS has responded to the paging call (8), the connection can be switched through.

Several variants for determining the route and interrogating the HLR exist, depending on how the MSRN was assigned and stored, whether the call is national or international and depending on the capabilities of the associated switching centers.

Effect of the MSRN assignment on routing

There are two ways to obtain the MSRN:

- obtaining the MSRN at location update;
- obtaining the MSRN on a per call basis.

For the first variant, an MSRN for the MS is assigned at the time of each location update which is stored in the HLR. In this way the HLR is in a position to immediately supply the routing information needed to switch a call through to the local MSC.

The second variant requires that the HLR has at least an identification for the currently responsible VLR. In this case, when routing information is requested from the HLR, the HLR first has to obtain the MSRN from the VLR. This MSRN is assigned on a per call basis, i.e. each call involves a new MSRN assignment.

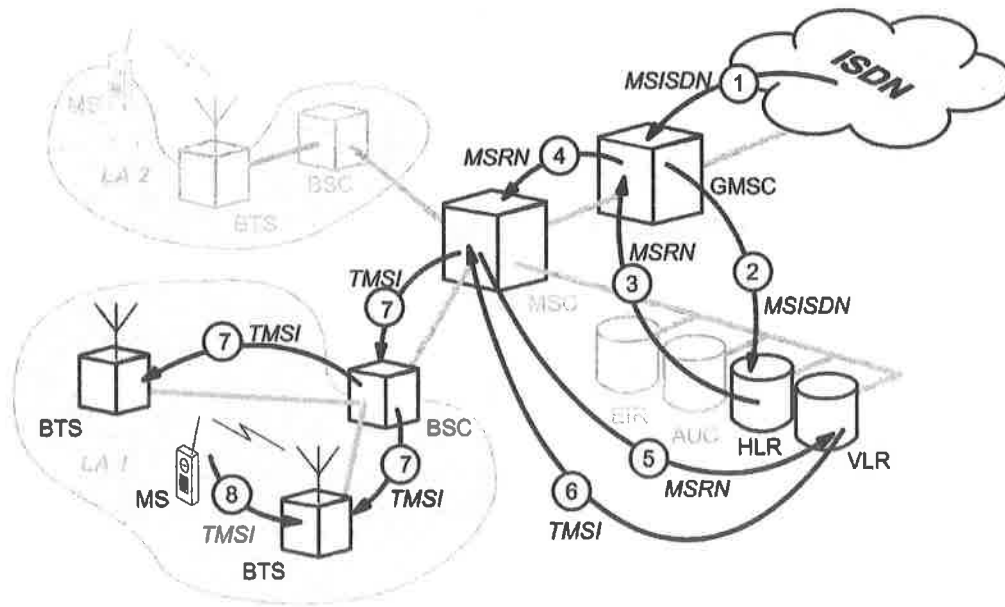


Figure 6.4 Principle of routing calls to mobile subscribers.

Placement of the protocol entities for HLR interrogation

Depending on the capabilities of the associated switches and the called target (national or international MSISDN), there are different routing procedures. In general, the local switching center analyzes the MSISDN. Owing to the NDC, this analysis of the MSISDN allows the separation of the mobile traffic from other traffic. The case that mobile call numbers are integrated into the numbering plan of the fixed network is currently not provided.

In the case of a national number, the local exchange recognizes from the NDC that the number is a mobile ISDN number. The fixed network and home PLMN of the called subscriber reside in the same country. In the ideal case, the local switch can interrogate the HLR responsible for this MSISDN (HLR in the home PLMN of the subscriber) and obtain the routing information (Figure 6.5(a)). The connection can then be switched through via fixed connections of the ISDN directly to the MSC.

If the local exchange does not have the required protocol intelligence for the interrogation of the HLR, the connection can be passed on preliminarily to a transit exchange, which then assumes the HLR interrogation and routing determination to the current MSC (Figure 6.5(b)). If the fixed network is not at all capable of performing a HLR interrogation, the connection has to be directed through a GMSC. This GMSC connects through to the current MSC (Figure 6.5(c)). For all three cases, the MS could also reside in a foreign PLMN (roaming); the connection is then made through international lines to the current MSC after interrogating the HLR of the home PLMN.

In the case of an international call number, the local exchange recognizes only the international CC and directs the call to an ISC. Then the ISC can recognize the NDC of the mobile network and process the call accordingly. Figures 6.6 and 6.7 show examples for the processing of routing information. An international call to a mobile subscriber involves at least three networks: the country from which the call originates; the country with the home

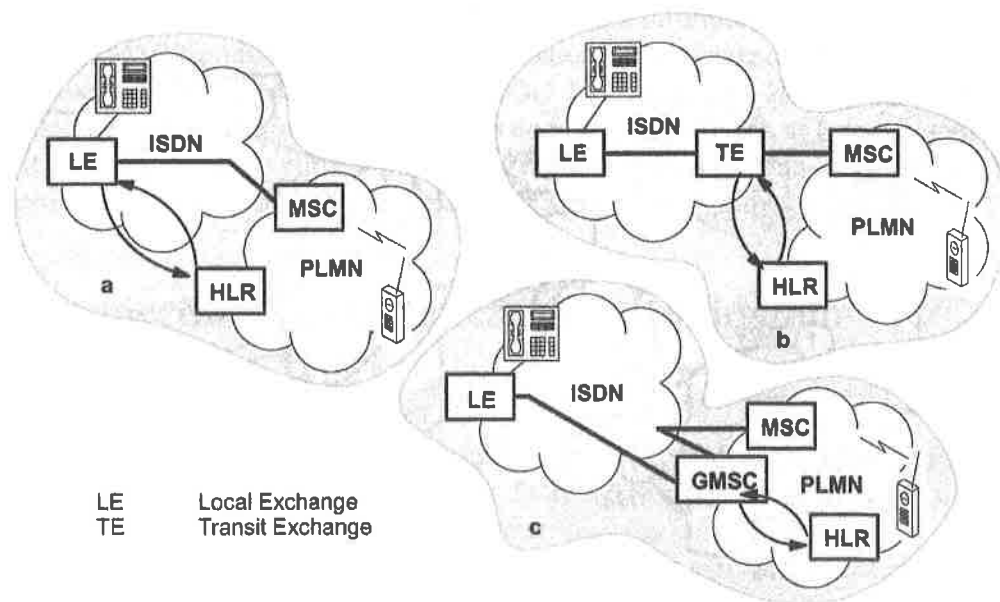


Figure 6.5 Routing variants for national MSISDN.

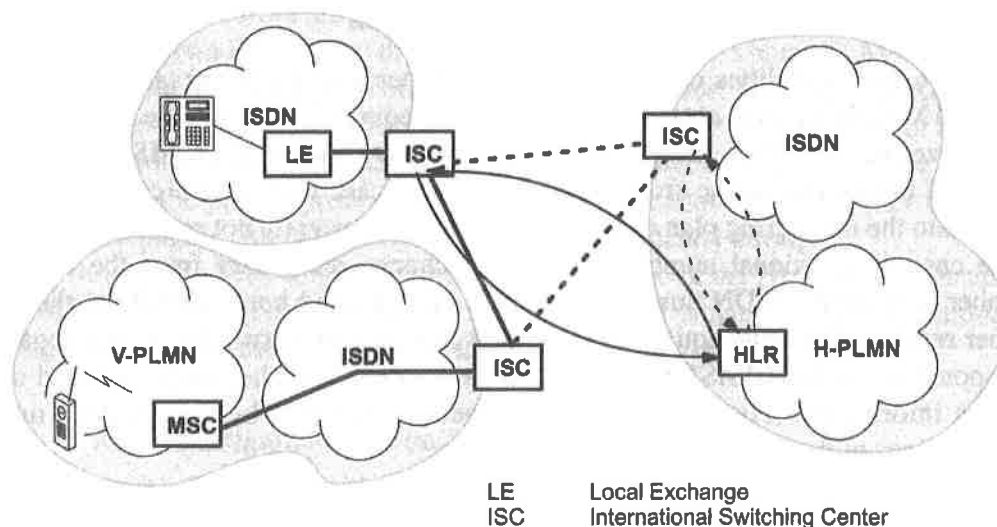


Figure 6.6 Routing for international MSISDN (HLR interrogation from ISC).

PLMN of the subscriber, Home PLMN (H-PLMN); and the country in which the mobile subscriber is currently roaming, Visited PLMN (V-PLMN). The traffic between countries is routed through ISCs. Depending on the capabilities of the ISC, there are several routing variants for international calls to mobile subscribers. The difference is determined by the entity that performs the HLR interrogation, resulting in differently occupied line capacities.

If the ISC performs the HLR interrogation, the routing to the current MSC is performed either by the ISC of the originating call or by the ISC of the mobile subscriber's H-PLMN

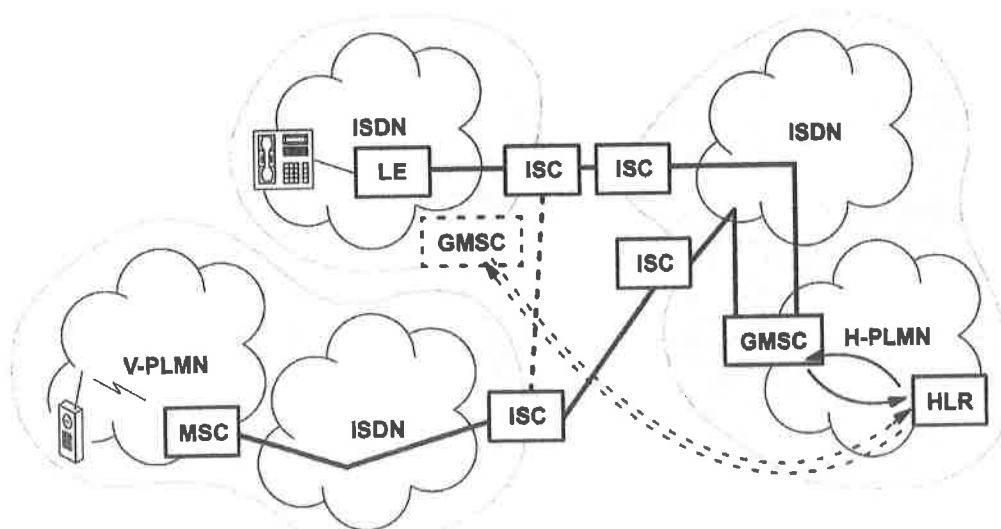


Figure 6.7 Routing through GMSC for international MSISDN.

(Figure 6.6). If no ISC can process the routing, again a GMSC has to become involved, either a GMSC in the country where the call originates or the GMSC of the H-PLMN (Figure 6.7).

For the routing procedures explained here, it does not matter which kind of subscriber is calling, i.e. the subscriber may be in the fixed network or in the mobile network. However, for calls from mobile subscribers, the HLR interrogation is usually performed at the local exchange (MSC).

6.3.2 Call establishment and corresponding MAP procedures

Call establishment in GSM at the air interface is similar to ISDN call establishment at the user network interface (Q.931) (Bocker, 1990). The procedure is supplemented by several functions: random access to establish a signaling channel (SDCCH) for call setup signaling, the authentication part, the start of ciphering and the assignment of a radio channel.

The establishment of a connection always contains a verification of user identity (authentication) independent of whether it is a mobile-originated call setup or a mobile-terminated call setup. The authentication is performed in the same way as for location updating. The VLR supplements its database entry for this MS with a set of security data, which replaces the 'consumed' 3-tuple (RAND, SRES, Kc). After successful authentication, the ciphering process for the encryption of user data is started.

Outgoing connection setup

For outgoing connection setup (Figure 6.8), first the MS announces its connection request to the MSC with a `SETUP INDICATION` message, which is a pseudo-message. It is generated between the MM entity of the MSC and the MAP entity, when the MSC receives the message `CM-SERVICE REQUEST` from the MS, which indicates in this way the request for a MM connection (Figure 5.27). Then the MSC signals to the VLR that the MS identified by the temporary TMSI in the location area LAI has requested service access (`PROCESS ACCESS`

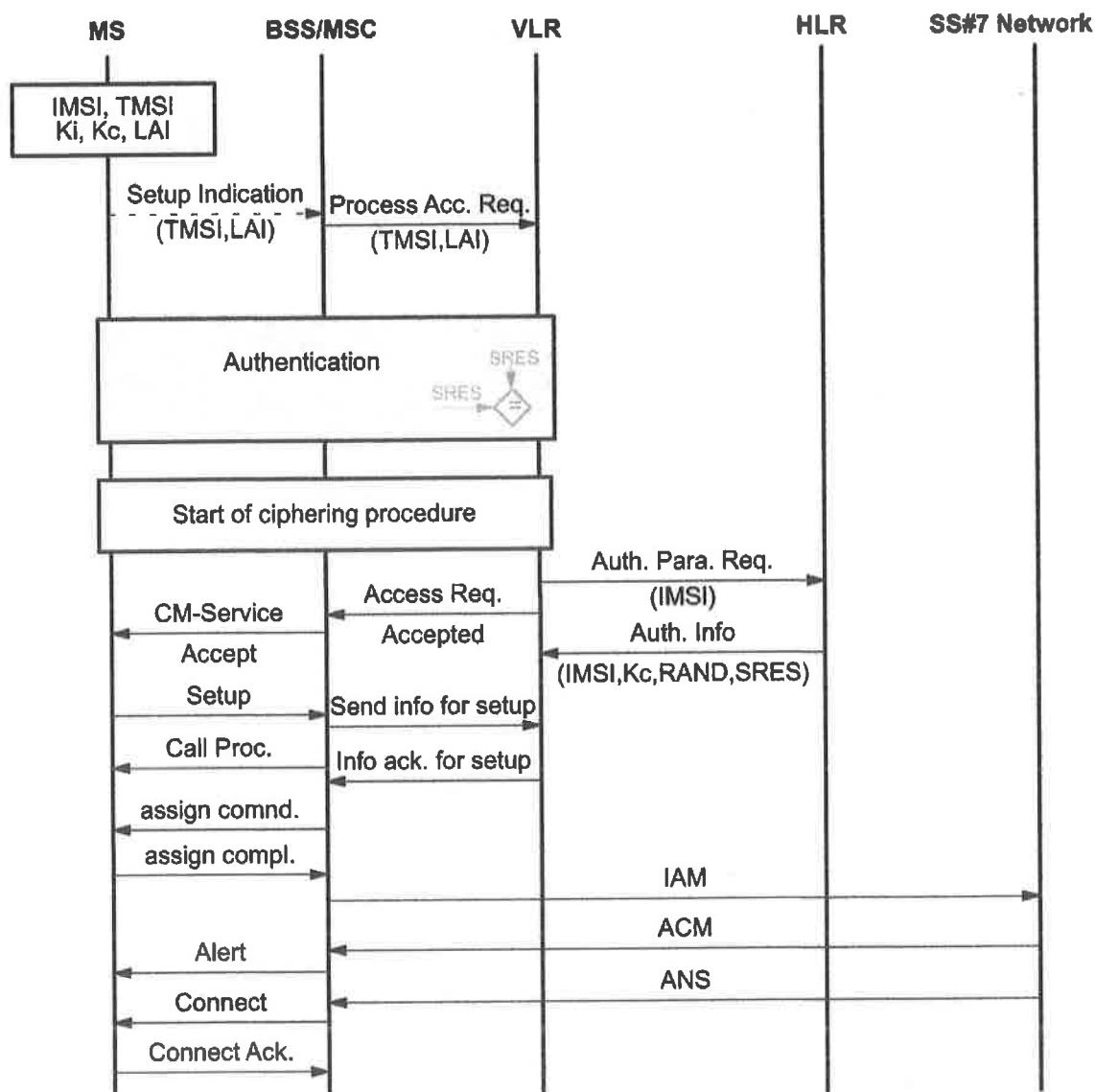


Figure 6.8 Overview of an outgoing call setup.

REQUEST) which is an implicit request for a random number RAND from the VLR, to be able to start the authentication of the MS. This random number is transmitted to the MS, its response with authentication result SRES is returned to the VLR, which now examines the authenticity of the MS's identity (compare authentication at registration; Figure 6.1).

After successful authentication, the ciphering process is started on the air interface, and this way the MM connection between MS and MSC has been completely established (CM-SERVICE ACCEPT). Subsequently, all signaling messages can be sent in encrypted form. Only now the MS reports the desired calling target. While the MS is informed with a CALL PROCEEDING message that processing of its connection request has been started, the MSC reserves a channel for the conversation and assigns it to the MS (ASSIGN). The connection request is signaled to the remote network exchange through the signaling system

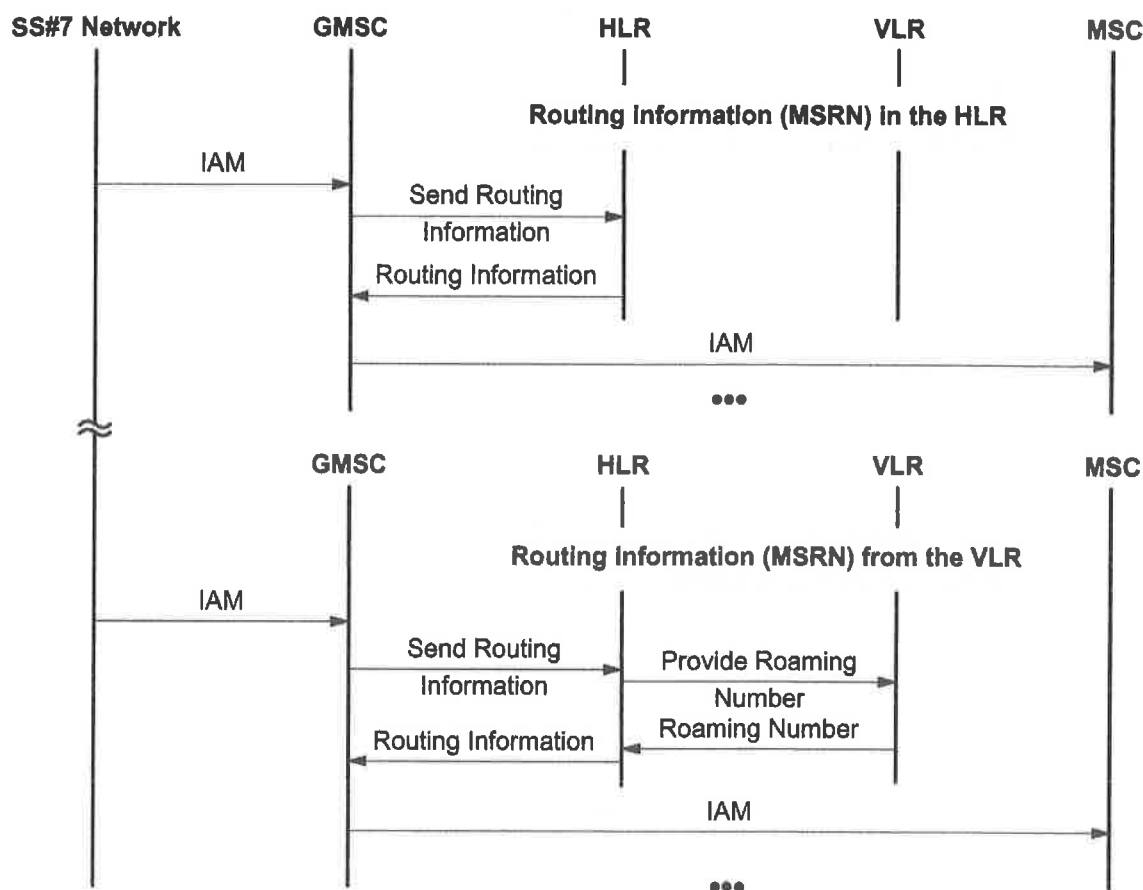


Figure 6.9 Interrogation of routing information for an incoming call.

SS#7 with the ISUP message IAM (Bocker, 1990). When the remote exchange answers (ACM), the delivery of the call can be indicated to the MS (ALERT). Finally, when the called partner goes off-hook, the connection can be switched through (CONNECT, ANS, CONNECT ACKNOWLEDGE).

Incoming connection setup

For incoming connection setup, it is necessary to determine the exact location of a MS in order to route the call to the currently responsible MSC. A call to a MS is therefore always routed to an entity which is able to interrogate the HLR for temporary routing information and to use it to forward the call. Usually, this entity is a GMSC of the home PLMN of the MS (section 6.3.1). Through this HLR interrogation, the GMSC obtains the current MSRN of the MS and forwards it to the current MSC (Figure 6.9).

Depending on whether the MSRN is stored in the HLR or first has to be obtained from the VLR, two variants of the HLR interrogation exist. In the first case, the interrogated HLR can supply the MSRN immediately (ROUTING INFORMATION). In the second case, the HLR has only received and stored the current VLR address during location update. Therefore, the HLR first has to request the current routing information from the VLR before the call can be switched through to the local MSC.

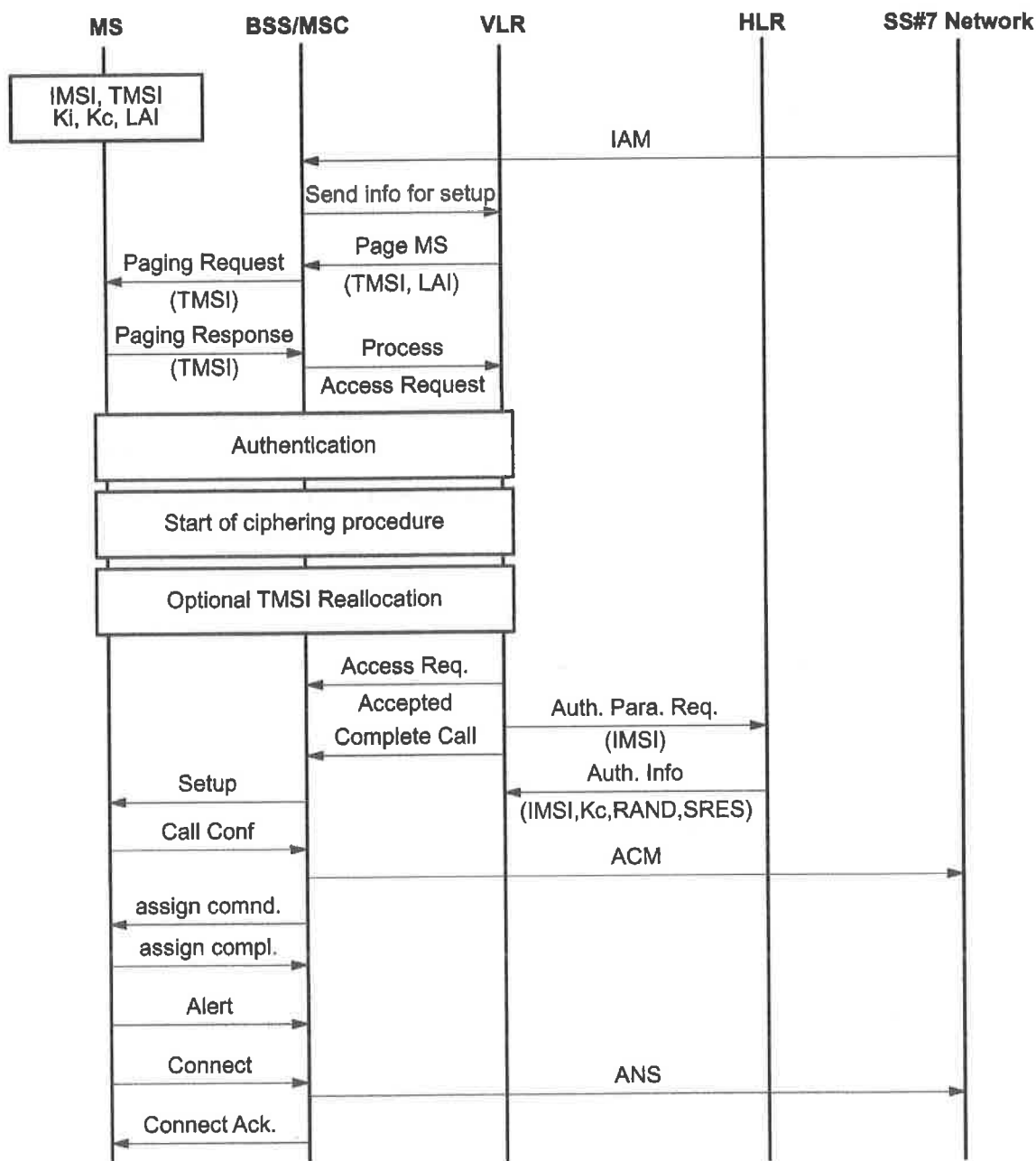


Figure 6.10 Overview of an incoming call setup.

Call processing is interrupted again in the local MSC in order to determine the exact location of the MS within the MSC area (SEND INFO FOR SETUP, Figure 6.10). The current LAI is stored in the location registers, but an LA can comprise several cells. Therefore, a broadcast (paging call) in all cells of the LA is used to determine the exact location, i.e. cell, of the MS. Paging is initiated from the VLR using the MAP (PAGE MS) and transformed by the MSC into the paging procedure at the air interface. When a MS receives a paging call, it responds directly and thus allows the current cell to be determined.

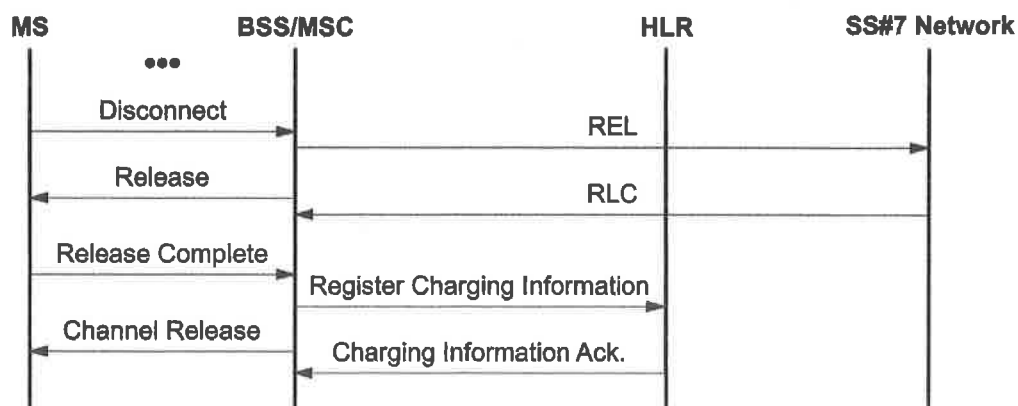


Figure 6.11 Mobile-initiated call termination and storing of charging information.

Thereafter, the VLR instructs the MSC to authenticate the MS and to start ciphering on the signaling channel. Optionally, the VLR can execute a reallocation of the TMSI (TMSI reallocation procedure) during call setup. Only at this point, after the network internal connection has been established (section 5.4.4), can the connection setup proper be processed (command **COMPLETE CALL** from VLR to MSC). The MS is told about the connection request with a **SETUP** message, and after answering **CALL COMPLETE** it receives a channel. After ringing (**ALERT**) and going off-hook, the connection is switched through (**CONNECT**, **CONNECT**, **ACKNOWLEDGE**), and this fact is also signaled to the remote exchange (**ACM**, **ANS**).

6.3.3 Call termination

At the air interface, a given call can be terminated either by the mobile equipment or by the network. The taking down of the connection is initiated at the Um interface by means of the CC messages **DISCONNECT**, **RELEASE** and **RELEASE COMPLETE**. This is followed by an explicit release of occupied radio resources (**CHANNEL RELEASE**). On the network side, the connection between the involved switching centers (MSC, etc.) is terminated using the ISUP messages **REL** and **RLC** in the SS#7 network (Figure 6.11).

After the connection has been taken down, information about charges (**CHARGING INFORMATION**) is stored in the VLR or HLR using the MAP. This charging data can also be required for an incoming call, e.g. if roaming charges are due because the called subscriber is not in their home PLMN.

6.3.4 MAP procedures and routing for short messages

A connectionless relay protocol has been defined for the transport of short messages (section 5.4.8) at the air interface, which has a counterpart in the network in a store-and-forward operation for short messages. This forwarding of transport PDUs of the SMS uses MAP procedures. For an incoming short message which arrives from the SMS-SC at a SMS-GMSC, the exact location of the MS is the first item that needs to be determined just as for an incoming call. The current MSC of the MS is first obtained with a HLR

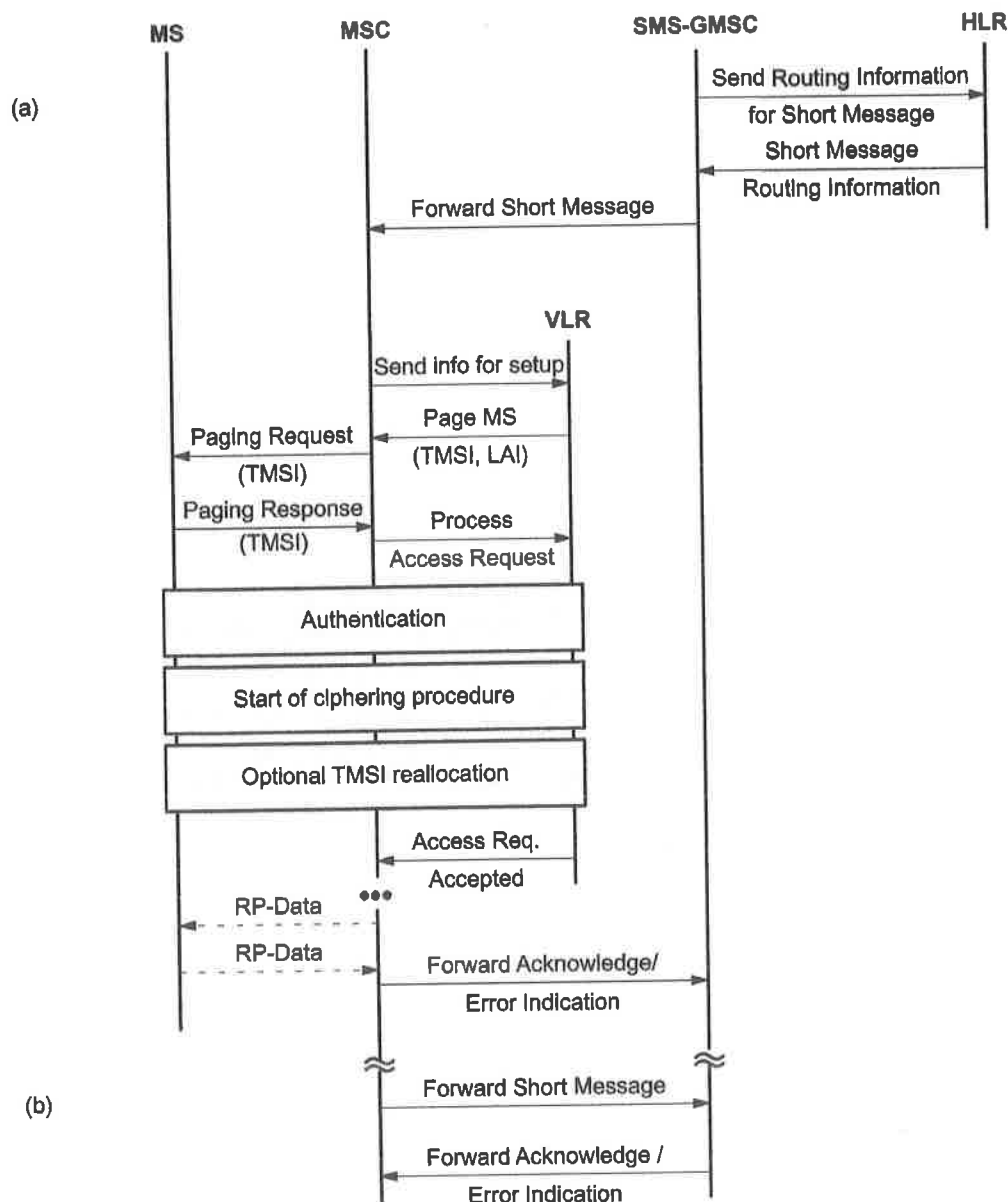


Figure 6.12 Forwarding short messages in a PLMN.

interrogation (SHORT MESSAGE ROUTING INFORMATION; Figure 6.12(a)). The short message is then passed to this MSC (FORWARD SHORT MESSAGE) and is locally delivered after paging and SMS connection setup. Success or failure are reported to the SMS-GMSC in another MAP message (FORWARD ACKNOWLEDGEMENT/ERROR INDICATION) which then informs the service center.

In the reverse case, for an outgoing short message, no routing interrogation is needed, since the SMS-GMSC is known to all MSCs, so the message can be passed immediately to the SMS-GMSC (Figure 6.12(b)).

6.4 Handover

6.4.1 Overview

Handover is the transfer of an existing voice connection to a new base station. There are different reasons for the handover to become necessary. In GSM, a handover decision is made by the network, not the MS, and it is based on BSS criteria (received signal level, channel quality, distance between MS and BTS) and on network operation criteria (e.g. current traffic load of the cell and ongoing maintenance work).

The functions for preparation of handover are part of the radio subsystem link control. Above all, this includes the measurement of the channel. Periodically, a MS checks the signal field strength of its current downlinks as well as those of the neighboring base stations, including their BSICs. The MS sends measurement reports to its current base station (quality monitoring); section 4.5.1. On the network side, the signal quality of the uplink is monitored, the measurement reports are evaluated, and handover decisions are made.

As a matter of principle, handovers are only performed between base stations of the same PLMN. Handovers between BSSs in different networks are not allowed. Two kinds of handover are distinguished (Figure 6.13).

- *Intracell handover*: for administrative reasons or because of channel quality (channel-selective interferences), the MS is assigned a new channel within the same cell. This decision is made locally by the RR of the BSS and is also executed within the BSS.
- *Intercell handover*: the connection to a MS is transferred over the cell boundary to a new BTS. The decision about the time of handover is made by the RR protocol module of the network based on measurement data from MSs and BSSs. The MSC, however, can participate in the selection of the new cell or BTS. The intercell handover occurs most often when it is recognized from weak signal field strength and bad channel quality (high bit error ratio) that a MS is moving near the cell boundary. However, an intercell handover can also occur due to administrative reasons, say for traffic load balancing. The decision about such a network-directed handover is made by the MSC, which instructs the BSS to select candidates for such a handover.

Two cases need to be distinguished with regard to participation of network components in the handover, depending on whether the signaling sequences of a handover execution also involve a MSC. Since the RR module of the network resides in the BSC (see Figure 5.11), the BSS can perform the handover without participation of the MSC. Such handovers occur between cells which are controlled by the same BSC and are called internal handover. They can be performed independently by the BSS; the MSC is only informed about the successful execution of internal handovers. All other handovers require participation of at least one MSC, or their BSSMAP and MAP parts, respectively. These handovers are known as external handovers.

Participating MSCs can act in the role of MSC-A or MSC-B. MSC-A is the MSC which performed the initial connection setup, and it keeps the MSC-A role and complete control (anchor MSC) for the entire life of the connection. A handover is therefore, in general, the extension of the connection from the anchor MSC-A to another MSC (MSC-B). In this case, the mobile connection is passed from MSC-A to MSC-B with MSC-A keeping the ultimate control over the connection. An example is presented in Figure 6.14. A MS occupies an

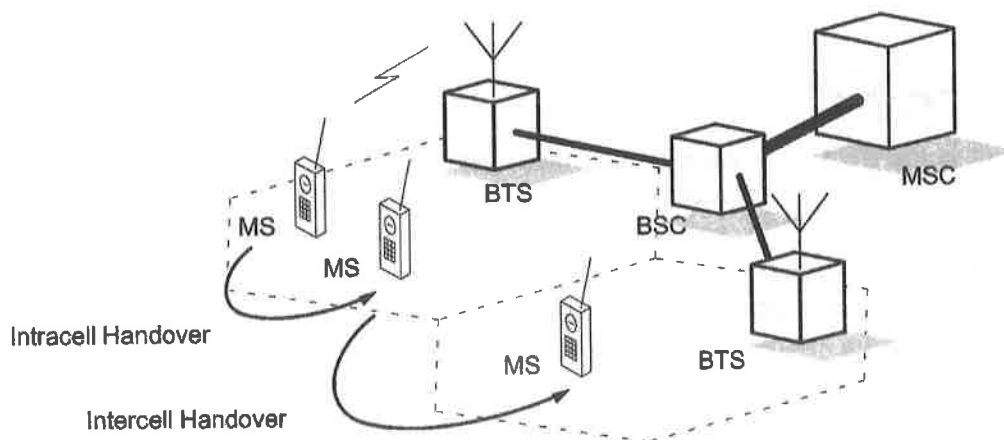


Figure 6.13 Intracell and intercell handover.

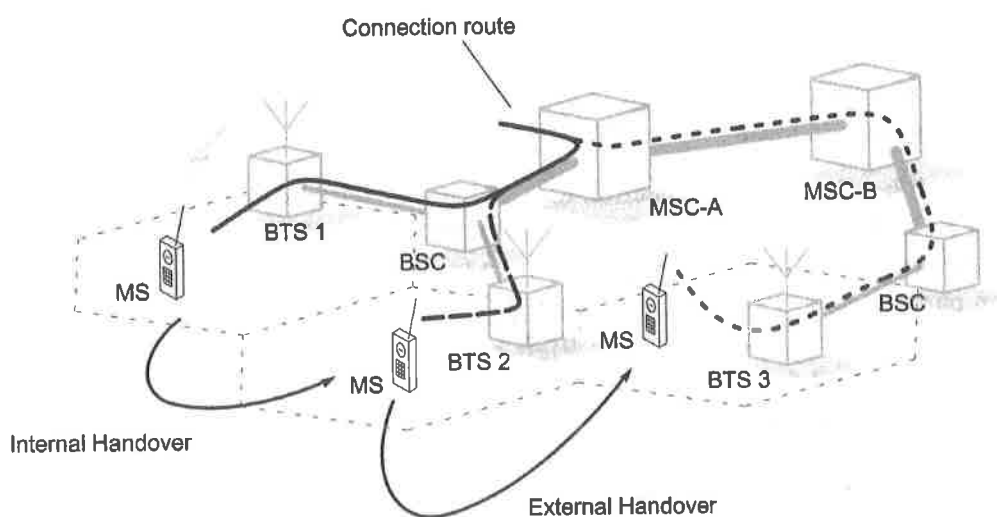


Figure 6.14 Internal and external handover.

active connection via BTS1 and moves into the next cell. This cell of BTS2 is controlled by the same BSC so that an internal handover is indicated. The connection is now carried from MSC-A over the BSC and the BTS2 to the MS; the connections of BTS1 (radio channel and ISDN channel between BTS and BSC) were taken down. As the MS moves on to the cell handled by BTS3, it enters a new BSS which requires an external handover. In addition, this BSS belongs to another MSC, which now has to play the role of MSC-B. Logically, the connection is extended from MSC-A to MSC-B and carried over the BSS to the MS. At the next change of the MSC, the connection element between MSC-A and MSC-B is taken down, and a connection to the new MSC from MSC-A is set up. Then the new MSC takes over the role of MSC-B.

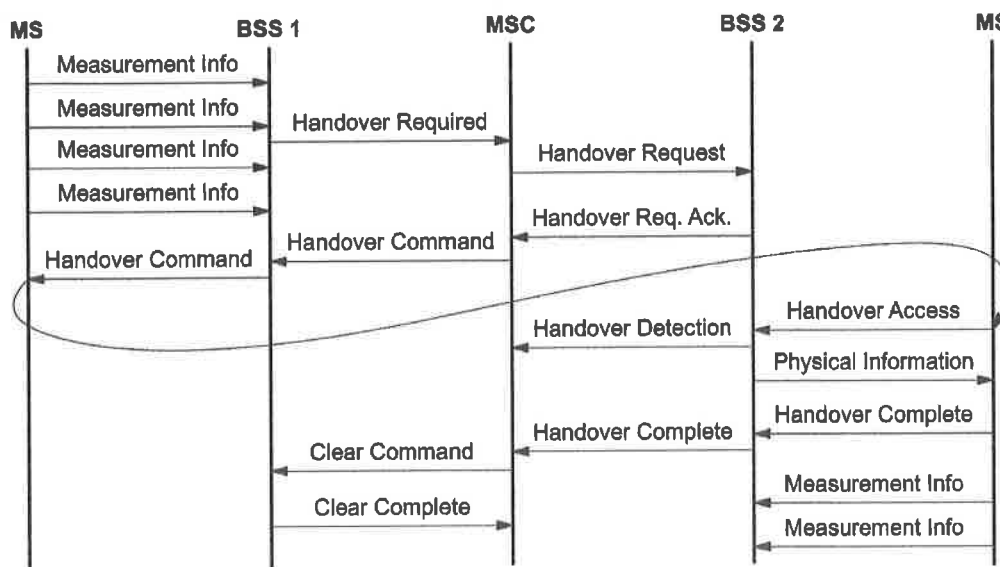


Figure 6.15 Principal signaling sequence for an intra-MSC handover.

6.4.2 Intra-MSC handover

The basic structure for an external handover is the handover between two cells of the same MSC (Figure 6.15). The MS continually transmits measurement reports with channel monitoring data on its SACCH to the current base station (BSS 1). Based on these measurement results, the BSS decides when to perform a handover and requests this handover from the MSC (message `HANDOVER REQUIRED`). The respective measurement results can be transmitted in this message to the MSC, to enable its participation in the handover decision. The MSC causes the new BSS to prepare a channel for the handover, and frees the handover to the MS (`HANDOVER COMMAND`), as soon as the reservation is acknowledged by the new BSS. The MS now reports to the new BSS (`HANDOVER ACCESS`) and receives information about the properties of the physical channel. This includes synchronization data such as the new timing advance value and also the new transmitter power level. Once the MS is able to occupy the channel successfully, it acknowledges this fact with a message `HANDOVER COMPLETE`. The resources of the old BSS can then be released.

6.4.3 Decision algorithm for handover timing

The basis for processing a successful handover is a decision algorithm which uses measurement results from the MS and base station to identify possible other base stations as targets for handovers and which determines the optimal moment to execute the handover. The objective is to keep the number of handovers per cell change as low as possible. Ideally, there should not be more than one handover per cell change. In reality, this is often not achievable. When a MS leaves the radio range of a base station and enters one of a neighboring station, the radio conditions are often not very stable, so that several handovers must be executed before a stable state is reached. Simulation results of Mende (1991) and Junius and Marger (1992) give a mean value of about 1.5–5 handovers per cell change.

Since every handover incurs not only increased traffic load for the signaling and transport system but also reductions in speech quality, the importance of a well-dimensioned handover decision algorithm is obvious, an algorithm which also takes into account the momentary local conditions. This is also a reason for the lack of a standardized, uniform algorithm for the determination of the moment of the handover in GSM. For this decision about when to perform a handover, network operators can develop and deploy their own algorithms which are optimally tuned for their networks. This is made possible through standardizing only the signaling interface that defines the processing of the handover and through transferring the handover decision to the BSS. The GSM handover is thus a network-originated handover as opposed to a mobile-originated handover, where the handover decision is made by the MS. An advantage of this handover approach is that the software of the MS need not be changed when the handover strategy or the handover decision algorithm is changed in all or part of the network. Even though the GSM standard does not prescribe a mandatory handover decision algorithm, a simple algorithm is proposed, which can be selected by the network operator or replaced by a more complex algorithm.

In principle, a GSM handover always proceeds in three steps (Figure 6.16), which are based on the measurement data provided by the MS over the SACCH, and on the measurements performed by the BSS itself. Foremost among these data items are the current channel's received signal level (RXLEV) and the signal quality (RXQUAL), both on the uplink (measured by the BSS) and on the downlink (measured by the MS). In order to be able to identify neighboring cells as potential targets for a handover, the MS also measures the received signal level RXLEV_CELL(n) of up to 16 neighboring base stations. The RXLEV values of the six base stations which can be received best are reported every 480 ms to the BSS. Further criteria for the handover decision algorithm are the distance between MS and BTS measured via the TA of the adaptive frame alignment (section 4.3.2) and measurements of the interference in unused time slots. A new value of each of these measurements is available every 480 ms.

Measurement preprocessing calculates average values from these measurements, whereby at least the last 32 values of RXLEV and RXQUAL must be averaged. The resulting mean values are continuously compared with thresholds (see Table 6.1) after every SACCH interval.

These threshold values can be configured individually for each BSS through management interfaces of the OMSS (see Chapter 3). The principle used for the comparison of measurements with the threshold is to conduct a so-called Bernoulli experiment: if out of the last N_i mean values of a criterion i more than P_i go under (RXLEV) or over (RXQUAL, MS_RANGE) the threshold, then a handover may be necessary. The values of N_i and P_i can also be configured through network management. Their allowed range is defined as the interval [0; 31].

In addition to these mean values, a BSS can calculate the current power budget (PBGT(n)), which represents a measure for the respective path loss between MS and current base station or a neighboring base station n . Using this criterion, a handover can always be caused to occur to the base station with the least path loss for the signals from or to the MS. The PBGT takes into consideration not only the RXLEV_DL of the current downlink and the RXLEV_NCELL(n) of the neighboring BCCH but also the maximal transmitter power P (see Table 4.8) of a MS, the maximal power MS_TXPWR_MAX allowed to a MS in the current cell, and the maximal power MS_TXPWR_MAX(n) allowed to mobiles in

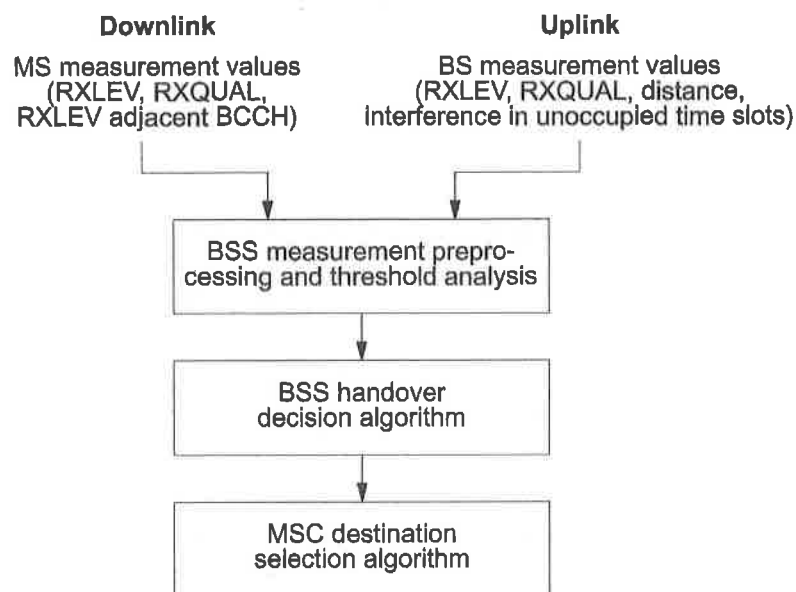


Figure 6.16 Decision steps in a GSM handover.

the neighboring cells. In addition, the calculation uses the value PWR_C_D , which is the difference between maximal transmitter power on the downlink and current transmitter power of the BTS in the downlink, a measure for the available power control reserve.

Thus, the power budget for a neighboring base station n is calculated as follows:

$$PBGT(n) = (\text{Minimum}(\text{MS_TXPWR_MAX}, P) - \text{RXLEV_DL} - PWR_C_D) \\ - (\text{Minimum}(\text{MS_TXPWR_MAX}(n), P) - \text{RXLEV_NCELL}(n)).$$

A handover to a neighboring base station can be requested, if the power budget is $PBGT(n) > 0$ and greater than the threshold $HO_MARGIN(n)$. The causes for handover which are possible using these criteria are summarized in Table 6.2. As can be seen, the signal criteria of the uplink and downlink as well as the distance from the base station and $PBGT$ can lead to a handover.

The BSS makes a handover decision by first determining the necessity of a handover using the threshold values of Table 6.1. In principle, one can distinguish three categories:

- handover because of more favorable path loss conditions;
- mandatory intercell handover;
- mandatory intracell handover.

Situations where a neighboring base station shows more favorable propagation conditions and therefore lower path loss, do not necessarily force a handover. Such potential handover situations to a neighboring cell are discovered through the $PBGT(n)$ calculations. To make a handover necessary, the power budget of the neighboring cell must be greater than the threshold $HO_MARGIN(n)$.

Table 6.1 Threshold values for the GSM handover.

Threshold value	Typical value	Meaning
L_RXLEV_UL_H	103 to 73 dBm	Upper handover threshold of the received signal level in the uplink
L_RXLEV_DL_H	103 to 73 dBm	Upper handover threshold of the received signal level in the downlink
L_RXLEV_UL_IH	85 to 40 dBm	Lower(!) received signal level threshold in the uplink for internal handover
L_RXLEV_DL_IH	85 to 40 dBm	Lower(!) received signal level threshold in the downlink for internal handover
RXLEV_MIN(<i>n</i>)	Approximately 85 dBm	Minimum required RXLEV of BCCH of cell <i>n</i> to perform a handover to this cell
L_RXQUAL_UL_H	–	Lower handover threshold of the bit error ratio in the uplink
L_RXQUAL_DL_H	–	Lower handover threshold of the bit error ratio in the downlink
MS_RANGE_MAX	2 to 35 km	Maximum distance between the MS and base station
HO_MARGIN(<i>n</i>)	0 to 24 dB	Hysteresis to avoid multiple handovers between two cells

Table 6.2 Handover causes.

Handover cause	Meaning
UL_RXLEV	Uplink received signal level too low
DL_RXLEV	Downlink received signal level too low
UL_RXQUAL	Uplink bit error ratio too high
DL_RXQUAL	Downlink bit error ratio too high
PWR_CTRL_FAIL	Power control range exceeded

The recognition of a mandatory handover situation (Figure 6.17) within the framework of the radio subsystem link control (section 4.5 and Figure 4.19) is based on the received signal level and signal quality in uplink and downlink as well as on the distance between the MS and BTS. Going over or under the respective thresholds always necessitates a handover. Here are the typical situations for a mandatory handover:

- The received signal level in the uplink or downlink (RXLEV_UL/RXLEV_DL) drops below the respective handover threshold value (L_RXLEV_UL_H/L_RXLEV_DL_H) and the power control range has been exhausted, i.e. the MS and/or the BSS have reached their maximal transmitter power (section 4.5.2).

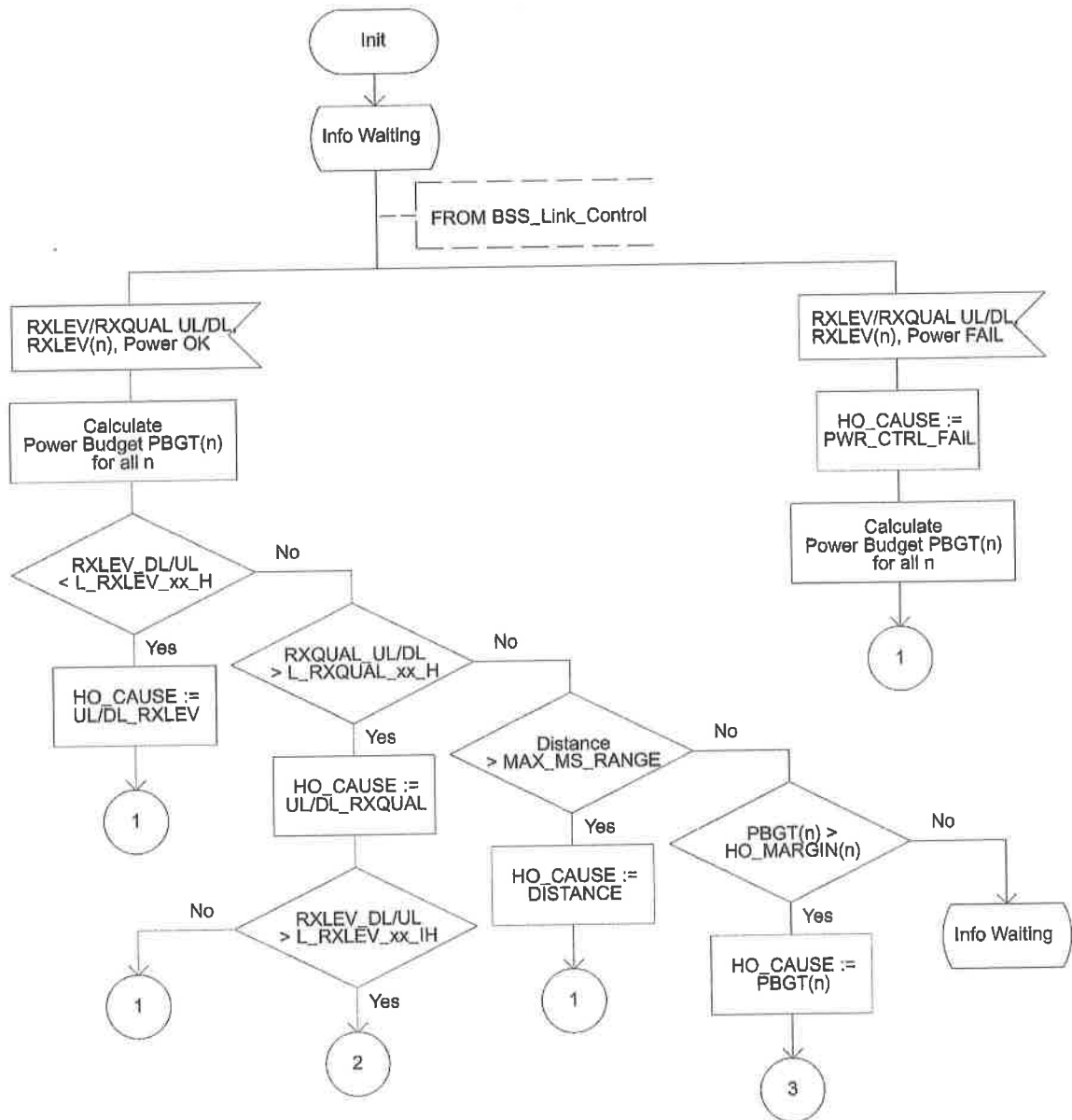


Figure 6.17 Detection of mandatory handover.

- The bit error ratio as a measure of signal quality in uplink and/or downlink (RXQUAL_UL/RXQUAL_DL) exceeds the respective handover threshold value (L_RXQUAL_UL_H/L_RXQUAL_DL_H), while at the same time the received signal level drops into the neighborhood of the threshold value.
- The maximum distance to the base station (MAX_MS_RANGE) has been reached.

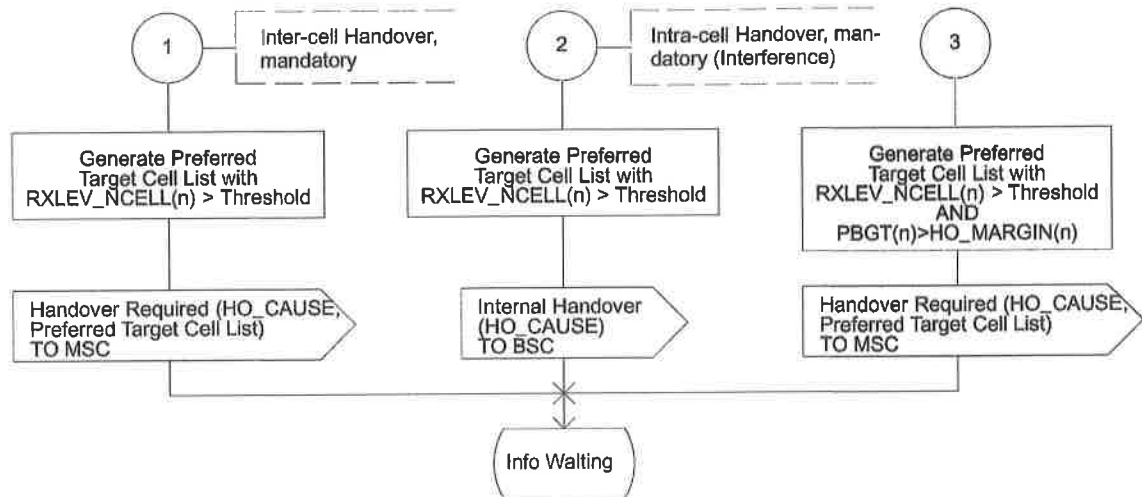


Figure 6.18 Completion of the handover decision in the BSS.

A handover can also become mandatory when the handover thresholds are not exceeded if the lower thresholds of the transmitter power control are exceeded ($L_{RXLEV_xx_P}/L_{RXQUAL_xx_P}$; Table 4.9), even though the maximum transmitter power has already been reached. The cause of handover indicated is the failure of the transmitter power control (PWR_CTR_FAIL ; Table 6.2).

A special handover situation exists if the bit error ratio $RXQUAL$ as a measurement for signal quality in the uplink and/or downlink exceeds its threshold and at the same time the received signal level is greater than the thresholds $L_{RXLEC_UL_IH}/L_{RXLEC_DL_IH}$. This strongly hints at an existing severe cochannel interference. This problem can be solved with an (internal) intracell handover, which the BSS can perform on its own without support from the MSC. It is also considered as a mandatory handover.

If the BSS has detected a handover situation, a list of candidates as possible handover targets is assembled using the BSS decision algorithm. For this purpose, one first determines which BCCH of the neighboring cell n is received with sufficient signal level:

$$RXLEV_NCELL(n) > RXLEV_MIN(n) + \text{Maximum}(0, (MS_TXPWR_MAX(n) - P)).$$

The potential handover targets are then assembled in an ordered list of preferred cells according to their path loss compared with the current cell (Figure 6.18). For this purpose, the power budget of the neighboring cells in question is again evaluated:

$$PBG(n) - HO_MARGIN(n) > 0.$$

All cells n which are potential targets for a handover due to $RXLEV_NCELL(n)$ and lower path loss than the current channel are then reported to the MSC with the message **HANDOVER REQUIRED** (Figure 6.18) as possible handover targets. This list is sorted by priority according to the difference $(PBG(n) - HO_MARGIN(n))$. The same message **HANDOVER REQUIRED** is also generated if the MSC has sent a message **HANDOVER CANDIDATE ENQUIRY** to the BSS.

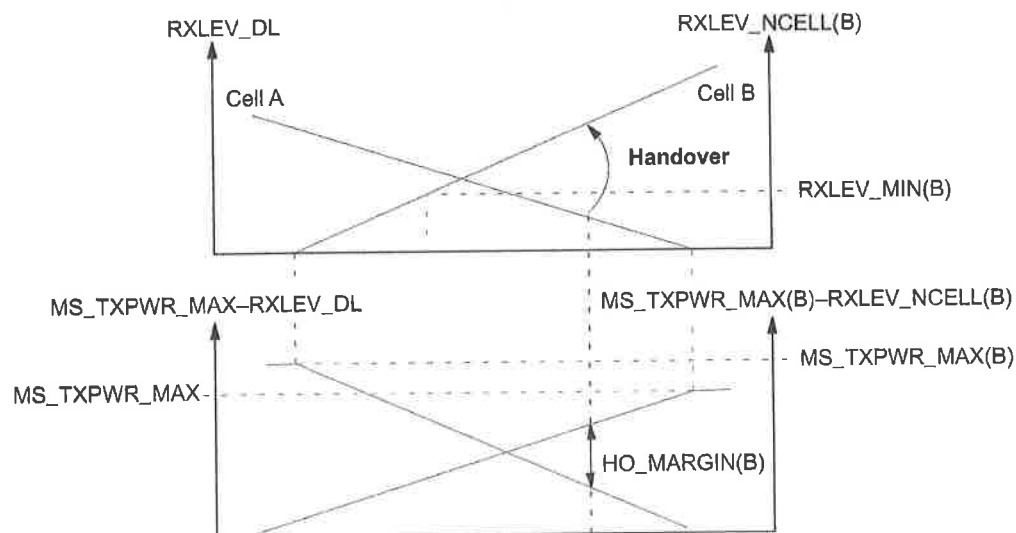


Figure 6.19 Handover criteria for exhausted transmitter power control.

The conditions at a cell boundary in the case of exhausted transmitter power control ($PWR_C_D = 0$) are shown in Figure 6.19 with a MS moving from the current cell to a cell B. The threshold $RXLEV_MIN(B)$ is reached very early; however, the handover is somewhat moved in the direction of cell B because of the positive $HO_MARGIN(B)$ for the power budget. When moving in the opposite direction, the handover would be delayed in the other direction due to $HO_MARGIN(A)$ of cell A. This has the effect of a hysteresis which reduces repeated handovers between both cells due to fading (ping-pong handover). In addition to varying radio conditions (fading due to multipath propagation, shadowing, etc.) there are many other sources of error with this kind of handover. Note that, on the one hand, that there are substantial delays between measurement and reaction due to the averaging process. This leads to executing the handover too late on a few occasions. It is more important, however, that the current channel is compared with the BCCH of the neighboring cells rather than the traffic channel to be used after the handover decision, which could suffer from different propagation conditions (frequency-selective fading, etc.). Finally, the MSC decides about the target cell of the handover. This decision takes into consideration the following criteria in decreasing order of priority: handover due to signal quality (RXQUAL), received signal level (RXLEV), distance and path loss (PBGT). This prioritization is especially effective when there are not enough traffic channels available and handover requests are competing for the available channels.

The standard explicitly points out that all measurement results must be sent with the message `HANDOVER REQUIRED` to the MSC, so that in the end the option remains open to implement the complete handover decision algorithm in the MSC.

6.4.4 MAP and inter-MSC handover

The most general form of handover is the inter-MSC handover. The MS moves over a cell boundary and enters the area of responsibility of a new MSC. The handover caused by this

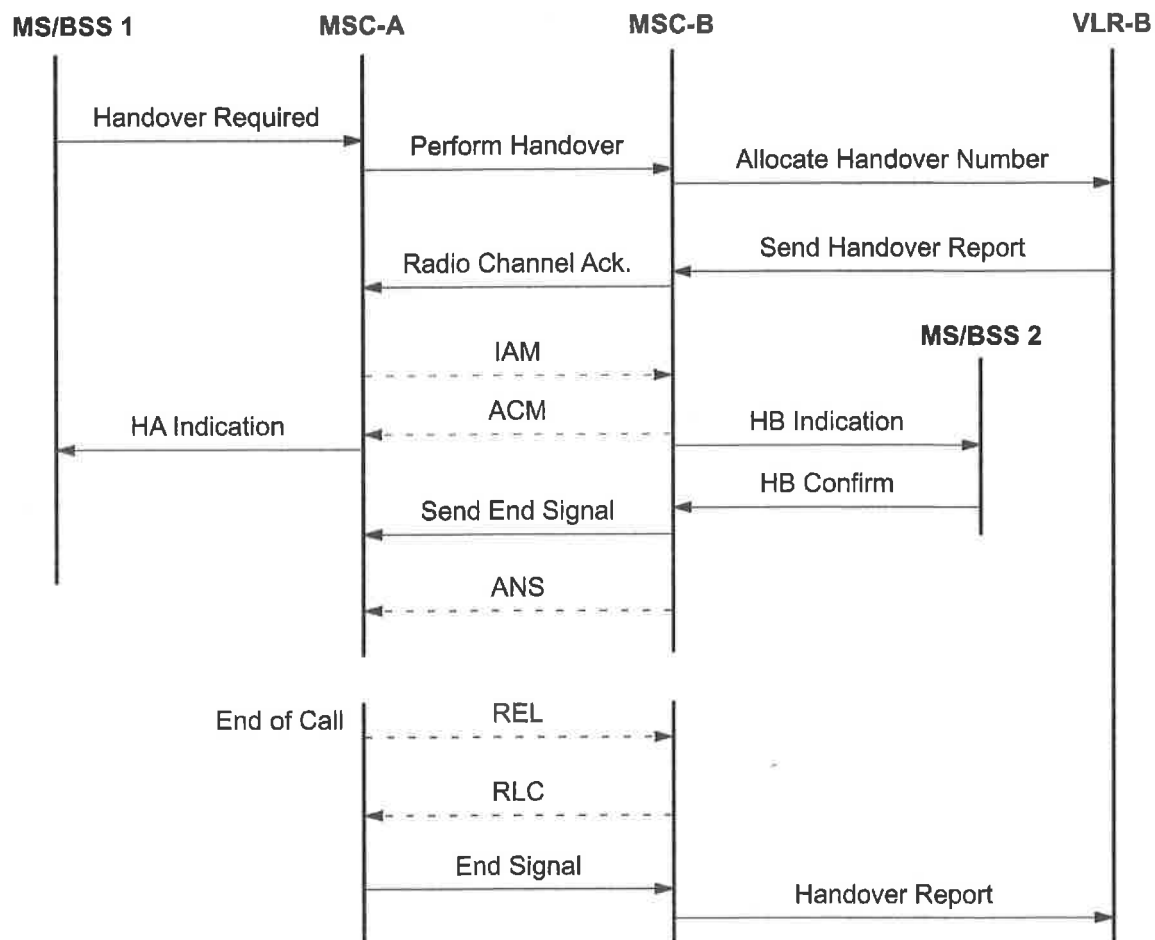


Figure 6.20 Principal operation of a basic handover.

move requires communication between the involved MSCs. This occurs through the SS#7 using transactions of the MAP.

Basic handover between two MSCs

The principal sequence of operations for a basic handover between two MSCs is shown in Figure 6.20. The MS has indicated the conditions for the handover, and the BSS requests the handover from MSC-A (HANDOVER REQUIRED). MSC-A decides positively for a handover and sends a message PERFORM HANDOVER to MSC-B. This message contains the necessary data to enable MSC-B to reserve a radio channel for the MS. Above all, it identifies the BSS which is to receive the connection. MSC-B assigns a handover number and tries to allocate a channel for the MS. If a channel is available, the response RADIO CHANNEL ACKNOWLEDGE contains the new MSRN to the MS and the designation of the new channel. If no channel is available, this is also reported to MSC-A which then terminates the handover procedure.

When a RADIO CHANNEL ACKNOWLEDGE is successful, an ISDN channel is switched through between the two MSCs (ISUP messages IAM and ACM), and both MSCs send

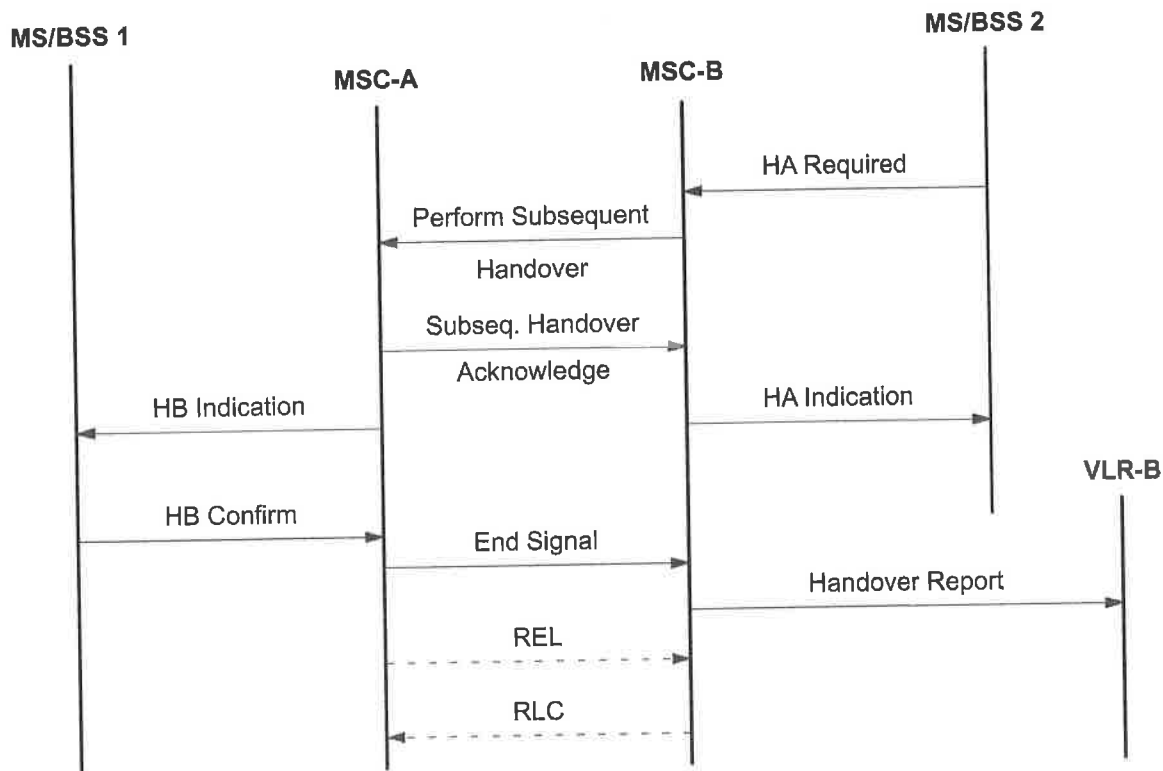


Figure 6.21 Principle of subsequent handover from MSC-B to MSC-A (handback).

an acknowledgement to the MS (HA INDICATION, HB INDICATION). The MS then resumes the connection on the new channel after a short interruption (HB CONFIRM). MSC-B then sends a message SEND END SIGNAL to MSC-A and thus causes the release of the old radio connection. After the end of the connection (ISUP messages REL, RLC), MSC-A generates a message END SIGNAL for MSC-B which then sends a HANDOVER REPORT to its VLR.

Subsequent handover

After a first basic handover of a connection from MSC-A to MSC-B, a MS can move on freely. Further intra-MSC handovers can occur (Figure 6.15), which are processed by MSC-B.

If, however, the MS leaves the area of MSC-B during this connection, a subsequent handover becomes necessary. Two cases are distinguished between: in the first case, the MS returns to the area of MSC-A, whereas in the second case it enters the area of a new MSC, now called MSC-B'. In both cases, the connection is newly routed from MSC-A. The connection between MSC-A and MSC-B is taken down after a successful subsequent handover.

A subsequent handover from MSC-B back to MSC-A is also called handback (Figure 6.21). In this case, MSC-A, as the controlling entity, does not need to assign a handover number and can search directly for a new radio channel for the MS. If a radio channel can be allocated in time, both MSCs start their handover procedures at the air interface (HA/HB INDICATION) and complete the handover. After completion, MSC-A

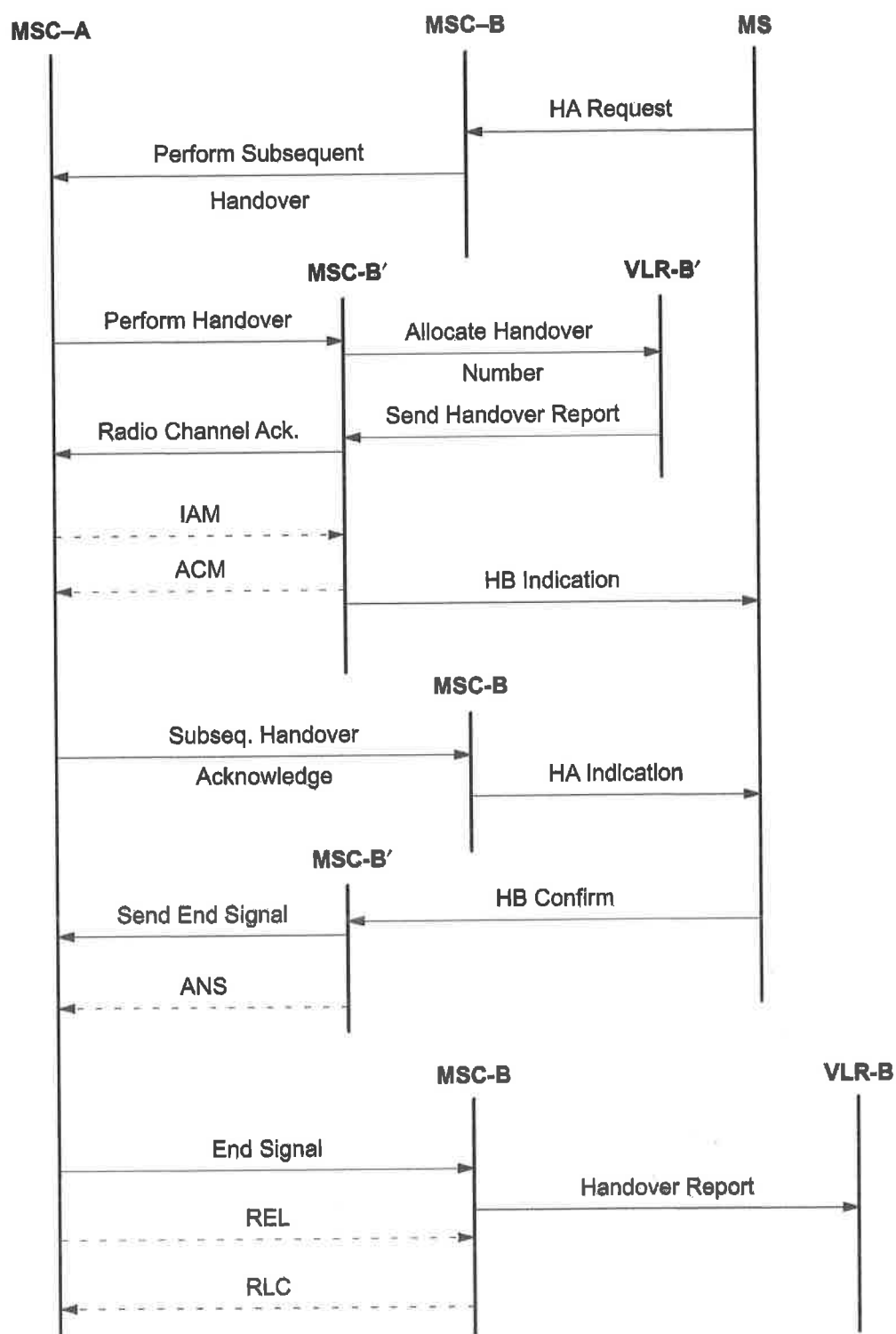


Figure 6.22 Principle of subsequent handover from MSC-B to MSC-B'.

terminates the connection to MSC-B. The message END SIGNAL terminates the MAP process in MSC-B and causes a HANDOVER REPORT to be sent to the VLR of MSC-B; the ISUP message RELEASE releases the ISDN connection.

The procedure for a subsequent handover from MSC-B to MSC-B is more complicated. It consists of two parts:

- a subsequent handover from MSC-B to MSC-A;
- a basic handover between MSC-A and MSC-B'.

The principal operation of this handover is illustrated in Figure 6.22.

In this case, MSC-A recognizes from the message PERFORM SUBSEQUENT HANDOVER, sent by MSC-B, that it is a case of handover to an MSC-B', and it initiates a basic handover to MSC-B'. MSC-A informs MSC-B after receiving the ISUP message ACM from MSC-B about the start of handover at MSC-B' and thereby frees the handover procedure at the radio interface from MSC-B. Once MSC-A receives the MAP message SEND END SIGNAL from MSC-B, it considers the handover as complete, sends the message END SIGNAL to MSC-B to terminate the MAP procedure and cancels the ISDN connection.

7

Services

In this section we summarize and describe the most important services provided in GSM systems.

7.1 Classical GSM services

7.1.1 Teleservices

Voice

Voice services had to be implemented by each operator in the start-up phase (E1) by 1991. In this category, two teleservices were distinguished: regular telephone service (TS11) and emergency service (TS12). For the transmission of the digitally coded speech signals, both services use a bidirectional, symmetric, full-duplex, point-to-point connection, which is set up on user demand. The sole difference between TS11 and TS12 teleservices is that regular service requires an international IWF, whereas the emergency service stays within the boundaries of a national network.

Fax transmission

As a teleservice for the second implementation phase (E2), the implementation of a transparent fax service (TS61) for Group 3 fax was planned. The fax service is called transparent because it uses a transparent bearer service for the transmission of fax data. The coding and transmission of the facsimile data uses the fax protocol according to the ITU-T recommendation T30. The network operator also has the option to implement TS61 on a nontransparent bearer service in order to improve the transmission quality. TS61 is transmitted over a traffic channel that is alternately used for voice or fax. Another optional alternative is designated as a fax transfer with automatic call acceptance (TS61). This service can be offered by a network operator when multinumbersing is used as the interworking solution. In the case of multinumbersing, a subscriber is assigned several MSISDN numbers, and a separate interworking profile is stored for each of them. In this way a specific teleservice

can be associated with each MSISDN, the fax service being one of them. If a mobile subscriber is called on their GSM-fax number, the required resources in the IWF of the MSC as well as in the MS can be activated; in the case of TS61, fax calls arrive with the same number as voice calls (no multinumbers) and have to be switched over to fax reception manually.

7.2 Popular GSM services: SMS and MMS

Next to voice services, which have been the main focus of GSM since the start, SMS has proven to be extremely popular and successful in GSM. To follow this success, similar but enhanced services have been standardized, such as the Enhanced Messaging Service (EMS) and the Multimedia Messaging Service (MMS). A brief description of these services follows in the next sections.

7.2.1 SMS

One of the most important services in GSM systems today, in terms of popularity at the user side as well as in terms of revenue generation at the provider side, is the capability to receive or send short messages at the MS: SMS, TS21 and TS22. This service was supposed to be offered in the third phase (E3) at the latest from 1996 on all GSM networks. TS21 is the point-to-point version of the SMS, which allows a single station to be sent a message of up to 160 characters. Conversely, TS22 has been defined as an optional implementation of the capability to send short messages from a MS. The combinations of SMS with other added-value services, e.g. mailbox systems with automatic notification of newly arrived messages or the transmission by short message of incurred charges, clearly show how the services offered by GSM networks go significantly beyond the services offered in fixed networks.

For SMS, the network operator has to establish a service center which accepts short messages from the fixed network and processes them in a store-and-forward mode. The interface has not been specified and can be by DTMF signaling, special order, email, fax, etc. The delivery can be time-shifted and is of course independent of the current location of the MS. Conversely, a service center can accept short messages from MSs which can also be forwarded to subscribers in the fixed network, for example by fax or email. The transmission of short messages uses a connectionless, protected, packet-switching protocol. The reception of a message must be acknowledged by the MS or the service center; in the case of failure, retransmission occurs. TS21 and TS22 are the only teleservices which can be used simultaneously with other services, i.e. short messages can also be received or transmitted during an ongoing call.

A further variation of the SMS is the cell broadcast service TS23, SMSCB. SMSCB messages are broadcast only in a limited region of the network. They can only be received by MSs in idle mode, and reception is not acknowledged. A MS itself cannot send SMSCB messages. With this service, messages contain a category designation, so that MSs can select categories of interest which they want to receive and store. The maximum length of SMSCB messages is 93 characters, but by using a special reassembly mechanism, the network can transmit longer messages of up to 15 subsequent SMSCB messages.

Table 7.1 SMS, EMS and MMS.

Service	Introduced	Payload size	Content
SMS	1995	160 byte	Text
EMS	2000	160 byte	Text, pictures, animations
MMS	2001	100 kbyte	Text, voice, pictures, photos, video

7.2.2 EMS

EMS is an extension of SMS. SMS was limited to text messages only. However, as ring tones and pictures gained a lot of popularity, EMS was introduced. EMS was developed by major GSM manufacturers as an open 3GPP standard. It allows unicolor pictures with 16×16 or 32×32 pixels to be sent and the pictures to be modified in the handset. Picture sequences can comprise six pictures. Fonts can be formatted in EMS and tones of three octaves can be included, from the pitch of C to the pitch of B++. The duration of tones can be 150, 225, 300 or 450 ms and up to 80 notes can be included in one EMS. However, before EMS had a chance to become popular, the MMS standard, which is much richer, took over.

7.2.3 MMS

MMS is similar to SMS or EMS, however has much higher capabilities in terms of size and flexibility. The MMS standard was developed by a consortium of industry partners and has become a 3GPP standard. In addition to pure text, MMS is capable of transmitting pictures, melodies and multimedia sequences of different kinds. MMS can transmit up to 100 kbyte of data and can handle AMR-coded speech, pictures (e.g. JPEG or GIF), music and even video. From the network point of view, a MMS-Center, called MMS-C, is required, which is responsible for storing, converting and forwarding MMS data. The MMS-C also stores information about the preferences of users as well as their terminal capabilities. Therefore, it is possible to avoid the transmission of MMS messages to a terminal which cannot deal with the specific format. Instead, the MMS message can possibly be transformed at the MMS-C into a format which the receiving terminal can handle. A comparison between SMS, EMS and MMS is provided in Table 7.1.

MMS architecture

The Multimedia Messaging Service Network Architecture (MMSNA) (Figure 7.1) comprises all required elements to provide a complete MMS to a user. This includes interworking between service providers. The Multimedia Messaging Service Environment (MMSE) is a collection of MMS-specific network elements which is controlled by a single administration. In the case of roaming, the visited network is part of the MMSE of the user in question, while subscribers of a different service provider are part of a different MMSE. An important role is taken on by the MMS relay/server, which is responsible for storing and handling both incoming and outgoing messages. It is also in charge of the transfer of messages between different messaging systems. The MMS relay/server can either be a single logical element

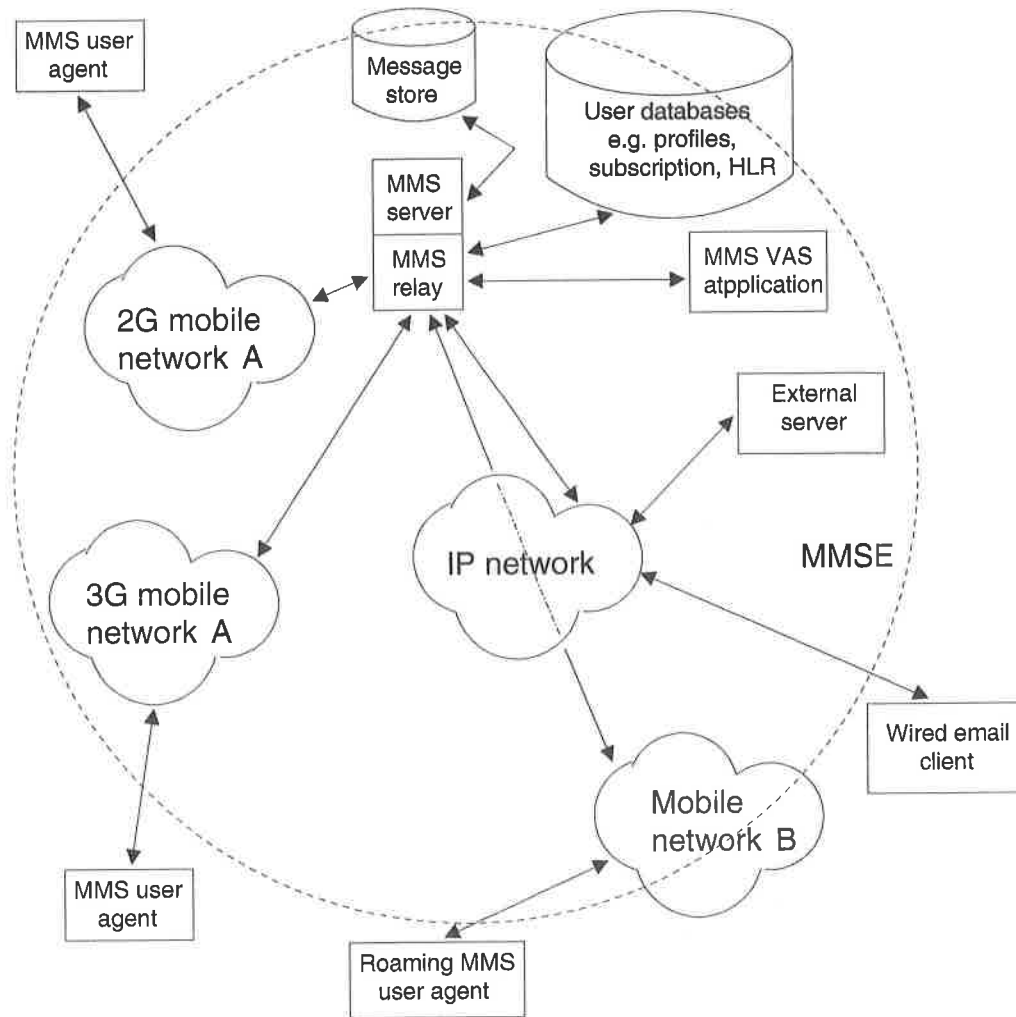


Figure 7.1 Multimedia Messaging Service Network Architecture (MMSNA).

or it may be separated into two single elements, a MMS relay and a MMS server. The MMS relay/server must also be able to generate charging data, when receiving Multimedia Messages (MMs) from or delivering MMs to other elements of the architecture. The MMS user database contains user-related information, such as subscription, configuration and capability data. The MMS user database can be either a single entity or it can be distributed. The MMS user agent is an application layer function, providing the users with the ability to view, compose and handle MMs. The MMS user agent resides on the mobile device. Finally, the MMS Value Added Services (VAS) applications offer value-added services to MMS users. Several MMS VAS applications may be connected to a MMSE.

7.3 Overview of GSM services in Phase 2+

The GSM standards have always been enhanced: Phase 1 of the GSM implementation contained basic teleservices – in the first place voice communication – and a few supplementary services, which had to be offered by all network operators in 1991 when GSM

was introduced into the market. The standardization of Phase 2 was completed in 1995 with market introduction following in 1996. Essentially, ETSI added more of the supplementary services, which had been planned already when GSM was initially conceived and which were adopted from the fixed ISDN. These new services made it necessary to rework large parts of the GSM standards. For this reason, networks operating according to the revised standard are also called GSM Phase 2 (Mouly and Pautet, 1995). However, all networks and terminals of Phase 2 preserve the compatibility with the old terminals and network equipment of Phase 1, i.e. all new standard development had to be strictly backwards compatible.

The GSM Phase 2+ introduces many aspects ranging from radio transmission to communication and call processing. However, there is no complete revision of the GSM standard; rather single subject areas are treated as separate standardization units, with the intent of allowing them to be implemented and introduced independently of each other.

Thus, GSM systems can evolve gradually, and standardization can meet market needs in a flexible way. However, with this approach, a unique identification of a GSM standard version becomes impossible. The designation GSM Phase 2+ is supposed to indicate this openness (Mouly and Pautet, 1995), suggesting an evolutionary process with no endpoint in time or prescribed target dates for the introduction of new services. The GSM standards are now published in so-called releases (e.g. Release 97, 98, 99 and 2000).

A large menu of technical questions is being addressed, only a few of which are presented as examples in the following. Figure 7.2 illustrates the evolution of GSM, from the initial digital speech services towards the third generation of mobile communications (UMTS/IMT-2000). In particular, it shows the services of Phase 2+ that are covered in this book. Most of these services are already offered by GSM network providers today and can be used with enhanced mobile equipment.

7.4 Bearer and teleservices of GSM Phase 2+

Whereas GSM Phase 2 defined essentially a set of new supplementary services, Phase 2+ is also addressing new bearer and teleservices. In this section we give an overview of these new speech and data services. They significantly improve the GSM speech quality and make the utilization of available radio resources much more efficient. Furthermore, the new data services are an important step towards wireless Internet access via cellular networks.

7.4.1 Advanced speech call items

The GSM systems of Phase 2 offer inadequate features for group communications. For example, group call or 'push-to-talk' services with fast connection setup as known from private radio or digital trunked radio systems (e.g. TETRA) are not offered. However, such services are indispensable for most closed user groups (e.g. police, airport staff, railroad or taxi companies). In particular, railroad operators had a strong request for such features. In 1992, their international organization, the Union Internationale des Chemins de Fer (UIC), selected the GSM system as their standard (Mouly and Pautet, 1995). This GSM-based uniform international railway communication system should replace a multitude of incompatible radio systems.

In this section we describe the standardized speech teleservices that offer functionality for group communication: the Voice Broadcast Service (VBS) and the Voice Group Call

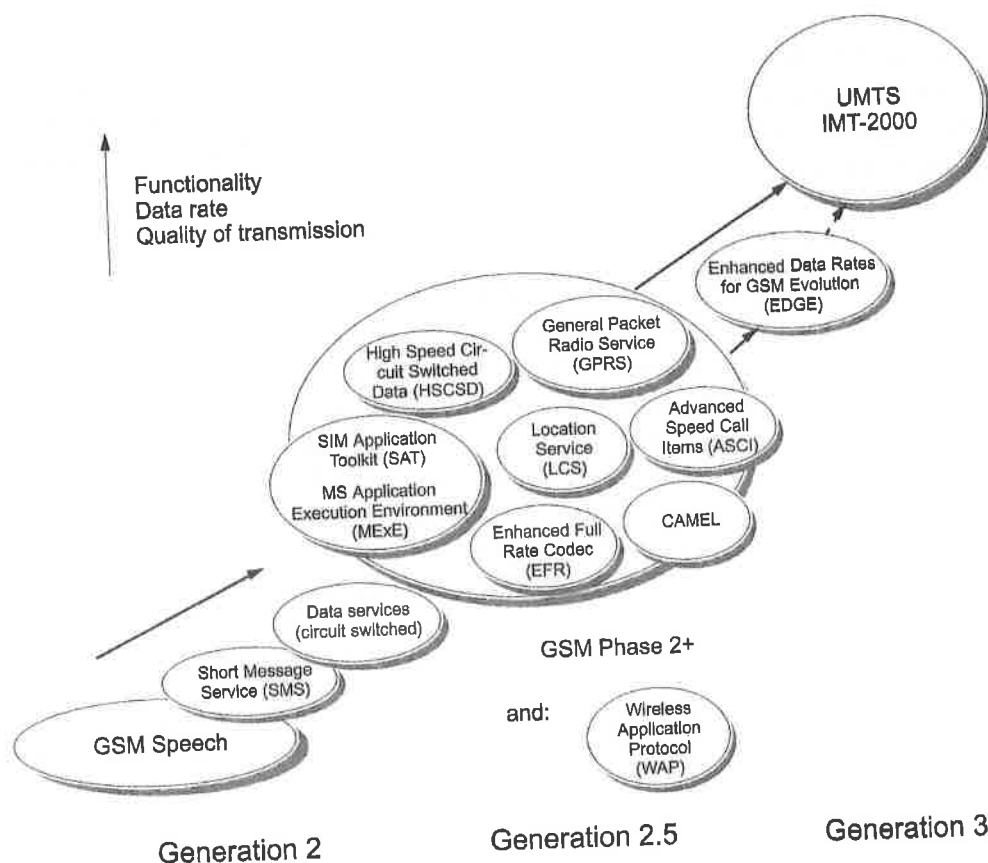


Figure 7.2 Evolution of GSM.

Service (VGCS). In addition, the Enhanced Multi-Level Precedence and Pre-emption Service (eMLPP) is used to assign and control priorities to users and their calls (e.g. for emergency calls). All of these services together are referred to as Advanced Speed Call Items (ASCI).

Voice broadcast service

VBS allows a user to broadcast a speech message to several other users within a certain geographical area. The user who initiates the call can only send ('speaker') and all others can only listen ('listeners').

Figure 7.3 gives a schematic illustration of a VBS scenario. Mobile users who are interested in a certain VBS group subscribe to it and will then receive broadcast calls of this group. Special permission is needed, however, for the right to send broadcast calls, i.e. for the right to act as a speaker. The subscribed VBS groups are stored on the user's SIM card, and if a subscriber does not want to receive VBS calls for a certain time, they can deactivate them. In addition to mobile GSM users, a predefined group of fixed telephone connections can also participate in the VBS service (e.g. dispatchers, supervisors, operators or recording machines).

System concept and group call register. The area in which a speech broadcast call is offered is referred to as the group call area. As illustrated in Figure 7.4, in general, this area

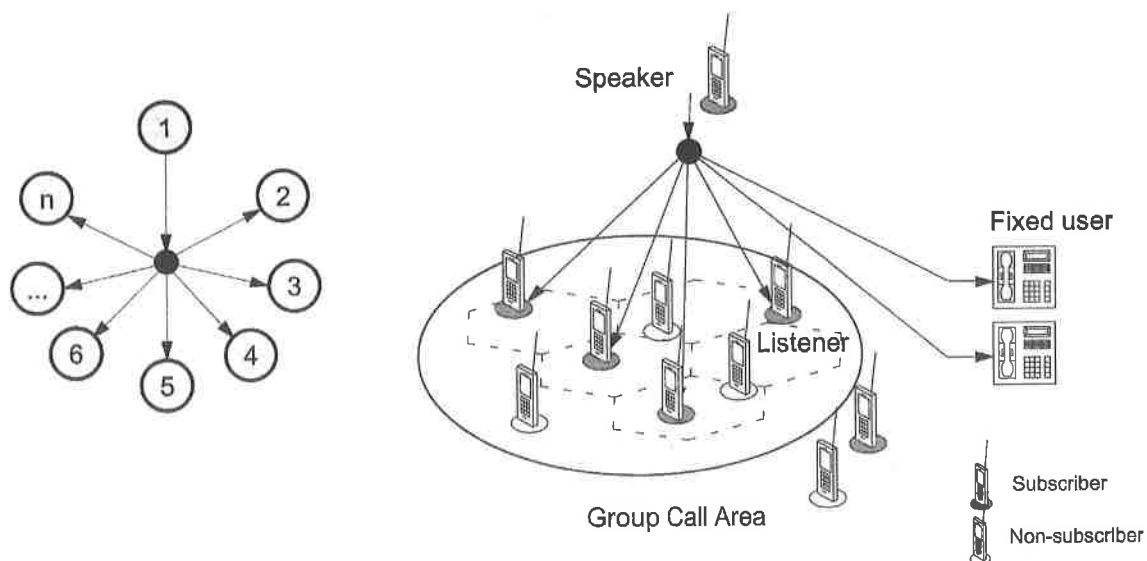


Figure 7.3 VBS scenario.

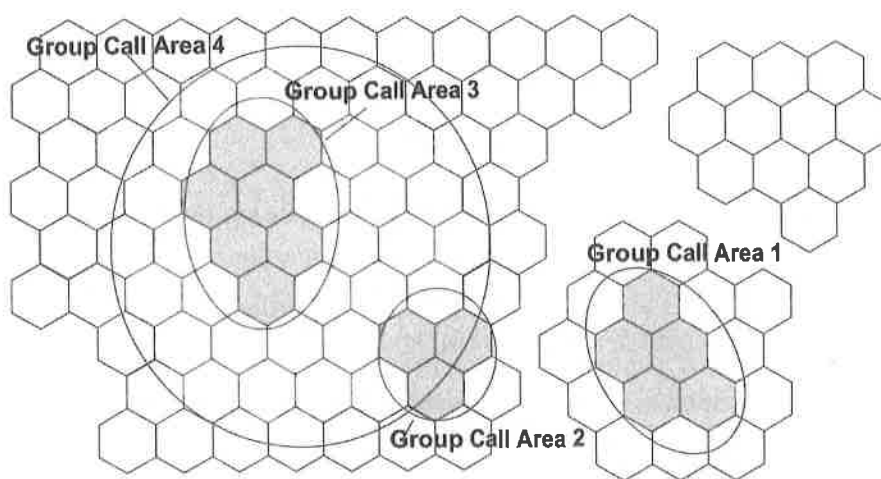


Figure 7.4 Some examples of group call areas.

consists of several cells. A group call area may comprise cells of several MSC areas and even of several PLMNs. One MSC is responsible for the handling of the VBS. It is called the anchor MSC. If a voice broadcast is also transmitted in cells that are not within the service area of this MSC (i.e. if the group call area also contains cells belonging to other MSCs), the MSCs of those cells are also involved. They are then denoted as relay MSCs.

The VBS-specific data are stored in a Group Call Register (GCR). Figure 7.5 shows the extended GSM system architecture. The GCR contains the broadcast call attributes for each VBS group, which are needed for call forwarding and authentication. Some examples follow.

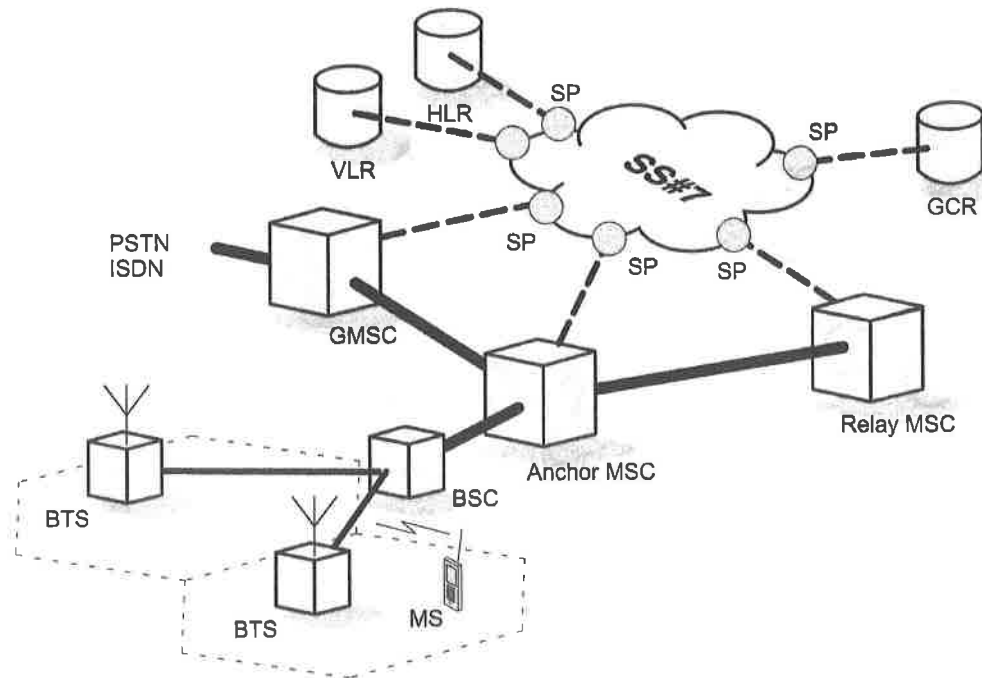


Figure 7.5 Extension of the GSM system architecture with the GCR.

- Which cells belong to the group call area?
- Which MSC is the responsible anchor MSC?
- In which cells are group members currently located, i.e. in which cells is a voice message to be broadcast?
- To which other MSCs is the voice message to be forwarded to reach all group members who are currently located in the group call area?
- To which external fixed telephone connections is the broadcast message addressed?
- Which fixed telephone connections are allowed to act as speakers?

Call establishment and logical channels. A MS that intends to initiate a voice broadcast call sends a service request to the BSS. The request contains the group ID of the VBS group to be called. Thereupon, the responsible MSC queries the user's profile from the VLR and checks whether the user is allowed to act as speaker for the stated group. Next, some VBS-specific attributes are requested from the GCR. If the broadcast call should also be transmitted in cells that do not belong to the current MSC, an anchor MSC is determined. The anchor MSC then forwards the VBS attributes to all relay MSCs, which then request all affected BSCs to allocate a traffic channel in the respective cells, and to send out notification messages on the NCH (section 4.1). When a MS receives such a message and is also subscribing to the respective VBS group, it changes to the given traffic channel and listens to the voice broadcast in the downlink. The speaker is then informed about the successful connection setup and can

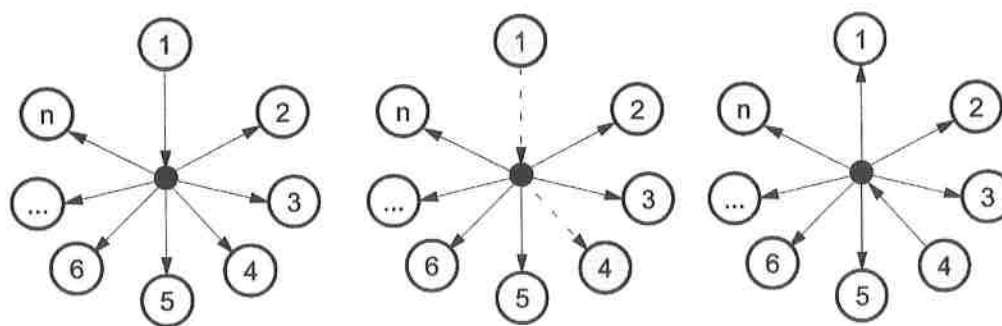


Figure 7.6 Group call scenario.

start talking. The notification message is periodically repeated on the NCH until the speaker terminates the call.

In contrast to the paging procedure in conventional GSM calls, the individual mobile users and their MSs are not explicitly addressed by an IMSI or TMSI but with the group ID of the VBS group. Furthermore, the MSs do not acknowledge the reception of VBS calls to the network. To realize the service, traffic channels are not allocated to individual subscribers, but the voice signal of the speaker is broadcast to all listening participants in a cell on one group channel. Thus, in each participating cell, only one full-rate channel is occupied (as in regular voice calls).

Voice Group Call Service

Another group communication service is the VGCS. The VGCS defines a closed user group communication service, where the right to talk can now be passed along within the group during a call by using a push-to-talk mechanism as in mobile radio. This principle is illustrated in Figure 7.6: user 1 initializes a group call and speaks, while the other users listen. Next, user 1 releases the channel and changes into listener mode. Now, each of the subscribers may apply for the right to become speaker. For example, user 4 requests the channel, and the network assigns it to them. They talk, release the channel and change back to listener mode. Finally, the group call is terminated by the initiator (in general). Whereas the information flow in the VBS is simplex, the VGCS can be regarded as a half-duplex system (compare Figures 7.3 and 7.6).

The fundamental concepts and entities of the VBS, e.g. the definition of group call areas, group IDs, the GCR and anchor and relay MSCs, are also used in the VGCS.

Logical channels. A traffic channel is allocated in each cell of the group call area that is involved in the VGCS. All group members listen to this channel in the downlink, and only the speaker uses it in the uplink. Therefore, in addition to the tasks for VBS calls, the network must also control uplink radio resources. The network indicates in the downlink to all MSs whether the uplink channel is in use or not. If the channel is free, the group members may send ABs. Collisions that occur with simultaneous requests are resolved, and the network chooses one user who obtains the channel and thus has the right to talk.

Table 7.2 Priority classes in eMLPP.

Class	Used by	Connection setup	Call interruption (pre-emption)	Example
A	Operator	Fast (1–2 s)	Yes	Highest priority; VBS/VGCS emergency calls
B	Operator	Normal (<5 s)	Yes	Calls of operator
0	Subscriber	Normal (<5 s)	Yes	Emergency calls of users
1	Subscriber	Slow (<10 s)	Yes	
2	Subscriber	Slow (<10 s)	No	
3	Subscriber	Slow (< 10 s)	No	Standard priority
4	Subscriber	Slow (< 10 s)	No	Lowest priority

Enhanced Multi-Level Precedence and Pre-emption

Priority services enable a network to process calls with a priority class (precedence level). If the network load is high, calls with high priority can then be treated in a preferred manner and resources for low priority calls can be deallocated. In the extreme case, a call with low priority can be dropped because a call with high priority arrives (pre-emption).

The priorities in GSM are controlled by eMLPP. It is a supplementary service for point-to-point speech services as well as for VBS and VGCS. The principle of eMLPP is based on the Multi-Level Precedence and Pre-emption (MLPP) (ITU-T Recommendation Q.735, 2008) method used in SS#7. In doing so, MLPP has been enhanced with functions for priority control at the air interface. Table 7.2 lists all priority classes of eMLPP. In addition to the five precedence levels that are used in MLPP (classes 0–4), two additional levels with higher priority are defined (classes A and B). The table also shows whether a call with higher priority may terminate a call with lower priority. It is important to note that only the operator may use calls of class A and B, such that, for example, an emergency call over VBS or VGCS can be initiated in disaster situations. Calls of this class can only be employed within the service area of one MSC. The other five classes can be utilized within the entire PLMN and also in combination with the MLPP of ISDN. The highest priority call that a subscriber is allowed to use is stored on their SIM card and in the HLR.

7.4.2 New data services and higher data rates: HSCSD, GPRS and EDGE

As discussed in Chapter 8, the maximal data rate of 9.6 kbit/s for data services in conventional GSM is rather low compared with fixed networks. The desire for higher data rates in GSM networks was the motivation to introduce higher data rates and more flexible data services. Accordingly, one of the GSM standardization groups specified the HSCSD service. Later the new packet data service, GPRS, was standardized and has since been introduced by many network operators. It offers a genuine packet-switched bearer service at the air interface. As for HSCSD, new multislot-capable MSs are required (which can use, e.g., four time slots in the downlink and two time slots in the uplink). The GPRS chapter of

this book (Chapter 8) discusses in detail the system architecture, protocols, air interface, multiple access and interworking with the Internet. Additional information can be found in Bettstetter *et al.* (1999), Brasche and Walke (1997), Faccin *et al.* (1999), Granbohm and Wiklund (1999), Kalden *et al.* (2000) and Walke (1999). Release 99 extended the GPRS standard with some new functions, e.g. point-to-multipoint services and prepaid services. Furthermore, existing functionality has been improved.

In order to increase the data rate and spectral efficiency on a single time slot, EDGE has been developed, as described in Chapter 8. It utilizes higher-order modulation schemes and a series of different coding schemes, in order to adapt the data rate perfectly to the current channel conditions of a terminal. Combining EDGE with GPRS and HSCSD, we obtain EGPRS and ECSD, respectively, now offering significantly higher data rates than pure HSCSD or GPRS.

7.5 Supplementary services in GSM Phase 2+

7.5.1 Supplementary services for speech

Most of the supplementary service characteristics known from ISDN have in one way or another already been implemented in GSM. The mobility of the users, however, creates the need for new supplementary services. Examples of supplementary services known from ISDN or newly defined are mobile access hunting, short message forwarding, multiple subscriber profile, call transfer or Completion of Calls to Busy Subscribers (CCBS).

The example of the CCBS service clearly shows how much the role of the HLR is changing from its original function as a database to a more active role as a service control component, similar to the Service Control Point (SCP) of the Intelligent Network (IN). The supplementary service CCBS basically realizes 'call back if busy'. If a called subscriber does momentarily not accept a call due to an ongoing connection, the calling subscriber can activate the supplementary service CCBS which causes the network to notify them at the end of the called subscriber's ongoing call and automatically set up the new connection. The subscriber mobility adds more complexity to the implementation of this service. In the fixed network, implementation would require the establishment of queues for call-back requests in the switching center of the calling and called subscribers, respectively. In a mobile network, this may involve additional switches, because after activation of the CCBS service, the calling subscriber may be roaming into another switching center area. If the implementation of the service were only in the MSC, either there could be a centralized solution or the queuing lists would have to be forwarded to the new MSC – which may even be in another network. The targeted solution is centralized in the HLR, which has to store the subscriber's callback queues (if existing) in addition to the current MSC designation. If the MS changes the MSC area, the callback queue is transferred to the new MSC. In this case, therefore, the HLR has to assume an additional server role and perform call control beyond the originally planned restriction to a pure database function.

7.5.2 Location service

GSM release 99 introduced a Location Service (LCS) making it possible to determine the exact location of a MS down to a few meters. One of the motivations for this service has been

a law in the USA which demands the location of a person to be determined in the case of an emergency call.

From GSM mobility management, the network already knows the current cell of the user (cell identifier). However, this location accuracy is not sufficient in most cases, and therefore investigations have been made to find a more sophisticated solution. In the so-called Time Of Arrival (TOA) method, the network listens to handover ABs of the MS and is then able to triangulate its position. In contrast, using the Enhanced Observed Time Difference (E-OTD) method, the MSs now measure the time difference of received bursts from different base stations. Both methods only work if a MS has contact with at least three base stations. The accuracy of E-OTD schemes lies between 50 and 125 m, and that of TOA is worse (Buckingham, 1999). E-OTD schemes require a software update on the mobile equipment as well as modifications in the network, whereas for the TOA method it is mainly sufficient to modify network components. However, the functionality of TOA is provided by synchronization of the cellular network (using GPS or precise clocks at each BTS). This capability is currently not provided in asynchronous GSM networks. The most precise way to find the position of a MS is to integrate a GPS receiver into each piece of mobile equipment. The MS then receives its current position from GPS satellites. A substantial disadvantage of this approach is that MSs cannot always have intervisibility with GPS satellites (e.g. inside buildings). We observe that each of the three methods has its advantages and disadvantages.

In addition to the technical implementation of the location service, two new network nodes have been defined for this type of service: the Gateway Mobile Location Center (GMLC) and the Serving Mobile Location Center (SMLC). The GMLC acts as an interface to applications that use the positioning information of users in a specific way – so-called location-based or location-aware services. Examples are navigation services (such as ‘Where is the closest gas station?’) or virtual tourist guides (‘What is the building on my left-hand side?’). A service provider stores, e.g., the locations of gas stations and sightseeing attractions in a database and adds other useful information. At the request of a mobile user, the provider can obtain the current position of the user from the GMLC and send back the requested information. Other location-based applications include location-based charging (‘home zone’), vehicle tracking (e.g. stolen cars) and localized news, weather and traffic information.

7.6 Service platforms

The procedures for the development of the GSM standards required close cooperation between the involved manufacturers and network operators. The international standardization of services and interfaces led to a set of common successful performance characteristics in GSM networks, most prominently the international roaming capability. The more a performance criterion is standardized, the lower the costs of development and introduction are, since all manufacturers and operators contribute to paying the costs. On the other hand, the network operators desire service differentiation to be able to gain competitive advantages. The standardization of services and service performance criteria reduces the possibility for differentiation among competitors. Moreover, the time-to-market is often extended because of the prolonged process of standardization.

For these reasons, the service platform concept has been introduced in GSM on both the network and the terminal side. These platforms offer mechanisms, functions and protocols

for the definition and control of services and applications. Those services/applications can be operator-specific, such that an international standardization process is not needed in general. The required generic functions can be made available in each MS and network node, and they can be used and combined in a flexible way for service execution.

The GSM supplementary services can be regarded as the simplest form of service platform usage. An extended concept are the so-called service nodes, such as a voice mail server and a SMS-SC. However, both concepts have significant disadvantages: supplementary services are subject to international standardization and, on the other hand, these services might not be available to roaming users in foreign networks, since network providers are not obligated to implement all supplementary services. The situation is similar with service nodes, which are often accessible only in the home network. We conclude that these two types of platforms allow the definition of vertical/operator-specific services in only a limited way, and their use in foreign networks is often not possible or rather complicated.

An extension of the platform concept, which has been taken up by ETSI in the Phase 2+ standardization, attempts to overcome this dilemma. Instead of specifying services and supplementary services directly or completely, only mechanisms are standardized which enable the introduction of new services. With this approach it is possible to restrict the implementation of a service to a few switches in the home network of a subscriber, whereas local (visited) switches have to provide only a fixed set of basic functions and the capability to communicate with the home network switch containing service logic.

This group of GSM standards within Phase 2+ is known under the name Support of Operator-Specific Services (SOSS), or also as Customized Applications for Mobile Network Enhanced Logic (CAMEL). The answer on the terminal side is the SIM Application Toolkit (SAT) and Mobile Station Execution Environment (MExE). They are explained in the following.

7.6.1 CAMEL: GSM and INs

Essentially, CAMEL represents a convergence of GSM and IN technologies. The fundamental concept of IN is to enable flexible implementation, the introduction and control of services in public networks and to use the idea of dividing the switching functionality into basic switching functionality, residing in Service Switching Points (SSPs) and centralized service control functionality, residing in Service Control Points (SCPs). Both network components communicate with each other over the signaling network using the generic SS#7 protocol extension called the Intelligent Network Application Part (INAP). This approach enables a centralized, flexible and rapid introduction of new services (Ambrosch *et al.*, 1989).

There are already some features in GSM which parallel an IN. Even though GSM standards use neither IN terminology nor IN protocols, i.e. INAP, the GSM network structure follows the IN philosophy (Laitinen and Rantale, 1995). In the GSM architecture, the separation into functional units such as MSC and HLR and the consistent use of SS#7 and its MAP extensions are in conformity with the IN architecture, which is split into SSPs and SCPs that communicate using INAP.

The philosophy of CAMEL is to proceed with the implementation of services in GSM in a similar way as in INs. This is reflected in separating a set of basic call processing functions in the MSC or GMSC (which act as SSPs), from the intelligent service control functions (SCP) in the home network of the respective subscriber. The HLR in a GSM network already has

functions similar to the SCP, especially with regards to supplementary services. Beyond that, the CAMEL approach provides its own dedicated SCPs. Imagine specialized SCPs for the translation of abbreviated numbers in Virtual Private Networks (VPNs) or for future extended SMSs. With this configuration, the service implementation with its service logic is needed only once, namely in the home network SCP. The network operator offering the service thus has sole control over the features and performance range of the service. Owing to the complete range of generic functions that have to be provided at each SSP (MSC, GMSC, etc.), new services can immediately be provided in each network, and an uninterrupted service availability is guaranteed for roaming subscribers. The sole responsibility and control for the introduction of new services lies in SOSS/CAMEL with the operator of the home network, the contract partner of the subscriber. This opens new competitive possibilities among network operators. Operator-specific services can be introduced rapidly without having to go through the standardization process, and yet they are available worldwide.

Figure 7.7 shows the resulting architecture. The CAMEL specification requires a GSM-specific version of IN. Similar to the IN approach, GSM defines a basic call processing function as GSM Service Switching Function (gsmSSF) and a service logic function GSM Service Control Function (gsmSCF). In addition to the MAP signaling interfaces already existing in Phase 1 and Phase 2 for communication between visited and home networks (GMSC, VLR, HLR), new signaling interfaces are needed for communication between basic switching and service logic in the visited and home networks. For this signaling, a new application part of SS#7 is being specified, the CAMEL Application Part (CAP), which assumes the functions similar to INAP. These functions and protocols represent the basic structure for the realization of intelligent services and their flexible introduction.

The prerequisites for CAMEL are the definition of a standardized extended call model with appropriate trigger points, and the specification of the generic range of services which must be provided by the SSP. More precisely, the new extended call model must also include a model of subscriber behavior, because in addition to normal call processing aspects, it also contains events such as location updating. For each subscriber, this behavior model is stored in the HLR and supplied from the home network to the currently visited SSP/MSC. In this way, the SSP/MSC has a set of trigger points with corresponding SCP addresses for each subscriber roaming in its area. When a trigger condition is satisfied, the call and transaction processing in the SSP/MSC is interrupted and the SCP is notified. The SCP can now analyze the context and, according to the service implementation, give instructions to the SSP to perform particular functions. Typical functions the SSP has to implement are call forwarding, call termination or other stimuli to the subscriber (Mouly and Pautet, 1995). Based on this behavior model and the corresponding control protocol between mobile SSP and home SCP, which are connected through a set of generic SSP functions, we can expect to see a large variety of operator-specific services in the future.

7.6.2 Service platforms on the terminal side

SIM application toolkit

SAT has been a further step toward provider-specific vertical services. The GSM SIM card is provided completely by the network operator, in particular because it contains security functions. From this fact, the basic approach arose to equip the SIM card with additional, operator-specific functions. Without a standardized interface to the mobile equipment,

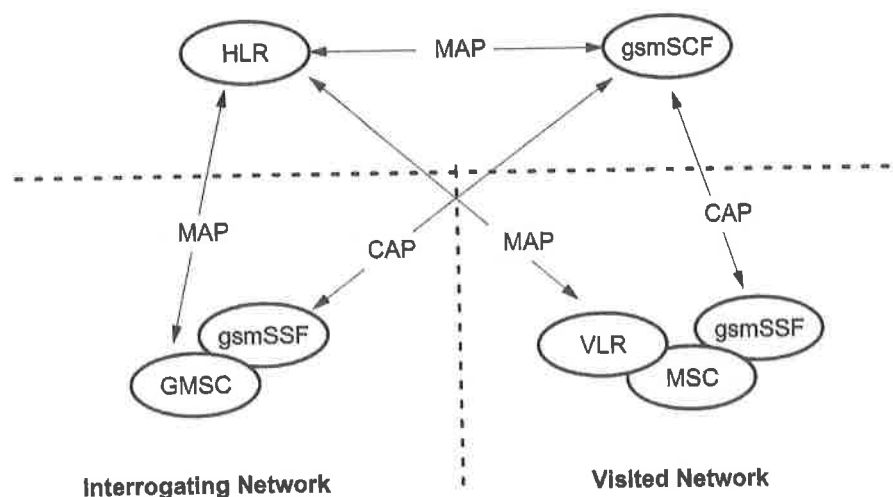


Figure 7.7 Functional architecture for CAMEL.

this was only possible in a very limited manner and only in close cooperation with equipment manufactures. SAT removes these restrictions by defining a standardized interface between mobile equipment and SIM card. In this way, operator-specific applications can run on the SIM card and can thereby control clearly defined, selected functions of the terminal. Corresponding applications can be carried out in the PLMN or even outside the PLMN on dedicated servers making it possible to implement completely new services. The communication between the SIM card application and its counterpart in the network is currently implemented over SMS, but in the near future other bearer services (in particular, GPRS) are also possible. The functions defined in the SAT framework can be categorized into SIM data download and proactive SIM. The functional interface between SIM card and terminal is through proactive SIM mechanisms. They include:

- display of text;
- transmission of SMS messages;
- connection setup (speech and data) triggered by the SIM card;
- playing of sounds in the mobile equipment;
- read-out of local information from the equipment into the SIM card.

With these mechanisms, a broad variety of new features can be offered, for example, download of data to the SIM card. This includes the download of new or existing commands and applications to be installed. With the toolkit, the SIM card is able to display new, operator-specific menu options to the user, and to read out user actions from the mobile equipment. Most far-reaching are the functions for call control, where each number typed in can be analyzed by the SIM card. This allows for operator-specific treatment of telephone numbers, e.g., the mapping of numbers or barring functions. In a further standardization step, the functions of SAT have been enhanced with security and encryption mechanisms. SAT-capable MSs have been available for a few years.

Mobile station application execution environment

Of similar scope is the MExE, which implements a generic application platform in the terminal. The most important components are a virtual machine for execution of Java code and WAP. Both techniques open the door for a variety of new services and applications. With a virtual machine running on the mobile terminal, applications can be uploaded and executed. This demands a high computational effort in the MSs. The WAP is explained in the following section.

7.7 Wireless application protocol

WAP is a major step in building the wireless Internet, where people on-the-go can access the Internet through their wireless devices to get information such as emails, news headlines, stock reports, map directions and sports scores when they need it and where they need.

(Chuck Parish, Founding Member and Chairman (1998–1999) WAP Forum)

WAP is regarded as an important step in the move of today's GSM networks towards a 'mobile Internet'. During the last few years, WAP has been developed and standardized by the WAP Forum 1999a; 1999b. This industry consortium was founded by Nokia, Ericsson, Phone.com (formerly Unwired Planet) and Motorola in December 1997 and has several hundred members today.

The philosophy of WAP is to transfer Internet content and other interactive services to MSs to make them accessible to mobile users. For this purpose, WAP defines a system architecture, a protocol family, and an application environment for the transmission and display of WWW-like pages for mobile devices.

The motivation for the development of WAP was the fundamental restrictions posed by mobile equipment and cellular networks in comparison to PCs and fixed wired networks. These are, in particular, the limited opportunities for display and input (small displays, number keypad and no mouse) as well as the limited memory and processing power. Furthermore, the power consumption of a MS should be as low as possible. On the network side, it is clear that the wireless transmission has lower bandwidth, a higher bit error probability and less stable connections than wired networks.

The protocols and the application environment defined for WAP consider these limitations. The protocols of the WAP architecture are basically a modification, optimization and enhancement of the IP stack used in the World Wide Web for use in mobile and wireless environments. WAP focuses on applications tailored to the capabilities of cellular phones and the needs of mobile users. One can say that WAP 'creates an information Web for cellular phones, distinct from the PC-centric Web' (Goodman, 2000).

7.7.1 Wireless markup language

With respect to the mentioned requirements, the Wireless Markup Language (WML) has been developed. It represents a pendant to the Hypertext Markup Language (HTML) used in the World Wide Web. WML is defined as a document type of the meta language the Extensible Markup Language (XML). It contains some phone-specific tags and requires only a phone

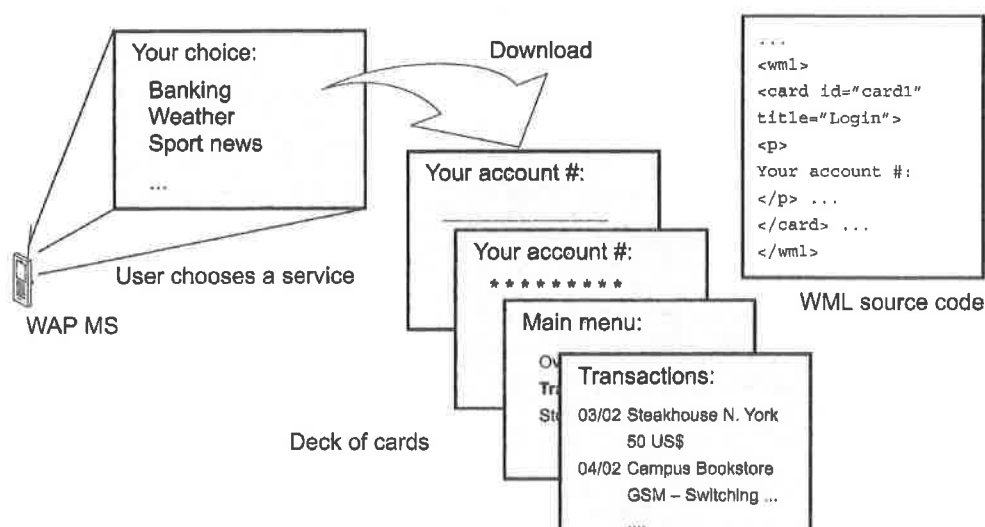


Figure 7.8 WAP example.

keypad for input. For display of monochrome graphics the Wireless Bitmap (WBMP) format has been defined.

A microbrowser, which is running on each WAP terminal, interprets the received WML documents and displays their content (text, pictures, links) to the user. Such a microbrowser is also referred to as a WML browser and is the pendant to a Web browser used in PCs.

In doing so, the presentation of WML documents is not limited to classical mobile telephones, but there also exist WML browsers for other devices, such as for PDAs under the operating systems PalmOS, Windows CE or EPOC systems. These devices may be linked over infrared or Bluetooth (Bluetooth SIG, 2008) with a GSM MS, or they have their own GSM/GPRS air interface.

WML documents are organized into cards and decks (see Figure 7.8). When a subscriber chooses a service, a deck of cards is downloaded to the MS. The user can then view these cards with their WML browser, make inputs and navigate between the cards. Each card is designed for one user interaction.

Figure 7.9 illustrates how an automatic parallel creation of WML and HTML documents may look (WAP Forum, 1999c). The World Wide Web Consortium (W3C) currently specifies the Extensible Style Language (XSL) (WWW Consortium, 2008). Using XSL style sheets, WML and HTML documents can be automatically generated from content written in XML.

7.7.2 Protocol architecture

The WAP architecture is shown in Figure 7.10. As mentioned before, WAP is based on the WWW protocol stack and adjusts those protocols to the requirements of wireless transmission and small portable devices.

For applications, a uniform microbrowser environment has been specified: the Wireless Application Environment (WAE). It comprises the following functionality and formats:

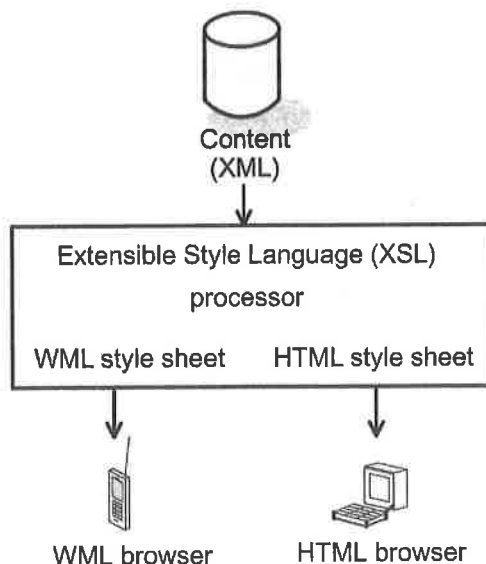


Figure 7.9 Generation of WML and HTML documents.

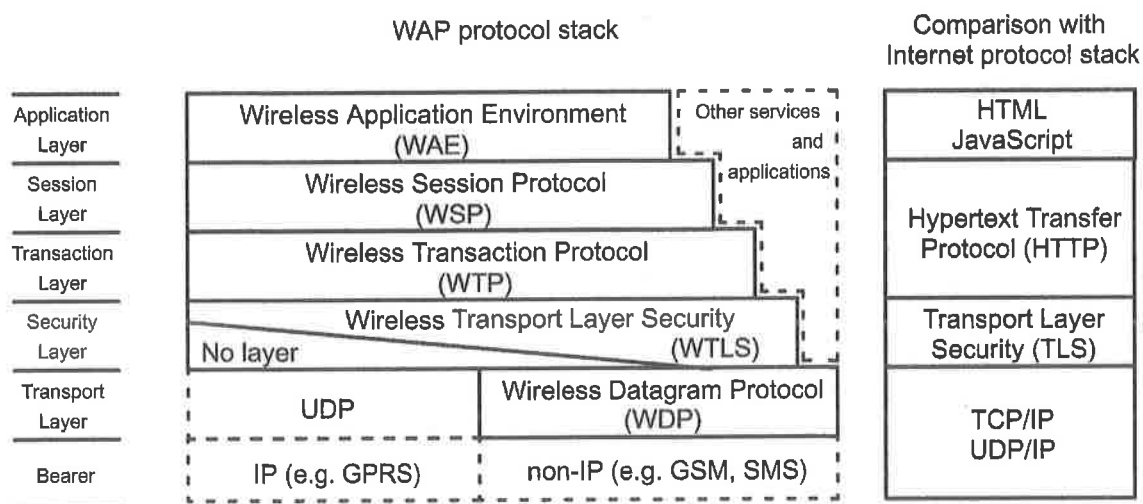


Figure 7.10 WAP architecture.

- the WML;
- a simple script language WMLScript, which is based on JavaScript;
- programming interfaces for control of telephony services (Wireless Telephony Application (WTA) interface); and
- data formats for pictures, electronic business cards (vCard) and entries of the phone directory and calendar (vCalendar).

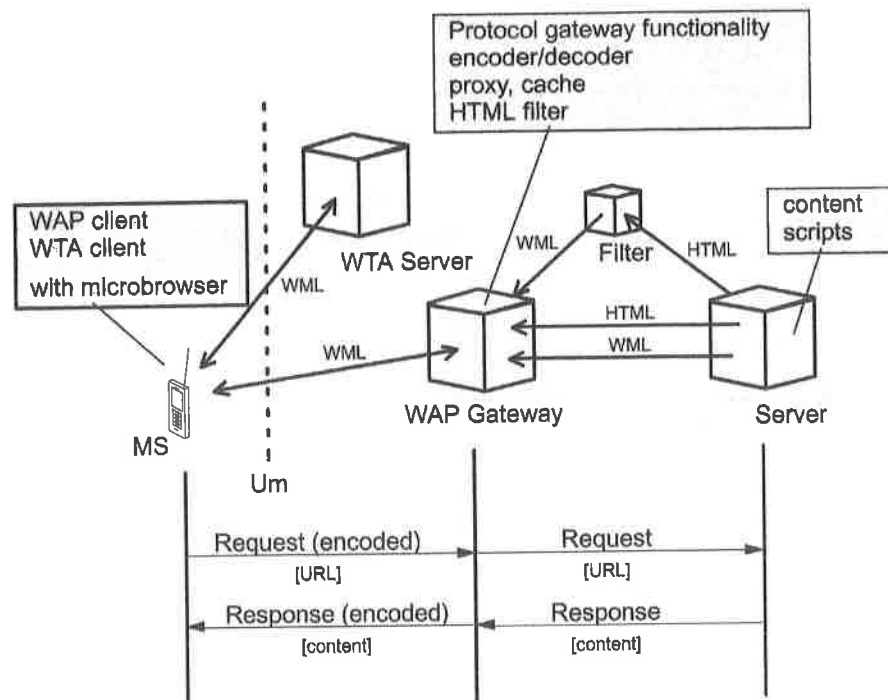


Figure 7.11 WAP system architecture and REQUEST/RESPONSE transaction.

The WTA interface allows the microbrowser to interact with telephony functions. For example, it specifies how calls are initiated from the microbrowser or how entries from the phone directory are sent out.

The main task of the Wireless Session Protocol (WSP) is the establishment and termination of a session between the MS and the WAP gateway (Figure 7.11). Thereby, connection-oriented (over WTP) as well as connectionless (over datagram services, e.g. WTP) sessions are defined. In the case of a radio connection breaking down, the session can be stopped for a certain period of time and resumed later.

The Wireless Transaction Protocol (WTP) is a lightweight transaction-oriented protocol. Its task is to guarantee the reliable exchange of the MS's request and the WAP gateway's response messages (Figure 7.11). It thus constitutes the basis for interactive browsing. WTP includes functions for the acknowledgement of messages, retransmission of erroneous or lost messages, and the removal of duplicate messages. In addition, an acknowledged and an unacknowledged datagram service is defined for push services, where the server can send content to a MS without an initiating request from the mobile user. The server may send an emergency warning, for example.

Optionally, the Wireless Transport Layer Security (WTLS) protocol may be employed. It is based on the Transport Layer Security (TLS) protocol, which is used in the Internet and was formerly known as Secure Socket Layer (SSL). WTLS offers basic security functions, such as data integrity, encryption, user identity confidentiality and authentication between the server and MS. Moreover, protection against denial-of-service attacks is provided. The functionality of WTLS can be made effective (or not) according to the application and security of the used network. For example, if an application already uses strict security techniques, the complete

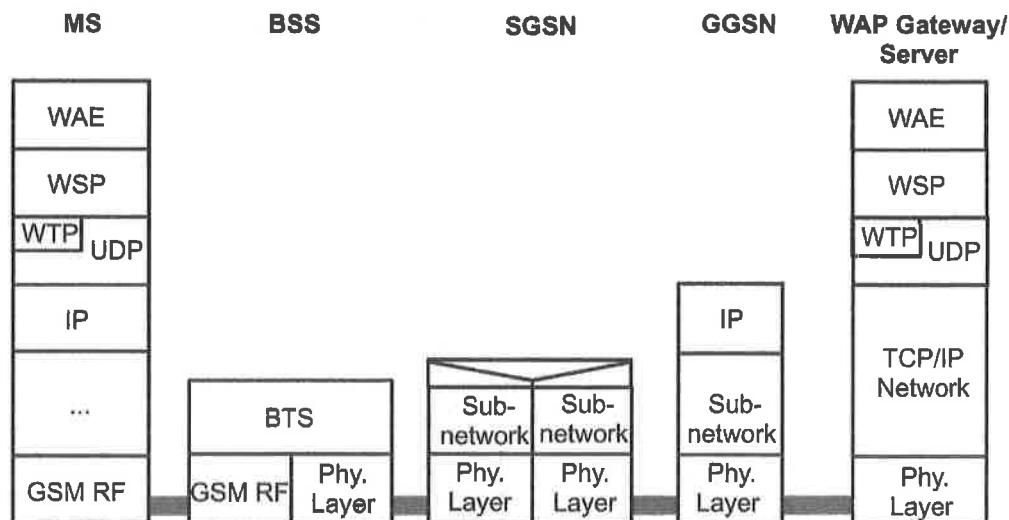


Figure 7.12 Protocol architecture WAP over GPRS (compare with Figure 8.7).

scope of WTLS functions will not be needed. It is worth mentioning that WTLS can also be used for secure data transfer between two MSs (e.g. for authenticated exchange of electronic business cards).

The WAP transport protocol is known as the Wireless Datagram Protocol (WDP). It is for example, used instead of UDP for bearer services that are not based on IP (Figure 7.10). GSM bearer services for WAP can be either circuit-switched data services (e.g. SMS) or the GPRS, which of course offers faster data transfer and volume-based billing.

Figure 7.10 indicates that nonWAP protocols can also access specific layers of the WAP stack. Furthermore, not all WAP protocols must be used always. Certain applications may, for example, only require the services of WTP and underlying layers. Figure 7.12 gives an example, where WAP comes into operation over GPRS as a bearer service.

7.7.3 System architecture

Figure 7.11 gives a schematic illustration of a typical WAP system architecture. The principle of how content is stored in a distributed way within the network and finally offered to the user is similar to the principle of the WWW. Servers store content directly as a WML document or content is generated with scripts. MSs download this content from the server to their microbrowser, which then presents them to the user. In theory, it is possible to store content in HTML and subsequently convert it to WML, however, in practice, applications and content offered directly in WML are much better suited (WAP Forum, 1999a).

As shown in Figure 7.11, a WAP Gateway acts as an interface between external servers and the MSs. Its main tasks include:

- conversion of requests from the WAP protocol stack to the WWW protocol stack (HTTP over TCP/IP) and vice versa (i.e. a protocol gateway functionality);
- encoding and decoding of WML documents into a binary format

The WAP gateway also represents a proxy server and acts as a cache for frequently requested contents.

The following example illustrates the transaction procedure between a mobile user, the WAP gateway and an external server: A subscriber intends to view a document which is offered on a server. Their WML browser sends a WSP REQUEST to the appropriate address of the server. The request is forwarded to the WAP gateway, which then converts it into an HTTP REQUEST and contacts the server. Next, the server transmits the requested content in WML format to the WAP gateway, which writes the content into its cache and sends it in binary-encoded form to the MS. The latter presents the first card of the deck on the microbrowser to the user. If the external server transmitted the document in HTML format, the gateway would convert it into WML format.

7.7.4 Services and applications

The first specification of WAP was released by the WAP Forum in April 1998. Version 1.1 followed in June 1999 and Version 1.2 in December 1999. WAP terminals have been introduced around February 1999 for the first time, and today there exist a broad variety of WAP products: mobile equipment, gateways, development tools, WML browsers and editors.

In addition to the technical implementation in the network and the development of new WAP-capable mobile equipment, innovative WAP services are, in particular, in demand. These days, several information services are offered over WAP. Subscribers can retrieve news, weather forecasts, stock reports and local restaurant and event guides with their WAP phone. Furthermore, mobile e-commerce services (e.g. ticket reservation, mobile banking and online auctions) are becoming increasingly popular. There is much scope left for new applications. Push services, for example, may transmit important information to MSs without the need to request them actively. Highly interesting are so-called location-based services, in which the service knows the current physical location of the user and may use this information in a specific way. Navigation services with displayed maps on the browser or virtual tourist guides ('I would like to have information about the building on my left-hand side') are two examples.

Improved data services in GSM: GPRS, HSCSD and EDGE

The main data service used in modern GSM systems is the GPRS. Therefore, the major part of this chapter is devoted to GPRS. However, HSCSD is also of importance. HSCSD was available earlier than GPRS and was therefore chosen by some network providers in order to provide higher data rate services in GSM as fast as possible and it is still used in many networks. A third important aspect of providing improved data rates in GSM systems is EDGE, which helps to increase the data rate of both GPRS and HSCSD by allowing for higher-order modulation schemes when the signal strength is sufficiently high. Let us now first focus on GPRS in the following.

8.1 GPRS

Packet data transmission has already been standardized in GSM phase 2, offering access to the Packet Switched Public Data Network (PSPDN); see Appendix A. However, on the air interface such access occupies a complete circuit switched traffic channel for the entire call period. In the case of bursty traffic (e.g. Internet traffic), such access leads to a highly inefficient resource utilization. It is obvious that in this case, packet switched bearer services result in a much better utilization of the traffic channels. This is because a packet channel will only be allocated when needed and will be released after the transmission of the packets. With this principle, multiple users can share one physical channel (statistical multiplexing).

In order to address these inefficiencies, GPRS has been developed in GSM phase 2+. It offers a genuine packet-switched bearer service for GSM also at the air interface. GPRS is thus a huge improvement and simplification of the wireless access to packet data networks. Networks based on IP (e.g. the global Internet or private/corporate intranets) and X.25 networks are supported. In order to introduce GPRS to existing GSM networks, several modifications and enhancements must be made in the network infrastructure as well as in the MSs.

Users of GPRS benefit from higher data rates and shorter access times. In conventional GSM, the connection setup takes several seconds and rates for data transmission are restricted to 9.6 kbit/s. GPRS, in practice, offers almost ISDN-like data rates up to approximately 40–50 kbit/s and session establishment times below one second. Furthermore, GPRS supports a more user-friendly billing than that offered by circuit-switched data services. In circuit-switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic, since the user must pay for the entire airtime even for idle periods when no packets are sent (e.g. when the user reads a Web page). In contrast to this, with packet-switched services, billing can be based on the amount of transmitted data (e.g. Mbyte) and the Quality of Service (QoS). The advantage for the user is that they can be ‘online’ over a long period of time but will be billed mainly based on the transmitted data volume. The network operators can utilize their radio resources in a more efficient way and simplify the access to external data networks.

The structure of this chapter is as follows.¹ Section 8.1.1 gives an overview of the GPRS system architecture and explains the fundamental functionality. Next, in section 8.1.2, we describe the offered services and the QoS parameters. Section 8.1.3 explains the session and mobility management and routing. It answers for example, the following questions. How does a GPRS MS register with the network? How does the network keep track of the MS’s location? Section 8.1.4 gives an overview of the GPRS protocol architecture and briefly introduces the protocols developed for GPRS. Next, an example of a GPRS–Internet interconnection is given (section 8.1.6). Section 8.1.7 discusses the air interface, including the multiple access concept and radio resource management. Moreover, the logical channels and their mapping onto physical channels are explained. Section 8.1.7 considers GPRS channel coding. GPRS security issues are treated in section 8.1.8 and, finally, a brief summary of the main features of GPRS is given.

8.1.1 System architecture of GPRS

In order to integrate GPRS into the existing GSM architecture (Chapter 3), a new class of network nodes, called GPRS Support Nodes (GSNs), has been introduced. GSNs are responsible for the delivery and routing of data packets between the MSs and external Packet Data Networks (PDNs). Figure 8.1 illustrates the resulting system architecture.

A Serving GPRS Support Node (SGSN) delivers data packets from and to the MSs within its service area. Its tasks include packet routing and transfer, functions for attach/detach of MSs and their authentication, and logical link management. The location register of the SGSN stores location information (e.g. current cell, current VLR) and user profiles (e.g. IMSI, address used in the packet data network) of all GPRS users registered with this SGSN.

A Gateway GPRS Support Node (GGSN) acts as an interface to external packet data networks (e.g. to the Internet). It converts GPRS packets coming from the SGSN into the appropriate Packet Data Protocol (PDP) format (i.e. IP or X.25) and sends them out on the corresponding external network. In the other direction, the PDP address of incoming data packets (e.g. the IP destination address) is converted into the GSM address of the destination

¹Parts of this chapter are based on: Ch. Bettstetter, H.-J. Vögel, J. Eberspächer. GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols, and Air Interface. *IEEE Communications Surveys*, Special Issue on Packet Radio Networks, vol. 2, no. 3, 1999, which can be obtained at <http://www.comsoc.org/pubs/surveys>. © 1999 IEEE.

Users of GPRS benefit from higher data rates and shorter access times. In conventional GSM, the connection setup takes several seconds and rates for data transmission are restricted to 9.6 kbit/s. GPRS, in practice, offers almost ISDN-like data rates up to approximately 40–50 kbit/s and session establishment times below one second. Furthermore, GPRS supports a more user-friendly billing than that offered by circuit-switched data services. In circuit-switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic, since the user must pay for the entire airtime even for idle periods when no packets are sent (e.g. when the user reads a Web page). In contrast to this, with packet-switched services, billing can be based on the amount of transmitted data (e.g. Mbyte) and the Quality of Service (QoS). The advantage for the user is that they can be ‘online’ over a long period of time but will be billed mainly based on the transmitted data volume. The network operators can utilize their radio resources in a more efficient way and simplify the access to external data networks.

The structure of this chapter is as follows.¹ Section 8.1.1 gives an overview of the GPRS system architecture and explains the fundamental functionality. Next, in section 8.1.2, we describe the offered services and the QoS parameters. Section 8.1.3 explains the session and mobility management and routing. It answers for example, the following questions. How does a GPRS MS register with the network? How does the network keep track of the MS’s location? Section 8.1.4 gives an overview of the GPRS protocol architecture and briefly introduces the protocols developed for GPRS. Next, an example of a GPRS–Internet interconnection is given (section 8.1.6). Section 8.1.7 discusses the air interface, including the multiple access concept and radio resource management. Moreover, the logical channels and their mapping onto physical channels are explained. Section 8.1.7 considers GPRS channel coding. GPRS security issues are treated in section 8.1.8 and, finally, a brief summary of the main features of GPRS is given.

8.1.1 System architecture of GPRS

In order to integrate GPRS into the existing GSM architecture (Chapter 3), a new class of network nodes, called GPRS Support Nodes (GSNs), has been introduced. GSNs are responsible for the delivery and routing of data packets between the MSs and external Packet Data Networks (PDNs). Figure 8.1 illustrates the resulting system architecture.

A Serving GPRS Support Node (SGSN) delivers data packets from and to the MSs within its service area. Its tasks include packet routing and transfer, functions for attach/detach of MSs and their authentication, and logical link management. The location register of the SGSN stores location information (e.g. current cell, current VLR) and user profiles (e.g. IMSI, address used in the packet data network) of all GPRS users registered with this SGSN.

A Gateway GPRS Support Node (GGSN) acts as an interface to external packet data networks (e.g. to the Internet). It converts GPRS packets coming from the SGSN into the appropriate Packet Data Protocol (PDP) format (i.e. IP or X.25) and sends them out on the corresponding external network. In the other direction, the PDP address of incoming data packets (e.g. the IP destination address) is converted into the GSM address of the destination

¹ Parts of this chapter are based on: Ch. Bettstetter, H.-J. Vögel, J. Eberspächer. GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols, and Air Interface. *IEEE Communications Surveys*, Special Issue on Packet Radio Networks, vol. 2, no. 3, 1999, which can be obtained at <http://www.comsoc.org/pubs/surveys>. © 1999 IEEE.

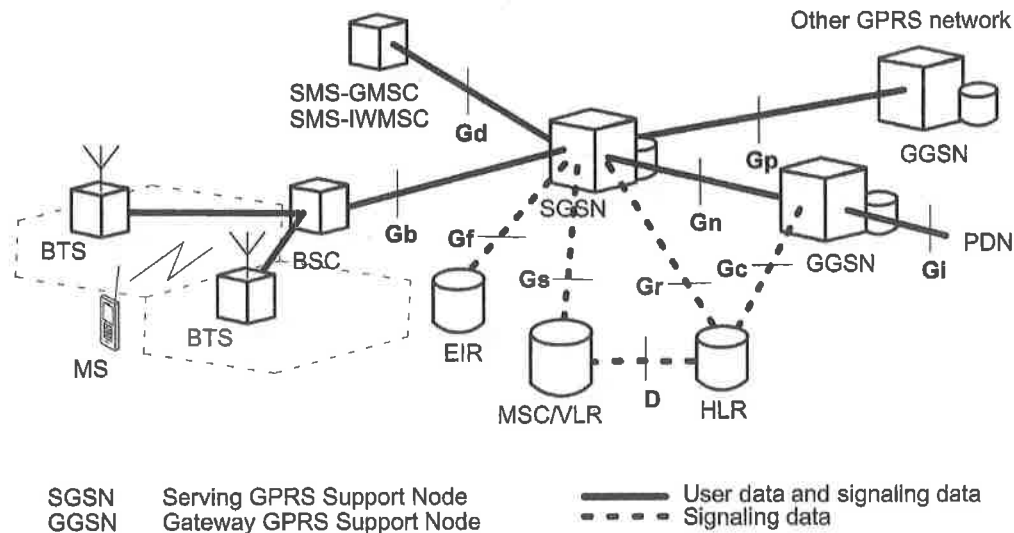


Figure 8.1 GPRS system architecture and interfaces.

user. The readdressed packets are sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN addresses and profiles of registered users in its location register.

In general, there is a many-to-many relationship between the SGSNs and the GGSNs: a GGSN is the interface to an external network for several SGSNs; an SGSN may route its packets to different GGSNs.

Figure 8.1 also shows the interfaces between the GPRS support nodes and the GSM network. The Gb interface connects the BSC with the SGSN. Via the Gn and the Gp interfaces, user and signaling data are transmitted between the GSNs. The Gn interface is used if SGSN and GGSN are located in the same PLMN, whereas the Gp interface is used if they are in different PLMNs.

All GSNs are connected via an IP-based GPRS backbone network. Within this backbone, the GSNs encapsulate the PDN packets and transmit (tunnel) them using the so-called GPRS Tunneling Protocol (GTP). In principle, we can distinguish between two kinds of GPRS backbones.

- Intra-PLMN backbones are IP-based networks owned by the GPRS network provider connecting the GSNs of the GPRS network.
- Inter-PLMN backbone networks connect GSNs of different GPRS networks. They are installed if there is a roaming agreement between two GPRS network providers.

Figure 8.2 shows, how two intra-PLMN backbone networks of different PLMNs are connected with an inter-PLMN backbone. The gateways between the PLMNs and the external inter-PLMN backbone are called Border Gateways (BGs). Their main task is to perform security functions in order to protect the private intra-PLMN backbones against unauthorized users and attacks. The illustrated routing example is explained later.

The Gn and Gp interfaces are also defined between two SGSNs. This allows the SGSNs to exchange user profiles when a MS moves from one SGSN area to another.

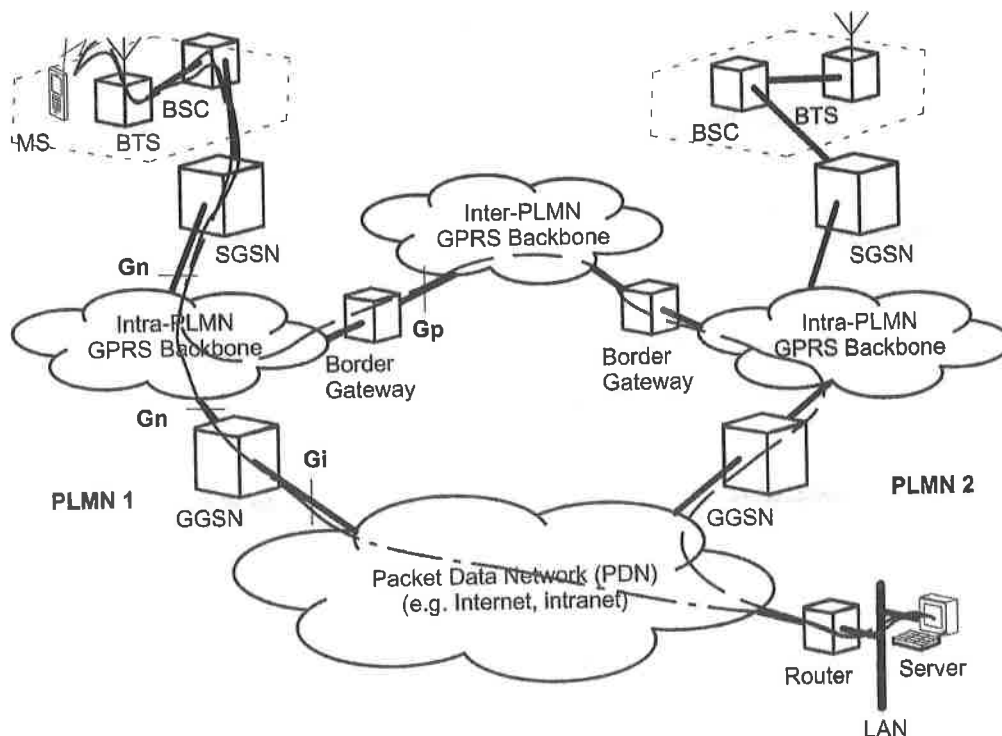


Figure 8.2 GPRS system architecture, interfaces and routing example.

Across the Gf interface, the SGSN may query and check the IMEI of a MS trying to register with the network.

The Gi interface connects the PLMN with external PDNs. In the GPRS standard, interfaces to IP (IPv4 and IPv6) and X.25 networks are supported.

GPRS also adds some more entries to the GSM registers. For MM, the user's entry in the HLR is extended with a link to its current SGSN. Moreover, their GPRS-specific profile and current PDP address(es) are stored. The Gr interface is used to exchange this information between HLR and SGSN. For example, the SGSN informs the HLR about the current location of the MS. When a MS registers with a new SGSN, the HLR will send the user profile to the new SGSN. In a similar manner, the signaling path between GGSN and HLR (Gc interface) may be used by the GGSN to query the location and profile of a user who is unknown to the GGSN.

In addition, the MSC/VLR may be extended with functions and register entries which allow efficient coordination between packet-switched (GPRS) and conventional circuit-switched GSM services. Examples for this are combined GPRS and GSM location updates and combined attachment procedures. Moreover, paging requests of circuit-switched GSM calls can be performed via the SGSN. For this purpose, the Gs interface connects the registers of SGSN and MSC/VLR.

Finally, it is worth mentioning that it is possible to exchange messages of the SMS via GPRS. The Gd interface interconnects SMS-GMSC with the SGSN.

8.1.2 Services

Bearer services and supplementary services

The bearer services of GPRS offer end-to-end packet switched data transfer to mobile subscribers. Currently, a Point-to-Point (PTP) service is specified, which comes in two variants: a connectionless mode (PTP Connectionless Network Service (PTP-CLNS), e.g. for IP) and a connection-oriented mode (PTP Connection Oriented Network Service (PTP-CONS), e.g. for X.25).

It is possible to use IP multicast routing protocols (see, e.g., Sahasrabuddhe and Mukherjee (2000)) over GPRS. Packets addressed to an IP multicast group will then be routed to all group members. Furthermore, SMS messages can be sent and received over GPRS.

Based on these standardized services, GPRS providers may offer additional nonstandardized services. Examples are access to information databases, messaging services (via store-and-forward mailboxes) and transaction services (e.g. credit card validations and electronic monitoring/surveillance systems). The most important application scenario, however, is the wireless access to the World Wide Web and to corporate intranets as well as e-mail communication.

Quality of service

The QoS requirements for the variety of mobile data applications, in which GPRS is used as transmission technology, are very diverse (for example, compare the requirements of real-time video conferencing with those of e-mail transfer with respect to packet delay and error-free transmission). Support of different QoS classes is therefore an important feature to support a broad variety of applications but still preserve radio and network resources in an efficient way. Moreover, QoS classes enable providers to offer different billing options. The billing can be based on the amount of transmitted data, the service type itself and the QoS profile. At the moment, four QoS parameters are defined in GPRS: service precedence, reliability, delay and throughput. Using these parameters, QoS profiles can be negotiated between the mobile user and the network for each session, depending on the QoS demand and the currently available resources.

The service precedence is the priority of a service (in relation to other services). There exist three levels of priority: high, normal and low. In the case of a heavy traffic load, for example, packets of low priority will be discarded first.

The reliability indicates the transmission characteristics required by an application. Three reliability classes are defined (see Table 8.1), which guarantee certain maximum values for the probability of packet loss, packet duplication, mis-sequencing and packet corruption (i.e. undetected error in a packet).

The delay parameters define maximum values for the mean delay and the 95th percentile delay (see Table 8.2). The latter is the maximum delay guaranteed in 95% of all transfers. Here, 'delay' is defined as the end-to-end transfer time between two communicating MSs or between a MS and the Gi interface to an external network, respectively. This includes all delays within the GPRS network, e.g., the delay for request and assignment of radio resources, transmission over the air interface and the transit delay in the GPRS backbone network. Delays outside the GPRS network, e.g. in external transit networks, are not taken

Table 8.1 Probability of various outcomes with the three reliability classes.

Class	Lost packet	Duplicated packet	Out of sequence packet	Corrupted packet
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

Table 8.2 Delay classes.

Class	128 byte packet		1024 byte packet	
	Mean delay (s)	95% delay (s)	Mean delay (s)	95% delay (s)
1	<0.5	<1.5	<2	<7
2	<5	<25	<15	<75
3	<50	<250	<75	<375
4	Best effort	Best effort	Best effort	Best effort

into account. Table 8.2 lists the four defined delay classes and their parameters for a 128 byte and 1024 byte packet, respectively.

Finally, the throughput parameter specifies the maximum/peak bit rate and the mean bit rate.

Simultaneous use of packet-switched and circuit-switched services

In a GSM/GPRS network, conventional circuit-switched services (GSM speech, data and SMS) and GPRS services can be used in parallel. The GPRS standard defines three classes of MSs: MSs of class A fully support simultaneous operation of GPRS and conventional GSM services. Class B MSs are able to register with the network for both GPRS and conventional GSM services simultaneously and listen to both types of signaling messages, but can only use one of the service types at a given time. Finally, class C MSs can attach for either GPRS or conventional GSM services at a given time. Simultaneous registration (and use) is not possible, except for SMS messages, which can be received and sent at any time.

8.1.3 Session management, mobility management and routing

In this section we describe how a MS registers with the GPRS network and becomes known to an external packet data network. We show how packets are routed to or from MSs, and how the network keeps track of the user's current location.

Attachment and detachment procedure

Before a MS can use GPRS services, it must attach to the network (similar to the IMSI attach used for circuit-switched GSM services). The MS's ATTACH REQUEST message is sent to

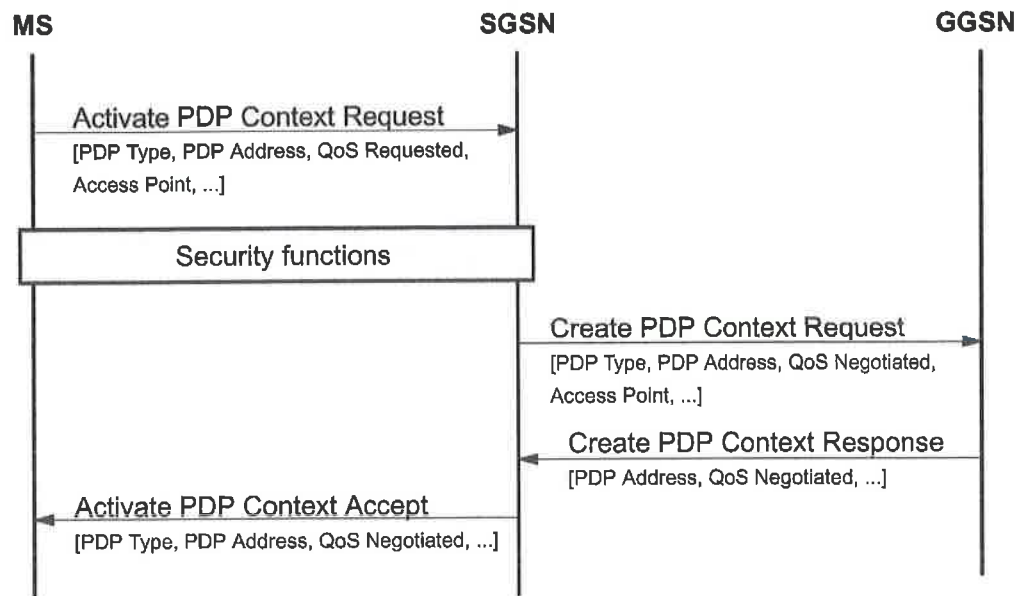


Figure 8.3 PDP context activation.

the SGSN. The network then checks whether the user is authorized, copies the user profile from the HLR to the SGSN, and assigns a Packet Temporary Mobile Subscriber Identity (P-TMSI) to the user. This procedure is called GPRS attach. For MSs using both circuit-switched and packet-switched services, it is possible to perform combined GPRS/IMSI attach procedures. The disconnection from the GPRS network is called GPRS detach. It can be initiated by the MS or by the network.

Session management and PDP context

To exchange data packets with external PDNs after a successful GPRS attach, a MS must apply for an address used in the PDN. In general, this address is called a PDP address. In case the PDN is an IP network, this will be an IP address.

For each session, a so-called PDP context is created, which describes the characteristics of the session. It contains the PDP type (e.g. IPv4), the PDP address assigned to the MS (e.g. an IP address), the requested QoS class and the address of a GGSN that serves as the access point to the external network. This context is stored in the MS, the SGSN and the GGSN. Once a MS has an active PDP context, it is 'visible' to the external network and can send and receive data packets. The mapping between the two addresses (PDP ↔ GSM address) makes the transfer of data packets between MS and GGSN possible.

The allocation of a PDP address can be static or dynamic. In the first case, the MS permanently owns a PDP address, which has been assigned by the network operator of the user's home PLMN. Using a dynamic addressing concept, a PDP address is assigned upon activation of a PDP context, i.e. each time a MS attaches to the network it will in general get a new PDP address, and after its GPRS detach this PDP address will again be available to other MSs. The PDP address can be assigned by the user's home-PLMN operator (dynamic

home-PLMN PDP address) or by the operator of the visited network (dynamic visited-PLMN PDP address). The GGSN is responsible for the allocation and deactivation of the addresses.

Figure 8.3 shows the PDP context activation procedure initialized by the MS. Using the message `ACTIVATE PDP CONTEXT REQUEST`, the MS informs the SGSN about the requested PDP context. If a dynamic address is requested, the parameter `PDP ADDRESS` will be left empty. Afterwards, the usual GSM security functions (e.g. authentication of the user) are performed. If access is granted, the SGSN will send a `CREATE PDP CONTEXT REQUEST` to the affected GGSN. The GGSN creates a new entry in its PDP context table, which enables the GGSN to route data packets between the SGSN and the external PDN. It confirms this to the SGSN with a message `CREATE PDP CONTEXT RESPONSE`, which also contains the dynamic PDP address (if needed). Finally, the SGSN updates its PDP context table and confirms the activation of the new PDP context to the MS (`ACTIVATE PDP CONTEXT ACCEPT`).

It is also worth mentioning that the GPRS standard supports anonymous PDP context activation, which is useful for special applications such as prepaid services. In such a session, the user (i.e. the IMSI) using the PDP context remains unknown to the network. Security functions as shown in Figure 8.3 are skipped. Only dynamic address allocation is possible in this case.

Routing

In Figure 8.2 we give an example of how packets can be routed in GPRS. We assume that the packet data network is an IP network.

A GPRS MS located in PLMN1 sends IP packets to a Web server connected to the Internet. The SGSN which the MS is registered with encapsulates the IP packets coming from the MS, examines the PDP context, and routes them through the GPRS backbone to the appropriate GGSN. The GGSN decapsulates the IP packets and sends them out on the IP network, where IP routing mechanisms transfer the packets to the access router of the destination network. The latter delivers the IP packets to the host.

Let us assume that the MS's home-PLMN is PLMN2 and that its IP address has been assigned from the PLMN2 address space – either in a dynamic or static way. When the Web server now addresses IP packets to the MS, they are routed to the GGSN of PLMN2 (the home-GGSN of the MS). This is because the MS's IP address has the same network prefix as the IP address of its home-GGSN. The GGSN queries the HLR and obtains the information that the MS is currently located in PLMN1. In the following, it encapsulates the incoming IP packets and tunnels them through the inter-PLMN GPRS backbone to the appropriate SGSN in PLMN1. The SGSN decapsulates the packets and delivers them to the MS.

Location management

As in circuit-switched GSM, the main task of location management is to keep track of the user's current location, so that incoming packets can be routed to their MS. For this purpose, the MS frequently sends location update messages to its SGSN.

How often should a MS send such a message? If it updates its current location (e.g. its cell) rather seldom, the network must perform a paging process in order to search the MS when packets are coming in. This will result in a significant delivery delay. On the other hand, if location updates happen very often, the MS's location is well known to the network

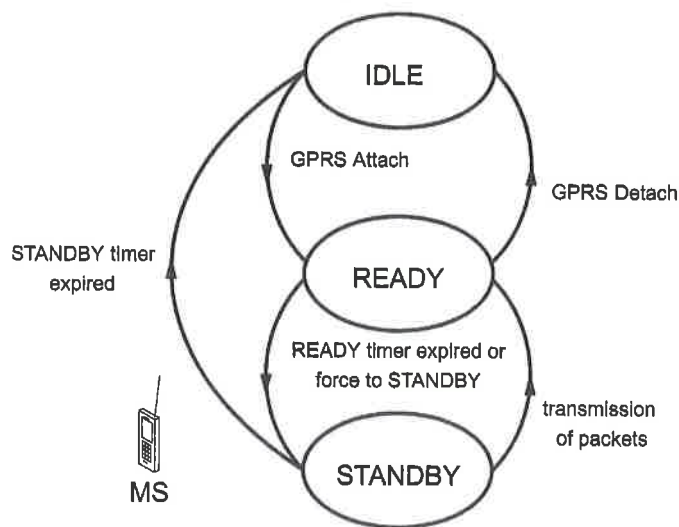


Figure 8.4 State model of a GPRS MS.

(and thus the packets can be delivered without any additional paging delay), but quite a lot of uplink radio bandwidth and battery power is used for MM in this case. Thus, a good location management strategy must be a compromise between these two extreme methods.

For this reason, a state model for GPRS MSs has been defined (shown in Figure 8.4). In IDLE state the MS is not reachable. Performing a GPRS attach, it turns into READY state. With a GPRS detach it may deregister from the network and fall back to IDLE state, and all PDP contexts will be deleted. The STANDBY state will be reached when a MS does not send any packets for a long period of time, and therefore the READY timer (which was started at GPRS attach and is reset for each incoming and outgoing transmission) expires. The location update frequency depends on the state in which the MS currently is. In IDLE state, no location updating is performed, i.e. the current location of the MS is unknown. If a MS is in READY state, it will inform its SGSN of every movement to a new cell. For the location management of a MS in STANDBY state, a GSM LA is divided into so-called Routing Areas (RAs). In general, an RA consists of several cells. The SGSN will only be informed, when a MS moves to a new RA; cell changes will not be indicated.

To find out the current cell of a MS that is in STANDBY state, paging of the MS within a certain RA must be performed (section 8.1.7). For MSs in READY state, no paging is necessary.

Whenever a MS moves to a new RA, it sends a ROUTING AREA UPDATE REQUEST to its assigned SGSN (Figure 8.5). The message contains the Routing Area Identity (RAI) of its old RA. The BSS adds the CI of the new cell to the request, from which the SGSN can derive the new RAI. Two different scenarios are possible:

- intra-SGSN routing area update (Figure 8.5);
- inter-SGSN routing area update (Figure 8.6).

In the Intra-SGSN case, the MS has moved to an RA which is assigned to the same SGSN as the old RA. In this case, the SGSN has already stored the necessary user profile and

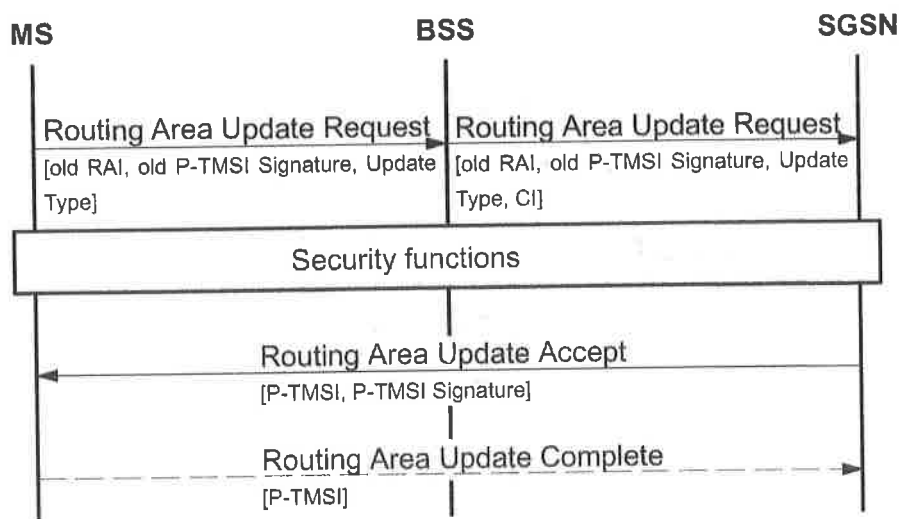


Figure 8.5 Intra-SGSN routing area update.

can immediately assign a new P-TMSI (ROUTING AREA UPDATE ACCEPT). Since the routing context does not change, there is no need to inform other network elements, such as GGSN or HLR.

In the inter-SGSN case, the new RA is administered by a different SGSN than the old RA. The new SGSN realizes that the MS has entered its area and requests the old SGSN to send the PDP contexts of the user (SGSN CONTEXT REQUEST, SGSN CONTEXT RESPONSE, SGSN CONTEXT ACKNOWLEDGE). Afterward, the new SGSN informs the involved GGSNs about the user's new routing context (UPDATE PDP CONTEXT REQUEST, UPDATE PDP CONTEXT RESPONSE). In addition, the HLR and (if needed) the MSC/VLR are informed about the user's new SGSN number (UPDATE LOCATION, ..., UPDATE LOCATION ACKNOWLEDGE; LOCATION UPDATE REQUEST, LOCATION UPDATE ACCEPT).

In addition to pure RA updates, there also exist combined RA/LA updates. They are performed whenever a MS using GPRS as well as conventional GSM services moves to a new LA. The MS sends a ROUTING AREA UPDATE REQUEST to the SGSN and uses a parameter update type to indicate that an LA update is needed. The message is then forwarded from the SGSN to the VLR.

To sum up, we can say that GPRS mobility management consists – as with GSM mobility management – of two levels: micro mobility management tracks the current RA or cell of the user; macro mobility management keeps track of the user's current SGSN and stores it in the HLR, VLR and GGSN.

8.1.4 Protocol architecture

Transmission plane

Figure 8.7 illustrates the protocol architecture of the GPRS transmission plane. The protocols offer transmission of user data and its associated signaling (e.g. for flow control, error

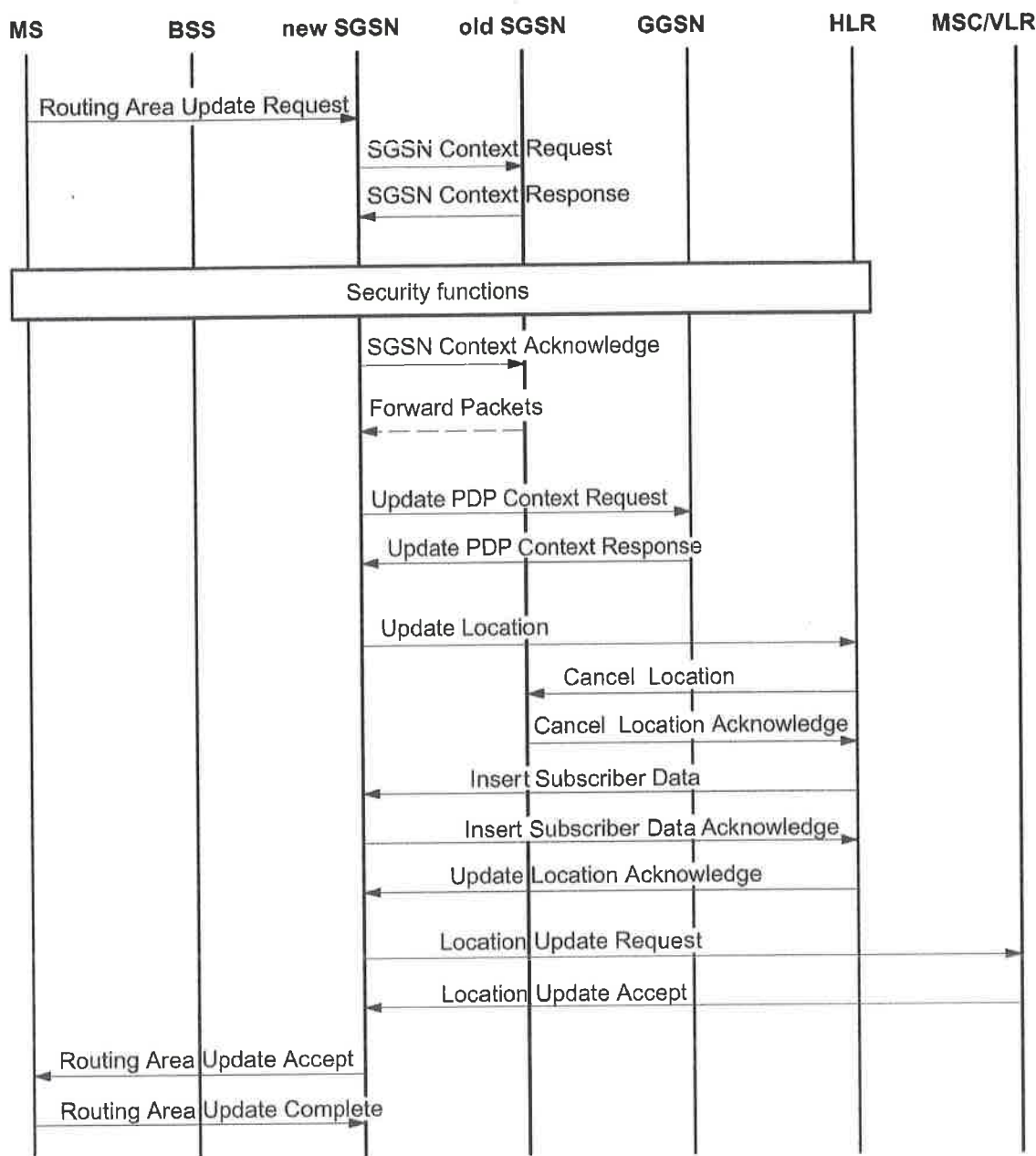


Figure 8.6 Inter-SGSN routing area update.

detection and error correction). An application running in the GPRS-MS (e.g. a browser) uses IP or X.25 in the network layer.

GPRS backbone: SGSN-GGSN. As mentioned earlier in this chapter, IP and X.25 packets are transmitted encapsulated within the GPRS backbone network. This is done using the GTP, i.e. GTP packets carry the user's IP or X.25 packets. GTP is defined both between

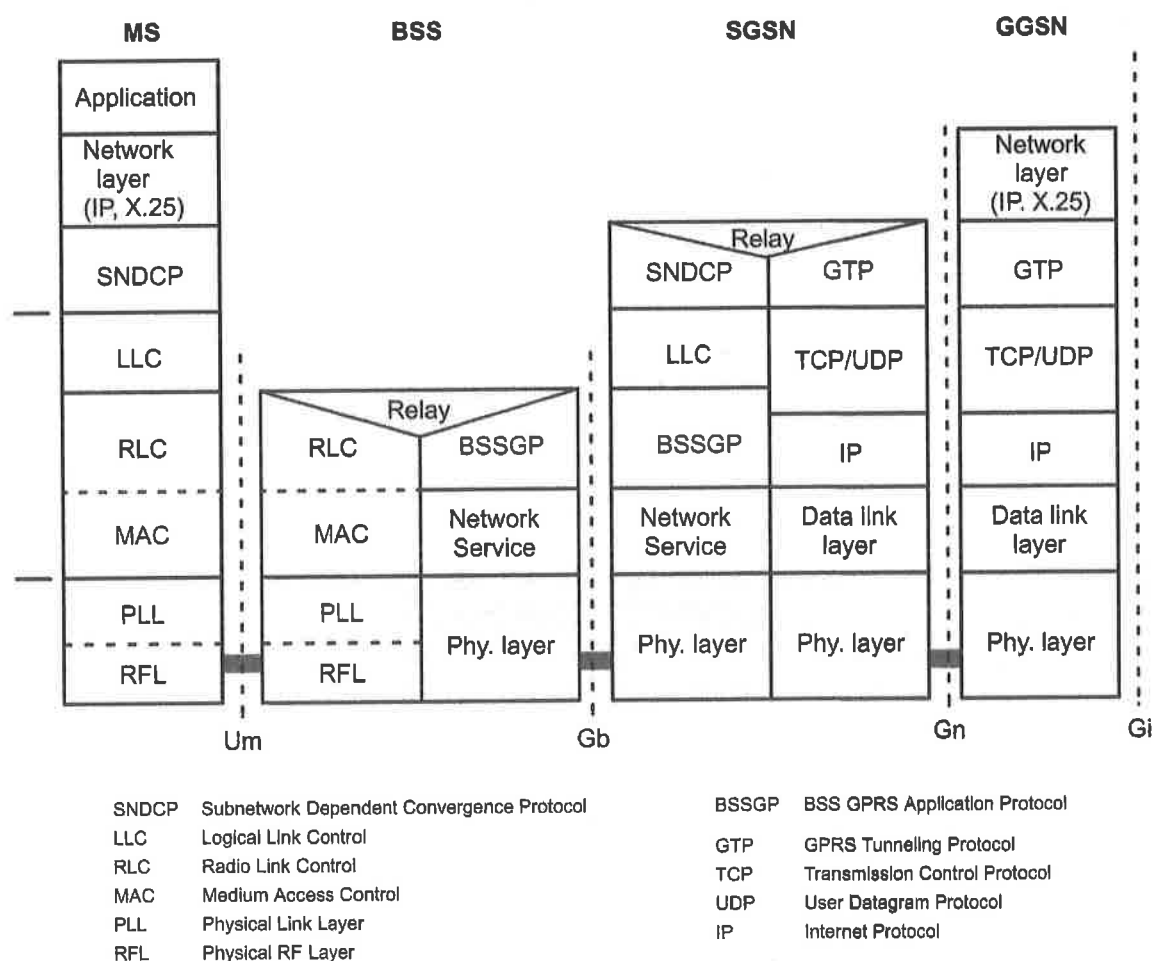


Figure 8.7 Protocol architecture: transmission plane.

GSNs within the same PLMN (Gn interface) and between GSNs of different PLMNs (Gp interface).

GTP contains procedures in the transmission plane as well as in the signaling plane. In the transmission plane, GTP employs a tunnel mechanism to transfer user data packets. In the signaling plane, GTP specifies a tunnel control and management protocol. The signaling is used to create, modify and delete tunnels. A Tunnel Identifier (TID), which is composed of the IMSI of the user and a Network Layer Service Access Point Identifier (NSAPI), uniquely indicates a PDP context. Below GTP, the standard protocols Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) are employed to transport the GTP packets within the backbone network. TCP is used for X.25 (since X.25 expects a reliable end-to-end connection) and UDP is used for access to IP-based networks (which do not expect reliability in the network layer or below). In the network layer, IP is employed to route the packets through the backbone. Ethernet, ISDN or Asynchronous Transfer Mode (ATM)-based protocols may be used below IP. To summarize, in the GPRS backbone we have an IP/X.25-over-GTP-over-UDP/TCP-over-IP protocol architecture.

Air interface. In the following we consider the air interface (Um) between MS and BSS or SGSN, respectively.

Subnetwork dependent convergence protocol. The Subnetwork Dependent Convergence Protocol (SNDCP) is used to transfer packets of the network layer (IP and X.25 packets) between the MSs and their SGSN. Its functionality includes:

- multiplexing of several PDP contexts of the network layer onto one virtual logical connection of the underlying Logical Link Control (LLC) layer; and
- segmentation of network layer packets onto one frame of the underlying LLC layer and reassembly on the receiver side.

Moreover, SNDCP offers compression and decompression of user data and redundant header information (e.g. TCP/IP header compression).

Data link layer. The data link layer is divided into two sublayers:

- LLC layer (between MS and SGSN); and
- RLC/Medium Access Control (MAC) layer (between MS and BSS).

The LLC layer provides a reliable logical link between a MS and its assigned SGSN. Its functionality is based on the LAPDm protocol (which is a protocol similar to HDLC and has been explained in section 5.3.1). LLC includes in-order delivery, flow control, error detection, retransmission of packets (ARQ) and ciphering functions. It supports variable frame lengths and different QoS classes, and besides point-to-point also point-to-multipoint transfer is possible. A logical link is uniquely addressed with a Temporary Logical Link Identifier (TLLI). Within one RA the mapping between TLLI and IMSI is unique. However, the user's identity remains confidential, since the TLLI is derived from the P-TMSI of the user.

The RLC/MAC layer has two functions. The purpose of the RLC layer is to establish a reliable link between the MS and the BSS. This includes the segmentation and reassembly of LLC frames into RLC data blocks and ARQ of uncorrectable blocks. The MAC layer controls the access attempts of MSs on the radio channel. It is based on a slotted-aloha principle (section 4.1). The MAC layer employs algorithms for contention resolution of access attempts, statistical multiplexing of channels and a scheduling and prioritizing scheme, which takes into account the negotiated QoS. On the one hand, the MAC protocol allows that a single MS simultaneously uses several physical channels (several time slots of the same TDMA frame). On the other hand, it also controls the statistical multiplexing, i.e. it controls how several MSs can access the same physical channel (the same time slot of successive TDMA frames). This is explained in more detail in section 8.1.7.

Physical layer. The physical layer between MS and BSS can be divided into the two sublayers: Physical Link Layer (PLL) and Physical RF Layer (RFL). The PLL provides a physical channel between the MS and the BSS. Its tasks include channel coding (i.e. detection of transmission errors, forward error correction and indication of uncorrectable codewords),

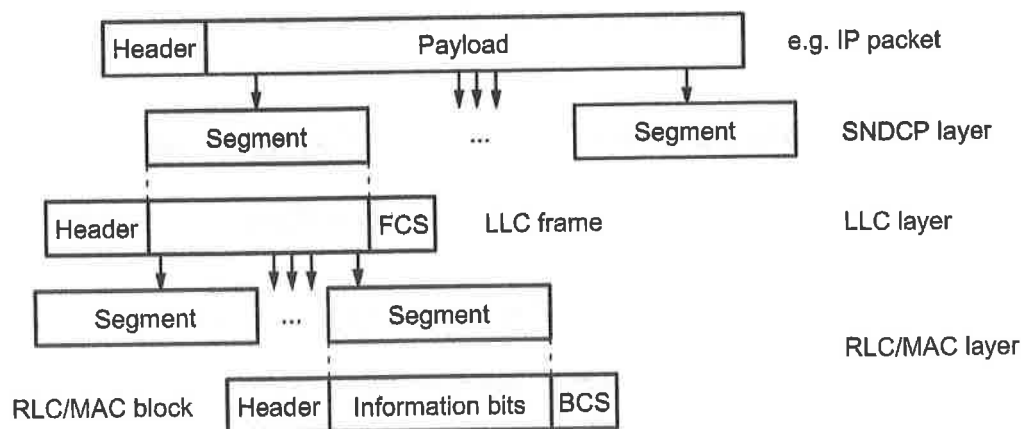


Figure 8.8 Data flow and segmentation between the protocol layers in the MS.

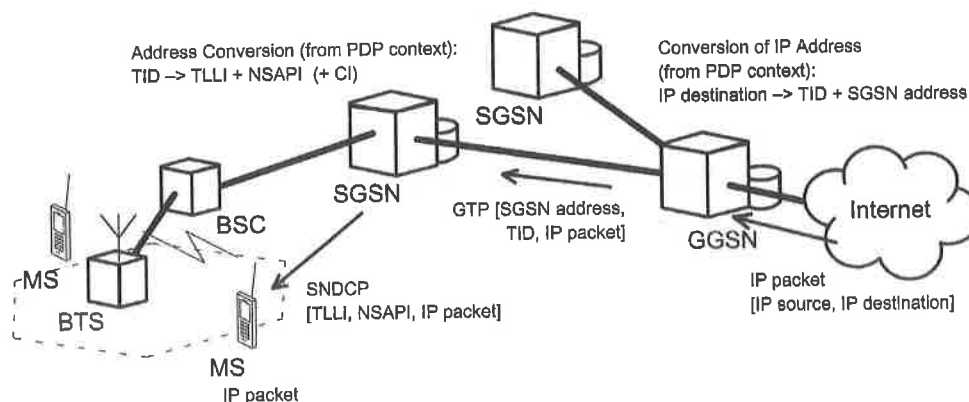
interleaving and detection of physical link congestion. The RFL, which operates below the PLL, includes modulation and demodulation.

To summarize this section, Figure 8.8 illustrates the data flow between the protocol layers in the MS. Packets of the network layer (e.g. IP packets) are passed down to the SNDCP layer, where they are segmented to LLC frames. After adding header information and a Frame Check Sequence (FCS) for error protection, these frames are segmented into one or several RLC data blocks. Those are then passed down to the MAC layer. One RLC/MAC block contains a MAC and RLC header, the RLC payload ('information bits') and a Block Check Sequence (BCS) at the end. The channel coding of RLC/MAC blocks and the mapping to a burst in the physical layer are explained in section 8.1.7.

BSS–SGSN interface. At the Gb interface, the BSS GPRS Application Protocol (BSSGP) is defined on Layer 3. It is derived from the BSSMAP, which has been explained in section 5.3.1. The BSSGP delivers routing and QoS-related information between BSS and SGSN. The underlying Network Service (NS) protocol is based on the frame relay protocol.

Routing and conversion of addresses

Now we explain the routing example of section 8.1.3 in detail. Figure 8.9 roughly illustrates the transfer of an incoming IP packet. It arrives at the GGSN, is then routed through the GPRS backbone to the responsible SGSN and finally to the MS. Using the PDP context, the GGSN determines from the IP destination address a TID and the IP address of the relevant SGSN. Between GGSN and the SGSN, the GTP is employed. The SGSN derives the TLLI from the TID and finally transfers the IP packet to the MS. The so-called NSAPI is part of the TID. It maps a given IP address to the corresponding PDP context. An NSAPI/TLLI pair is unique within one RA. Figure 8.10 gives a similar example with an outgoing (mobile originated) IP packet.

**Addresses:**

IP Destination address
 TID Tunnel Identifier
 SGSN Address IP Address of SGSN

TLLI Temporary Logical Link Identity
 NSAPI Network Layer Service Access Point Identifier
 CI Cell Identifier

Figure 8.9 Routing and address conversion: incoming IP packet (mobile-terminated data transfer).

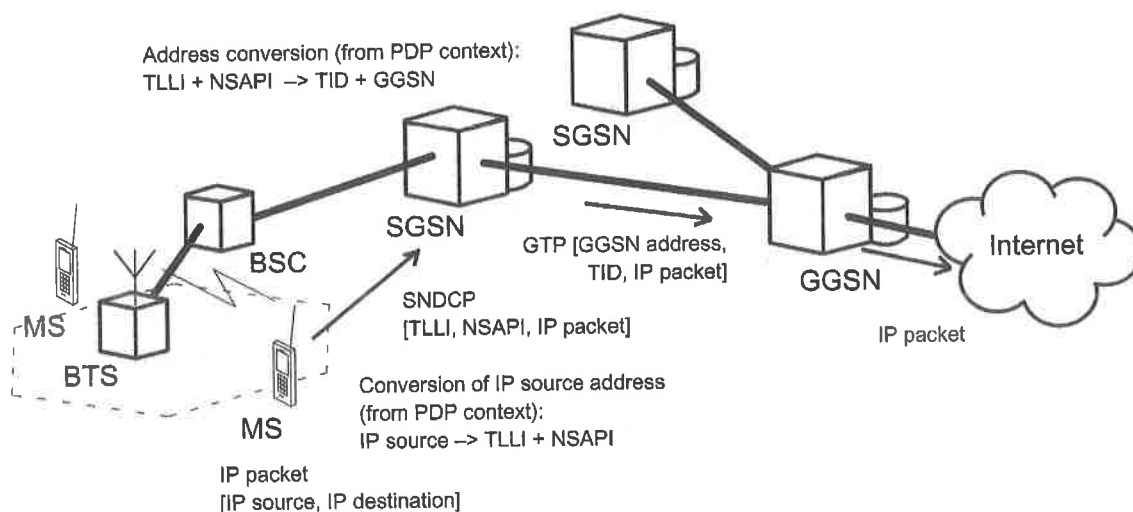


Figure 8.10 Routing and address conversion: outgoing IP packet (mobile-originated data transfer).

8.1.5 Signaling plane

The protocol architecture of the signaling plane comprises protocols for control and support of the functions of the transmission plane, e.g., for the execution of GPRS attach and detach, PDP context activation, the control of routing paths and the allocation of network resources.

Between MS and SGSN (Figure 8.11), the GPRS Mobility Management and Session Management (GMM/SM) protocol is responsible for mobility and session management.

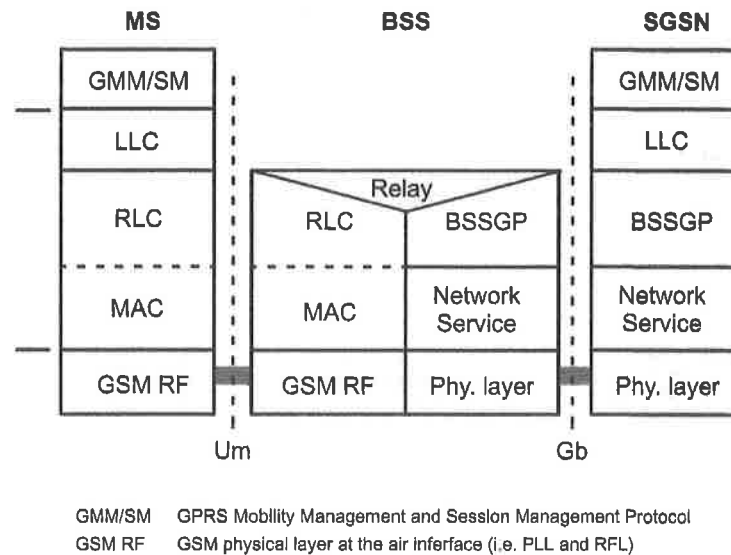


Figure 8.11 Signaling plane: MS-SGSN.

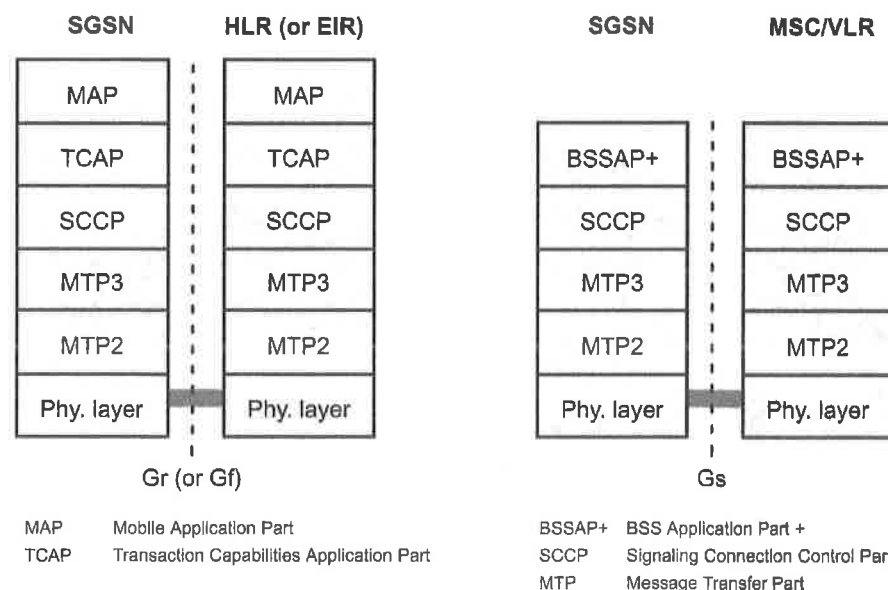


Figure 8.12 Signaling plane: SGSN-HLR, SGSN-EIR and SGSN-MSC/VLR.

It includes functions for GPRS attach/detach, PDP context activation, routing area updates and security procedures.

The signaling architecture between SGSN and the registers HLR, VLR and EIR (Figure 8.12) uses protocols known from conventional GSM (section 5.3) and partly extends them with GPRS-specific functionality. Between SGSN and HLR as well as between SGSN and EIR, an enhanced MAP is employed. The exchange of MAP messages is accomplished over the TCAP, the SCCP and the MTP.

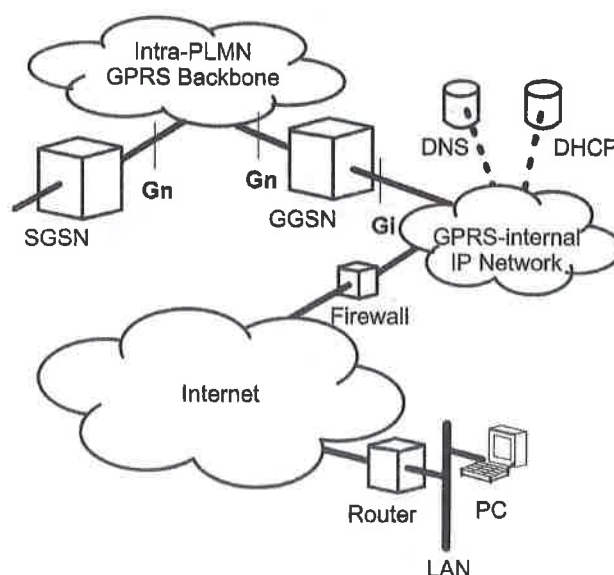


Figure 8.13 GPRS-Internet interconnection.

The BSS Application Part (BSSAP+) includes functions of GSM's BSSAP. It is applied to transfer signaling information between the SGSN and the VLR (Gs interface). This includes, in particular, signaling of the mobility management when coordination of GPRS and conventional GSM functions is necessary (e.g. for combined GPRS and nonGPRS location update, combined GPRS/IMSI attach or paging of a MS via GPRS for an incoming GSM call).

8.1.6 Interworking with IP networks

Figure 8.13 gives an example of how a GPRS network is interconnected with the Internet. From outside, i.e. from an external IP network's point of view, the GPRS network looks like any other IP subnetwork and the GGSN looks like a usual IP router.

As explained in section 8.1.3, each MS obtains an IP address after its GPRS attach, which is valid for the duration of the session. The network provider has reserved a certain number of IP addresses, and can dynamically assign these addresses to active MSs. To do so, the network provider may install a Dynamic Host Configuration Protocol (DHCP) server in its network. This server automatically manages the available address space. The address resolution between IP address and GSM address is performed by the GGSN, using the appropriate PDP context. The routing of IP packets and the tunneling through the intra-PLMN backbone (using GTP) has been explained in sections 8.1.1, 8.1.3 and 8.1.4.

Moreover, a Domain Name Server (DNS) is used to map between IP addresses and host names. To protect the PLMN from unauthorized access, a firewall is installed between the private GPRS network and the external IP network.

With this configuration, GPRS can be seen as a wireless extension of the Internet all the way to a MS. The mobile user has direct connection to the Internet.

8.1.7 Air interface

The enhanced air interface of GPRS offers higher data rates and a packet-oriented transmission. It is therefore considered one of the key aspects in GPRS. In this section, we explain how several MSs can share one physical channel (multiple access) and how the assignment of radio resources between circuit-switched GSM services and GPRS services is controlled. Afterwards, the logical channels and their mapping onto physical channels (using multiframe) is presented. Finally, GPRS channel coding concludes this chapter.

Multiple access and radio resource management

On the physical layer, GPRS uses the GSM combination of FDMA and TDMA with eight time slots per TDMA frame (as explained in section 4.2.2). However, several new methods are used for channel allocation and multiple access. They have a significant impact on the performance of GPRS.

In circuit-switched GSM, a physical channel (i.e. one time slot of successive TDMA frames) is permanently allocated for a particular MS during the entire call period (no matter whether data are transmitted or not). Moreover, it is assigned in the uplink as well as in the downlink.

GPRS enables a far more flexible resource allocation scheme for packet transmission. A GPRS MS can transmit on several of the eight time slots within the same TDMA frame (multislot operation). The number of time slots which a MS is able to use is called a multislot class. In addition, uplink and downlink are allocated separately, which saves radio resources, especially for asymmetric traffic (e.g. Web browsing).

A cell supporting GPRS must allocate physical channels for GPRS traffic. In other words, the radio resources of a cell are shared by all MSs (GSM and GPRS) located in this cell. The mapping of physical channels to either GPRS or circuit-switched GSM services can be performed in a dynamic way. A physical channel which has been allocated for GPRS transmission is denoted as a Packet Data Channel (PDCH). The number of PDCHs can be adjusted according to the current traffic demand (capacity on demand principle). For example, physical channels not currently in use by GSM calls can be allocated as PDCHs for GPRS to increase the QoS for GPRS. When there is a resource demand for GSM calls, PDCHs may be deallocated.

As already mentioned, physical channels for packet-switched transmission (PDCHs) are only allocated for a particular MS when this MS sends or receives data packets, and they are released after the transmission. With this dynamic channel allocation principle, multiple MSs can share one physical channel. For bursty traffic this results in a much more efficient usage of the radio resources.

The channel allocation is controlled by the BSC. To prevent collisions, the network indicates which channels are currently available in the downlink. An Uplink State Flag (USF) in the header of downlink packets shows which MS is allowed to use this channel in the uplink. The allocation of PDCHs to a MS also depends on its multislot class and the QoS of the session.

Table 8.3 Logical channels in GPRS.

Group		Channel	Function	Direction
Traffic channels	Packet data	PDTCH	Packet data	MS ↔ BSS
	traffic channel		traffic	
Signaling channels	Packet broadcast control channel	PBCCH	Packet broadcast control	MS ← BSS
	Packet common control channel (PCCCH)	PRACH	Packet random access	MS → BSS
		PAGCH	Packet access grant	MS ← BSS
		PPCH	Packet paging	MS ← BSS
		PNCH	Packet notification	MS ← BSS
	Packet dedicated control channels	PACCH	Packet associated control	MS ↔ BSS
		PTCCH	Packet timing advance control	MS ↔ BSS

Logical channels

Table 8.3 lists the packet data logical channels defined in GPRS. As with logical channels in conventional GSM, they can be divided into two categories: traffic channels and signaling (control) channels. The signaling channels can further be divided into packet broadcast control, packet common control, and packet dedicated control channels.

The Packet Data Traffic Channel (PDTCH) is employed for the transfer of user data. It is assigned to one MS (or, in the case of PTM, to multiple MSs). One MS can use several PDTCHs simultaneously.

The Packet Broadcast Control Channel (PBCCH) is a unidirectional point-to-multipoint signaling channel from the BSS to the MSs. It is used by the BSS to broadcast information about the organization of the GPRS radio network to all GPRS MSs of a cell. In addition to system information about GPRS, the PBCCH should also broadcast important system information about circuit-switched services, so that a GSM/GPRS MS does not need to listen to the BCCH.

The Packet Common Control Channel (PCCCH) transports signaling information for functions of the network access management, i.e. for allocation of radio channels, medium access control and paging. Four sub-channels are defined:

- the Packet Random Access Channel (PRACH) is used by the MSs to request one or more PDTCH;
- the Packet Access Grant Channel (PAGCH) is used to allocate one or more PDTCH to a MS;
- the Packet Paging Channel (PPCH) is used by the BSS to find the location of a MS (paging) prior to downlink packet transmission;
- the Packet Notification Channel (PNCH) is used to inform MSs of incoming PTM messages.

Figure 8.14 shows the principle of the uplink channel allocation (mobile-originated packet transfer). A MS requests a channel by sending a `PACKET CHANNEL REQUEST` on the

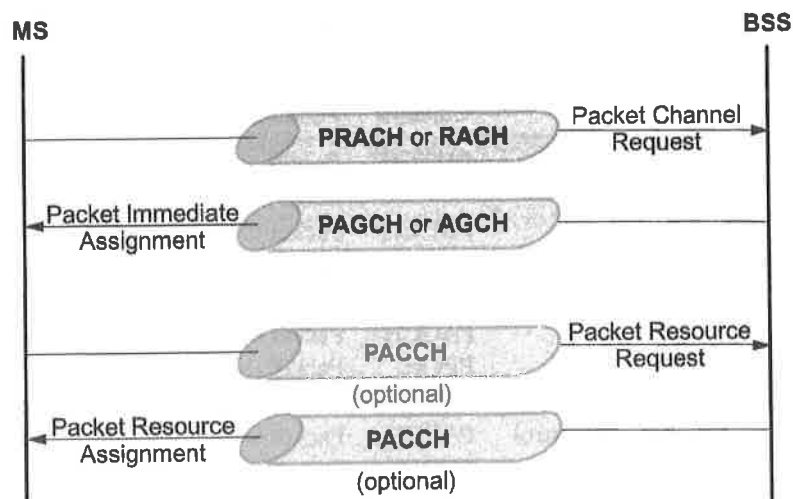


Figure 8.14 Uplink channel allocation (mobile-originated packet transfer).

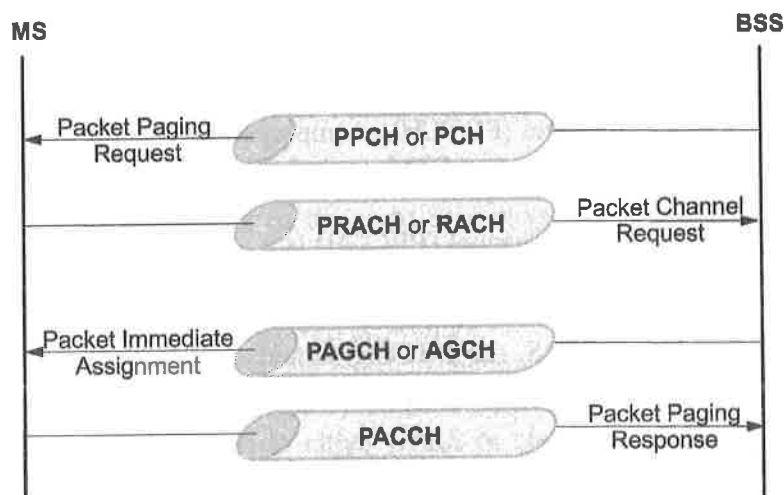


Figure 8.15 Paging (mobile-terminated packet transfer).

PRACH or RACH. The BSS answers on the PAGCH or AGCH, respectively. Once the PACKET CHANNEL REQUEST is successful, a so-called Temporary Block Flow (TBF) is established. With that, resources (e.g. PDTCH and buffers) are allocated for the MS, and data transmission can start. During transfer, the USF in the header of downlink blocks indicates to other MSs that this uplink PDTCH is already in use. On the receiver side, a Temporary Flow Identifier (TFI) helps to reassemble the packet. Once all data has been transmitted, the TBF and the resources are released again. Figure 8.15 illustrates the paging procedure of a mobile station (mobile-terminated packet transfer).

The packet dedicated control channel is a bidirectional point-to-point signaling channel. It contains the following channels.

Table 8.4 Logical channels in GPRS.

Channel type	Net data throughput (kbit/s)	Block length (bits)	Block distance (ms)
PDTCH (CS-1)	9.05	181	—
PDTCH (CS-2)	13.4	268	—
PDTCH (CS-3)	15.6	312	—
PDTCH (CS-4)	21.4	428	—
PACCH	Changes dynamically		
PBCCH	$s \times 181/120$	181	120
PAGCH	Changes dynamically	181	—
PNCH	Changes dynamically	181	—
PPCH	Changes dynamically	181	—
PRACH (8 bit Access burst)	Changes dynamically	8	—
PRACH (11 bit Access burst)	Changes dynamically	11	—

- The Packet Associated Control Channel (PACCH) is always allocated in combination with one or more PDTCH. It transports signaling information related to one specific MS (e.g. power control information).
- The Packet Timing Advance Control Channel (PTCCH) is used for adaptive frame synchronization. The MS sends over the uplink part of the PTCCH, the PTCCH/U, ABs to the BTS. From the delay of these bursts, the correct value for the TA can be derived; see section 4.3.2. This value is then transmitted in the downlink part, the PTCCH/D, to inform the MS.

Coordination between circuit-switched and packet-switched logical channels is also possible here. If the PCCCH is not available in a cell, a GPRS MS can use the CCCH of circuit-switched GSM to initiate the packet transfer. Moreover, if the PBCCH is not available, it can obtain the necessary system information via the BCCH.

Table 8.4 lists the block lengths and net data throughput of the logical GPRS channels (compare with Table 4.2). Four different coding schemes (CS-1 to CS-4) are defined for data transmission on the PDTCH. They are explained in section 8.1.7.

As with circuit-switched GSM, the GPRS logical channels can be used in certain combinations only. The allowed combinations for multiplexing logical channels onto physical channels are shown in Table 8.5. Moreover, Table 8.6 shows the channel configurations which a GPRS MS can use (dependent on its state). Combination M9 represents a MS in an IDLE state waiting for incoming packets. Combination M10 is a transmitting MS with multislots capabilities. Several PDTCHs are assigned to a single MS, where n denotes the number of PDTCHs which allow bidirectional transmission, and m denotes the number of PDTCHs which allow only unidirectional transmission. We have: $n = 1, \dots, 8$, $m = 0, \dots, 8$ and $n + m = 1, \dots, 8$.

Table 8.5 Combinations of logical GPRS channels.

	B10	B11	B12	B13
PDTCH				
PBCCH				
PCCCH				
PACCH				
PTCCH				

Table 8.6 Channel combinations used by the MS.

	M9	M10
PDTCH		<i>n+m</i>
PBCCH		
PCCCH		
PACCH		
PTCCH		

Mapping of packet data logical channels onto physical channels

From section 4.4 we know that the mapping of logical GSM channels onto physical channels has two components: mapping in frequency and mapping in time. The mapping in frequency is based on the TDMA frame number and the frequencies allocated to the BTS and the MS. The mapping in time is based on the definition of complex multiframe structures on top of the TDMA frames.

A multiframe structure for PDCHs consisting of 52 TDMA frames (each with eight time slots) is shown in Figure 8.16. The corresponding time slots of a PDCH of four consecutive TDMA frames form one radio block (blocks B0–B11). Two TDMA frames are reserved for transmission of the PTCCH, and the remaining two frames are IDLE frames. A multiframe has thus a duration of approximately 240 ms (52×4.615 ms). A radio block consists of 456 bits.

The mapping of the logical channels onto the blocks B0–B11 of the multiframe can vary from block to block and is controlled by parameters which are broadcast on the PBCCH. The GPRS recommendations define which time slots may be used by a logical channel.

In addition to the 52-multiframe structure, which can be used by all logical GPRS channels, a 51-multiframe structure is also defined. It is used for PDCHs carrying only the logical channels PCCCH and PBCCH (channel combination B13 in Table 8.5). In the downlink, it consists of 10 blocks each of 4 frames (B0–B9) and 10 IDLE frames. In the uplink, it has 51 random access frames. Its duration is 235.4 ms.

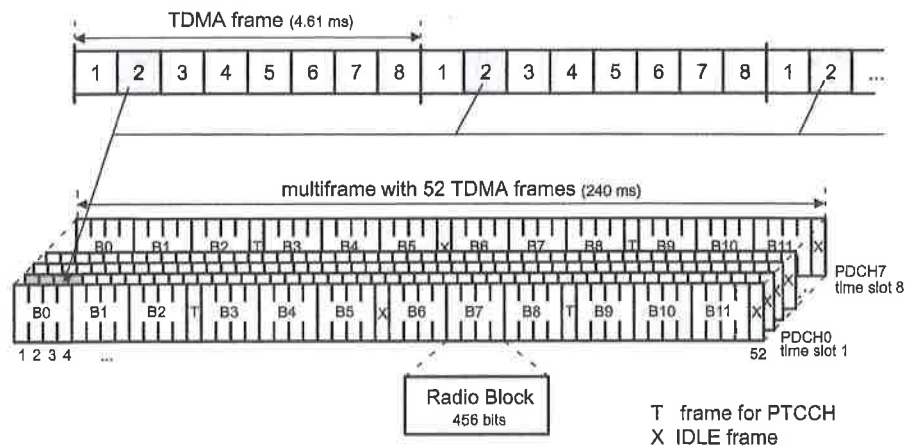


Figure 8.16 Multiframe structure with 52 TDMA frames.

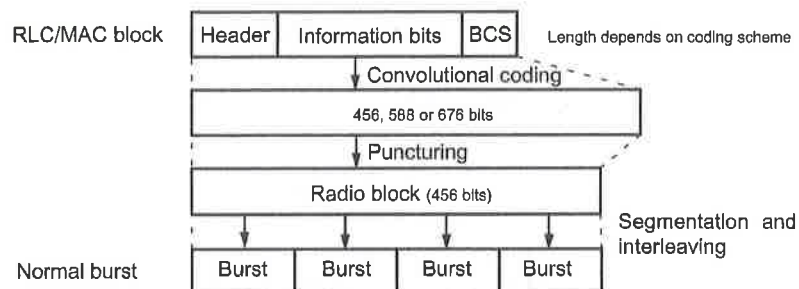


Figure 8.17 Physical layer at the air interface: channel coding, interleaving and formation of bursts (continued from Figure 8.8).

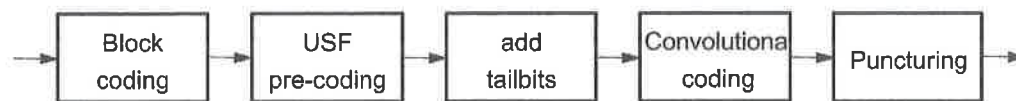


Figure 8.18 Encoding of GPRS data blocks.

Channel coding

Figure 8.17 shows how a block of the RLC/MAC layer (compare with Figure 8.8) is encoded and mapped onto four bursts. Channel coding is used to protect the transmitted data packets against errors and perform forward error correction. The channel coding technique in GPRS is quite similar to that employed in conventional GSM. An outer block coding, an inner convolutional coding and an interleaving scheme are used (Figure 4.29).

Four coding schemes with different code rates are defined. Their parameters are listed in Table 8.7. For each scheme, a block of 456 bits results after encoding. Figure 8.18 illustrates the encoding process, which is briefly explained in the following.

Table 8.7 Channel coding schemes for the traffic channels in GPRS.

Coding scheme	Pre-encoded USF	Infobits without USF and BCS	Parity bits BCS	Tail bits	Output convolutional encoder	Punctured bits	Code rate	Data rate (kbit/s)
CS-1	3	181	40	4	456	0	1/2	9.05
CS-2	6	268	16	4	588	132	$\approx 2/3$	13.4
CS-3	6	312	16	4	676	220	$\approx 3/4$	15.6
CS-4	12	428	16	–	456	–	1	21.4

Let us employ coding scheme CS-2. First of all, the 271 information bits of an RLC/MAC block (268 bits plus 3 bits USF; Table 8.4) are mapped to 287 bits using a systematic block encoder, i.e. 16 parity bits are added. These parity bits are denoted as a BCS. The USF pre-encoding maps the first 3 bits of the block (i.e. the USF) to 6 bits in a systematic way. Afterwards, 4 zero bits (tail bits) are added at the end of the entire block. The tail bits are needed for the termination of the subsequent convolutional coding.

For the convolutional coding, a nonsystematic rate-1/2 encoder with memory 4 is used, which is defined by the generator polynomials

$$G_0(d) = 1 + d^3 + d^4,$$

$$G_1(d) = 1 + d + d^3 + d^4.$$

This is the same encoder as used in conventional GSM. A possible encoder realization is shown in Figure 4.32. At the output of the convolutional encoder a codeword of length 588 bits results. Following this, 132 bits are punctured, resulting in a radio block of length 456 bits. Thus, we obtain a code rate of the convolutional encoder (including the puncturing) of

$$r = \frac{6 + 268 + 16 + 4}{456} \approx \frac{2}{3}.$$

Coding scheme CS-1 is equivalent to the coding of the SACCH. A systematic fire code is used for block coding (see section 4.8.1, first paragraph). There is no pre-coding of the USF bits. The convolutional coding is performed with the known rate-1/2 encoder, however, this time the output sequence is not punctured. Using CS-4, the 3 USF bits are mapped to 12 bits, and no convolutional coding is applied.

For the coding of the traffic channels (PDTCH), one of the four coding schemes is chosen, depending on the quality of the signal. The two SFs in a NB (Figure 4.7) are used to indicate which coding scheme is used. Under very bad channel conditions, CS-1 yields a data rate of only 9.05 kbit/s per time slot, but a very reliable coding. Under good channel conditions, convolutional coding is skipped (CS-4), and we achieve a data rate of 21.4 kbit/s per time slot. Thus, we obtain a theoretical maximum data rate of 171.2 kbit/s per TDMA frame. In practice, multiple users share the time slots and, thus, a much lower bit rate is available to the individual user. Moreover, the quality of the radio channel will not always allow us to use CS-4 (or CS-4 is not supported by the mobile terminal or by the network operator). The data rate available to the user depends (among other things) on the current total traffic load in the cell (i.e. the number of users and their traffic characteristics), the used coding scheme,

and the multislot class of the MS. Data rates between 10 and 50 kbit/s are realistic values. A simulative study on GPRS performance can be found in Kalden *et al.* (2000).

After encoding, the codewords are input into a block interleaver of depth 4. For all coding schemes, the interleaving scheme known from the interleaving of the SACCH (see section 4.8.3, last paragraph) is employed. On the receiver side, the codewords are deinterleaved. As in GSM, the decoding is performed using the Viterbi algorithm.

The signaling channels are encoded using CS-1. An exception is the PRACH. It can transmit two very short bursts, one burst with 8 information bits and one burst with 11 information bits. The coding for the 8-bit burst is the one used for the RACH (see sections 4.8.1 and 4.8.2) and the coding for the 11-bit burst is a punctured version of it.

8.1.8 Authentication and ciphering

The security principles inside the GPRS network are almost equivalent to those used in conventional GSM (section 5.6). Security functions in the GPRS network:

- protect against unauthorized use of services (by authentication and service request validation);
- provide data confidentiality (using ciphering); and
- provide confidentiality of the subscriber identity.

As in GSM, two keys are used: the subscriber authentication key K_i and the cipher key K_c . The main difference is that the SGSN, not the MSC, which handles authentication. Moreover, a special GPRS ciphering algorithm (A5) has been defined, which is optimized for encryption of packet data.

User authentication

Figures 8.19 and 8.20 illustrate the GPRS authentication process. The standard GSM algorithms are used to generate security data. The algorithm A3 calculates the signature response (SRES) from the subscriber authentication key (K_i) and a random number (RAND).

If the SGSN does not have authentication sets for a user (K_c , RAND, SRES), it requests them from the HLR by sending a message SEND AUTHENTICATION INFO. The HLR responds with a SEND AUTHENTICATION INFO ACK which includes the security data. Now, the SGSN offers a random number RAND to the MS (AUTHENTICATION AND CIPHERING REQUEST). The MS calculates SRES and transmits it back to the SGSN (AUTHENTICATION AND CIPHERING RESPONSE). If the SRES of the MS is equal to the SRES calculated (or maintained) by the SGSN, the user is authenticated and is allowed to use the network.

Ciphering

The ciphering functionality is performed in the LLC layer between MS and SGSN (see Figures 8.7 and 8.11). Thus, the ciphering scope reaches from the MS all the way to the SGSN (and vice versa), whereas in conventional GSM the scope is only between MS and BTS/BSC.

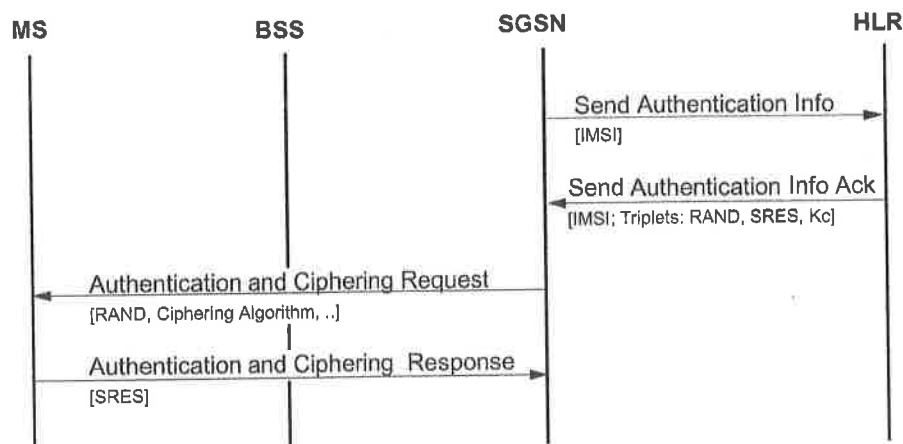


Figure 8.19 Subscriber authentication in GPRS.

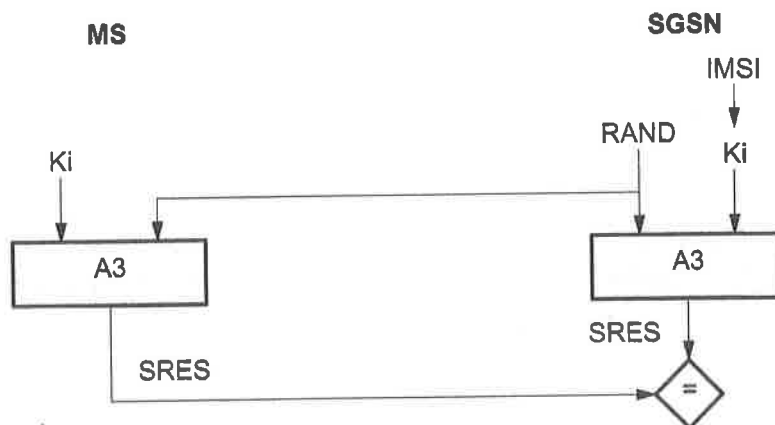


Figure 8.20 Principle of subscriber authentication in GPRS.

As in GSM ciphering, the algorithm A8 generates the cipher key Kc from the key Ki and a random number RAND (see Figure 5.53). Kc is then used by the GPRS Encryption Algorithm (GEA) for data encryption (algorithm A5). Note that the key Kc which is handled by the SGSN is independent of the key Kc handled by the MSC for conventional GSM services. A MS may thus have more than one Kc key.

The MS and the SGSN start ciphering after the message AUTHENTICATION AND CIPHERING RESPONSE is sent or received, respectively. Afterwards, GPRS user data and signaling during data transfer are transmitted in an encrypted manner.

Subscriber identity confidentiality

As in GSM, the identity of the subscriber is confidential. This is done by using temporary identities on the radio channel. In particular, the user's IMSI is not transmitted unencrypted, instead a Packet Temporary Mobile Subscriber Identity (P-TMSI) is assigned to each user by the SGSN. This address is temporary and is only valid and unique in the service area of this

SGSN. From the P-TMSI, a TLLI can be derived. The mapping between these temporary identities and the IMSI is stored only in the MS and in the SGSN.

8.1.9 Summary of GPRS

GPRS has been an important step in the evolution of cellular networks towards 3G and mobile Internet. Its packet-oriented transmission technology enables efficient and simplified wireless access to IP networks.

GPRS extends the existing GSM infrastructure in particular with two network nodes, namely the SGSN and GGSN. In section 8.1.1 their tasks and the interworking with GSM nodes and registers (HLR, VLR and EIR) has been explained.

An important feature of GPRS is its QoS support. An individual QoS profile (service precedence, reliability, delay, and throughput) can be negotiated for each PDP context. For the simultaneous use of GPRS and conventional GSM services, three classes of MSs are defined in the standard.

Before a GPRS MS can use GPRS services it must obtain an address used in the external packet data network (e.g. an IP address) and create a PDP context. This context describes the essential characteristics of the session (PDP type, PDP address, QoS, and GGSN). In order to support a large number of mobile users, it is essential to use dynamic address allocation, e.g., using DHCP for dynamic IP address assignment.

Once a MS has an active PDP context, packets addressed from the external packet data network to the MS will be routed to the responsible GGSN. The GGSN then tunnels them to the current SGSN of the mobile user, which finally forwards the data to the MS. The GPRS location management is based on the definition of a MS state model. Depending on the state of the MS (READY, STANDBY, or IDLE), it performs many or only few location updates. For this purpose, special routing areas are defined, which are sub-areas of the location areas defined in GSM. Although GPRS has its own mobility management, it cooperates with the GSM mobility management. This results, for example, in a more efficient paging mechanism for MSs that use circuit- and packet-based services simultaneously.

In section 8.1.4 we showed the protocol architecture of the GPRS transmission and signaling plane. GPRS-specific protocols include GTP, the GMM/SM protocol, and SNDCP. Some GSM protocols, such as MAP, have been extended for use with GPRS.

The packet-oriented air interface is one of the key aspects of GPRS. MSs with multislots capability can transmit on several time slots of a TDMA frame, uplink and downlink are allocated separately, and physical channels are only assigned for the duration of the transmission, which leads to a statistical multiplex gain. This flexibility in the channel allocation results in a more efficient utilization of the radio resources. On top of the physical channels, a number of logical packet channels have been standardized. The traffic channel PDTCH is used for payload transmission. The GPRS signaling channels are used, e.g., for broadcast of system information (PBCCH), access control (PRACH, PAGCH), paging (PPCH), and notification of incoming PTM messages (PNCH). Again, the coordination between GPRS and GSM channels saves radio resources.

GPRS channel coding defines four different coding schemes, which allows the tradeoff between the level of error protection and data rate to be adjusted, depending on the current radio channel quality. GPRS security principles include authentication, ciphering, and subscriber identity confidentiality. The SGSN handles authentication, and a special GEA

has been defined. Moreover, GPRS operators protect their network with firewalls to external networks and border gateways to other GPRS networks. IP security protocols (IPsec) may be used to communicate over insecure external IP networks.

Typical scenarios for GPRS are wireless access to the Internet, e-mail communication, WAP over GPRS, and applications in the telemetry field. Users can access the Internet without first requiring to dial into an Internet service provider. In particular, mobile e-commerce and location-based services (e.g. tourist guides) have gained importance in the last few years. The main advantages for the users are the higher data rates and volume-based billing. The latter allows them to stay online for a long time.

8.2 HSCSD

As the name implies, the High Speed Circuit Switched Data Service is, in contrast to GPRS, circuit-switched. That is, the user has a fixed data rate bearer available for the duration of the data connection. This is independent of the amount of data actually transmitted, such that the connection has to be paid for, even during periods, in which no data are transmitted, according to the respective higher layer services used. This means that HSCSD is specifically useful for applications which demand for a fixed data rate. The advantage of this, however, is that the data rate is guaranteed during the connection time, in case a transparent bearer service is applied. On the other hand, the QoS is secured, if a nontransparent bearer service is applied. HSCSD supports both options.

Just as in GPRS, also HSCSD allows for the parallel use of several, say n , traffic channels to provide higher data rates. Figure 8.21 depicts an example with $n = 2$, in which timeslots TS1 and TS2 are used for one HSCSD connection, both in uplink and downlink. The principal restriction for the number of timeslots n is given by the requirement that they all have to reside on the same frequency channel. Therefore, the standard allows for up to $n = 8$ timeslots or channels to be assigned to one user. This gives us the maximal data rate achievable: using eight channels at once, each carrying a full-rate traffic channel TCH/F9.6, a sum data rate of 76.8 kbit/s could be achieved. However, it should be recalled that, even though GSM applies FDD, uplink and downlink timeslots of the same TCH have an offset, such that the mobile terminal can perform transmission and reception subsequently. This because terminals with the ability to perform transmit and receive operations in parallel would imply much higher complexity at the terminal and thus would make terminals much more expensive. Therefore, earlier versions of the HSCSD standard only allowed for up to $n = 4$ timeslots to be used at once. This would present us with a data rate of 38.4 kbit/s, when four TCH/F9.6 channels are used. In fact, by applying a different coding scheme, a maximum data rate of 57.6 kbit/s is achieved with $n = 4$. Figure 8.21 shows, for the example of $n = 2$, how the required operations in the mobile terminal can still be performed sequentially, as was originally intended in classical GSM: the mobile is receiving in timeslots TS1 and TS2 of the downlink frame. Owing to the time offset of three timeslots between the uplink and the downlink frames, the terminal has already completed reception, when it has to start transmitting on the uplink, also using TS1 and TS2, but now on the uplink frames. After completion of transmission, and before having to receive data again in the following TS1 and TS2 on the downlink, there is still enough time to monitor BCCH carriers of neighboring cells, which is important, e.g., for handover issues.

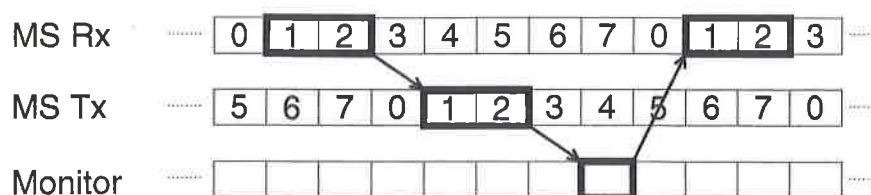


Figure 8.21 Example HSCSD channel occupation with $n = 2$.

When assigning timeslots, the HSCSD service takes the so-called multislot class of the MS into consideration. A list of the multislot classes considered for HSCSD is shown in Table 8.8. It lists the class name, the maximum allowed number of downlink timeslots (Rx), uplink timeslots (Tx), and sum of downlink and uplink timeslots. For instance, multislot class 3 terminals might use up to two timeslots for reception (downlink) and up to two timeslots for transmission (uplink). However, the sum of uplink and downlink timeslots must never be larger than three. When a mobile of a certain multislot class initiates a HSCSD connection, the RRM must consider the restrictions of the respective multislot class, when assigning timeslots. The last column in Table 8.8 refers to the type of the MS: type 1 terminals do not have the ability to transmit and receive at the same time. Therefore, the RRM must ensure the appropriate selection of timeslots. In contrast, type 2 mobiles do have the ability to transmit and receive in parallel, which gives the RRM more options to allocate timeslots for HSCSD.

8.2.1 Architecture

From an architectural point of view, HSCSD does not demand many changes as compared with standard GSM data services (see Appendix A). The GSM architecture for HSCSD support is depicted in Figure 8.22. At the U_m interface between MS and BTS up to $n = 8$ TCH/F channels are used, which are forwarded transparently via the A_{bis} interface from the BTS to the BSC. Here the data from all parallel channels are multiplexed on a single 64 kbit/s connection and transmitted over the A interface to the MSC. The n full rate channels are considered independent of each other and are treated individually for the purpose of, e.g., air interface error control. However, logically they belong to the same HSCSD configuration and are controlled as one radio link by the network for the purpose of cellular operations, such as handover. This requires new BSS functionality.

The main difference to the standard GSM data services is in a combining and splitting functionality that is demanded at the MS and the MSC, combining and splitting, respectively, the multiple data streams that are transmitted between both entities. This functionality is provided in the Terminal Adoption Function (TAF) at the MS and in the IWF at the MSC, respectively (Figure 8.22).

8.2.2 Air interface

As described above at the air interface, a HSCSD connection comprises n traffic channels (TCH). All n channels use the same hopping sequences, if frequency hopping is applied. Also the training sequence assigned, is the same for all n traffic channels. However, each traffic channel is assigned an independent SACCH signaling channel, allowing for

Table 8.8 HSCSD MS multislot classes.

Multislot class	Maximum number of slots			Type
	Rx	Tx	Sum	
1	1	1	2	1
2	2	1	3	1
3	2	2	3	1
4	3	1	4	1
5	2	2	4	1
6	3	2	4	1
7	3	3	4	1
8	4	1	5	1
9	3	2	5	1
10	4	2	5	1
11	4	3	5	1
12	4	4	5	1
13	3	3	NA	2
14	4	4	NA	2
15	5	5	NA	2
16	6	6	NA	2
17	7	7	NA	2
18	8	8	NA	2

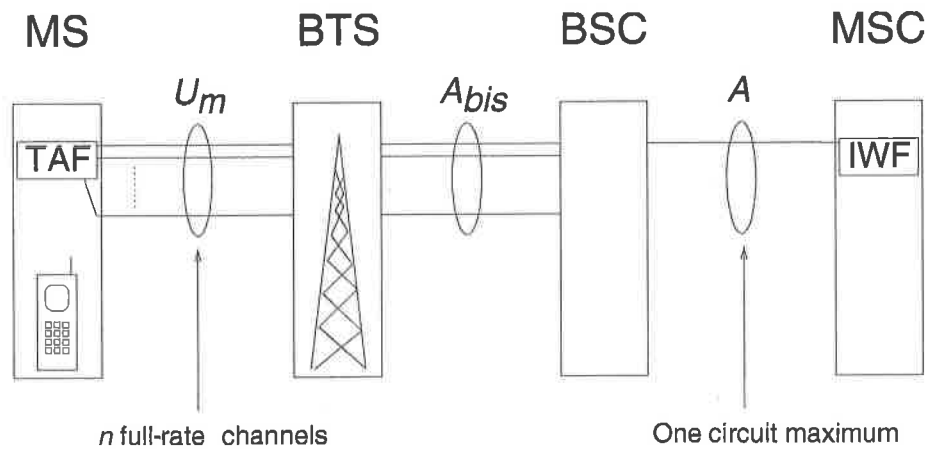


Figure 8.22 GSM architecture for HSCSD support.

independent signal level and quality reporting on each timeslot, in turn, allowing for individual power control on each timeslot. This is done, since the interference level can be different on each timeslot such that different power levels might be required in order to secure the required signal quality on every single timeslot. The HSCSD connection

has just one FACCH control channel assigned for management purposes. For all HSCSD channels, the same channel coding is applied, however, for nontransparent services, different channel codings can be used for uplink and downlink, respectively. For each HSCSD channel, different ciphering keys are used, derived from K_c . The channel assignment configuration can be either symmetric or asymmetric and channels can be allocated either on consecutive or on nonconsecutive timeslots of the same carrier, as long as the restrictions of the given multislot class of the MS are considered.

Symmetric connections comprise a bidirectional FACCH as well as co-allocated bidirectional TCH/F and SACCH channels. In contrast, asymmetric connections can have unidirectional and/or bidirectional TCH/f and SACCH channels in addition to the bidirectional FACCH. Unidirectional channels in HSCSD are always downlink channels only. Both symmetric and asymmetric HSCSD channels have a bidirectional main channel, which carries the FACCH.

8.2.3 HSCSD resource allocation and capacity issues

When initiating a HSCSD connection, the user indicates during setup the maximum number of traffic channels, the multislot class of the terminal, acceptable channel codings, and a wanted fixed network user rate. In the case of a nontransparent connection, the wanted air interface user rate is also indicated. The connection requirements can be symmetric or asymmetric, considering uplink and downlink. These parameters are then used by the network to allocate appropriate resources and to setup the demanded HSCSD connection. The minimum channel requirement is always one TCH/F. This means that transparent and nontransparent connections can be established with any number of TCH/F from one up to the specified maximum number. When the user rate requirements cannot be met, the network will give priority to fulfill the air interface user requirement in downlink direction, possibly using an asymmetric configuration. The network can use dynamic resource allocation for nontransparent HSCSD connections, as long as the allocated channel configurations are always in line with the limiting values defined by the MS and with the multislot class of the terminal. In the case of transparent HSCSD connections, dynamic resource allocation is only allowed if the air interface user data rate is kept constant. The network performs the change of channel allocation configurations during the HSCSD connection, by means of resource upgrading and resource downgrading procedures. If indicated by the MS during call setup, the MS may issue a request an upgrade or downgrade of service level anytime during the HSCSD connection.

Obviously, HSCSD can increase the data rate of a single user. This, however, is achieved at the cost of assigning more frequency resources to a single user. This implies that from the point of view of a network provider, resources are more frequently occupied. A single HSCSD user using $n = 4$ TCHs will occupy the resources of four potential voice connections. Therefore, when many users utilize HSCSD at once in a single cell, the blocking performance in that cell will deteriorate. This will influence the radio resource management strategy that a network provider will use: if possible, the provider might try to assign more frequency carriers to cells in areas where the frequent use of HSCSD seems likely, for instance at airports or in business areas of a city. Also, the provider has the option of restricting the number of HSCSD connections in a cell in favor of voice connections.

Another interesting aspect of the HSCSD radio resource management is the handover. When a handover of the HSCSD connection to a neighboring cell becomes necessary, it might not be possible to find n free TCHs on a single frequency channel in the target cell. In this case, two options are possible: either the HSCSD connection is simply dropped or the connection is resumed with a lower number of TCHs. For this purpose, the resource downgrading procedure is applied, as described above for the case of dynamic resource allocation. With this concept, the probability of a handover being blocked and thus a HSCSD call being dropped can be reduced. Later, a resource upgrading procedure can be applied if an appropriate resource becomes available, and the original channel allocation configuration can be recreated.

8.3 EDGE

As discussed above in this chapter, HSCSD and GPRS achieve higher data rates because a MS can use several time slots of the same TDMA frame and partly because new coding schemes are employed. The EDGE² system goes one step further, by improving the spectral efficiency on the physical layer on a single timeslot (Furuskär *et al.*, 1999). Technically speaking, EDGE can be considered mainly as an air interface improvement. However, in effect it is a system concept that is used in order to introduce new bearer services into GSM systems. In this context it is interesting to note that both GPRS and EDGE have also been standardized for the North American cellular network TDMA-136 (GPRS-136 and GPRS-136HS EDGE). Within the GSM context, EDGE is used to improve the existing data services with a focus on GPRS and HSCSD, which become Enhanced GPRS (EGPRS) and Enhanced Circuit Switched Data (ECSD), respectively, when combined with EDGE technology.

8.3.1 The EDGE concept

A classical GSM system is designed and planned in a worst-case fashion: the radio network planning is carried out such that there is a high probability that all users in the network will experience a minimum signal quality that is sufficient for low error probability with a fixed modulation and error coding scheme. In fact, the main restrictions for the radio network planning come from those users that are located at the cell edges, far away from base stations. So, it can be said that the GSM network is designed for the cell edge users. However, users located closer to the base stations are likely to experience signal quality levels that are much better than required for the standard GSM modulation and coding schemes. To this end, EDGE introduces several additional combinations of modulation and coding schemes, which allow terminals to adapt their data rates to their individual signal quality levels. For this purpose a link adaptation technique is introduced with EDGE, which dynamically chooses a modulation and coding scheme according to the current radio channel conditions.

²EDGE used to stand for Enhanced Data Rates for GSM Evolution, however, GSM was replaced with *Global*, since EDGE, as mainly an air interface enhancement, can be, and actually is, used not only in GSM but in various cellular networks with different standards.

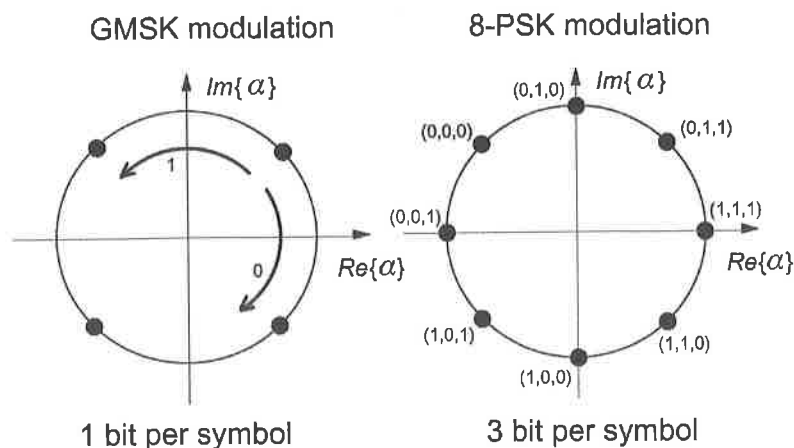


Figure 8.23 Symbol space constellations for GMSK and 8-PSK.

Figure 8.24 The EDGE burst has a training sequence of 26 symbols in the middle, three tail symbols at either end, and 8.25 guard symbols at the end. The burst carries 2×58 data symbols.

8.3.2 EDGE physical layer, modulation and coding

For EDGE, in addition to the GMSK modulation scheme used in GSM, an 8-Phase Shift Keying (8-PSK) scheme is available, which achieves an approximately three times higher data rate per time slot and hence a higher spectral efficiency. Using GMSK, one data bit d_i is mapped to one symbol a_i (see section 4.2.1); with 8-PSK, three data bits d_i are combined into one symbol a_i and transmitted together. Figure 8.23 shows the symbol constellations in the complex plane and the associated bit sequences. As opposed to GMSK, 8-PSK does not have a constant envelope and therefore puts higher requirements on new transceivers in BTSs and MSs.

In order to achieve compatibility with the GSM system, most EDGE physical layer parameters are the same as in GSM: the carrier spacing is 200 kHz and the TDMA frame structure remains unchanged. The burst format for the 8-PSK modulated transmission is also similar to the standard GSM frames (Figure 8.24): A burst comprises a 26-symbol training sequence as midamble, three tail symbols at the beginning and end of the frame, and 8.25 guard symbols at the end. Before and after the midamble, the frame carries 58 data symbols, each symbol representing three bits according to the 8-PSK modulation applied.

Several different coding schemes with different code rates can be combined with the two different modulation schemes available (Tables 8.9 and 8.10) (Molkdar *et al.*, 2002). In order to select the optimal scheme, EDGE applies a link adaptation based on the current channel quality.

In addition to the additional modulation and coding schemes, EDGE also introduces a code combining technique called incremental redundancy, also known as Hybrid Automatic Repeat Request (HARQ). In the incremental redundancy mode, the first RLC data block can be transmitted with some or even no redundancy added. If the data block cannot be decoded correctly, in the next retransmission, more redundancy is sent, applying a different puncturing scheme on the same RLC block. The erroneous blocks are stored, such that they can be combined with each retransmission required, until the RLC can be decoded correctly.

Also, the RLC/MAC layer has been enhanced with appropriate RLC/burst mapping functionality. The improved RLC/MAC layer allows for resegmentation to enable for retransmission with different coding schemes, independent coding of RLC/MAC headers and an increased ACK/NACK window size. As for the segmentation, each LLC PDU is broken into 20 ms RLC data blocks, to match the TDMA burst structure of GSM. Depending on the selected coding scheme by the link adaptation, the number of bits that fit into a RLC data block varies. The required RLC/MAC headers are appended to the user data before transmission. The content of the RLC/MAC headers includes a Block Sequence Number (BSN), and a Coding and Puncturing Scheme (CPS) indicator, that is required for the code combining process in the HARQ procedure. Then, check sequences for the user data (BCS) and for the header (HCS) are added to form a RLC radio block. The RLC radio block is then passed to the physical layer. There the user data and the header are coded separately and finally mapped to two or four TDMA bursts, depending on the coding scheme. The modulation and coding scheme can be changed for each RLC block, i.e. typically every four TDMA bursts. However, the modifications will be based on channel quality monitoring and changes will, in fact, be more seldom, depending on the channel measurement and reporting frequency.

8.3.3 EDGE: effects on the GSM system architecture

It is mainly the improved data rate of EDGE that imposes new requirements also for the GSM/GPRS network architecture: the main bottleneck for EDGE in GSM is the A_{bis} interface between BTS and BSC. In standard GSM, this interface supports only 16 kbit/s per traffic channel. However, EDGE can support close to 64 kbit/s for one traffic channel. Therefore, EDGE requires the allocation of multiple A_{bis} slots to one traffic channel. In future 3G network architectures, this requirement might also be fulfilled by applying ATM or IP-based solutions. The A interface between BSC and MSC can handle 64 kbit/s already in standard GSM and therefore does not present a problem. Other than that, the GSM/GPRS network architecture is not affected by the introduction of EDGE. This is due to the fact that EDGE is foremost just an enhanced air interface technology. Two different types of EDGE mobile terminals are considered in the standard: terminals that are capable of 8-PSK modulation on the downlink only, and terminals which provide 8-PSK capability on both the uplink and downlink. The first class of terminals can benefit from higher data rates on the downlink, which is still considered to be the link of higher importance, due to the popularity of services which are heavy on the downlink data amount, such as browsing and file downloads. On the other hand, the second class of terminals can support higher bandwidth on both links and of course makes a more efficient use of the scarce frequency resource, even when nonsymmetric services are considered. The necessity to have this capability information in the network has some minor implications on control plane layers: mobility management modifications are

Table 8.9 EGPRS transmission modes.

Channel name	Code rate	Modulation	Bitrate per timeslot (kbit/s)
MCS-1	0.53	GMSK	8.8
MCS-2	0.66	GMSK	11.2
MCS-3	0.85	GMSK	14.8
MCS-4	1	GMSK	17.6
MCS-5	0.37	8-PSK	22.4
MCS-6	0.49	8-PSK	29.6
MCS-7	0.76	8-PSK	44.8
MCS-8	0.92	8-PSK	54.4
MCS-9	1	8-PSK	59.2

Table 8.10 ECSD transmission modes.

Channel name	Code rate	Modulation	Bitrate per timeslot (kbit/s)
TCH/F2.4	0.16	GMSK	3.6
TCH/F4.8	0.26	GMSK	6
TCH/F9.6	0.53	GMSK	12
TCH/F14.4	0.64	GMSK	14.5
ECSD TCS-1	0.42	8-PSK	29
ECSD TCS-2	0.46	8-PSK	32
ECSD TCS-3	0.56	8-PSK	38.8

related to the introduction of EGPRS capability information of the respective terminal. These include the multislot class as well as the EDGE modulation capabilities (downlink or uplink and downlink) and in addition an 8-PSK power class. Some modifications are also required on the RRM layer for supporting, setting up, and maintaining EGPRS temporary block flows. In addition, signaling to support the radio link control, the link quality control, and measurement procedures are introduced. There is, however, no impact on session management.

8.3.4 ECSD and EGPRS

EDGE can be used to improve both GPRS and HSCSD data services in GSM systems. In combination with EDGE, GPRS becomes EGPRS. Likewise, HSCSD becomes ECSD when enhanced by EDGE. The different achievable data rates per timeslot for the different combinations of modulation and coding schemes are summarized in Tables 8.9 and 8.10, respectively. The table shows which combinations of modulation scheme and code rate can be applied in EGPRS and ECSD, respectively. The highest data rate is achieved in EGPRS when the 8-PSK modulation scheme is combined with a code rate of one. This, however, demands extremely good channel conditions, since the code rate of one implies that there is in fact no error protection. So it will, in fact, rarely be possible to apply this mode, unless

the respective application can tolerate packet losses to a good extent. The data rates that can be achieved with EGPRS and ECSD will be obviously multiples of the values in the tables when several timeslots are combined.

The link adaptation for both EGPRS and ECSD requires appropriate signaling. For this purpose, existing signaling mechanisms are applied, specifically the RR channel mode modify procedure, the assignment procedure, and the intra-cell handover procedure.

8.3.5 EDGE Classic and EDGE Compact

EDGE standardization was started when it was introduced as a work item in ETSI in 1997. The objective was to enhance the performance of HSCSD and GPRS, as described above. The result was the above-discussed so-called EDGE Phase I with ECSD and EGPRS. The EDGE specifications of Release 99 extend the previous standard by including two different air interface configurations, namely EDGE Classic and EDGE Compact. The novelty is the addition of EDGE Compact, which is only defined for packet-based services, i.e. it is only considered for EGPRS, not ECSD. The main idea behind EDGE Compact is as follows. Classical GSM systems have a relatively sparse reuse in order to secure sufficient signal quality for voice services. A typical reuse pattern in today's GSM systems would be a three sector system with a cell cluster of four. This means that the number of required channel groups is three times four, that is, 12. Given the frequency channel bandwidth of 200 kHz in GSM systems, the minimum bandwidth requirement for such a network configuration becomes 12 times 200 kHz, that is, 2.4 MHz of spectrum. For voice services, which can hardly tolerate retransmissions due to delay requirements, the C/I requirements are quite severe and cannot easily be relaxed, which means that it not advisable to work with a denser reuse. In contrast to this, data applications can tolerate delay to a greater extent. Therefore, it is possible to apply, e.g., EGPRS in a reuse scenario with a denser frequency reuse and thus a lower C/I and compensate for the higher bit error ratios induced on the channel by retransmissions and HARQ. To this end, EDGE Compact allows for a reuse configuration with three sectors and a cell cluster of just one. That means, each cell reuses the frequencies, however, within each cell three different channel groups are assigned to each of the three sectors. The minimum bandwidth requirement for such an EDGE Compact system is thus only three times 200 kHz, that is 0.6 MHz. So far it could be conceived that EDGE Compact is just EDGE Classic with a denser frequency reuse. The architectural difference, however, comes from the requirement, that in contrast to the EDGE Compact traffic channels, the control channels should still have the traditional high C/I values, known from classical GSM systems. For this purpose, GSM Compact devises a time sharing of timeslots for control channels: Co-channel sites take turns on transmitting common control channels on the downlink. The cells are separated into different time groups according to a cell cluster size of four or three, and the time group membership determines when a cell can use (downlink and uplink) control channels. For details, see, e.g., Sexton (2000) or Molkdar and Featherstone (2001).

Beyond GSM and UMTS: 4G

Today, many network operators have already introduced UMTS and most of them have integrated the UMTS Terrestrial Radio Access Network (UTRAN) into existing GSM backbone infrastructure and architecture. Figure 9.1 shows the respective evolution scenario for the migration from GSM to UMTS. On the basis of the existing circuit- and packet-switched infrastructure (GSM/GPRS) and entities for mobility management (HLR, MAP), the UTRAN with the new air interface has already been introduced (UMTS Phase 1). Here, UTRANs are installed in parallel to BSSs of GSM and partly even reusing existing locations. In a further step (UMTS Phase 2) the network architecture and backbone transportation facilities are adapted to the requirements of broadband packet-switched services, as the systems evolve.

In the meantime, the UMTS air interface has already been extended by the development of the fast-scheduled, packet-switched data services High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA). Both, HSDPA and HSUPA have already been fully specified through standardization within 3GPP. Similar to EDGE in GSM, the HSxPA services apply higher-order modulation schemes and offer a series of different coding schemes, such that the data rate can be adapted to the channel conditions through the process of link adaptation. In addition, fast scheduling is applied utilizing a channel feedback with a frequency of up to once per 2 ms. Combined with clever scheduling algorithms, this is used to allow the benefits of multi-user diversity to be reaped. In theory, up to 14 Mbit/s can be achieved with HSDPA. However, in practice a couple of megabits per second are achieved. These services will further be improved, e.g., by incorporating multiple antennas at both the base station and mobile terminal and utilizing MIMO capabilities to transform the given channel diversity into link capacity gains. This is done by applying specific strategies, such as transmitting parallel data streams over different antenna pairs, and requires smart signal processing with reliable channel state information.

In parallel to the evolution of 3G systems towards UMTS/HSxPA networks, research and conceptual work is carried out towards a fully novel air interface and network architecture for future packet-switched broadband multimedia systems. Most notably the 3GPP Long Term Evolution (LTE) should be mentioned here. Even though LTE is still far from becoming an actual standard, some important properties can be listed.

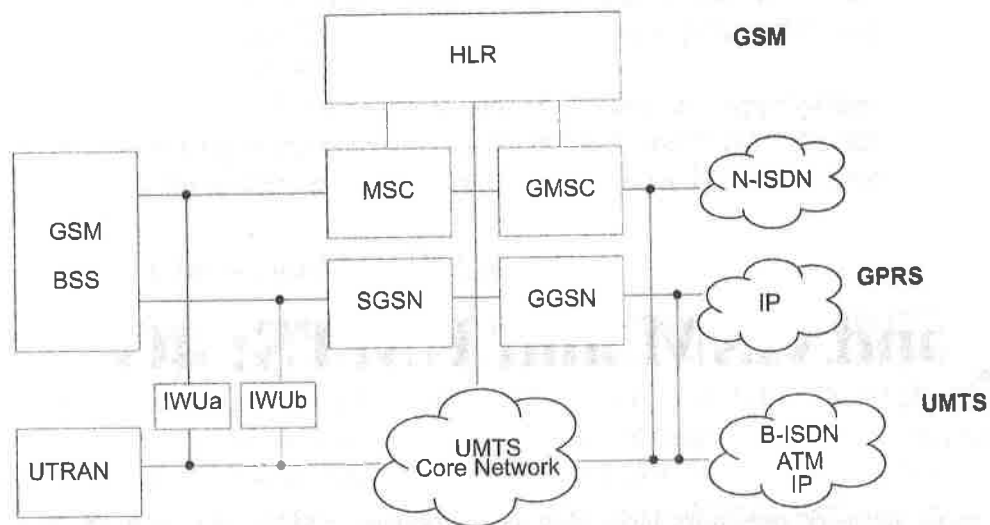


Figure 9.1 Evolution steps from GSM to UMTS.

- The air interface will be based on Orthogonal FDMA (OFDMA) on the downlink and on Single-Carrier FDMA (SC-FDMA) on the uplink.
- Fast channel feedback will allow for fast channel adaptive scheduling, achieving high data throughput.
- A frequency reuse of one is desired: it should be possible to reuse frequency resources in neighboring cells. This will, in fact, require adaptive channel and interference management strategies in order to avoid excessive interference. This is currently a major focus of research.
- The backbone node architecture will be flattened: Radio Network Controllers (RNCs), as used in UMTS in the same way as the BSC in GSM, will no longer exist. Instead, base stations will be connected directly to powerful IP routers. This implies that base stations will be much more complex than in GSM or UMTS, because functionalities such as resource allocation, packet scheduling, interference management and Hybrid ARQ (HARQ) will be moved to the base station.

At the moment it is not clear at all when a novel standard for a fourth-generation (4G) system will be available. From today's perspective it seems safe to assume that GSM networks will still be of major importance for many years. In particular, since new GSM networks will be going on air during the next couple of years in many regions of the world, the growth of GSM has not yet slowed.

Appendices

A

Data communication and networking

For the third edition of this book, we have moved this chapter on classical GSM data services from the main body to an appendix because we believe that with the advent of GSM Phase 2+ services, such as HSCSD and most prominently GPRS, the classical GSM data services are of minor importance and hardly used anymore. However, we did not want to remove them completely from the book and rather present them in this appendix for completeness.

A.1 Reference configuration

GSM was conceived in accordance with the guidelines of ISDN. Therefore, a reference configuration is also defined for GSM systems, similar to that used in ISDN systems. Using the reference configuration, one can get an impression of the range of services and the kinds of interfaces to be provided by MSs. Furthermore, the reference configuration indicates at which interface which protocols or functions terminate and where adaptation functions may have to be provided.

The GSM reference configuration comprises the functional blocks of a MS (Figure A.1) at the user-network interface Um. The mobile equipment is subdivided into a Mobile Termination (MT) and various combinations of Terminal Adapter (TA) and TE, depending on the kind of service access and interfaces offered to the subscriber.

At the interface to the mobile network, the air interface Um, MT units are defined. An integrated mobile speech or data terminal is represented only by an MT0. The MT1 unit goes one step further and offers an interface for standard-conforming equipment at the ISDN S reference point, which can be connected directly as end equipment. Likewise, normal data terminal equipment with a standard interface (e.g. V.24) can be connected via a TA and this way use the mobile transmission services. Finally, the TA functionality has been integrated into units of type MT2.

At the S or R reference point, the GSM bearer or data services are available (access points 1 and 2 in Figure A.1), whereas the teleservices are offered at the user interfaces of the TE (access point 3, Figure A.1). Among the bearer services, in addition to the transmission of digitized speech, there are circuit-switched and packet-switched data transmission. Typical

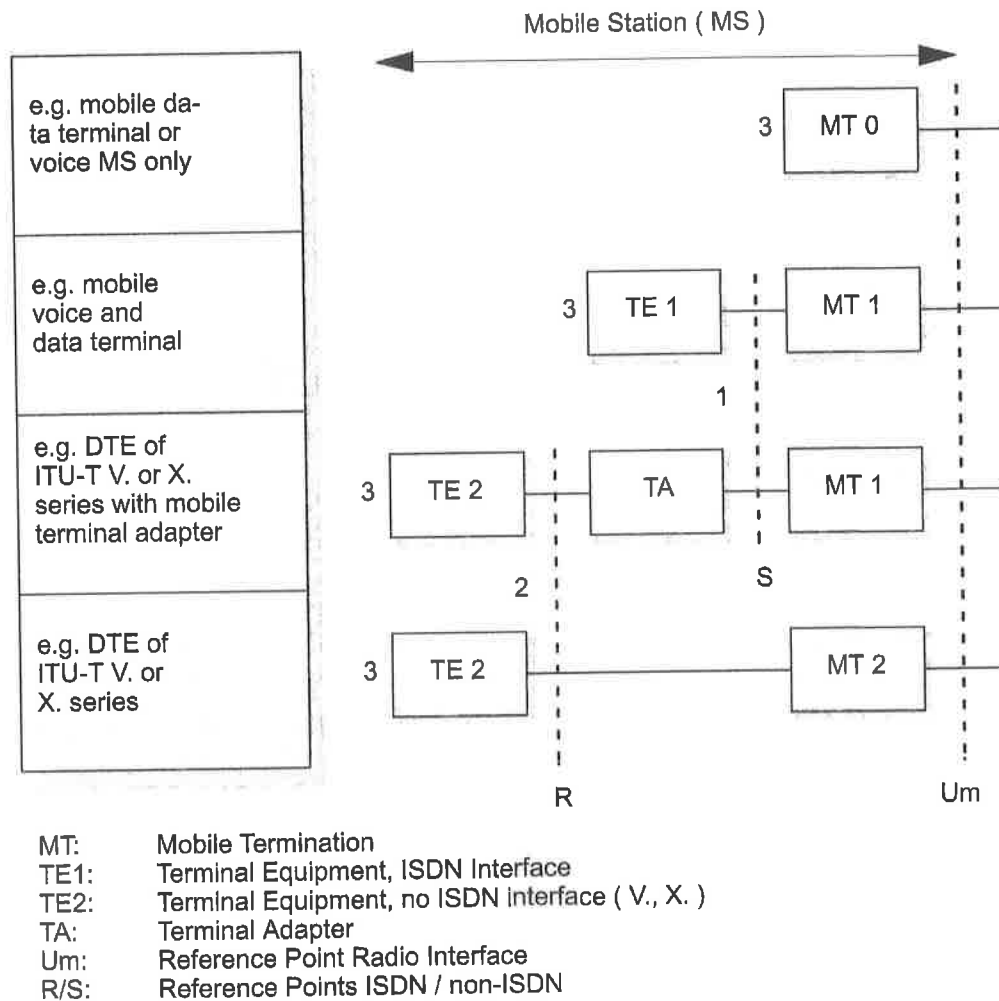


Figure A.1 GSM reference configuration.

teleservices besides telephony are, for example, SMS, group 3 fax service or emergency calls from anywhere.

A.2 Overview of data communication

The voice service needs only a switched-through physical connection, which changes its bit rate in the BSS due to the speech transcoding in the TRAU. From the MSC on, the speech signals in GSM networks are transported in standard ISDN format with a bit rate of 64 kbit/s. In comparison, realizing data services and the other teleservices such as group 3 fax is considerably more complicated. Owing to the psychoacoustic compression procedures of the GSM speech codec, data cannot be simply transmitted as a voiceband signal as in the analog network – a complete reconstruction of the data signal would not be possible. Therefore, a solution to digitize the voiceband signal similar to ISDN is not possible. Rather the available digital data must be transmitted in unchanged digital form by avoiding speech codecs in the PLMN, as is possible in ISDN. Here we have to distinguish two areas where

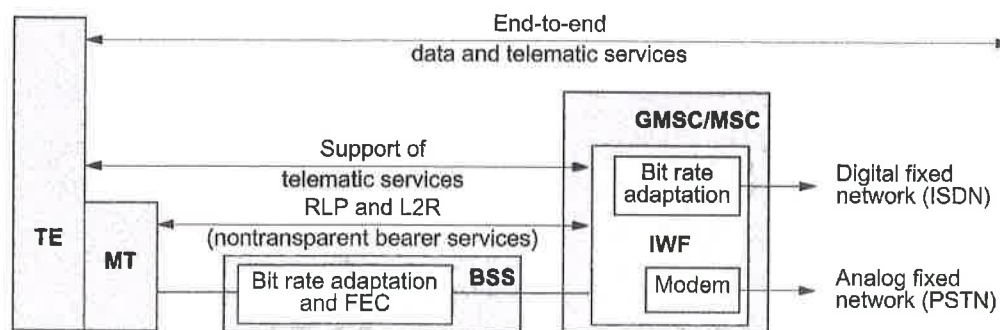


Figure A.2 Bearer services, interworking, and teleservices.

special measures have to be taken: first, the realization of data and teleservices at the air interface or within the mobile network and, second, at the transition between mobile and fixed network with the associated mapping of service features. These two areas are illustrated schematically in Figure A.2.

A PLMN offers transparent and nontransparent services. These bearer services carry data between the MT of the MS and the IWF of the MSC. For the realization of bearer services, the individual units of the GSM network define several functions:

- Bit Rate Adaptation (RA);
- Forward Error Correction (FEC);
- ARQ error correction with RLP;
- adaptation protocol L2R.

For the transmission of transparent and nontransparent data, several rate adaptation stages are required to adapt the bit rates of the bearer services to the channel data rates of the radio interface (traffic channels with 3.6, 6 and 12 kbit/s) and to the transmission rate of the fixed connections. A bearer service for data transmission can be realized in the following two ways: 9.6 kbit/s data service requires a full-rate traffic channel; all other data services can either be realized on a full-rate or half-rate channel. A MS must support both types of data traffic channels, independent of what is used for speech transmission. The data signals are transcoded first from the user data rate (9.6, 4.8, 2.4 kbit/s, etc.) to the channel data rate of the traffic channel, then further to the data rate of the fixed connection between BSS and MSC (64 kbit/s) and finally back to the user data rate. This bit rate adaptation (RA) in GSM corresponds in essence to the bit rate adaptation in the ITU-T standard V.110, which specifies the support of data terminals with an interface according to the V. series on an ISDN network (ITU-T Recommendation V.110, 2008).

On the radio channel, data are protected through the forward error correction procedures (FEC) of the GSM PLMN; and for nontransparent data services, data are additionally protected by the ARQ procedure of RLP on the whole network path between MT and MSC. Thus, RLP is terminated in the MT and MSC. The protocol adaptation to RLP of Layers 1 and 2 at the user interface is done by the L2R protocol.

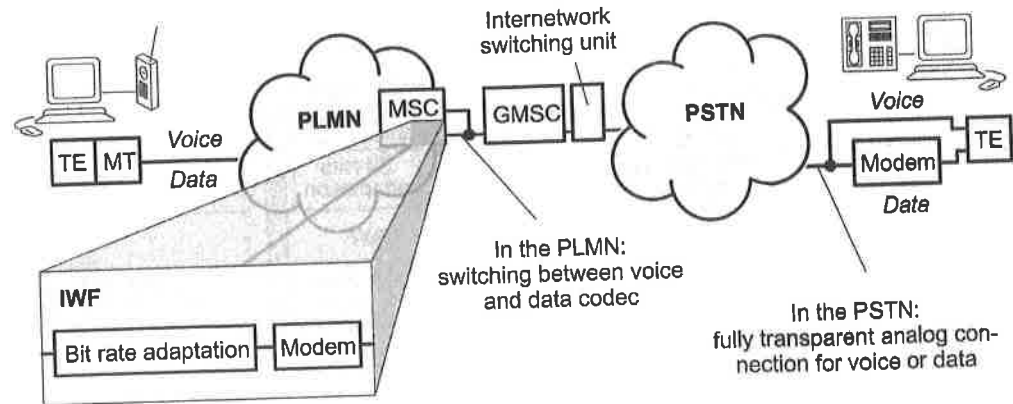


Figure A.3 Interworking scenario PLMN-PSTN for transparent data services.

Finally, the data are passed on from MSC or GMSC over an IWF to the respective data connection. The bearer services of the PLMN are transformed to the bearer services of the ISDN or another PLMN in the IWF, which is usually activated in a MSC near the MS, but could also reside in the GMSC of the network transition. In the case of ISDN this transition is relatively simple, since it may just require a potential bit rate adaptation. In the case of an analog PSTN, the available digital data must be transformed by a modem into a voiceband signal, which can then be transmitted on an analog voiceband of 3.1 kHz.

The bearer services realized in this way can offer the protocols that may be required for the support of teleservices between TE and IWF. An example is the fax adaptation protocol. The fax adapter is a special TE which maps the group 3 fax protocols with their analog physical interface upon the digital bearer services of a GSM PLMN. Thus, after another adaptation into an analog fax signal in the IWF of the MSC, it enables the end-to-end transfer of fax messages according to the ITU-T Standard T.30.

A possible interworking scenario for transparent data services of GSM with transition to a PSTN is shown in Figure A.3. The analog circuit-switched connection of the PSTN represents a transparent channel which can be used to transport arbitrary digital data signals in the voiceband. In the analog network, a subscriber selects telephone or modem depending on whether they want to transmit speech or data. In the PLMN, however, the channel coding has to be changed for different services (error protection for different bearer services; section 4.8). The bit rate adaptation has to be activated and the speech coding deactivated. In the IWF of the MSC, in addition to the bit rate adaptation, a modem needs to be added for data communication with the partner in the fixed network. In the GSM network, voice signals therefore take a different path than data signals; in the case shown in Figure A.3, the data signals are directed from the IWF to the modem, where they are digitized, then passed on after bit rate adaptation to transmission on the radio channel. In the opposite direction, the IWF passes the PCM-coded information on an ISDN channel (64 kbit/s) to the GMSC. From there it is transformed into an analog signal in a network transition switching unit and carried as a voiceband signal in the PSTN to the analog terminal.

After these introductory remarks, the GSM data and teleservices and their realization are discussed in more detail in the following sections.

A.3 Service selection at transitions between networks

A specific interworking problem arises for data services between PLMN and ISDN/ PSTN networks. Mobile-terminated calls require that the calling subscriber (ISDN or PSTN subscriber) tells the GMSC which service (speech, data, fax, etc.) they want to use. In ISDN, a Bearer Capability (BC) information element would have to be included in the SETUP message. This BC information element could then be passed on by the network transition switching unit to the GMSC and from there to the local MSC, which could thus activate the required resources. In the course of call processing (CC; section 5.4.5), the MS would also be informed about the kind of service requested by the calling subscriber and could activate the required functions. However, if there is no ISDN signaling as in analog networks, the calling subscriber is not able to do this kind of BC signaling. The service selection therefore has to use another mechanism. The GSM standard proposes two possible solutions, which are always to be used for service selection independent of the type of originating network (ISDN or PSTN).

- *Multinumbering*: the home network with this option assigns to each mobile subscriber several MSISDN numbers, each with a specific BC, which can be obtained at each call from the HLR. In this way the service that an incoming call wants is always uniquely determined. The BC information element is given to the MS when the call is being set up, so the MS can decide based on its technical features whether it wants to accept the call.
- *Single numbering*: only a single MSISDN is assigned to the mobile subscriber, and there is no BC information element transmitted with an incoming call. The MS recognizes then that a specific BC is needed when a call is accepted and requests the BC from the MSC. If the network is able to offer the requested service, the call is switched through.

Usually, the multinumbering solution is favored, since one can already verify at call arrival time in the MSC whether the requested resources are available, and the MSC side can decide about accepting the call. There is no negotiation about the BC between MS and MSC, so no radio resources are occupied unnecessarily, and the call set-up phase is not extended.

A.4 Bit rate adaptation

Five basic traffic channels are available in GSM for the realization of bearer services: TCH/H2.4, TCH/H4.8, TCH/F2.4, TCH/F4.8, TCH/F9.6 (see Tables 4.2 and 4.11) with bit rates of 3.6, 6 and 12 kbit/s. In recent standardization efforts, a TCH/F14.4 has also been defined. The bearer services (Table 4.2) with bit rates from 300 bit/s up to 9.6 kbit/s must be realized on these traffic channels. Furthermore, on the fixed connections of the GSM network, the data signals are transmitted with a data rate of 64 kbit/s.

The terminals connected at reference point R have the conventional asynchronous and synchronous interfaces. The data services at these interfaces work at bit rates as realized by GSM bearer services. Therefore, the data terminals at the R reference point have to be bit rate

Table A.1 Data rates for GSM bit rate adaptation.

Reference point	Data rate (kbit/s)		Interface (kbit/s)	
	User R	Intermediate	Radio Um	S
RA1	≤ 2.4	8		
RA1	4.8	8		
RA1	9.6	16		
RA2		8		64
RA2		16		64
RA1/RA1'		8	3.6	
RA1/RA1'		8	6	
RA1/RA1'		16	12	

adapted to the radio interface. This bit rate adaptation is derived from the V.110 standard used in ISDN in which the bit rates of the synchronous data streams are going through a two-step procedure; first, frames are formed at an intermediate rate which is a multiple of 8 kbit/s; this stream is converted to the channel bit rate of 64 kbit/s (Bocker, 1990). The asynchronous services are preprocessed by a stuffing procedure using stop bits to form a synchronous data stream.

A V.110 procedure modified according to the requirements of the air interface is also used in GSM. In essence, GSM performs a transformation of the data signals from the user data rate (e.g. 2.4 or 9.6 kbit/s) at the R reference point to the intermediate data rate (8 or 16 kbit/s) and finally to the ISDN bit rate of 64 kbit/s. The adaptation function from user to intermediate rate is called RA1; the adaptation function from intermediate rate to ISDN is called RA2. A GSM-specific bit rate adaptation step is added between the intermediate rate and the channel data rate (3.6, 6 or 12 kbit/s) of the traffic channel at the reference point Um of the air interface. This adaptation function from intermediate to channel bit rate is designated as RA1/RA1'. An adaptation function RA1' performs the direct adaptation from user to channel data rate without going through the intermediate data rate. Table A.1 gives an overview of the bit rates at the reference points and the intermediate data rates between the RA modules.

Adaptation frames are defined for the individual bit rate adaptation steps. These frames contain signaling and synchronization data in addition to the user data. They are defined based on V.110 frames, and one distinguishes three types of GSM adaptation frames according to their length (36, 60 and 80 bits) as shown in Figures A.4 and A.5.

The conversion of data signals from user to intermediate rate in the RA1 stage uses the regular 80-bit frame of the V.110 standard. In this adaptation step, groups of 48 user data bits are supplemented with 17 fill bits and 15 signaling bits to form an 80-bit V.110 frame. Owing to the ratio 0.6 of user data to total frame length, this adaptation step converts user data rates from 4.8 into 8 kbit/s and from 9.6 into 16 kbit/s. All user data frames of less than 4.8 kbit/s are 'inflated' to a data signal of 4.8 kbit/s by repeating the individual data bits; for example, a 2.4 kbit/s signal all bits are doubled, or with a 600 bit/s signal the bits are written eight times into an RA1 frame.

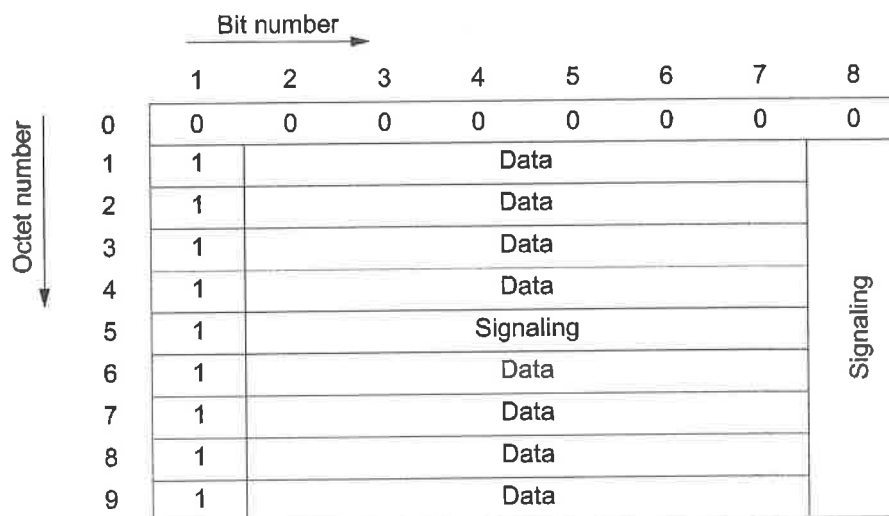


Figure A.4 V.110 80-bit adaptation frame for the RA1 stage.

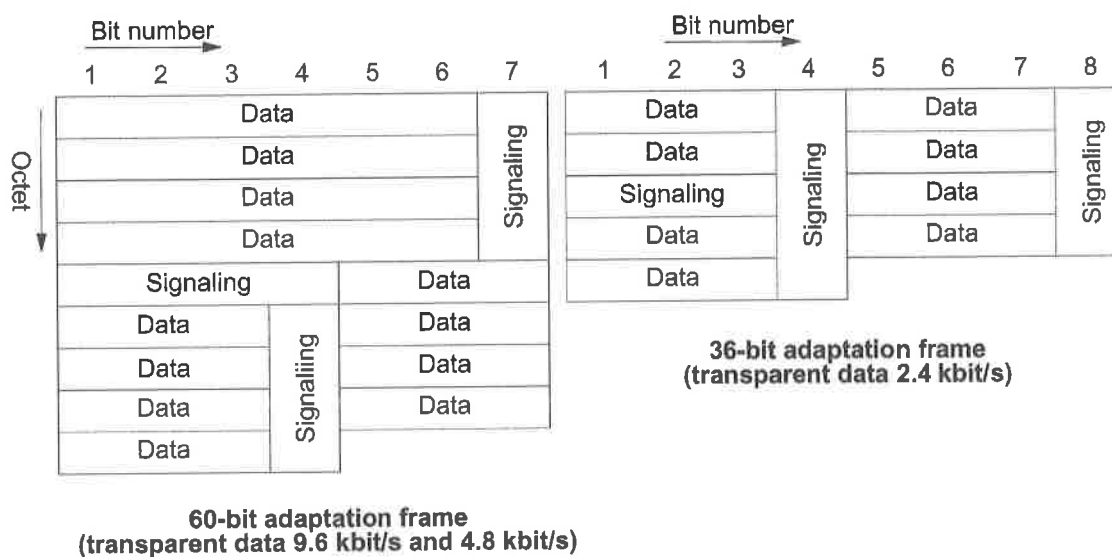


Figure A.5 Modified V.110 adaptation frame for the RA1' stage.

At the conversion of the intermediate data rate to the channel data rate in the RA1/RA1 stage, the 17 fill bits and 3 of the signaling bits are removed from the RA1 frame, since they are only used for synchronization and not needed for transmission across the air interface. This yields a modified V.100 frame of length 60 bits (Figure A.5), and the data rate is adapted from 16 to 12 kbit/s or from 8 to 6 kbit/s, respectively.

In the case of user data rates of 4.8 or 9.6 kbit/s, adaptation to the channel data rate is already complete. Only for user data rates of less than 4.8 kbit/s do additional parts of the multiple user bits need to be removed, which results in a modified V.110 frame of 36 bits. Thus, the user data rates of less than 4.8 kbit/s are adapted to a channel data rate of 3.6 kbit/s.

The user data bits of a 2.4 kbit/s signal are then no longer transmitted twice or the 600 bit/s user data signals are only written four times into the frames of the RA1' stage. This is, however, only true for the transparent bearer services. For the nontransparent bearer services, the modified 60-bit V.110 frame is used completely for the transmission of the 60 data bits of an RLP PDU. The required signaling bits are multiplexed with user data into the RLP frame through L2R.

The modem used for communication over the PSTN resides in the IWF of the MSC, since data are transmitted from here on in digital form within the PLMN. For congestion and flow control and other functions at the modem interface, the interface signals must therefore be carried from the modem through the PLMN to the MS. For this purpose, signaling bits are reserved in the frames of the bit rate adaptation function, which represent these signals and, thus, give the MS direct modem control. The connection of such a bearer service is therefore transparent not only for user data, but also for out-of-band signaling of the (serial) modem interface in the IWF.

A.5 Asynchronous data services

Asynchronous data transmission based on the V. and X. series interfaces is widespread in fixed networks. In order to support such 'nonGSM' interfaces, the MS can include a TA over which standard terminals with a V. or X. interface (e.g. V.24) can be connected. Such an adaptation unit can also be integrated into the MS (MT2, Figure A.1).

Flow control between TA and IWF can be supported in different ways, just as in ISDN.

- *No flow control*: it is handled end-to-end in higher protocol layers (e.g. the transport layer).
- *Inband flow control*: with the X-ON/X-OFF protocol.
- *Out-of-band flow control*: according to V.110 through interface leads 105 and 106.

A.5.1 Transparent transmission in the mobile network

In the case of transparent transmission, data are transmitted with pure Layer 1 functionality. In addition to error protection at the air interface, only bit rate adaptations are performed.

User data are adapted to the traffic channel at the air interface according to the data rate and protected with forward error-correcting codes (FECs) against transmission errors. As an example, Figure A.6 shows the protocol model for transparent asynchronous data transmission over an MT1 with an S interface. Data are first converted in the TE1 or TA into a synchronous data stream by bit rate adaptation (stage RA0). In further stages, data rates are adapted with an MT1 to the standard ISDN (RA1, RA2), and then converted in MT1 over RA2, RA1 and RA1' into the channel bit rate at the air interface. Provided with a FEC, the data are transmitted and then converted again in the BSS by the inverse operations of bit rate adaptation to 64 kbit/s at the MSC interface. However, much more frequently than an MT1 with an (internal) S interface, MSs realize a pure R interface without internal conversion to the full ISDN rate in the RA2 stage. This avoids the bit rate adaptation step RA2 and thus the conversion to the intermediate data rate in the RA1 stage. The signal is converted

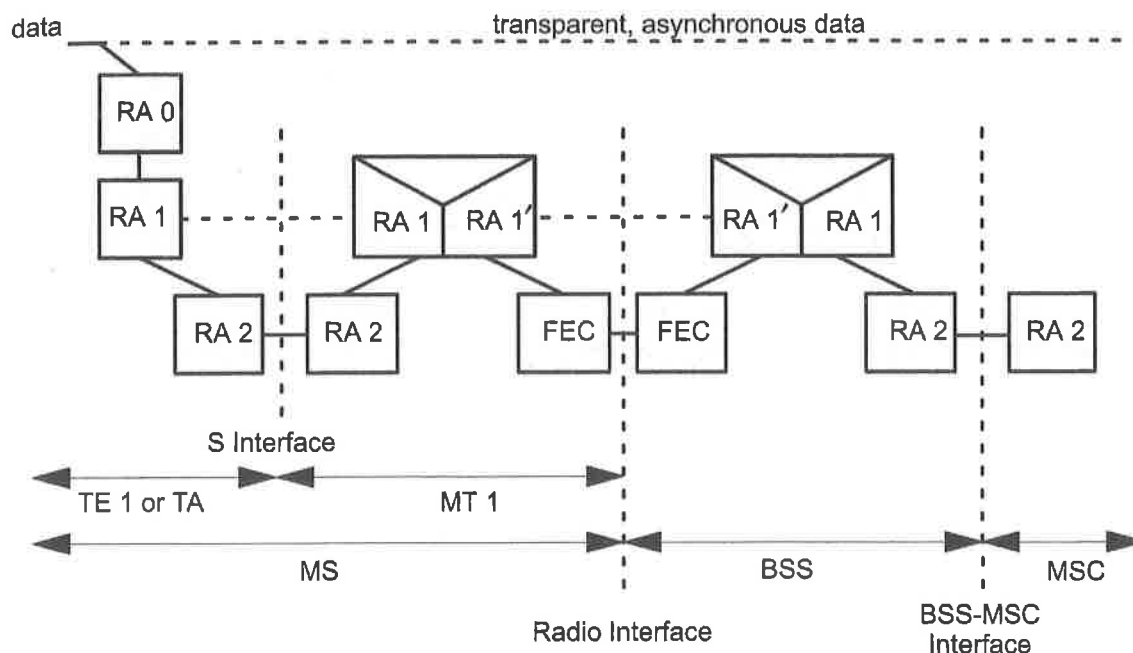


Figure A.6 Transparent transmission of asynchronous data in GSM.

immediately after the asynchronous-synchronous conversion in the RA0 stage from the user data rate to the channel data rate (stage RA1').

A variation without a terminal adapter is shown schematically in Figure A.7. Here the complete interface functionality, Interface Circuit (I/Fcct), for a serial V. interface is integrated with the required adaptation units. The data signals D are converted into a synchronous signal in MT2 (RA0), packed into a modified V.100 frame together with signaling information S from the V. interface, and adapted to the channel data rate (RA1'). After FEC, the data signals are transmitted over the air interface and finally converted for further transmission to the data rate of an ISDN B channel after decoding and potential error correction in the BSS (RA2).

Figure A.8 shows a complete scenario with all appropriate network transitions for a transparent bearer service with modem in the interworking function for the conversion of the digital data signals into an analog voiceband signal. A mobile data terminal uses the transparent bearer service of a GSM PLMN over an R interface (it is also possible to use an S interface). The data are circuit-switched to the IWF in the MSC. To communicate with a modem in the fixed network, the IWF activates an appropriate modem function and converts the digital data signals into an analog voiceband signal. The IWF digitizes this voiceband signal again and passes the data on in PCM-coded format through the GMSC. After the network transition, the data signal is finally transmitted to the modem of the communication partner. This modem can be within a terminal in the PSTN or belong to an ISDN terminal. Before being transmitted in the PSTN, the PCM-coded signal is again converted into an analog voiceband signal. In ISDN the signal is transmitted as a PCM-coded signal of category 3.1 kHz audio; a repeated conversion is not necessary. An ISDN subscriber

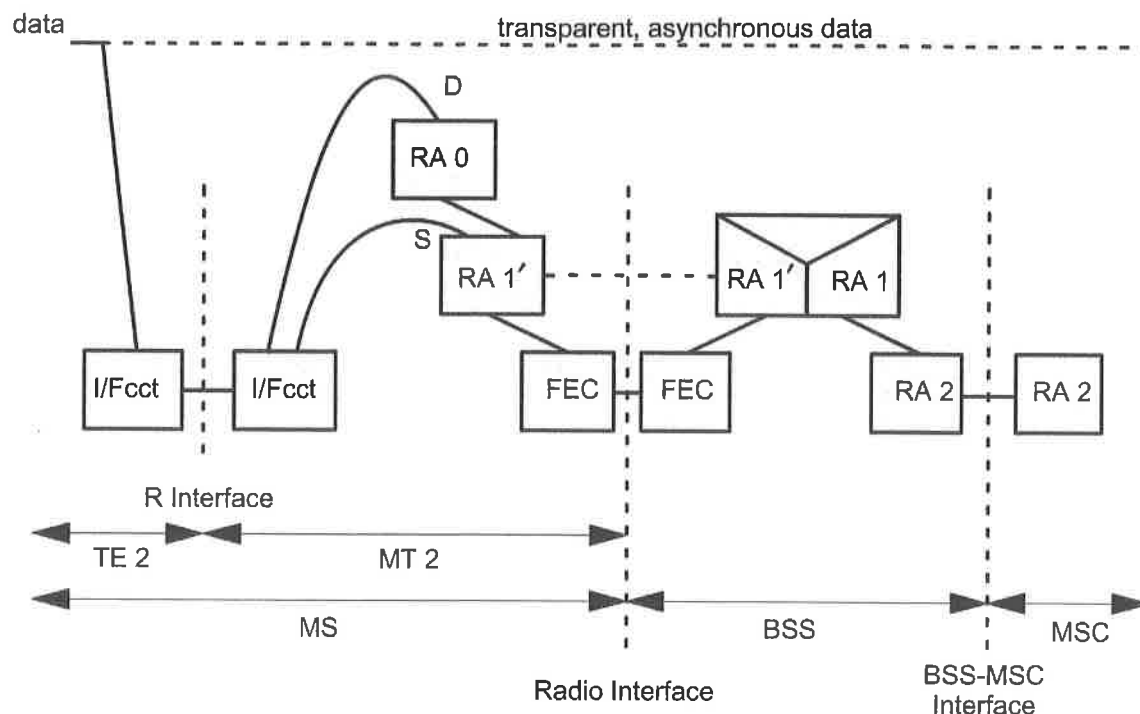


Figure A.7 Transparent transmission of asynchronous data across the R interface.

needs an adaptation unit TA' for the conversion of the digital voiceband signal into an analog signal, which can then be processed further with a modem and passed on to the data terminal.

Another variant consists of a circuit-switched modem connection to a packet-switched network access node, as is possible from fixed connection ports. In these access nodes, the asynchronous modem signals are combined into packets in a Packet-Assembler/Disassembler (PAD) module and then transmitted through the packet-switched network. This variant of packet network access has the disadvantage that one has to switch through to the PAD over a long path, especially in the case of international roaming, since the nearest PAD is not usually the one allowed to access to packet networks.

It is also possible to connect to standard ISDN terminals without an analog modem based on the digital data transmission capability of ISDN. For this purpose, the transmission mode unrestricted digital has been defined. In this case, there is only a bit rate adaptation according to V.110 (Figure A.9). The data arrives at the MSC from the BSS in V.110 frames on an ISDN channel with 64 kbit/s and transparently is passed on to the ISDN using a B channel again in V.110 frames. The otherwise necessary modems are entirely unnecessary in the case of unrestricted digital connections. However, an ISDN subscriber can connect a terminal through an analog modem by using an adaptation unit TA' which converts the unrestricted digital signal into a voiceband signal according to one of the V. standards.

The quality of transparent data services in GSM varies with the radio field conditions. This is illustrated by examples of comparative field measurements of the transparent data service BS26 with 9.6 kbit/s data rate, comparing a moving and a standing MS. Figure A.10 shows the weighted distribution of the bit errors of these two cases for a block length of 1024 bits. The weighted distribution indicates the frequency with which m bit errors occur in a block of

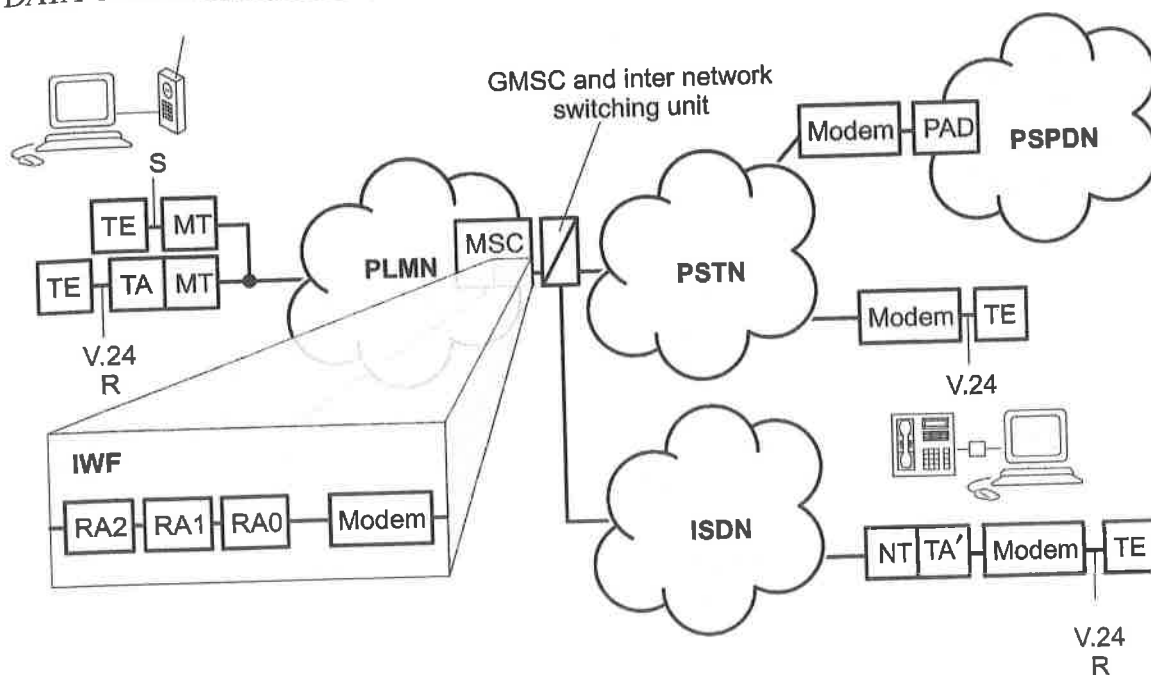


Figure A.8 Principle of transparent asynchronous data transfer (variant with a modem).

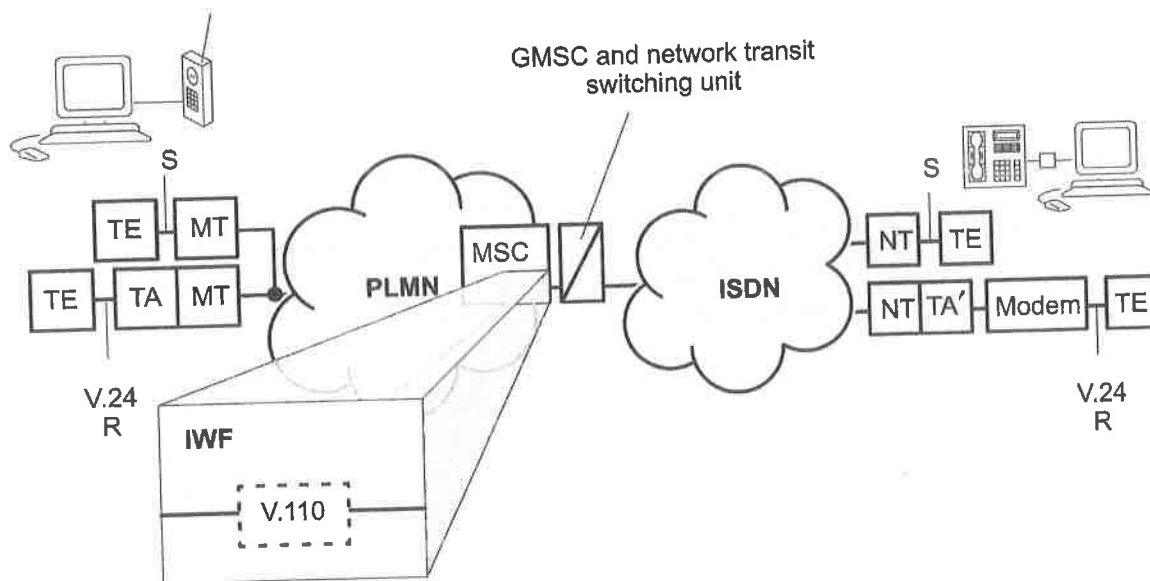


Figure A.9 Transparent data transfer to an ISDN (unrestricted digital).

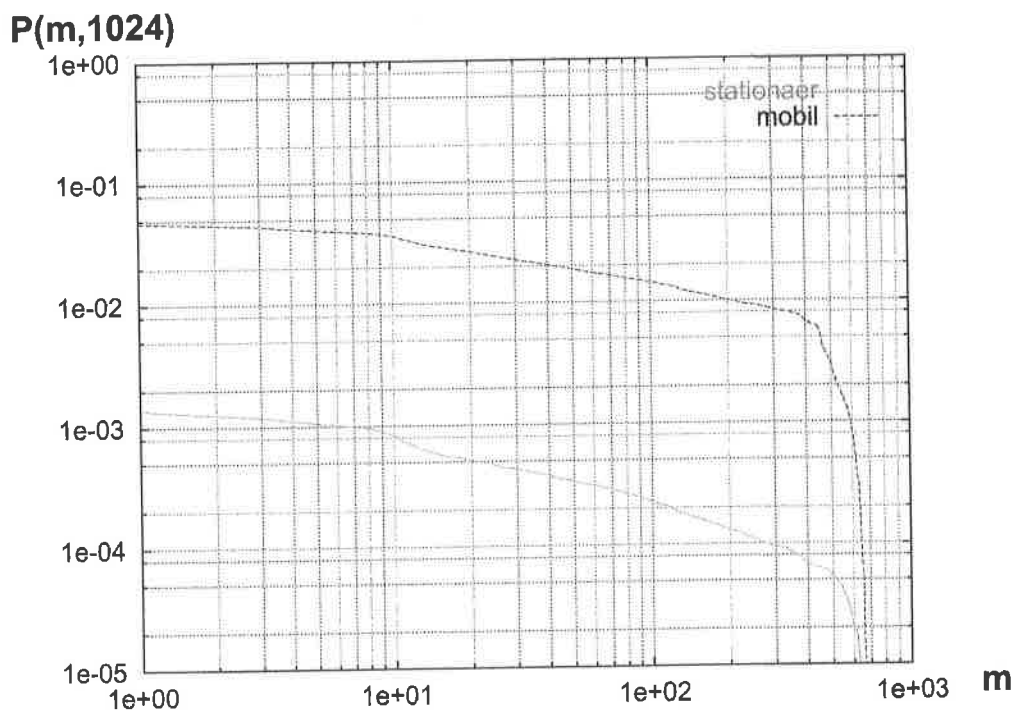


Figure A.10 Weighted distribution of a transparent GSM bearer service (BS26).

length n bits (here $n = 1024$):

$$P(m, n) = \sum_{i=m}^{\infty} P(i \text{ errors in } n\text{-bit-block}).$$

The distribution shown in Figure A.10 represents measurements of the error statistics of BS26 which were performed in 1994 in a suburban area for moving and standing MSs (Vögel *et al.*, 1995). Note that the error frequency for the standing MS ('stationær') is clearly lower than for the moving MS ('mobil'). This result is obtained by averaging measurements over several locations and measurement tours. The resulting mean shows, for the MS, a sometimes heavily varying channel due to the unavoidable fading phenomena, which frequently cause bursts with high bit error ratios, again resulting in an aggregate higher mean bit error ratio and thus also a higher packet error ratio $P(1, 1024)$.

A.5.2 Nontransparent data transmission

In contrast to the transparent transmission mode, the nontransparent mode in GSM data services protects the user data within the PLMN through a Layer 2 protocol, the RLP, in addition to the forward error correction procedures (convolutional coding, interleaving). This protection protocol further reduces the residual bit error ratio of data transmission in the mobile network. However, the automatic repeat requests (ARQ) of the RLP introduces additional transmission delays on the data path, and the effective user data throughput is reduced (protocol overhead).

User data between MT and MSC/IWF is protected on Layer 2 by the RLP. Two kinds of transmission errors are corrected this way: first, those caused by radio interference and remaining uncorrected by forward error correction and, second, those caused through the interruptions of handover. For signaling on the FACCH, time slots are 'stolen' from the data traffic channel, which can cause data losses. The RLP also protects user data against such losses.

For nontransparent data transfer with RLP, an additional sublayer in Layer 2 is required, the L2R protocol. This relay protocol maps user data and status information of the IWF user-modem interface onto the information frames of the RLP. Depending on the kind of user data (character- or bit-oriented), one of two variations of the L2R is used: L2R Bit Oriented Protocol (L2RBOP) or L2R Character Oriented Protocol (L2RCOP). A L2R PDU is handed to RLP as an SDU and inserted into the RLP frame as a data field. The first octet of a L2R PDU always contains control information, such as the status of the signaling lines of the serial interface. Beyond that, the L2R PDU can contain an arbitrary number of such status octets. They are always inserted into the user data stream when the state of the interface changes (e.g. hardware flow control). Thus, of the 200 user data bits (Figure 5.10), only a maximum of 192 can be used for payload. However, since the signaling information is already contained in the L2R PDU, these bits must not be considered for bit rate adaptation. Thus, the modified 60-bit V.110 frame (Figure A.5) can be completely occupied with data bits, and the full channel rate of maximum 12 kbit/s can be used for the transmission of RLP data. Next come a set of four modified V.110 frames which carry a complete RLP frame. Considering the protocol overhead of RLP (16.7%) and the minimum overhead of an L2R PDU (0.5%), one obtains a usable subscriber data rate of up to 9.95 kbit/s.

The protocol model for asynchronous nontransparent character-oriented data transmission over the S interface in GSM is now presented as an example (Figure A.11). Data are transmitted by the L2R protocol, L2RCOP and RLP from the MT1 termination to the MSC. In between, as in the transparent case, are FEC, RA1, RA1' and RA2. The RLP frames are transported in a synchronous mode. Only the user data stream at the user interface is asynchronous, and in the case of the model in Figure A.11 the user data stream must be converted for the S interface into a synchronous data stream (RA0). In the case of a terminal with a V. interface and an MT2 termination (reference point R), this bit rate adaptation at the S interface would be avoided. The asynchronous data are then directly accepted at the serial interface by the L2R (I/Fcct); potential start/stop bits are removed and data are combined into L2R PDUs.

A complete scenario for network transition with nontransparent asynchronous GSM data services is shown in Figure A.12. The RLP is terminated in the MSC/IWF, and user data are converted again into an asynchronous data stream by the associated L2R. For the nontransparent case too, the IWF offers both variants for the network transition: first, using modems and, second, unrestricted digital. In the case of a network transition to the PSTN or to a 3.1 kHz audio connection into ISDN, the respective modem function is inserted and passes PCM-coded data to the GMSC (not shown in Figure A.12), which directs them into the fixed networks. Using several bit rate adaptation steps (RA0 – RA1 – RA2; Figure A.12), the user data can also be converted in the IWF into a synchronous unrestricted digital signal, which is then carried transparently over an ISDN B channel with 64 kbit/s.

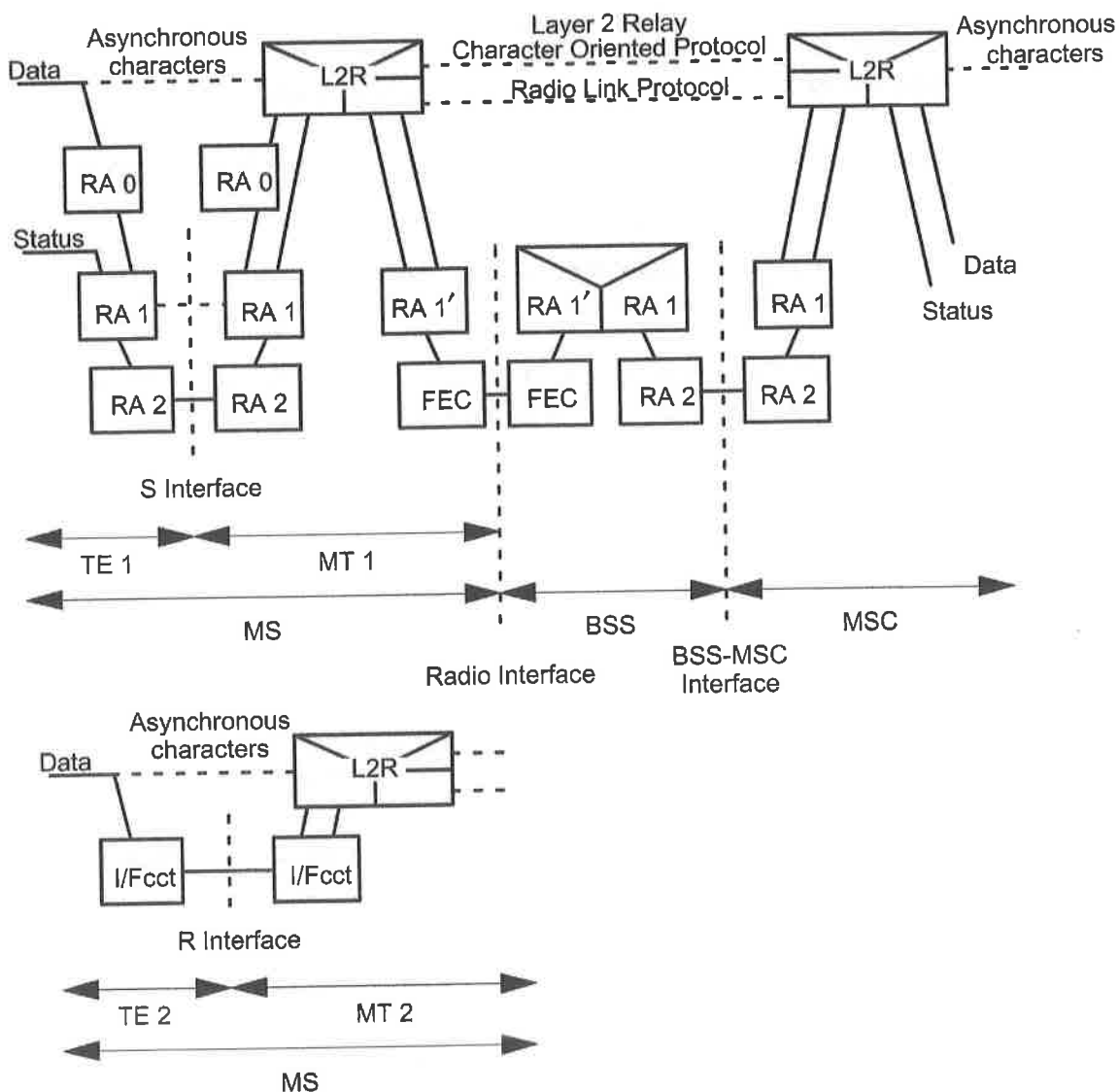


Figure A.11 Nontransparent data transmission in GSM.

A.5.3 PAD access to public packet-switched data networks

Asynchronous connection to PSPDN PADs

As shown in Figures A.8 and A.12, access to PSPDNs, e.g. Accunet in the USA or Datex-P in Germany, is already possible using the asynchronous services of GSM. This requires a PAD in the PSPDN, which packages the asynchronous data on the modem path into X.25 packets and also performs the reverse operation of unpacking. PAD access uses the protocols X.3, X.28 and X.29 (triple X profile). Just as from the fixed network, the mobile subscriber dials the extension of a PAD for access to the service of the PSPDN, provided packet network access is allowed. In this way, the subscriber has the same kind of access to the packet network as a subscriber from the fixed network, aside from the longer transmission delays

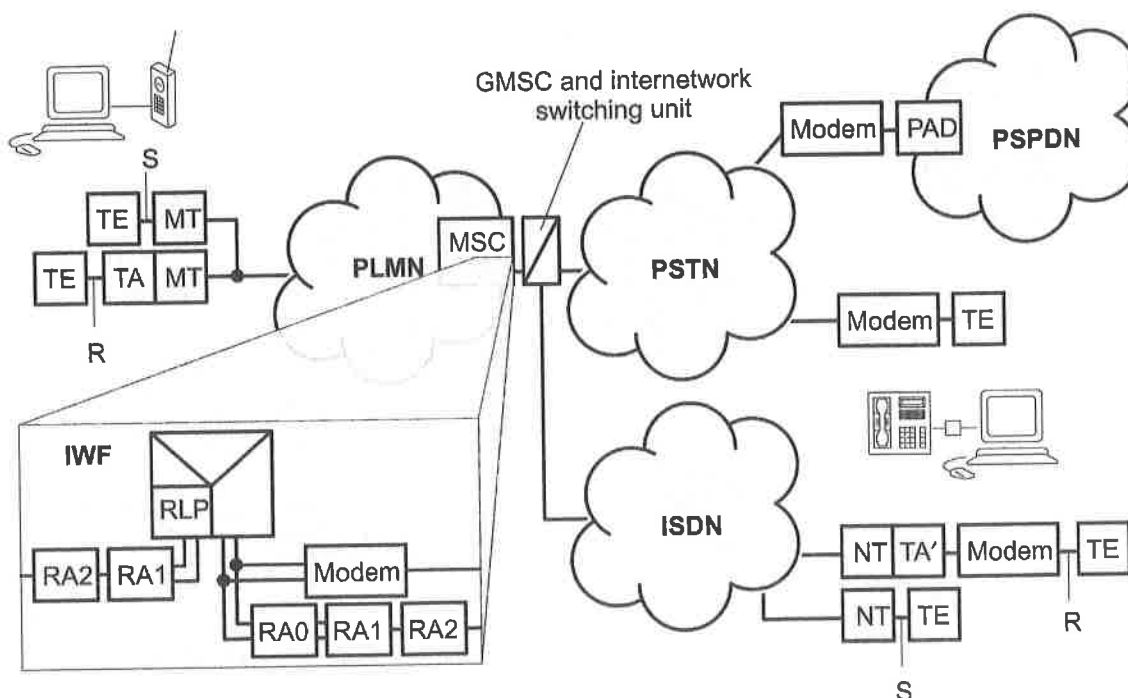


Figure A.12 Principle of nontransparent data transfer.

and the higher bit error ratios. It is therefore recommended to transmit data for PAD access across the air interface in the PLMN in nontransparent mode with RLP (Fuhrmann *et al.*, 1993).

Dedicated PAD access in GSM

However, direct access to packet data networks through the asynchronous GSM data services has disadvantages.

- One needs another subscription to a packet data network operator in addition to GSM.
- Independent of the current mobile subscriber's location, a circuit-switched connection to a PAD of a packet service provider is needed. Sometimes the packet network access is only allowed to specific PADs. This is a particular disadvantage if the mobile subscriber is currently in a foreign GSM network and incurs fees for international lines.

Therefore, GSM has defined another PSPDN access without these disadvantages: dedicated PAD access (Figure A.13). The services are defined as bearer services BS41 through BS46 (Table 4.2). With this kind of PSPDN access from a PLMN, each PLMN has at least one PAD that is responsible for the packaging/unpackaging of the X.25 packets of the respective mobile subscriber.

For this purpose, a PAD is activated as an additional resource in the IWF or in a specially reserved MSC (Figure A.13). This PAD can be reached in asynchronous mode again over transparent or nontransparent PLMN connections. However, with this solution

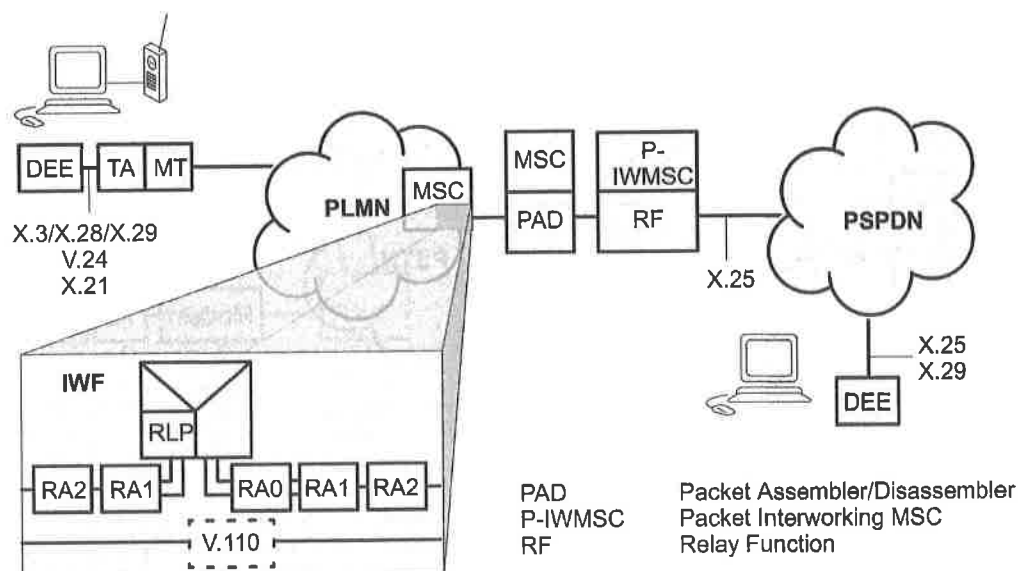


Figure A.13 Dedicated PAD access through asynchronous GSM data services.

the connection to the PAD is as short as possible, since a PAD is already reached in the nearest IWF, and international lines are never occupied for PAD access. Packetization of user data is already performed within the mobile network rather than in the remote PAD of a packet network operator, hence there is no need for a separate subscriber agreement with this packet network operator. The dedicated PAD of the current PLMN is now responsible for the packaging/unpackaging of the asynchronous data into/from X.25 packets, which are then passed on through a specific interworking MSC (P-IW MSC) to a public PSPDN (e.g. Transpac in France or Sprint's Telenet in the USA) (Fuhrmann *et al.*, 1993).

The dedicated PAD has a uniform profile in all GSM networks; it is reached in each network with the same access procedure. Even in foreign PLMNs, a MS therefore gets the earliest and lowest-cost access to the packet data network. Charging occurs to the account of the GSM extension (MSISDN) of the mobile subscriber; a separate Network User Identification (NUI) for the PSPDN is not necessary. However, only outgoing packet connections are possible.

A.6 Synchronous data services

A.6.1 Overview

Synchronous data services allow access to synchronous modems in the PSTN or ISDN as well as to circuit-switched data networks. Such access is not very significant; however, synchronous data services are defined in GSM. The essential differences to the asynchronous data transmission procedures are in bit rate adaptation and modems. For a synchronous data service, no RA0 bit rate adaptation is needed (conversion from asynchronous to synchronous), since data are already in synchronous format. Instead, special synchronous modems are required in the IWF. Synchronous data services can only be offered in

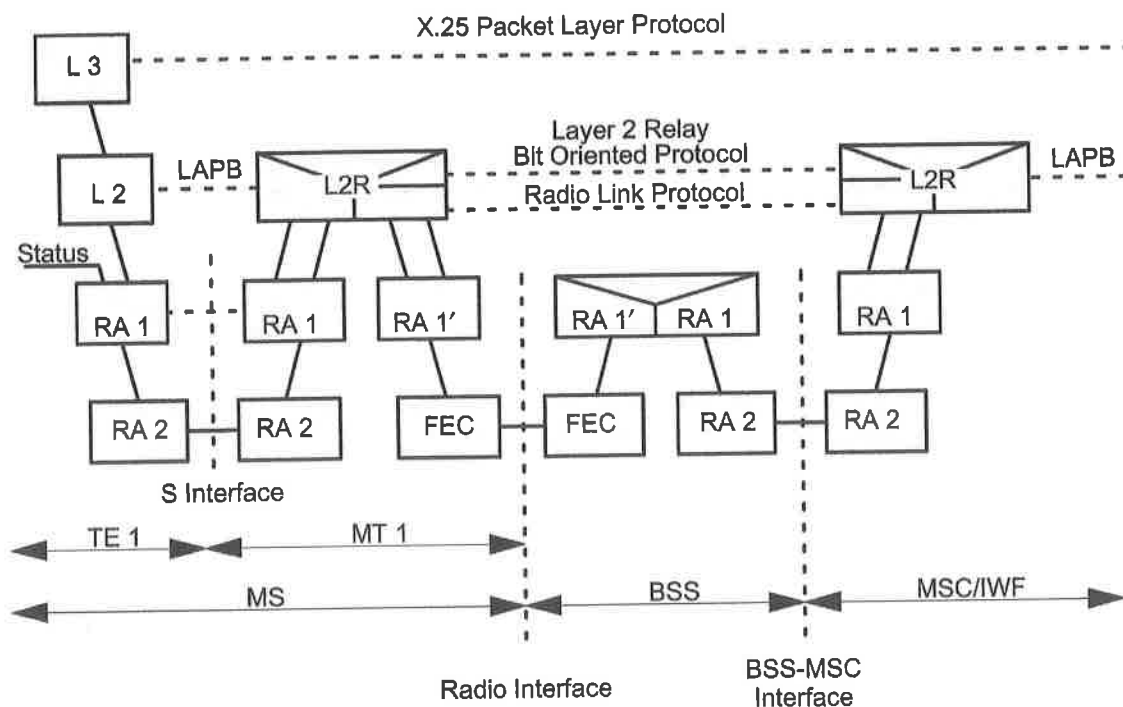


Figure A.14 X.25 access at the ISDN S interface.

transparent mode, with the exception of access to X.25 packet networks, which are a significant application of synchronous data service in GSM.

A.6.2 Synchronous X.25 packet data network access

The protocol model shown in Figure A.14 is the model for synchronous data transmission in nontransparent mode with the packet data access protocol according to the ITU-T standard X.25. Owing to the nontransparent transmission procedure, the X.25 Link Access Procedure B (LAPB) must be terminated in the MT as well as in the IWF. Since LAPB of the X.25 protocol stack operates in a bit-oriented mode, the L2RBOP is required.

Basic packet mode

Two variants of PSPDN access can be realized with the protocol model in Figure A.14:

- PSPDN access according to ITU-T X.32;
- access to PSPDN packet handlers according to ITU-T X.31 Case A (basic packet mode); PSPDN access according to X.32 has not met much acceptance with the applications; the X.31 procedure is used more often.

PSPDN access according to X.32 is the simpler variant. The X.25 packets can be transferred directly over a synchronous modem in the IWF to the PSPDN. This does not necessarily require nontransparent transmission in GSM, but it helps because of the lower bit error ratio. In case of the nontransparent transmission, the LAPB protocol has to be

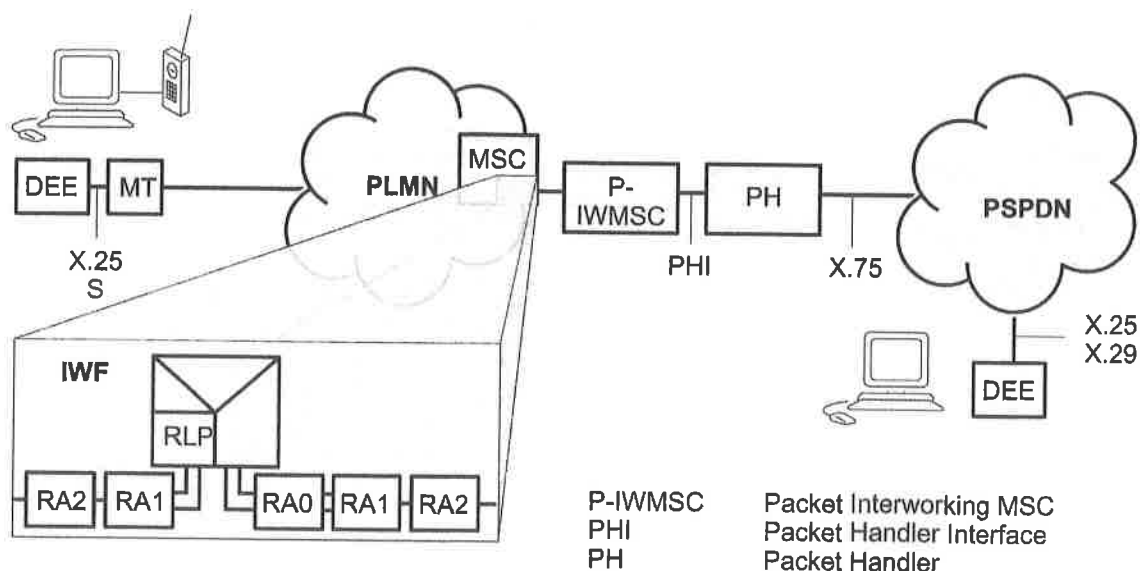


Figure A.15 Dedicated packet mode with packet handler in GSM.

terminated in MT and IWF (see above). The subscriber needs a NUI. Incoming and outgoing packet connections are possible, but again there is the problem of needing circuit-switched connections to the home PLMN, just as in the case of international roaming.

The access procedure according to ITU-T standard X.31 Case A (basic packet mode) is the more favored variant of this group of services. The X.25 packets of the mobile subscriber are passed from the IWF to the packet handler of the ISDN. Since speed adaptation with the X.31 procedure is performed in the ISDN B channel by flag stuffing, the protocol has to be terminated in the IWF, which means that the nontransparent mode of GSM can be used. In this case too, there are connections possible only through the packet handler of the home network.

Dedicated packet mode

As in the case of asynchronous PAD access to packet data networks (see section A.5.3), the synchronous case of the X.25 access protocol also offers an alternative, which allows the most immediate transition to the PSPDN, even if the MS is in a foreign network (international roaming). For this purpose, a dedicated mode is also defined with each PLMN having its own packet handler.

Figure A.15 shows the principle of this dedicated packet mode. It essentially includes the functions of the basic packet mode, with the difference that the packet handler is integrated into the GSM network. Data are transmitted in the PLMN in nontransparent and synchronous mode. Access to the packet handler is the same in all PLMNs, and is also available to foreign mobile subscribers. Since packet data networks do not know roaming, only outgoing data calls are possible.

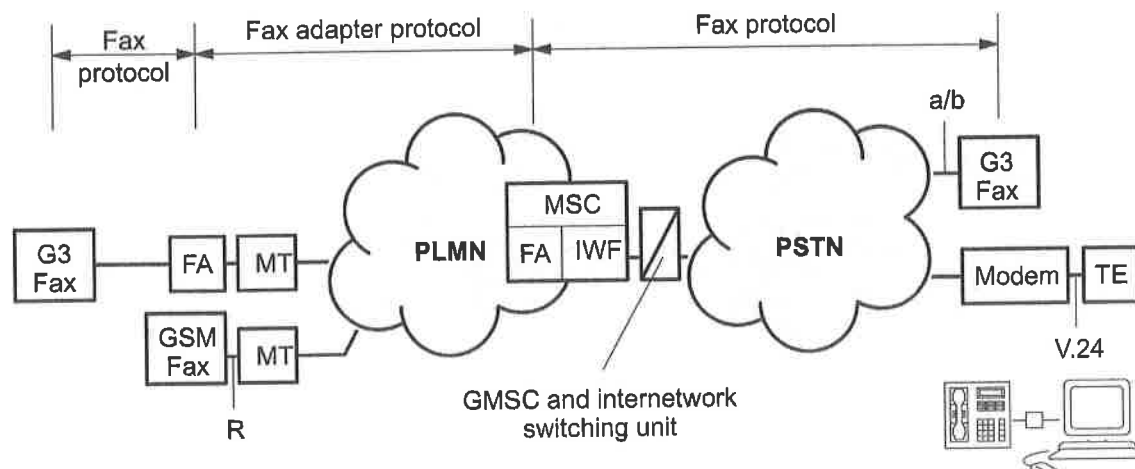


Figure A.16 Fax adapter in GSM.

A.7 Teleservices: fax

In the following, we briefly explain the realization of the GSM fax service.

The GSM standard considers the connection of a regular group 3 fax terminal with its two-wire interface to an appropriately equipped MS as the standard configuration of a mobile fax application. The GSM fax service is supposed to enable this configuration to conduct fax transmissions with standard group 3 fax terminals over mobile connections. This requires mapping the fax protocol of the analog two-wire interface onto the digital GSM transmission, because the fax procedure defines a complete protocol stack with its own modulation, coding, user data compression, inband signaling, etc. Therefore, the Fax Adapter (FA) has been defined for this mapping. The principle is summarized in Figure A.16. The FA of the MS converts the fax protocol of a standard group 3 fax terminal on an analog two-wire line into a GSM internal FA protocol. The PDUs of the adapter protocol are transmitted over the MT with the GSM data services to the FA in the IWF of the MSC, and there they are again converted into the T.30 protocol on the analog line, or transmitted to the ISDN in PCM-coded format, where again a terminal adapter allows the connection of a group 3 fax terminal (not shown in Figure A.16).

A more compact version of a mobile fax terminal is possible if the FA and the group 3 fax terminal are integrated into a compact terminal (GSM fax, Figure A.16). Such equipment can be connected at reference point R to an MT2. It delivers a digital signal directly. With this integration, the analog two-wire line interface becomes superfluous.

Hence, all of the analog functions can be omitted such as demodulation and digitalization of the group 3 fax signals, i.e. the GSM fax needs no analog components such as a modem building block. Therefore, the integrated GSM fax must implement the FA protocol and terminate it at reference point R in order to guarantee correct control of the analog fax components in the FA of the IWF.

A complete fax scenario with the required analog components in the FA is illustrated in Figure A.17. The FA needs several function blocks in the MS as well as in the IWF for the conversion of the fax protocol of the analog a/b interface to the digital transmission procedure

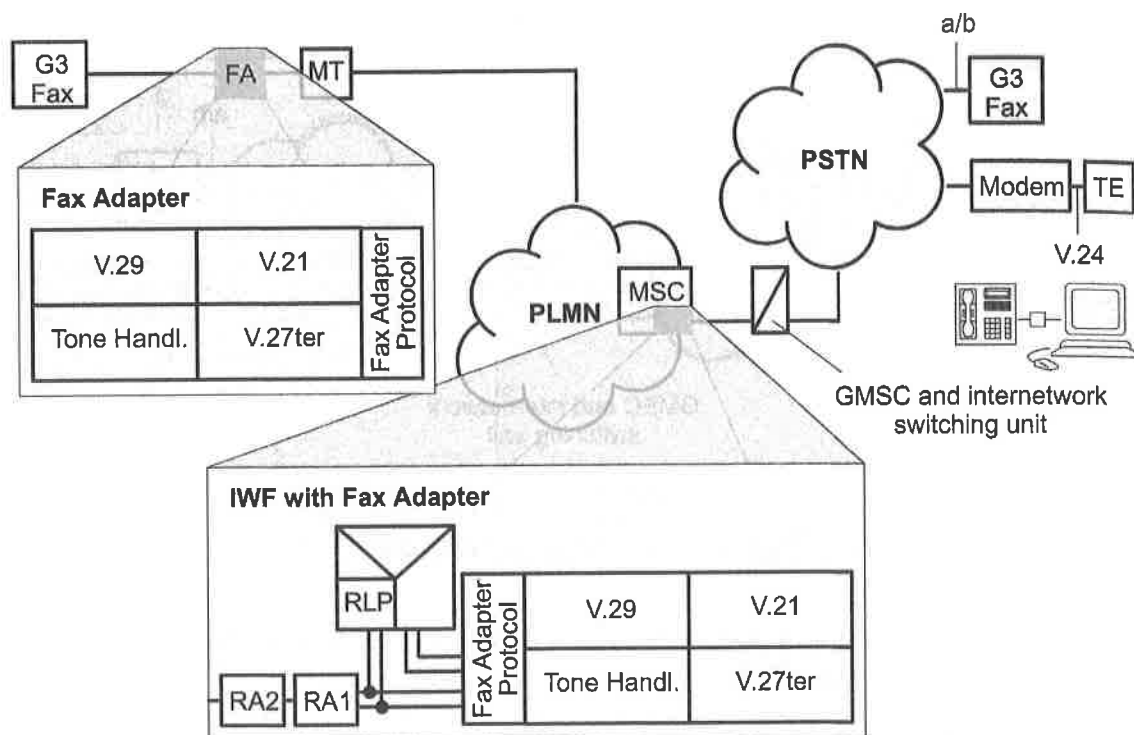


Figure A.17 Overview of the GSM procedure for fax service.

in the PLMN. Group 3 fax equipment according to ITU-T standard T.30 employs three modem building blocks, all three operating in half-duplex mode. A V.21 modem (300 bit/s) is used for the signaling phase to set up a fax connection, whereas the information transfer phase uses a V.27ter modem (4.8 or 2.4 kbit/s) or a V.29 modem (9.6, 4.8 and 2.4 kbit/s). For conversion from analog signaling tones into messages of the fax adapter protocol, the fax adapter needs an additional tone handler. It is used to transfer the (re)digitized fax signals over either a transparent or a nontransparent GSM bearer service to the IWF in the MSC. The fax adapter protocol provides a complete mapping of the T.30 protocol, such that the IWF is able to handle the complete fax protocol with the partner entity. From the view of the partner entity, the complete GSM connection consisting of FA, MS and IWF represents a physical connection with a mobile group 3 fax terminal.

Fax service poses special demands on the service quality of the data channel which the GSM network provides for this teleservice. In particular, propagation delays must remain below a maximum threshold, since timers of the T.30 protocol expire otherwise. This is especially critical if RLP is used to reduce transmission errors, which introduces additional delays into the data path through its ARQ procedure.

Two fax services are specified: the transparent procedure and the nontransparent procedure, depending on the kind of bearer service used. The resulting protocol models are shown in Figures A.18 and A.19, respectively. It is evident that in both cases the fax protocol is superimposed onto the respective bearer service. The transparent fax procedure is easier to realize, although with its transparent bearer service, it incurs a correspondingly variable fax quality.

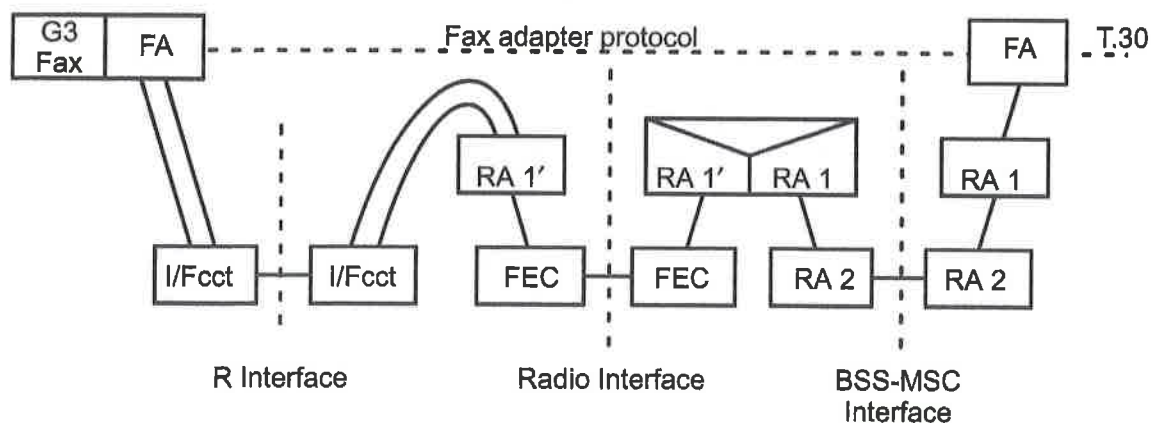


Figure A.18 Transparent fax procedure in GSM radio interface BSS–MSC.

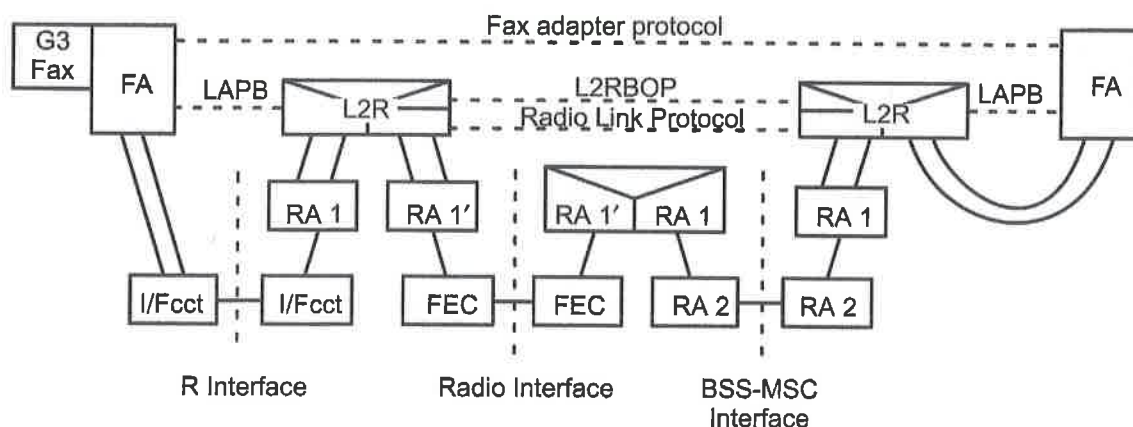


Figure A.19 Nontransparent fax procedure in GSM.

In contrast, the nontransparent fax procedure based on RLP is very well protected against transmission errors, and it delivers very acceptable quality of the transmitted documents over a wide range of distances. However, due to the varying transmission conditions, there are also variable delays of the RLP which lead to intermediate buffering of fax signals in the FA and which, in the worst case, can cause the breakdown of the fax transfer (Decker and Pertz, 1993).

B

Aspects of network operation

For the efficient and successful operation of a modern communication network such as a GSM PLMN, comprehensive Network Management (NM) is mandatory. NM encompasses all functions and activities which control, monitor and record the usage and resource performance of a telecommunication network, with the objective of offering the subscribers telecommunication services of a certain objective level of quality. Various aspects of quality are either defined and prescribed in standards or laid down in operator-specific definitions. Special attention has to be paid to the gap between (mostly simple) measurable technical performance data of the network and the QoS experienced (subjectively) by the subscriber. Modern NM systems should therefore also include (automated) capabilities to accept reports and complaints from subscribers and convert them into measures to be taken by NM (e.g. trouble ticketing systems).

B.1 Objectives of GSM NM

Along with the communication network which realizes the services with its functional units (MS, BSS, MSC, HLR, VLR), one needs to operate a corresponding NM system for support and administration. This NM system is responsible for operation and maintenance of the functional PLMN units and the collection of operational data. The operational data comprise all of the measurement data which characterize performance, load, reliability and usage of the network elements, including times of usage by individual subscribers, which are the basis for the calculation of connection fees (billing). Furthermore, in GSM systems in particular, the techniques supporting security must have counterparts in security management functions of network management. This security management is based on two registers: the Authentication Center (AUC) provides key management for authentication and encryption and the Equipment Identity Register (EIR) provides barring of service access for individual equipment, 'blacklisting'. To summarize, for all functions of the telecommunication network and its individual functional units (network elements), there are corresponding NM functions.

The GSM standard has defined the following overall objectives of NM:

- international operation of NM;
- cost limitation of GSM systems with regard to short-term as well as long-term aspects;
- achievement of service quality which at least matches the competing analog mobile radio systems.

The international operation of a GSM system includes among others the interoperability with other GSM networks (including different countries) and with ISDN networks, as well as the information exchange among network operators (billing, statistical data, subscriber complaints, invalid IMEI, etc.). These NM functions are in large part necessary for network operation allowing international roaming of subscribers, and therefore they must be standardized. Their implementation is mandatory.

The costs of a telecommunication system consist of invested capital and operational costs. The investments comprise the cost of the installation of the network and of the NM, as well as development and licensing costs. The periodically incurred costs include operation, maintenance and administration as well as interest, amortization and taxes. Lost revenues due to failing equipment or partial or complete network failure must be included in the periodically incurred costs, whereas consequential losses due to cases of failure, e.g. because of lost customers, cannot be estimated and included. Therefore, the reliability and maintainability of the network equipment is of course of immense importance and has a large impact on costs. The installation of a NM system on the one hand increases the need for investment capital for the infrastructure as well as for spare capacities in the network. On the other hand, these costs for a standardized comprehensive NM system must be compared with the expenses for administration, operation and maintenance of network elements with manufacturer-proprietary management, or the costs which arise from not recognizing and repairing network failures early enough. Therefore, it has to be the objective of a cost-efficient NM system to define and implement uniform vendor-independent NM concepts and protocols for all network elements, and also to guarantee interoperability of network components from different manufacturers through uniform interfaces within the network.

The QoS to be achieved can be characterized with technical criteria such as speech quality, bit error ratio, network capacity, blocking probability, call disconnection rates, supply probability and availability, and it can also be characterized with nontechnical criteria such as ease of operation and comfort of subscriber access or even hotline and support services.

Considering these objectives, the following functional areas for NM systems can be identified:

- administrative and business area (subscribers, terminal equipment, charging, billing, statistics);
- security management;
- operation and performance management;
- system version control;
- maintenance.

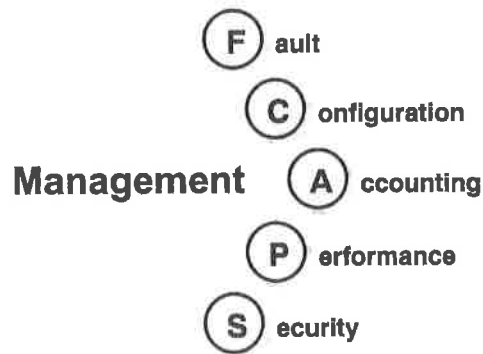


Figure B.1 Functional areas of TMN systems.

These functions are realized in GSM based on the concept of the TMN. In general, they are summarized with the acronym FCAPS – Fault, Configuration, Accounting, Performance and Security management (Figure B.1).

Fault management includes functions such as failure recognition, failure diagnosis, alarm administration and filtering as well as capabilities for the identification of causes of failures or alarms and keeping of failure logs. Configuration management administers network configurations and handles changes, activates/deactivates equipment and provides tools for the automatic determination of network topology and connectivity. Accounting management deals with the subscribers and is responsible for the establishment and administration of subscriber accounts and service profiles. Periodic billing for the individual subscribers originates here, based on measured usage times and durations; statistics are calculated, in certain circumstances only for network subareas (billing domains). In performance management, one observes, measures and monitors performance (throughput, failure rates, response times, etc.) and utilization of network components (hardware and software). The objective is on the one hand to ensure a good utilization of resources and on the other hand to recognize trends leading to overload and to be able to start counter-measures early enough. Finally, security management provides thorough access control, the authentication of subscribers and an effective encryption of sensitive data.

B.2 Telecommunication management network

TMN was standardized within ITU-T/ETSI/CEPT almost simultaneously with the pan-European mobile radio system GSM. The guidelines of the M. series of the ITU-T (M.20, M.30) serve as a framework.

TMN defines an open system with standardized interfaces. This standardization enables a platform-independent multivendor environment for management of all components of a telecommunication network. Essentially, it realizes the communication of a management system with network elements it administers, which are considered as managed objects. These objects are abstract information models of the physical resources. A manager can send commands to these administered objects over a standardized interface, can request or change parameters, or be informed by the objects about events that occurred (notification). For this purpose, an agent resides in the managed object, which generates the management

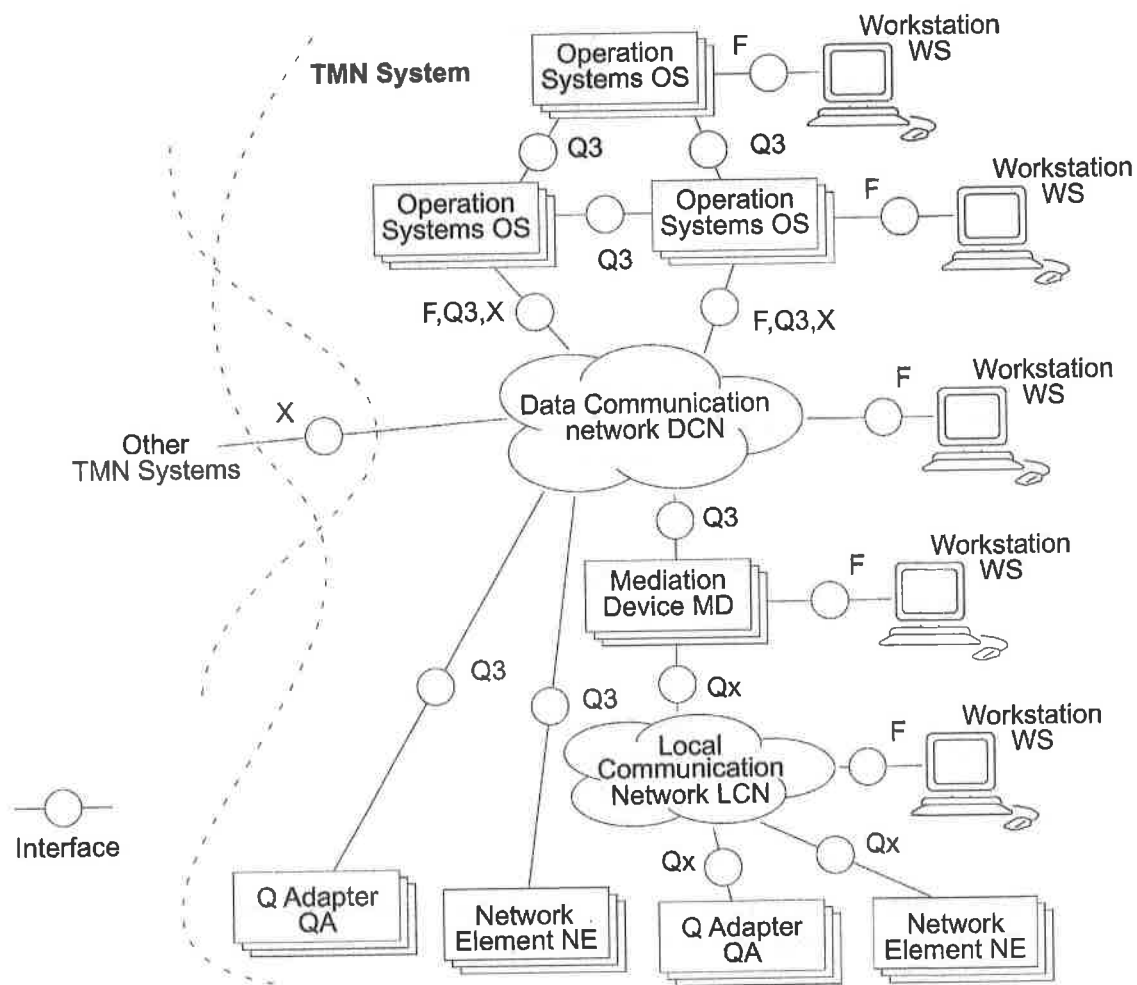


Figure B.2 TMN architecture (according to M.3010 (CCITT Recommendation M.3010, 1992)).

messages or evaluates the requests from the manager, and maps them onto corresponding operations or manipulations of the physical resources. This mapping is system specific as well as implementation dependent and, hence, not standardized. The generalized architecture of a TMN is illustrated in Figure B.2.

The NM proper is realized in an Operation System (OS). The OSs represent the surveillance and control systems of a TMN system. These systems can communicate with each other directly or form hierarchies. A standardized interface Q3 serves for the communication of the OSs within a TMN, whereas the interconnection of two TMN systems occurs over the X interface (Figure B.2). The management functionality can also be subdivided into several logical layers according to the OSI hierarchy. For this approach, TMN provides the Logical Layered Architecture (LLA) as a framework. The exact numbering and corresponding functionality of each LLA plane were not yet finalized in the standardization process at the time of writing, however, the following planes have been found to be useful (Figure B.3): Business Management Layer (BML), Service Management Layer (SML), Network Management Layer (NML) and Element Management Layer (EML).

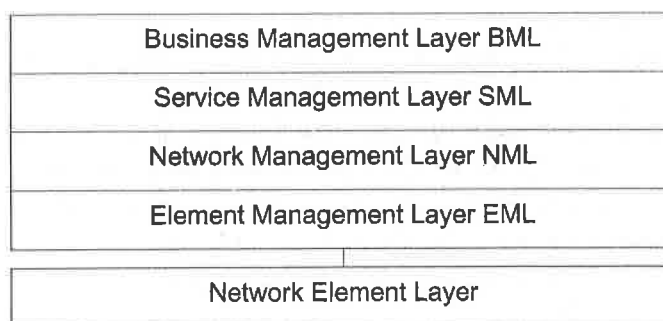


Figure B.3 Logical layered architecture of a TMN system.

The TMN functions of the EML are realized by the network elements (NEs) and contain basic TMN functions such as performance data collection, alarm generation and collection, self diagnosis, address conversion and protocol conversion. Frequently, the EML is also known as a Network EML (NEML) or a Subnetwork Management Layer (SNML) (Sahin, 1993). The NML-TMN functions are normally performed by operation systems and used for the realization of NM applications, which require a network-wide scope. For this purpose, the NML receives aggregate data from the EML and generates a global system view from them. On the SML plane, management activities are performed which concern the subscriber and their service profile rather than physical network components. The customer contact is administered in the SML, which includes functions such as establishing a subscriber account, initializing supplementary services and several others. The highest degree of abstraction is reached in the BML, which has the responsibility for the total network operation. The BML supports strategic network planning and the cooperation among network operators (Sahin, 1993).

For example, an operation system OS could act as a basic OS and be in charge only of a region with a subset of NEs, or it could be a Network OS which communicates with all of the basic OSs and implements network-wide management functionality. As a service OS, an OS assumes network-wide responsibility for the management of one service, whereas on the BML plane, care is taken for charging, billing and administration of the whole network and its services.

The individual functional units of the telecommunication network are mapped into NEs. These elements are abstract representations of the physical components of the telecommunication network, which is administered by this TMN. The OSs communicate with the network elements over a comprehensive data network, a Data Communication Network (DCN). For this purpose, an interface Q3 has been defined, whose protocols comprise all seven layers of the OSI model. However, not every NE must support the full range of Q3 interface capabilities.

For NEs whose TMN interface contains a reduced range of functionality (Qx), a Mediation Device (MD) is interposed, which essentially performs the task of protocol conversion between Qx and Q3. A mediator can serve several NEs with incomplete Q3 interfaces, which can be connected to the mediator through a Local Communication Network (LCN). The functions of a mediator are difficult to define in general and depend on the respective application, since the range of restrictions of a Qx interface with regard to the Q3 interface

is not standardized (Glitho and Hayes, 1995). Therefore, a mediator could, for example, realize functions such as data storage, filtering, protocol adaptation or data aggregation and compression.

In spite of ongoing TMN standardization, new network elements and systems without a TMN interface are continuously added and must be integrated. For such cases, the function of the Q adapter (QA) has been defined. In contrast to the mediator MD, which is prefixed to TMN-capable devices with reduced functionality at the Q interface, a QA allows integration of devices which are not TMN capable, and the QA must therefore be tailored for each respective device.

Finally, the operator personnel have access to the TMN system at the F interface through management Workstations (WSs) in order to perform management transactions and to check or change parameters. Thus, a TMN system gives the network operator at a WS the capability to supply any network element with configuration data, to receive and analyze failure reports and alarms or to download locally collected measurement data and usage information. The TMN protocol stack required for this purpose is based on OSI protocols and comprises all seven layers (see also Figure B.6). The main element of the TMN protocol architecture is the Common Management Information Service Element (CMISE) from the OSI system management, which resides in the application layer (OSI Layer 7) (Sahin, 1993). The CMISE consists of a service definition, the Common Management Information Service (CMIS), and a protocol definition, the Common Management Information Protocol (CMIP). The CMISE defines a uniform message format for requests and notifications between management OS and the managed elements NE or the respective QA.

B.3 TMN realization in GSM networks

TMN and GSM were standardized at approximately the same time, so that there was a good opportunity to apply TMN principles and methods in a complete TMN system for NM in GSM from the beginning and from ground up. For this purpose, specific working groups were founded for the five TMN categories (Figure B.1) as well as for architecture and protocol questions which were supposed to develop as much as possible of the TMN system and its services, while following the top-down methodology (CCITT Recommendation M.3010, 1992; CCITT Recommendation M.3020, 1992) recommended by the ITU-T. This objective could be pretty much achieved, only that the development methodology was complemented by a bottom-up approach which was rooted in the detailed knowledge about the network components being specified at the same time. The intent was to reach the objective of a complete standard earlier (Lin, 1997; Towle, 1995). The five TMN categories are essentially realized for all of the GSM system; however, there are some limitations in failure, configuration and security management. Failure and configuration management are specified only for the BSS; the reasons are that on the one hand the databases (HLR, VLR) were assigned to accounting management, and on the other hand standardization efforts were to concentrate on GSM-specific areas. Concentration on GSM-specific areas thereby excluded failure and configuration management for the MSC, which from the management point of view is essentially a standard ISDN switching exchange. For the same reasons, security management is also limited to GSM-specific areas.

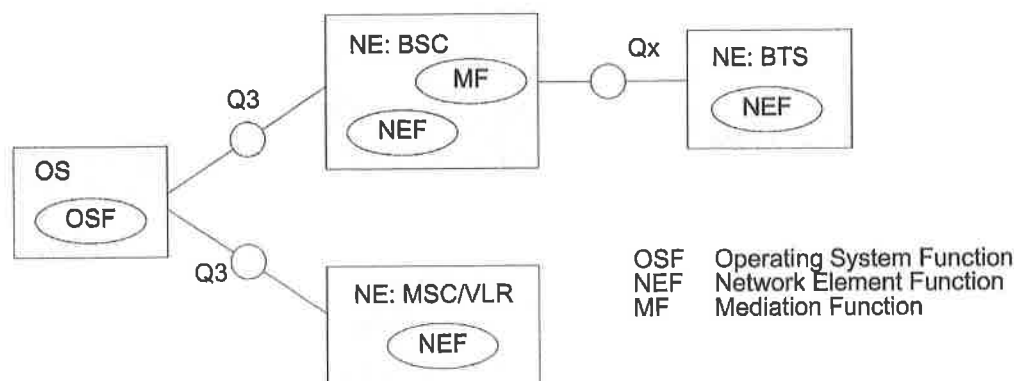


Figure B.4 A simple TMN architecture of a GSM system (according to Towle (1995)).

The resulting GSM TMN architecture is shown schematically in Figure B.4. In GSM, the BSC and the MSC have a Q3 interface as network elements to the OS. In addition to the BSS management, the BSC NE always contains a Mediation Function (MF) and a Qx interface to the NE supporting the BTS functionality.

An object-oriented information model of the network has been defined for the realization of the GSM TMN services. The model contains more than 100 Managed Object Classes (MOCs) with a total of about 500 attributes. This includes the ITU-T standard objects as well as GSM-specific objects, which include the GSM NEs (BSS, HLR, VLR, MSC, AUC, EIR) on the one hand, but also represent network and management resources (e.g. for SMS service realization or for file transfer between OS and NE) as managed objects. These objects usually contain a state space and attributes which can be checked or changed (request) as well as mechanisms for notification, which report the state or attribute changes. In addition, there are commands for creation or deletion of objects, e.g. in the HLR with create/modify/delete subscriber or create/modify/delete MSISDN or in the EIR with create/interrogate/delete equipment (Towle, 1995). File transfer objects are used, in particular, in the information model dealing with the registers, since it involves the movement of large amounts of data.

The TMN communication platform to be used as a DCN can be either an OSI X.25 packet network or the SS#7 signaling network (MTP and SCCP). Both offer a packet-switching service which can be used to transport management messages. Each NE is connected to this MN over a Management Network Access Point (MNAP); see Figure B.5.

If the TMN uses X.25, the DCN can be the public PSPDN or a dedicated packet-switching network within the PLMN with the MSC as a packet-switching node. In addition, the MSC can include an interworking function for protocol conversion from an external X.25 link to the SS#7 SCCP, which realizes the connection of the OMC to the PLMN through an external X.25 link. Further transport of management messages is then performed by the SS#7 network internal to the PLMN.

The framework defined for the GSM TMN protocol stack at the Q3 interface is presented in Figure B.6. The end-to-end transport of messages between OS and NE is realized with the OSI Class 2 transport protocol (TP2), which allows the setup and multiplexing of end-to-end transport connections over an X.25 or SCCP connection. Error detection and data security are

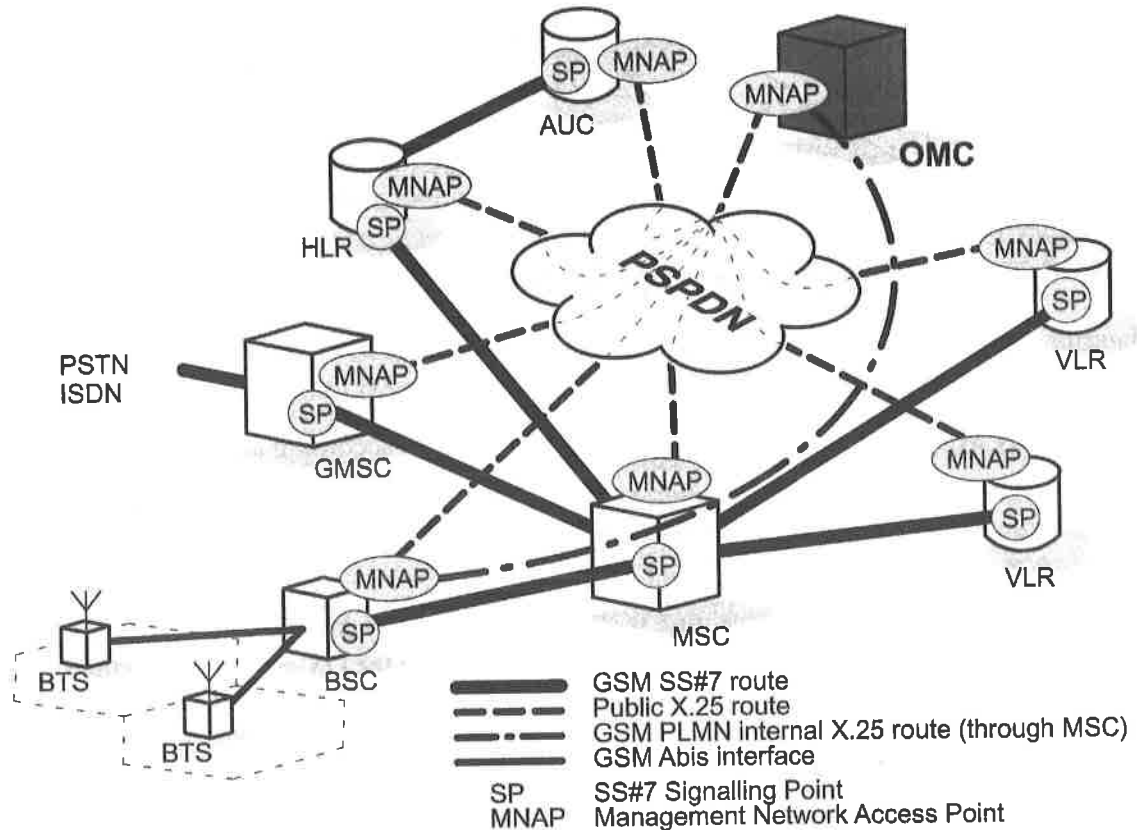


Figure B.5 Potential signaling interfaces in a GSM TMN.

not provided in TP2; they are not needed since X.25 as well as SCCP offer a secure message transport service already.

Of course, the OSI protocol stack also needs the protocols for the data link and presentation layers. The OSI CMISE plays the central role in GSM network management. Its services are used by a System Management Application Process (SMAP) to issue commands, to receive notifications, to check parameters, etc. For file transfer between objects, GSM TMN uses the OSI File Transfer Access and Management (FTAM) protocol. It is designed for the efficient transport of large volumes of data.

CMISE needs a few more Service Elements (SEs) in the application layer for providing services: the Association Control Service Element (ACSE) and the Remote Operations Service Element (ROSE). The ACSE is a sublayer of the application layer which allows application elements (here CMISE) to set up and take down connections between each other. The ROSE services are realized with a protocol which enables initiation or execution of operations on remote systems. In this way ROSE implements the paradigm also known as Remote Procedure Call (RPC).

There is also a management system for the signaling components of a GSM system. This SS#7 SMAP uses the services of the Operation Maintenance and Administration Part (OMAP) which allows observation, configuration and control of the SS#7 network resources. Essentially, the OMAP consists of two Application Service Elements (ASEs), the MTP

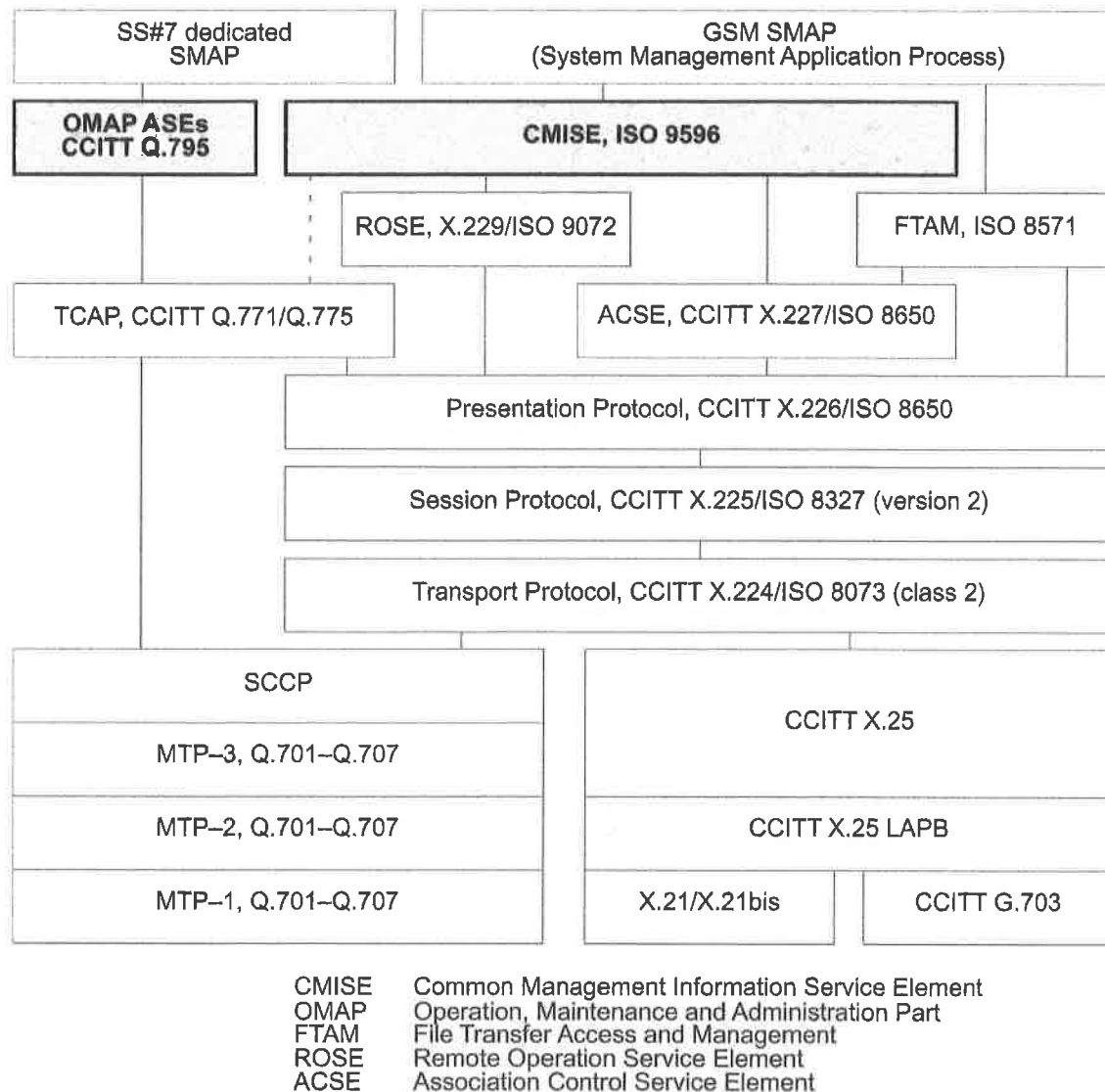


Figure B.6 GSM network management protocols at the Q3-interface.

Routing Verification Test (MRVT) and the SCCP Routing Verification Test (SRVT), which allow verification of whether the SS#7 network works properly on the MTP or SCCP planes. Another management application part is BSSOMAP which is used to transport management messages from OMC to BSC through the MSC over the A interface and to execute management activities for the BSS (Figure B.7; and compare it with Figure 5.11) (Schmidt, 1993).

Network management is usually organized in a geographically centralized way. For the remote surveillance and control of NM functions there are usually one or more Operation and Maintenance Centers (OMCs). For efficient NM, these OMCs can be operated as regional subcenters according to the LLA hierarchy of the various TMN management planes, and they can be combined under a central Network Management Center (NMC); see Figure B.8.

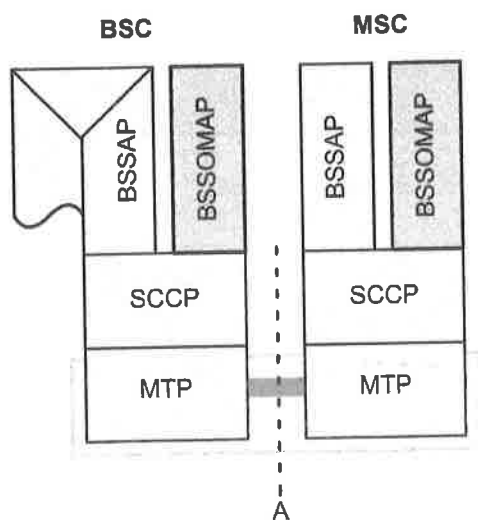


Figure B.7 Operation and maintenance of the BSS.

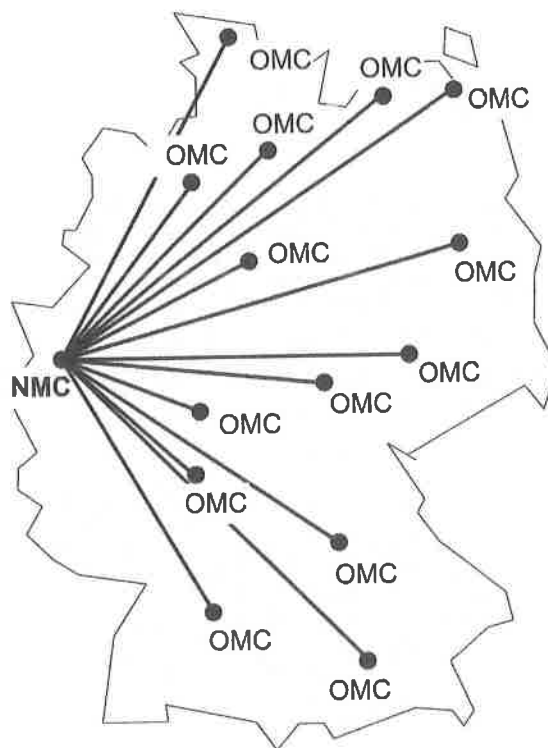


Figure B.8 Hierarchical organization of network management within Germany.

C

GSM Addresses

BCC Base Transceiver Station Color Code
BSIC Base Transceiver Station Identity Code
(M)CC (Mobile) Country Code
CI Cell Identifier
FAC Final Assembly Code
GCI Global Cell Identity
IMEI International Mobile Equipment Identity
IMSI International Mobile Subscriber Identity
LAC Location Area Code
LAI Location Area Identity
LMSI Local Mobile Subscriber Identity
MNC Mobile Network Code
MSIN Mobile Subscriber Identification Number
MSISDN Mobile Station ISDN Number
MSRN Mobile Station Roaming Number
NCC Network Colour Code
NDC National Destination Code
NMSI National Mobile Subscriber Identity
SN Subscriber Number
SNR Serial Number
TAC Type Approval Code
TMSI Temporary Mobile Subscriber Identity

Additional Addresses for GPRS

APN Access Point Name
GSN Address GPRS Support Node Address
(e.g. IP address of SGSN and GGSN)
GSN Number GPRS Support Node Number
(for SGSN and GGSN for communication
with e.g. HLR and VLR)
IP Address Internet Protocol address
NSAPI Network layer Service Access Point
Identifier
P-TMSI Packet Temporary Mobile Subscriber
Identity
PDP Address PDP Address (e.g. IP address,
X.25 address)
RAC Routing Area Code
RAI Routing Area Identity
TID Tunnel Identifier (= MSI + NSAPI)
TLLI Temporary Logical Link Identifier

D

List of Acronyms

3GPP 3rd Generation Partnership Project	BIC-Roam Barring of Incoming Calls when Roaming Outside the Home PLMN
3GPP2 3rd Generation Partnership Project 2	B-ISDN Broadband ISDN
3PTY Three Party Service	Bm Mobile B Channel
8-PSK 8 Phase Shift Keying	BN Bit Number
A3, A5, A8 Encryption Algorithms	BOIC Barring of Outgoing International Calls
AB Access Burst	BOIC-exHC Barring of Outgoing International Calls except those to Home PLMN
Abis BTS-BSC Interface	BSC Base Station Controller
ACELP Algebraic Code Excitation Linear Prediction	BSIC Base Transceiver Station Identity Code
ACSE Association Control Service Element	BSN Block Sequence Number
AGCH Access Grant Channel	BSS Base Station Subsystem
AMR Adaptive Multi-rate (codec)	BSSAP Base Station System Application Part
AOC Advice of Charge	BSSAP+ Base Station System Application Part +
ARQ Automatic Repeat Request	BSSGP Base Station System GPRS Application Protocol
ASCI Advanced Speech Call Items	BSSMAP Base Station System Management Application Part
ASE Application Service Element	BTS Base Transceiver Station
ATM Asynchronous Transfer Mode	BTSM Base Transceiver Station Management
AUC Authentication Center	CA Cell Allocation
BAIC Barring of All Incoming Calls	CAMEL Customized Applications for Mobile Network Enhanced Logic
BAOC Barring of All Outgoing Calls	CAP CAMEL Application Part
BCC Base Transceiver Station Color Code	CBCH Cell Broadcast Channel
BCCH Broadcast Control Channel	CC Country Code
BCH Broadcast Channel	
BCS Block Check Sequence	
BFI Bad Frame Indication	
BG Border Gateway	

CCBS Completion of Call to Busy Subscriber	DHCP Dynamic Host Configuration Protocol
CCCH Common Control Channel	Dm Mobile D Channel
CDMA Code Division Multiple Access	DNS Domain Name Service
CELP Code Excited Linear Prediction Coding	DRX Discontinuous Reception
CFB Call Forwarding on Mobile Subscriber Busy	DSL Digital Subscriber Line
CFNRc Call Forwarding on Mobile Subscriber Not Reachable	DTMF Dual Tone Multiple Frequency
CFNRy Call Forwarding on No Reply	DTX Discontinuous Transmission
CFU Call Forwarding Unconditional	DTAP Direct Transfer Application Part
CI Cell Identifier	DVB Digital Video Broadcast
C/I Carrier-to-Interference Ratio	ECSD Enhanced Circuit Switched Data
CIR Carrier-to-Interference Ratio	EDGE Enhanced Data Rates for Global (GSM) Evolution
CLIP Calling Number Identification Presentation	EFR Enhanced Full Rate (CODEC)
CLIR Calling Number Identification Restriction	EGPRS Enhanced GPRS
CLNS Connectionless Network Service	EIR Equipment Identity Register
CM Connection Management	EMLPP Enhanced Multi-Level Precedence and Pre-emption Service
CMISE Common Management Information Service Element	EMS Enhanced Messaging Service
CN Core Network	E-OTD Enhanced Observed Time Difference
CODEC Coder/Decoder	ERMES European Radio Messaging Standard
COLP Connected Line Identification Presentation	ETSI European Telecommunication Standards Institute
COLR Connected Line Identification Restriction	FA Fax Adapter
CONF Conference Calling	FAC Final Assembly Code
CONS Connection-Oriented Network Service	FACCH Fast Associated Control Channel
CPS Coding and Puncturing Scheme	FCAPS Fault, Configuration, Accounting, Performance, Security
CRC Cyclic Redundancy Check	FB Frequency Correction Burst
CT Call Transfer	FCCH Frequency Correction Channel
CUG Closed User Group	FCS Frame Check Sequence
CW Call Waiting	FDD Frequency Division Duplex
DAB Digital Audio Broadcast	FDMA Frequency Division Multiple Access
DB Dummy Burst	FEC Forward Error Correction
DCCH Dedicated Control Channel	FN TDMA Frame Number
DCN Data Communication Network	FPH Freephone Service
DECT Digital Enhanced Cordless Telecommunication	FPLMTS Future Public Land Mobile Telecommunication System
	FTAM File Transfer Access and Management
	GCR Group Call Register
	GEA GPRS Encryption Algorithm

GGSN Gateway GPRS Support Node	L2RCOP Layer 2 Relay Character-Oriented Protocol
GMLC Gateway Mobile Location Center	LA Location Area
GMM/SM GPRS Mobility Management and Session Management protocol	LAC Location Area Code
GMSC Gateway MSC	LAI Location Area ID
GMSK Gaussian Minimum Shift Keying	LAPDm Link Access Procedure D mobile
GPRS General Packet Radio Service	LCN Local Communication Network
GPS Global Positioning System	LCS Location Service
GSC GSM Speech Codec	LEO Low Earth Orbiting satellite
GSM Global System for Mobile Communication	LLC Logical Link Control layer
GSMSS GSM Satellite System	LMSI Local Mobile Subscriber Identity
GSN GPRS Support Node	LPC Linear Predictive Coding
GTP GPRS Tunnelling Protocol	LTE Long Term Evolution
HARQ Hybrid Automatic Repeat Request	LTP Long Term Prediction
HCS Header Check Sequence	MA Mobile Allocation
HLR Home Location Register	MAC Medium Access Control layer
HSCSD High Speed Circuit Switched Data	MAH Mobile Access Hunting
HSDPA High Speed Downlink Packet Access	MAIO Mobile Allocation Index Offset
HSN Hopping Sequence Number	MAP Mobile Application Part
HSUPA High Speed Uplink Packet Access	MC Multi Carrier
HTML Hypertext Markup Language	MCI Malicious Call Identification
HTTP Hypertext Transport Protocol	MD Mediation Device
IMEI International Mobile Equipment Identity	MEO Medium Earth Orbiting satellite
IMSI International Mobile Subscriber Identity	MexE Mobile Station Application Execution Environment
IMT-2000 International Mobile Telephone System 2000	MHS Message Handling System
IN Intelligent Network	MIMO Multiple Input Multiple Output
INAP Intelligent Network Application Part	MM Mobility Management
IP Internet Protocol	MMI Man-Machine Interface
IPv4 Internet Protocol Version 4	MMS Multimedia Messaging Service
IPv6 Internet Protocol Version 6	MMS-C Multimedia Messaging Service-Center
ISC International Switching Center	MMSE Multimedia Messaging Service Environment
ISDN Integrated Services Digital Network	MMSNA Multimedia Messaging Service Network Architecture
IWF Interworking Function	MNC Mobile Network Code
Kc Cipher/Decipher Key	MOS Mean Opinion Score
Ki Subscriber Authentication Key	MS Mobile Station
L2R Layer 2 Relay	MSC Mobile Switching Center
L2RBOP Layer 2 Relay Bit-Oriented Protocol	MSIN Mobile Subscriber Identification Number

MSISDN Mobile Station ISDN Number	PDN Packet Data Network
MSK Minimum Shift Keying	PDP Packet Data Protocol
MSRN Mobile Station Roaming Number	PDTCH Packet Data Traffic Channel
MSS Mobile Satellite System	PDU Protocol Data Unit
MT Mobile Termination	PLL Physical Link Layer
MTP Message Transfer Part	PLMN Public Land Mobile Network
NB Normal Burst	PNCH Packet Notification Channel
NCC Network Colour Code	PPCH Packet Paging Channel
NCH Notification Channel	PRACH Packet Random Access Channel
NDC National Destination Code	PSK Phase Shift Keying
NE Network Element	PSPDN Packet Switched Public Data Network
NMSI National Mobile Subscriber Identity	PTCCH Packet Timing Advance Control Channel
NMT Nordic Mobile Telephone	PTM Point-to-Multipoint Service
NS Network Service	PTM-G Point-to-Multipoint Service – Group Call
NSAPI Network Layer Service Access Point Identifier	PTM-M Point-to-Multipoint Service – Multicast
OFDMA Orthogonal Frequency Division Multiple Access	P-TMSI Packet Temporary Mobile Subscriber Identity
OHG Operators Harmonization Group	PTP Point-to-Point Service
OMAP Operation, Maintenance and Administration Part	QN Quarter Bit Number
OMC Operation and Maintenance Center	QoS Quality of Service
OMSS Operation and Maintenance Subsystem	RA Rate Adaptation
OS Operation System	RA Routing Area
OSI Open Systems Interconnection	RACH Random Access Channel
P-IW MSC Packet Interworking MSC	RAI Routing Area Identity
PACCH Packet Associated Control Channel	RAND Random Number (for authentication)
PAD Packet Assembler/Disassembler	REVC Reverse Charging
PAGCH Packet Access Grant Channel	RFCH Radio Frequency Channel
PBCCH Packet Broadcast Control Channel	RFL Physical RF Layer
PBX Private Branch Exchange	RFN Reduced TDMA Frame Number
PCCCH Packet Common Control Channel	RLC Radio Link Control layer
PCH Paging Channel	RLL Radio in the Local Loop
PCN Personal Communication Network	RLP Radio Link Protocol
PCS Personal Communication System	ROSE Remote Operation Service Element
PDA Personal Digital Assistant	RPE Regular Pulse Excitation
PDCH Packet Data Channel	RR Radio Resource Management
PDN Public Data Network	SACCH Slow Associated Control Channel
	SAT SIM Application Toolkit
	SATIG Satellite Interest Group

SB Synchronization Burst	TA Timing Advance
SCCP Signaling Connection Control Part	TAC Type Approval Code
SC-FDMA Single Carrier FDMA	TACS Total Access System
SCH Synchronization Channel	TAF Terminal Adaptation Function
SCN Sub Channel Number	TBF Temporary Block Flow
SCP Service Control Point	TCAP Transaction Capabilities Application Part
SDCCH Stand-alone Dedicated Control Channel	TCH Traffic Channel
SDMA Space Division Multiple Access	TCP Transmission Control Protocol
SFIR Spatial Filtering for Interference Reduction	TD-CDMA Time Division CDMA
SGSN Serving GPRS Support Node	TDD Time Division Duplex
SID Silence Descriptor	TDMA Time Division Multiple Access
SIM Subscriber Identity Module	TD-SCDMA Time Division Synchronous CDMA
SM-CP Short Message Control Protocol	TETRA Terrestrial Trunked Radio
SM-RP Short Message Relay Protocol	TFI Temporary Flow Identifier
SMLC Serving Mobile Location Center	TFO Tandem Free Operation
SMS Short Message Service	TID Tunnel Identifier
SMS-GMSC Short Message Service – Gateway MSC	TLI Temporary Logical Link Identifier
SMS-IW MSC Short Message Service – Interworking MSC	TLS Transport Layer Security
SMS-SC Short Message Service – Service Center	TMN Telecommunication Management Network
SMSCB Short Message Service Cell Broadcast	TMSI Temporary Mobile Subscriber Identity
SMSS Switching and Management Subsystem	TN Time Slot Number
SN Subscriber Number	TOA Time of Arrival
SND CP Subnetwork Dependent Convergence Protocol	TSC Training Sequence Code
SNR Serial Number	UDI Unrestricted Digital Information
SNR Signal to Noise Ratio	UDP User Datagram Protocol
SOSS Support of Operator Specific Services	Um Air/Radio Interface
SP Signaling Point	UMTS Universal Mobile Telecommunication System
SPC Signaling Point Code	UPT Universal Personal Telecommunication
SRES Session Key (for authentication)	URAN UMTS Radio Access Network
SS Supplementary Services	URL Universal Resource Locator
SSL Secure Socket Layer	USF Uplink State Flag
SSP Service Switching Point	UTRA UMTS Terrestrial Radio Access
TA Terminal Adaptor	UTRAN UMTS Terrestrial Radio Access Network
	UUS User to User Signaling
	UWCC Universal Wireless Communications Consortium

VAD Voice Activity Detection	WML Wireless Markup Language
VBS Voice Broadcast Service	WRC World Radio Conference
VGCS Voice Group Call Service	WSP Wireless Session Protocol
VLR Visited Location Register, VLR Nummer	WTA Wireless Telephony Application
W3C World Wide Web Consortium	WTLS Wireless Transport Layer Security Protocol
WAE Wireless Application Environment	WTP Wireless Transaction Protocol
WAP Wireless Application Protocol	WWW World Wide Web
WBMP Wireless Bitmap (Format)	XML Extensible Markup Language
W-CDMA Wideband CDMA	XSL Extensible Style Language
WDP Wireless Datagram Protocol	
WLL Wireless Local Loop	

References

- Ambrosch, W. D., Maher, A. and Sassceer, B. (1989) *The Intelligent Network*, Springer, Berlin.
- Begin, G. and Haccoun, D. (1994) Performance of sequential decoding of high-rate punctured convolutional codes. *IEEE Transactions on Communications*, **42**(2), 966–978.
- Bertsekas, D. and Gallager, R. (1987) *Data Networks*, Prentice-Hall, Englewood Cliffs, NJ.
- Bettstetter, C., Vögel, H. J. and Eberspächer, J. (1999) GSM Phase 2+ General Packet Radio Service GPRS: Architecture, protocols, and air interface. *IEEE Communications Survey (Special Issue on Packet Radio Networks)*.
- Bluetooth SIG (2008) <http://www.bluetooth.com>.
- Bocker, P. (1990) *ISDN – Das Dienstintegrierende digitale Nachrichtennetz*, 3rd edn, Springer, Berlin.
- Bossert, M. (1991) D-netz-grundlagen – Funkübertragung in GSM-Systemen, Teil 1 und 2. *Funkschau*.
- Bossert, M. (1999) *Channel Coding for Telecommunications*, John Wiley & Sons, Ltd, Chichester.
- Brasche, G. and Walke, B. (1997) Concepts, services, and protocols of the new GSM Phase 2+ general packet radio service. *IEEE Communications Magazine*, **35**(8), 94–104.
- Bruhn, D., Ekudden, E. and Hellwig, K. (2000) *Adaptive Multi-rate: A New Speech Service for GSM and Beyond*. Proceedings 3rd ITG Conference Source and Channel Coding (ITG Technical Report 159), VDE-Verlag, Munich.
- Buckingham, S. (1999) Mobile positioning – an introduction <http://www.mobilepositioning.com>.
- CCITT Recommendation M.3010. *Principles for a Communications Management* (1992).
- CCITT Recommendation M.3020. *TMN Interface Specification Methodology* (1992).
- Damosso, E. (ed.) (1999) Digital mobile radio towards future generation systems. *Final Report of COST Action 231*, European Commission.
- David, K. and Benkner, T. (1996) *Digitale Mobilfunksysteme*, B. G. Teubner, Stuttgart.
- Decker, P. and Pertz, U. (1993) Simulative Leistungsbewertung der nichttransparenten Fax-Übertragung im GSM-System. Walke, B. (ed.), *Informationstechnische Gesellschaft im VDE: Mobile Kommunikation, Lectures of the ITG-Fachtagung*, Neu-Ulm (ITG Technical Report 124), VDE-Verlag, Berlin.
- Eberspächer, J., Vögel, H.-J. and Bettstetter, C. (2001) *GSM – Switching, Services and Protocols*, 2nd edn, John Wiley & Sons, Ltd., Chichester.
- Eberspächer, J. (ed.) (1999) *Vertrauenswürdige Kommunikation*. Proceedings of the Münchner Kreis Hühig, Heidelberg.
- ETSI (2008) <http://www.etsi.org>.
- Faccin, S., Hsu, L., Koodli, R., Le, K. and Purnadi, R. (1999) GPRS and IS-136 integration for flexible network and services evolution. *IEEE Personal Communications*.
- Fuhrmann, W., Brass, V., Janßen, U., Kühl, F. and Roth, W. (1993) *Digitale kommunikationsnetze. Tutorium ITG/GI Fachtagung Kommunikation in Verteilten Systemen KiVS*, Munich.

- Furuskär, A., Nälund, J. and Olofsson, H. (1999) GPRS – enhanced data rates for GSM and TDMA/136 evolution. *Review*, Ericsson.
- Geng, N. and Wiesbeck, W. (1998) *Planungsmethoden für die Mobilkommunikation*, 1st edn, Springer, Berlin.
- Glitho, R. H. and Hayes, S. (1995) Telecommunications management network: vision vs. reality. *IEEE Communications Magazine*, **33**(3), 47–52.
- Goodman, D. J. (2000) The wireless internet: promises and challenges. *IEEE Computer*, **33**(7), 36–41.
- Gottschalk, H. (1993) Zeichengabetechnische Anbindung digitaler Mobilfunknetze an das Festnetz der Telekom. Walke, B. (ed.), *Informationstechnische Gesellschaft im VDE: Mobile Kommunikation, Lectures of the ITG-Fachtagung*, Neu-Ulm (ITG Technical Report 124), VDE-Verlag, Berlin.
- Granbohm, H. and Wiklund, J. (1999) GPRS – general packet radio service. *Review*, Ericsson.
- GSM World (2008) <http://www.gsmworld.org>.
- Hagenauer, J., Seshadri, N. and Sundberg, C.-E. W. (1990) The performance of rate compatible punctured convolutional codes for digital mobile radio. *IEEE Transactions on Communications*, **38**(7), 966–980.
- Hartmann, C. and Eberspächer, J. (2001) Adaptive radio resource management in F/TDMA cellular networks using smart antennas. *European Transactions on Telecommunications*, **12**(5), 439–452.
- Hartmann, C. and Vögel, H. (1999) Teletraffic analysis of SDMA-systems with inhomogeneous MS location distribution and mobility. *Wireless Personal Communications*, **11**(1), 45–62.
- Hata, M. (1980) Empirical formula for propagation loss in land mobile radio services. *IEEE Transactions on Vehicular Technology*, **29**(3), 317–325.
- ISO/IEC 33091991. *Information Technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures – Frame structure*.
- ITU-T Recommendation Q.735. *Multi-Level and Preemption (MLPP)*.
- ITU-T Recommendation V.110. *Support of Data Terminal Equipment (DTEs) with V-Series Type Interfaces by an Integrated Services Digital Network (ISDN)*.
- Johannesson, R. and Zigangirov, K. S. (1999) *Fundamentals of Convolutional Codes*. IEEE Press, Piscataway, NJ.
- Junius, M. and Marger, X. (1992) *Simulation of the GSM Handover and Power Control Based on Propagation Measurements in the German D1 Network*. Proceedings of the 5th Nordic Seminar on Digital Mobile Radio Communications (DMR V), Helsinki.
- Kalden, R., Meirick, I. and Meyer, M. (2000) Wireless Internet access based on GPRS. *IEEE Personal Communications*, **7**(2), 8–18.
- Kallel, S. (1995) Complementary punctured convolutional (CPC) codes and their applications. *IEEE Transactions on Communications*, **43**(6), 2005–2009.
- Kleinrock, L. (1975) *Queueing Systems – Vol. 1: Theory*, John Wiley & Sons, Ltd., New York.
- Laitinen, M. and Rantale, J. (1995) Integration of intelligent network services into future GSM networks. *IEEE Communications Magazine*, **33**(6), 76–86.
- Lee, W. C. Y. (1989) *Mobile Cellular Telecommunication Systems*, McGraw-Hill, New York.
- Lin, Y. B. (1997) OA&M for the GSM network. *IEEE Network*, **11**(2), 46–51.
- Mende, W. (1991) *Bewertung ausgewählter Leistungsmerkmale von zellularen Mobilfunksystemen*, PhD Thesis, Fernuniversität, Hagen.
- Molkdar, D. and Featherstone, W. (2001) *System Level Performance Evaluation of EDGE Compact*. Proceedings of the IEEE Symposium on Personal Indoor and Mobile Radio Communication (PIMRC 2001), San Diego, CA.
- Molkdar, D., Featherstone, W. and Lambbotharan, S. (2002) An overview of EGPRS: the packet data component of EDGE. *Electronic and Communication Engineering Journal*, **14**(1), 21–38.
- Mouly, M. and Pautet, M. B. (1995) Current evolution of the GSM systems. *IEEE Personal Communications*, **2**(5), 9–19.

- Natwig, E. (1998) Evaluation of six medium bitrate coders for the pan-European digital mobile radio system. *IEEE Journal on Selected Areas in Communications*, 6(2), 324–331.
- Okumura, Y. (1968) Field strength and its variability in VHF and UHF land-mobile radio-services. *Review of the Electrical Communications Laboratory*, September/October, pp. 825–873.
- Proakis, J. G. (1995) *Digital Communications*, 3rd edn, McGraw-Hill, New York.
- Rappaport, T. S. (2002) *Wireless Communications: Principles and Practice*, Prentice-Hall, Englewood Cliffs, NJ.
- Sahasrabudde, L. H. and Mukherjee, B. (2000) Multicast routing algorithms and protocols: a tutorial. *IEEE Network*, 14(1), 90–102.
- Sahin, V. (1993) Telecommunications Management Network – principles, models, an applications. *Telecommunications Network Management into the 21st Century*. IEEE Press, Piscataway, NJ.
- Schmidt, S. (1993) Management (Operation & Maintenance) von GSM Base Station Subsystemen. Walke, B. (ed.), *Informationstechnische Gesellschaft im VDE: Mobile Kommunikation, Lectures of the ITG-Fachtagung*, Neu-Ulm (ITG Technical Report 124), VDE-Verlag, Berlin.
- Schwartz, M. (2005) *Mobile Wireless Communications*, Cambridge University Press, Cambridge, UK.
- Sexton, T. A. (2000) *EDGE Compact Control/Data Bandwidth Dimensioning*. Vehicular Technology Conference (VTC 2000).
- Steele, R. (1992) *Mobile Radio Communications*, Pentech Press, London.
- Steele, R. and Hanzo, L. (1999) *Mobile Radio Communications*, 2nd edn, John Wiley & Sons, Ltd., Chichester.
- Tanenbaum, A. S. (1996) *Computer Networks*, 3rd edn, Prentice-Hall, Englewood Cliffs, NJ.
- Towle, T. S. (1995) TMN as applied to the GSM network. *IEEE Communications Magazine*, 33(3), 68–73.
- Tran-Gia, P. (1996) *Analytische Leistungsbewertung verteilter Systeme*, Springer, Berlin.
- Vögel, H. J., Johr, H. and Grom, A. (1995) Messung und verbesserte Markov-Modellierung transparenter GSM-Datendienste. Walke, B. (ed.), *Mobile Kommunikation, Lectures of the ITG-Fachtagung*, Neu-Ulm (ITG Technical Report 135), VDE-Verlag, Berlin.
- Walke, B. (1999) *Mobile Radio Networks: Networking and Protocols*, John Wiley & Sons, Ltd., Chichester.
- WAP Forum (1999a) <http://www.wapforum.org>.
- WAP Forum (1999b) *Official Wireless Application Protocol – The Complete Standard*. John Wiley & Sons, Ltd, Chichester.
- WAP Forum (1999c) *Wireless Application Protocol, White Paper*, WAP Forum.
- Watson, C. (1993) Radio Equipment for GSM. *Cellular Radio Systems*, Artech House, Norwood, MA.
- WWW Consortium (2008) <http://www.w3.org>.
- Xu, G. and Li, S. Q. (1994) Throughput multiplication of wireless LANs for multimedia services: SDMA protocol design. *IEEE Globecom 94*, San Francisco, CA.

Index

- 3GPP Long Term Evolution (LTE), 269
- 4G, 269
- 8-Phase Shift Keying (8-PSK), 265
- A-law, 123
- A3 algorithm, 174
- A5 algorithm, 177, 258
- A8 algorithm, 175
- Abis interface, 54, 170
- Access Burst (AB), 69
- Access Grant Channel (AGCH), 59, 61
- acknowledged operation, 142
- acoustic background noise, 93
- Activation Password (PW), 180
- Adaptive Delta Pulse Code Modulation (ADPCM), 94
- adaptive frame alignment, 74
- adaptive frame synchronization, 73
- Adaptive Multi-rate (AMR) codec, 115, 117
 - channel encoding, 118
 - mode, 118
- address conversion, 247
- addressing, 43, 46
- Advanced Speech Call Items (ASCI), 215, 216
- ad hoc* communication, 4
- ad hoc* networks, 4
- air interface (Um), 54, 140, 142, 244, 250
- Algebraic Code Excitation – Linear Prediction (ACELP), 116
- anchor MSC, 197
- antenna gain G , 32
- architecture for CAMEL, 225
- architecture of HSCSD, 261
- artificial background noise, 93
- assignment, 160
- assignments of data, 132
- Associated Control Channel (ACCH), 59
- Association Control Service Element (ACSE), 302
- Asynchronous Transfer Mode (ATM), 244
- asymmetric connections, 263
- asynchronous data services, 280
- attachment procedure, 238
- authentication, 135, 154, 160, 173, 175
- authentication and ciphering for GPRS, 257
- Authentication Center (AUC), 44, 174, 295
- authentication key (Ki), 173
- Automatic Repeat Request (ARQ), 127, 143, 284
- Bad Frame Indication (BFI), 94
- barring, 165
- Barring Of Incoming Calls (BAIC), 163
- Barring Of Outgoing Calls (BAOC), 163
- Base Control Function (BCF), 124
- Base Station Controller (BSC), 43
- Base Station Subsystem (BSS), 44
- Base Station System Application Part (BSSAP), 54, 136
- Base Station System Management Application Part (BSSMAP), 136
- procedures, 168, 169
- Base Transceiver Station (BTS), 43
- Base Transceiver Station Color Code (BCC), 50
- Base Transceiver Station Identity Code (BSIC), 50, 197
- Base Transceiver Station Management (BTSM), 137
- basic handover, 206
- basic packet mode, 289
- Bit Number (BN), 72
- bit rate adaptation, 277
- black list, 46
- Block Check Sequence (BCS), 246, 266
- block code, 97

- block coding, 98
- block interleaving, 108
- Block Sequence Number (BSN), 266
- block-diagonal interleaving, 109
- blocking probability, 27, 32
- Border Gateways (BGs), 235
- brickwall antenna pattern, 32
- Broadcast Channel (BCH), 58
- Broadcast Control Channel (BCCH), 49, 58, 61, 184
- BSS Application Part (BSSAP+), 249
- BSS GPRS Application Protocol (BSSGP), 246
- Bundesnetzagentur, 65
- burst errors, 107
- bursts, 65
- bursty traffic, 233
- Business Management Layer (BML), 298
- busy hour call attempts (BHCA), 27
- C-Netz*, 5
- call arrival rate, 27
- call barring, 163
- Call Control (CC), 132
- call establishment, 191
- call forwarding, 164
- Call Forwarding Unconditional (CFU), 163
- call holding, 164
- call holding time, 27
- call queuing, 159
- call release, 162
- call setup, 157
- call termination, 158, 195
- call waiting, 162
- callback, 162
- camping, 89
- camping on a cell, 90
- candidates, 197
- carrier frequencies, 66
- Carrier-to-Interference Ratio (CIR or C/I), 24
- Cell Allocation (CA), 23
- Cell Broadcast Channel (CBCH), 61
- cell reselection, 89
- cell selection, 89
- cells (radio zones), 23
- cells per cluster, 25
- cellular principle, 9, 22
- CEPT (Conférence Européenne des Administrations des Postes et des Télécommunications), 5
- channel bit rate, 97
- channel change, 150, 151
- channel coding, 91, 96
- channel combinations, 62, 63
- channel encoder, 91, 97
- channel estimation, 68
- channel gain, 9
- channel measurement, 81, 144
- channel request, 149, 160
- charging, 195
- check sum, 100, 102
- chip rate, 18
- Cipher Key (Kc), 177
- ciphering, 152, 178
 - algorithm, 71
 - for GPRS, 257
- circuit-switched services, 238
- class I, 98
- class II, 98
- clock synchronization, 71
- clusters, 25
- Code Division Multiple Access (CDMA), 17
- Code Excited Linear Predictive Coding (CELP), 94
- codec (COder/DECOder), 92
- codeword, 101
- Coding and Puncturing Scheme (CPS), 266
- coding procedure, 93
- collision resolution, 160
- combining and splitting functionality, 261
- comfort noise, 93
- Command/Response (C/R) flag, 146
- common channel management, 171
- Common Control Channel (CCCH), 58
- Completion of Calls to Busy Subscribers (CCBS), 221
- confidentiality, 135, 173
- Connection End Point Identifier (CEPI), 143
- Connection End Points (CEPs), 143
- connection establishment, 188
- Connection Management (CM), 132, 135, 156
- connection setup, 61
- connectivity check, 87
- Continuous Phase Modulation (CPM), 64
- control plane, 121, 139
- conversion of addresses, 246
- convolutional coding, 97, 103
 - of logical channels, 105
- convolutional decoding, 97, 107
- convolutional encoder, 97

- Country Code (CC), 48, 135
- Customized Applications for Mobile Network
Enhanced Logic (CAMEL), 223
- cycle period, 76
- Cyclic Redundancy Check (CRC), 100

- D* (the frequency reuse distance), 23
- data burst, 66
- data flow and segmentation, 246
- Data Link Connection Identifiers (DLCIs),
143
- data link layer, 245
- data services, 233
- decision algorithm, 199
- decoding decision, 97
- decryption, 133
- dedicated channel management, 171
- Dedicated Control Channel (DCCH), 58
- dedicated packet mode, 290
- Dedicated/Associated Control Channels
(D/ACCH), 59
- deinterleaving, 97, 108
- delay classes, 238
- Destination Number (DN), 180
- detachment procedure, 238
- diagonal interleaving, 108
- Digital Audio Broadcast (DAB), 4
- Digital Communication System (DCS1800), 5
- Digital Enhanced Cordless
Telecommunications (DECT), 3
- digital fixed lines, 124
- Digital Subscriber Line (DSL), 1
- Digital Video Broadcast (DVB), 4
- Direct Sequence CDMA (DS-CDMA), 17, 18
- Direct Transfer Application Part (DTAP), 136
- disconnection, 87
- Discontinuous Reception (DRX), 91
- Discontinuous Transmission (DTX), 93
mode, 93
- Dm channel, 58
- Domain Name Server (DNS), 249
- downlink, 13
- downlink band, 13
- DTMF signaling, 160, 212
- Dual-Tone Multifrequency (DTMF), 136
signaling, 159
- Dummy Burst (DB), 69
- duplex, 12
- duplexing, 65

- Dynamic Host Configuration Protocol
(DHCP), 249
- dynamic IP address assignment, 259

- EDGE, 220, 233, 264
 - architecture, 266
 - burst, 265
 - classic, 268
 - compact, 268
 - physical layer, 265
- electronic business cards (vCard), 228
- electronic calendar (vCalendar), 228
- Element Management Layer (EML), 298
- encoding of GPRS, 255
- encryption, 133, 173, 176
 - of payload, 177
 - of user data, 178
- Engset blocking formula, 28
- Engset model, 27
- Enhanced Circuit Switched Data (ECSD),
221, 264, 267
 - transmission modes, 267
- Enhanced Full-Rate (EFR) codec, 115, 116
- Enhanced GPRS (EGPRS), 221, 264, 267
 - temporary block flows, 267
 - transmission modes, 267
- Enhanced Messaging Service (EMS), 213
- Enhanced Multi-Level Precedence and
Pre-emption (eMLPP), 216, 220
- equalizer, 68
- Equipment Identity Register (EIR), 44
- Erlang blocking formula, 27, 28
- error detection, 97, 103
- error protection coding, 97, 99
- error-free transmission, 101
- establishment of calls, 135
- ETSI (European Telecommunication
Standards Institute), 5
- Extensible Markup Language (XML), 226
- external error protection, 97, 98
- external handover, 198

- Fast Associated Control Channel (FACCH),
60
 - full rate, 61
 - half rate, 61
- fax teleservices, 291
- fax transmission, 211
- Federal Communication Commission in the
USA, 65
- feedback shift register, 101

- File Transfer Access and Management (FTAM), 302
- Final Assembly Code (FAC), 47
- Fixed Channel Allocation (FCA), 34
- Frame Check Sequence (FCS), 128, 246
- frame counter, 72
- Frame Number (FN), 69
- frequency channels, 15
- Frequency Correction Burst (FB), 68
- Frequency Correction Channel (FCCH), 59
- Frequency Division Duplex (FDD), 13
- Frequency Division Multiple Access (FDMA), 14
- frequency hopping, 16, 62, 69
- frequency hopping CDMA (FH-CDMA), 18
- frequency reuse distance D , 25
- frequency synchronization, 68, 71
- frequency synchrony, 70
- frequency-selective fading, 11
- full-duplex, 15
- full-rate channel, 76
- full-rate speech codec, 98
- full-rate TCH (TCH/F), 58
- Gateway GPRS Support Node (GGSN), 234
- Gateway Mobile Location Center (GMLC), 222
- Gateway MSC (GMSC), 43
- Gaussian Minimum Shift Keying (GMSK), 63, 265
- Gc interface, 236
- Gd interface, 236
- General Packet Radio Service (GPRS), 220, 233
 - attach, 239, 241
 - backbone, 243
 - channel coding, 255
 - channel coding schemes, 256
 - channel combinations, 254
 - detach, 239, 241
 - interfaces, 235
 - system architecture, 235, 236
- generator polynomial, 101, 103, 105, 106
- generator polynomials
 - for convolutional codes, 106
- Gf interface, 236
- Gi interface, 236
- Global System for Mobile Communication (GSM), 1
 - architecture for HSCSD, 262
 - handover, 201
 - network management protocols, 303
 - Phase 2+, 214, 215, 233
 - power classes, 86
 - reference configuration, 274
 - speech coder, 92, 95
 - speech decoder, 96
 - transmission chain, 91, 92
- Go-back-N, 130
- Gp interfaces, 235
- GPRS Encryption Algorithm (GEA), 258
- GPRS Mobility Management and Session Management (GMM/SM), 247
- GPRS Support Nodes (GSNs), 234
- GPRS Tunneling Protocol (GTP), 235
- group call areas, 217
- Group Call Register (GCR), 217
- Groupe Spécial Mobile, 5
- GSM Speech Codec (GSC), 123
- GSM standards
 - Release 2000, 215
 - Release 97, 215
 - Release 98, 215
 - Release 99, 215
- guard periods, 66
- half-rate channel, 76
- half-rate codec, 115
- half-rate TCH (TCH/H), 58
- handback, 207
- handover, 24, 87, 133, 151, 183, 197, 264
 - causes, 202
 - criteria, 205
 - decision, 84, 204
 - procedure, 151
 - targets, 84, 204
 - timing, 199
- Header Check Sequence (HCS), 266
- high compression rate, 101
- High Speed Circuit Switched Data (HSCSD), 220, 233, 260
 - air interface, 261
 - MS multislots classes, 262
 - resource allocation, 263
- High Speed Downlink Packet Access (HSDPA), 269
- High Speed Uplink Packet Access (HSUPA), 269

- High-level Data Link Control (HDLC), 128, 146
 - polling procedure, 146
- highly secure authentication, 176
- hold, 162
- Home Location Register (HLR), 44, 183, 184
 - interrogation, 189
- home location registers (HLR), 50
- Home PLMN (H-PLMN), 190
- Hopping Sequence Number (HSN), 69
- HSxPA, 269
- Hybrid Automatic Repeat Request (HARQ), 266, 270
- hyperframe, 76
- Hypertext Markup Language (HTML), 226
- hysteresis, 205
 - for cell reselection, 91
- identification, 133
- idle mode, 82, 89
- IDLE state, 241
- immediate assignment procedure, 149
- immediate assignment reject, 149
- impulse response, 64, 65
- in-call modification, 136, 162
- incoming call setup, 194
- incoming connection, 193
- Integrated Services Digital Network (ISDN), 43
- Intelligent Network (IN), 221
- Intelligent Network Application Part (INAP), 223
- inter-MSC handover, 205
- inter-PLMN backbone networks, 235
- inter-SGSN routing area update, 241, 243
- intercell handover, 197, 198
- interface
 - A, 54, 166, 167
 - Abis, 54
 - B, 54
 - C, 55
 - D, 54
 - E, 55
 - F, 54
 - G, 54
- Interface Protocol (IFP), 127
- interleaver, 97
- interleaving, 97, 99, 107
 - blocks, 113
 - depth, 108
 - merging, 108
 - spreading, 108
- internal error protection, 103
- internal handover, 198
- internal protection, 97
- International Mobile Station Equipment Identity (IMEI), 46
- International Mobile Subscriber Identity (IMSI), 47, 153, 173
 - attach, 135
 - detach, 135
 - detach procedure, 153
- International Switching Center (ISC), 43
- Internet traffic, 233
- intersymbol interference, 68
- Interworking Function (IWF), 43, 126
- interworking with IP networks, 249
- intra-MSC handover, 199
- intra-PLMN backbones, 235
- intra-SGSN routing area update, 241, 242
- intracell handover, 197, 198
- IP destination address, 234
- IP multicast routing protocols, 237
- IP networks, 233
- IP routing mechanism, 240
- IPv4, 236
- IPv6, 236
- ISDN User Part (ISUP), 53, 138
- Kc, 257
- key Kc, 177, 258
- key Ki, 177, 258
- L2R Bit Oriented Protocol (L2RBOP), 285
- L2R Character Oriented Protocol (L2RCOP), 285
- Layer 1, 140
- Layer 2, 142
- Layer 2 Management Link (L2ML), 168
- Layer 2 Relay protocol, 128
- Layer 3, 132
- Length Indicator (LI), 147
- Line of Sight (LOS), 11, 19
- Linear Predictive Coding (LPC), 94
 - coefficients, 117
 - filter, 94
- Link Access Procedure B (LAPB), 289
- Link Access Procedure D mobile (LAPDm), 146
 - frame formats, 145

- Link Access Procedure on Dm Channels (LAPDm), 130
- Link Access Protocol Channel D (LAPD), 130
- Local Communication Network (LCN), 299
- localization of the MS, 133
- Location Area (LA), 44
- Location Area Code (LAC), 49
- Location Area Identifier (LAI), 49, 153, 173, 184
- location management, 240
- location registration, 184
- Location Service (LCS), 221
- location update, 133, 154, 184
- location update procedure, 155, 186
- Log Area Ratios (LARs), 94
- logical channels, 57, 58, 61, 144
- logical channels in GPRS, 251
- Logical Layered Architecture (LLA), 298
- Logical Link Control (LLC), 245
- M/M/n loss system, 26
- main lobe β , 32
- Man-Machine Interface (MMI), 179
 - codes, 182
 - commands, 180
 - service codes, 181
- mandatory handover, 201
 - detection of, 203
- mapping of logical channels, 75
- Markov process, 26
- maximum allowed transmitter power, 90
- Mean Opinion Score (MOS), 95, 96
- measurement loop, 80
- measurement of channel quality, 132
- measurement report, 84
- measurement result (IE), 151
- Mediation Device (MD), 299
- Medium Access Control (MAC), 245
- Message Transfer Part (MTP), 136
- Message Type (MT), 147
- midamble, 68
- minimum received power level, 90
- Minimum Shift Keying (MSK), 64
- MMS-Center (MMS-C), 213
- Mobile Allocation (MA), 65
- Mobile Allocation Index Offset (MAIO), 69
- Mobile Application Part (MAP), 54, 137, 183
- Mobile Country Code (MCC), 47
- mobile D channel, 58
- Mobile Network Code (MNC), 47
- Mobile Station (MS), 43
- Mobile Station Execution Environment (MEExE), 223
- Mobile Station Roaming Number (MSRN), 48, 184
 - at location update, 188
 - on a per call basis, 188
- Mobile Subscriber Identification Number (MSIN), 47
- Mobile Subscriber ISDN Number (MSISDN), 47
- Mobile Switching Center (MSC), 43
- Mobile Termination (MT), 273
- mobile-initiated call setup, 161
- mobile-initiated SMS transfer, 165
- mobile-originating call, 156
- mobile-terminated SMS transfer, 165
- Mobility Management (MM), 88, 132, 133, 152, 183, 238
 - connection, 155
 - messages, 148
- modulation, 63
- modulation and coding schemes, 266
- monitoring, 132, 148
- MT0, 123
- MTP Routing Verification Test (MRVT), 302
- Multi-Carrier (MC), 65
- Multi-Level Precedence and Pre-emption (MLPP), 220
- multiframe
 - 26-frame, 77
 - 51-frame, 77
- multiframes, 76
- Multimedia Messages (MMs), 214
- Multimedia Messaging Service (MMS), 212, 213
 - relay/server, 213
- Multimedia Messaging Service Environment (MMSE), 213
- Multimedia Messaging Service Network Architecture (MMSNA), 213, 214
- multinumbering, 277
- multipath fading gain, 10
- multiple access, 13, 65, 250
- Multiple Input Multiple Output (MIMO), 269
- multislot class, 261
- multislot operation, 250

- National Destination Code (NDC), 48
- National Mobile Subscriber Identity (NMSI), 47
- Network Color Code (NCC), 50
- network interfaces, 53
- Network Layer Service Access Point Identifier (NSAPI), 244
- Network Management (NM), 295
- Network Management Center (NMC), 303
- Network Management Layer (NML), 298
- Network Switching Subsystem (NSS), 44
- noise-contrast effect, 94
- nontransparent data transmission, 127, 284
- Nontransparent Protocol (NTP), 127
- Normal Burst (NB), 66
- Notification Channel (NCH), 59, 61

- Off-Air Call Setup (OACSU), 159
- offered load *A*, 27
- Open Systems Interconnection (OSI), 57
- Operation and Maintenance Center (OMC), 44, 303
- Operation and Maintenance Link (OML), 168
- Operation and Maintenance Subsystem (OMSS), 44
- Operation Maintenance and Administration Part (OMAP), 302
- Operation System (OS), 298
- optimal cluster size, 25
- Orthogonal FDMA (OFDMA), 270
- OSI CMISE, 302
- outage probability, 31, 33
- outgoing call setup, 192
- outgoing connection, 191

- Packet Access Grant Channel (PAGCH), 251
- Packet Associated Control Channel (PACCH), 253
- Packet Broadcast Control Channel (PBCCH), 251
- Packet Common Control Channel (PCCCH), 251
- Packet Data Channel (PDCH), 250
- Packet Data Networks (PDNs), 234
- Packet Data Protocol (PDP), 234
 - address, 239
 - context, 239
 - context activation, 239
 - type, 239
- Packet Data Traffic Channel (PDTCH), 251
- Packet Notification Channel (PNCH), 251

- Packet Paging Channel (PPCH), 251
- Packet Random Access Channel (PRACH), 251
- Packet Timing Advance Control Channel (PTCCH), 253
- packet-switched services, 238
- paging, 148, 160, 241, 252
- paging call, 194
- Paging Channel (PCH), 59, 61
- paging group, 78
- parity bits, 97
- parity checking, 97
- path gain, 10
- path loss criterion, 89
- peer-to-peer signaling, 142
- physical channel configuration, 152
- physical channels, 62
- Physical Link Layer (PLL), 245
- Physical RF Layer (RFL), 245
- PIN, 180
- ping-pong handover, 205
- Point-to-Point (PTP), 237
- Poisson process, 26
- power classes, 86
- power control, 132
- power measurement, 69
- power spectrum, 71
- power-up scenario, 118
- priority classes in eMLPP, 220
- protocol architecture, 121, 244
 - for WAP, 227
 - of GPRS, 242
- Protocol Data Units (PDUs), 128
- protocols, 121
- PTP Connection Oriented Network Service (PTP-CONS), 237
- PTP Connectionless Network Service (PTP-CLNS), 237
- Public Land Mobile Network (PLMN), 90
- Public Switched Telephone Network (PSTN), 126
- Pulse Code Modulation (PCM), 94
- punctured convolutional code, 97
- puncturing, 97

- Q.931, 136
- quality monitoring, 69, 81, 132, 197
- Quality of Service (QoS), 234, 260
 - classes, 237
 - demand, 237

- parameters, 237
- profile, 237
- Quarter Bit Number (QN), 72
- Q adapter (QA), 300
- radio channel, 9
- Radio Frequency Channel (RFCH), 65
- radio link layer management, 170
- Radio Link Protocol (RLP) frame structure, 129
- radio resource management, 132, 146, 250
- Radio Signaling Link (RSL), 168
- radio subsystem link control, 80
- Random Access Channel (RACH), 59, 61
 - administration, 132
- Random Number (RAND), 174, 175, 257
- rate of the convolutional code, 97, 104
- Rayleigh fading, 11
- READY state, 241
- Received Signal Level (RXLEV), 82, 200
- Received Signal Quality (RXQUAL), 82
- Reduced Frame Number (RFN), 59
- redundancy, 91
- reference clock, 69
- Regular Pulse Excitation Long-Term Prediction (RPE-LTP), 94
- release, 149
- release and deallocation, 160
- reliability classes, 238
- Remote Operations Service Element (ROSE), 302
- Remote Procedure Call (RPC), 302
- required signal quality (C/I)_{min}, 25
- Rice distribution, 11
- RLP-ARQ, 127
- roaming, 183
- round-trip delay, 74
- routing, 188–191, 238, 240, 246, 247
- routing for short messages, 195
- RR connection, 150
- SCCP Routing Verification Test (SRVT), 303
- sectorization, 28
- Secure Socket Layer (SSL), 229
- security, 173
- security data, 175
- security-related registers (AUC), 51
- security-related registers (EIR), 51
- Service Access Point Identifier (SAPI), 143
- Service Access Points (SAPs), 132
- Service Control Point (SCP), 221, 223
- Service Data Unit (SDU), 143
- Service Management Layer (SML), 298
- service platforms, 222
- service request, 160
- Service Switching Points (SSPs), 223
- services, 211, 237
- Serving GPRS Support Node (SGSN), 234, 240
- Serving Mobile Location Center (SMLC), 222
- session management, 238, 239
- setup, 149
- shadowing gain, 10
- Short Message Control (SMC), 165
- Short Message Control Layer (SM-CL), 165
- Short Message Control Protocol (SM-CP), 139
- Short Message Relay (SMR), 165
- Short Message Relay Layer (SM-RL), 165
- Short Message Relay Protocol (SM-RP), 139
- Short Message Service (SMS), 132, 135
- Short Message Service Cell Broadcast (SMSCB), 61
- Short Message Service Center (SMS-SC), 139
- Short Message Service Interworking MSC (SMS-IWMSC), 139
- short message transfer, 166
- Short Message Transport Layer (SM-TL), 166
- sidelobe attenuation D , 32
- signal propagation time, 73
- signal quality (RXQUAL), 200
- Signal-to-Noise Ratio (SNR), 69
- signaling architecture, 130
- signaling channels, 58, 132
- Signaling Connection Control Part (SCCP), 136
- signaling plane, 121, 130, 139
- Signaling Point (SP), 55
- Signaling Point Code (SPC), 55
- Signature Response (SRES), 174, 175, 257
- SIM application toolkit, 224
- SIM card, 174
- Single numbering, 277
- Single-Carrier FDMA (SC-FDMA), 270
- size of a cluster, 25
- Slow Associated Control Channel (SACCH), 60
 - with SDCCH, 61
 - with TCH, 61
- SMS, 165, 212
- source coding, 91, 92

- source encoder, 91
- Space Division Multiple Access (SDMA), 18, 22
- Spatial filtering for interference reduction (SFIR), 31
- Special Mobile Group (SMG), 5
- special silence descriptor (SID), 93
- spectral efficiency, 265
- speech codec, 93
- speech frame, 92, 100
- speech processing, 91, 92
- speech transmission, 123
- Spreading Factor (SF), 18
- SS#7, 53
- Stand-alone Dedicated Control Channel (SDCCH), 59, 61
- STANDBY state, 241
- state model of a GPRS MS, 241
- Stealing Flags (SFs), 68
- stream cipher, 177
- Subchannel Number (SCN), 70
- Subnetwork Dependent Convergence Protocol (SNDTCP), 245
- subscriber authentication in GPRS, 258
- subscriber identity, 135, 173
- subscriber identity confidentiality in GPRS, 258
- Subscriber Identity Module (SIM), 45
- Subscriber Number (SN), 48
- subsequent handover, 207, 208
- superframe, 76
- Supplementary Services (SS), 132, 135, 136, 161, 162
- Support of Operator-Specific Services (SOSS), 223
- symmetric connections, 263
- synchronization, 70, 132
- Synchronization Burst (SB), 69
- Synchronization Channel (SCH), 59
- synchronous data services, 288
- system architecture, 43
 - for WAP, 230
 - of GPRS, 234
- System Management Application Process (SMAP), 302
- tail bits, 66, 68
- Tandem Free Operation (TFO), 116
- TCH/F, 100
- TCH/F14.4, 107
- TCH/F9.6, 98, 107
- TCH/Fxx, 102
- TCH/H, 100
- TCH/H4.8, 107
- TCH/Hxx, 102
- TDMA frames, 16, 66, 70, 71
 - long numbering cycle, 71
- Telecommunication Management Network (TMN), 44, 297
- teleservices, 211
- Temporary Block Flow (TBF), 252
- Temporary Flow Identifier (TFI), 252
- Temporary Logical Link Identifier (TLLI), 245
- Temporary Mobile Subscriber Identity (TMSI), 49, 153, 173, 184
 - assignment, 133
 - reallocation, 153
- Terminal Adapter (TA), 273
- terminal capabilities, 213
- Terminal Equipment Identifier (TEI), 168
- Terminal Equipment (TE), 127
- termination of calls, 136
- TETRA, 215
- Third Generation Partnership Project (3GPP), 5
- threshold values for the GSM handover, 202
- Time Division Duplex (TDD), 13
- Time Division Multiple Access (TDMA), 15
- time slot, 15
- time slot counter, 72
- Time Slot Number (TN), 70
- time spreading, 108
- time synchronization, 69
- time synchrony, 70
- Timing Advance (TA), 74, 144
- TMN architecture of a GSM system, 301
- Total Access Communication System (TACS), 5
- traffic capacity, 26
- Traffic Channel (TCH), 57
 - data, 14.4 kbit/s, 61
 - data, 4.8 kbit/s, 61
 - data, 9.6 kbit/s, 61
 - data, up to 2.4 kbit/s, 61
 - full-rate speech, 61
 - half-rate speech, 61
- Training Sequence Code (TSC), 68
- training sequences, 68

- Transaction Capabilities Application Part (TCAP), 137
- Transceiver Function (TRX), 124
- Transcoding and Rate Adaptation Unit (TRAU), 123
- Transmission Control Protocol (TCP), 244
- transmission power control, 86
- transmitter power, 144
- transparent data transmission, 126
- Transport Layer Security (TLS), 229
- TRX management, 171
- Tunnel Identifier (TID), 244
- Type Approval Code (TAC), 47
- UMTS Terrestrial Radio Access Network (UTRAN), 269
- UMTS/IMT-2000, 215
- unacknowledged operation, 142
- Unequal Error Protection (UEP), 98
- Universal Mobile Telecommunication System (UMTS), 5
- Unnumbered Information (UI), 143
- uplink, 13
- uplink band, 13
- Uplink State Flag (USF), 250
- user authentication for GPRS, 257
- user data encryption, 160
- User Datagram Protocol (UDP), 244
- user interface, 179
- user plane, 121, 123
- User–Network Interface (UNI), 121
- V.24 interface, 127
- Value Added Services (VAS), 214
- Visited Location Register (VLR), 44, 173, 183, 184
- visited location registers (VLR), 50
- Visited PLMN (V-PLMN), 190
- Voice Activity Detection (VAD), 93
- Voice Broadcast Service (VBS), 215, 216
- Voice Group Call Service (VGCS), 215, 219
- voice services, 211
- weakly secure authentication, 177
- white list, 46
- Wireless Application Environment (WAE), 227
- Wireless Application Protocol (WAP), 226
 - architecture, 228
 - Forum, 231
 - over GPRS, 260
 - products, 231
- Wireless Datagram Protocol (WDP), 230
- Wireless LAN (WLAN), 3
- Wireless Markup Language (WML), 226
- Wireless Session Protocol (WSP), 229
- Wireless Transaction Protocol (WTP), 229
- Wireless Transport Layer Security (WTLS), 229
- X.25 networks, 233
- zero termination, 97, 104

ERICSSON EXHIBIT 1008, Page 330

Printed in the USA/Agawam, MA
January 15, 2020



748268.009

GSM

Architecture, Protocols and Services

3RD EDITION

JÖRG EBERSPÄCHER, *Technische Universität München, Germany*

HANS-JÖRG VÖGEL, *BMW Group Research & Technology, Germany*

CHRISTIAN BETTSTETTER, *University of Klagenfurt, Austria*

CHRISTIAN HARTMANN, *Technische Universität München, Germany*

With around 3 billion subscribers, GSM is the world's most commonly used technology for wireless communication. Providing an overview of the innovations that have fuelled this phenomena, *GSM: Architecture, Protocols and Services, Third Edition* offers a clear introduction to the field of cellular systems. Special emphasis is placed on system architecture and protocol aspects, and topics range from addressing concepts through mobility management to network management.

This third edition contains around 25% new and reworked material and has been thoroughly updated to encompass recent advances and future trends. It serves as both an introductory textbook for graduate students as well as a reference resource for telecommunications engineers and researchers.

This edition:

- Presents capacity enhancement methods like sectorization, the application of adaptive antennas for Spatial Filtering for Interference Reduction (SFIR) and Space Division Multiple Access (SDMA)
- Provides a detailed introduction to GPRS, HSCSD, and EDGE for packet-switched services and higher data rates
- Features updated coverage on the vastly expanded range of GSM services, including an examination of Multimedia Messaging Service (MMS)
- Adopts a highly graphical approach with numerous illustrations



Enjoyed this book?

Why not tell others about it
and write a review on your
favourite online bookseller.



ERICSSON EXHIBIT 1008, Page 331

