

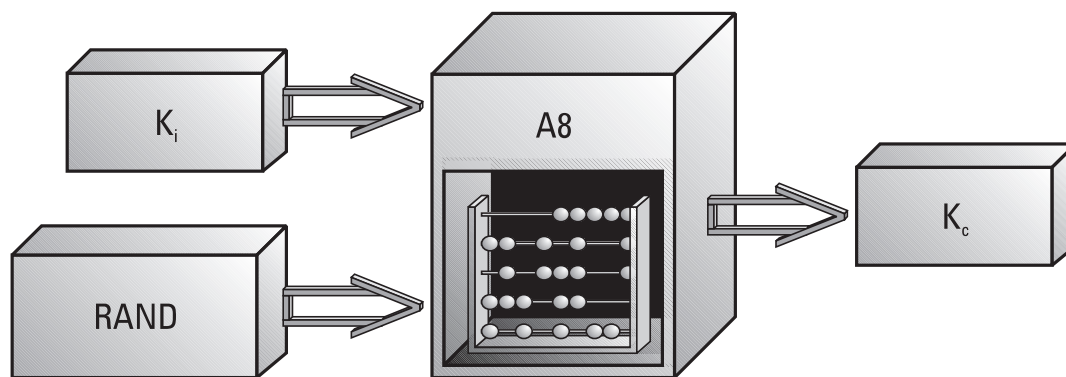


Figure G.19 Calculation of K_c from K_i and $RAND$ by use of $A8$.

7. The BTS retrieves the cipher key K_c and the information about the required ciphering algorithm from the $ENCR_CMD$ message and only forwards the information about the $A5/X$ algorithm in a $CIPH_MOD_CMD$ message to the MS. That message triggers the MS to enable ciphering of all outgoing data and deciphering of all incoming information. The MS confirms the change to ciphering mode by sending a $CIPH_MOD_COM$ message. The ciphering process is illustrated in Figure G.20.
8. The algorithm $A5/X$ uses the current value of the frame number (FN) at the time t_x together with the cipher key K_c as input parameters. The output of this operation are the so-called ciphering sequences, each 114 bits long, whereby one is needed for ciphering and the other one for deciphering.
9. As shown in Figure G.20, the first ciphering sequence and the 114 bits of “useful data” of a burst are XORED to provide the encrypted 114 bits that are actually sent over the Air-interface. Note that the ciphering sequences are altered with every frame number, which in turn changes the encryption with every frame number.
10. Deciphering takes place exactly the same way but in the opposite direction, as shown in Figure G.21.

Ciphering key sequence number See *CKSN*.

CKSN [GSM 03.08, 03.20] Ciphering key sequence number. A 3-bit-long value that references to a ciphering key, K_c . That is, when a particular K_c is stored in the MS and the MSC/VLR, a CKSN is assigned as well. The purpose is to allow the mobile station and the network a negotiation of the K_c to be

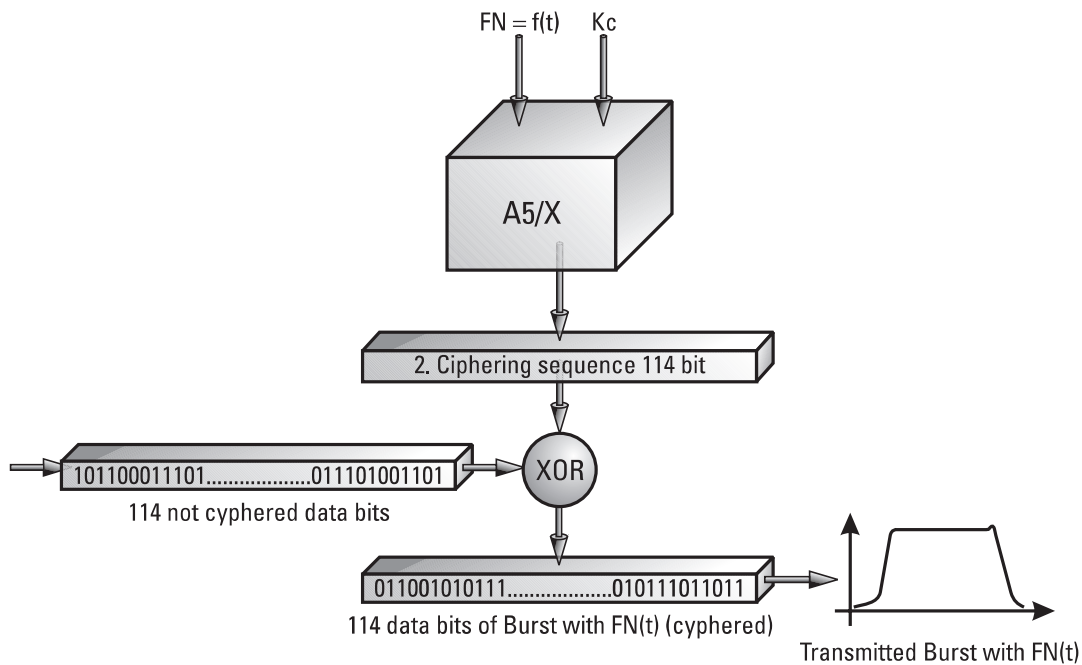


Figure G.20 Functionality of ciphering of data.

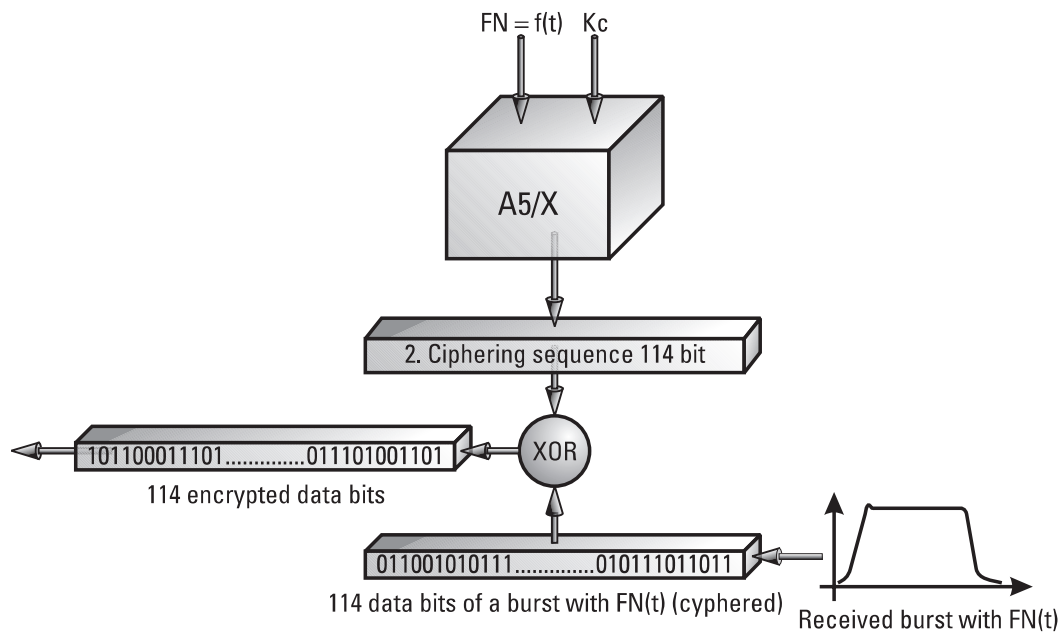


Figure G.21 Functionality of deciphering of data.

used, without compromising security by transmitting the value of K_c over the air. This applies particularly when an MS tries to establish an additional or subsequent operation with the network. In those cases, when the MS requests

a connection, it sends its last valid CKSN as a parameter of the LOC_UPD_REQ- or CM_SERV_REQ-... message to the VLR. The VLR then decides, based on the CKSN, if ciphering can start immediately or if another authentication is required. The VLR may decide to request another authentication, even if the CKSN matches the VLR's entry.

CLIP, CLIR See *SS*.

Closed user group See *CUG*.

CM Connection management.

COLP, COLR See *SS*.

Comfort noise [GSM 06.12] See *DTX*.

Constructor [X.208, X.209] A data type of the TCAP protocol that is composed of primitives or other constructors. A primitive, in contrast to the data type constructor, is "atomic," that is, it contains only one parameter for TCAP. See Chapter 11.

Convolutional code Procedure to secure data on the Air-interface against transmission errors. It is applied to signaling as well as to payload data. The idea is to add redundant information to the original data. The receiver then, by analyzing the redundant information, has the ability to detect errors and in some cases even correct corrupted data (channel coding).

The convolutional coder that GSM uses adds redundancy to the signaling data or to the payload by adding an additional bit to every input bit, thus doubling the amount of code. Hence, the code rate R equals one-half, that is, $R = 1/2$. The value of an added bit depends on the value of previous data bits stored in a shift register.

Figure G.22 provides the most simple convolutional coder, which is composed of a shift register, an element for modulus 2 addition, and a multiplexer. Note that this example is a simplification to illustrate the process. GSM uses a different procedure.

The length of the shift register determines the memory, which generally is referred to as M . The influence length (k) of such a coder indicates how many input bits are used to generate an output bit. In Figure G.22, k equals 2 ($k = 2 = M + 1$). A generator polynomial or a set of generator polynomials defines how a shift register and the input signal are coupled into the modulus 2 addition. That allows complete description of a convolutional coder.

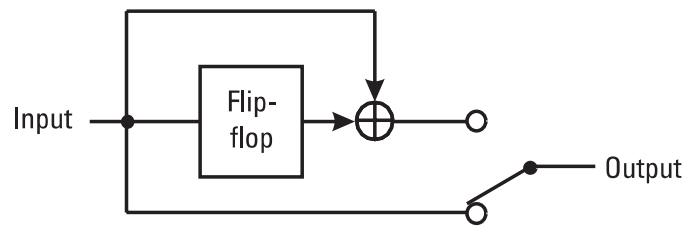


Figure G.22 Example of a convolutional coder.

Table G.6 is an example of coding where the flip-flop is preset with 0.

A so-called trellis diagram is a tool, or form of presentation, to determine the output code from the input data. This way of presentation is very helpful to better understand the principle of the decoder. The same example as above is used. Figure G.23 shows the input and output values, starting with the state s_0 , where the flip-flop is preset with a zero value. The state and the transition between states are important. The value of both states, s_0 and s_1 , is zero, the resulting code of this transition is 00. Note that the value of the output code and the value of the states (all 0) are only so for this case. The transition from s_2 to s_3 , where the value changes from 0 to 1, is represented by the output code 11.

Convolutional coding generally allows for error detection and error correction, without the need for retransmission (forward error correction). The gain that is attained from the coding is evaluated by the bit error rate and depends largely on the applied method for modulation, demodulation, and decoding. Various models to simulate interference of a channel on the Air-interface were used to determine the bit error rate and find a suitable decoder. GSM's choice was the Viterby decoder.

CRC Cyclic redundancy check. A term from the transmission technique.

CUG [GSM 02.85] Closed user group. Used in telecommunications to establish groups of users with specific relationships and privileges. Originally, the concept was used in data networks for security reasons to protect access to a network from unauthorized access. The concept has been extended as follows.

Table G.6
Example of Coding Where Flip-Flop is Preset with 0

Transition	s_0-s_1	s_1-s_2	s_2-s_3	s_3-s_4	s_4-s_5
Input data	0	0	1	1	0
Output code	00	00	11	10	01

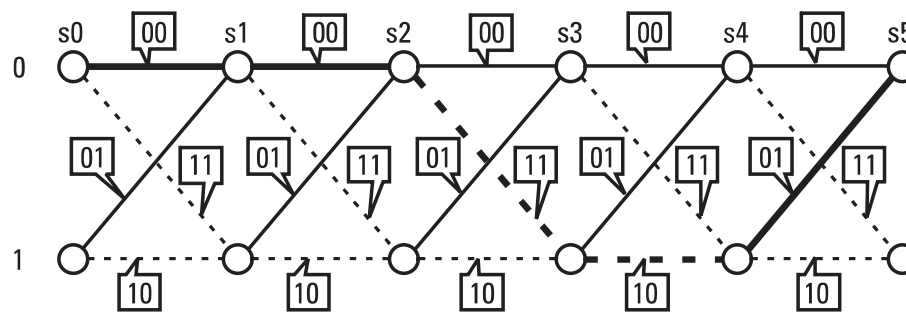


Figure G.23 Trellis diagram.

A CUG is a subset of subscribers of a PLMN (Figure G.24). Typical users of CUGs are companies (e.g., a shipping company) that have employees on the road and want to allow their employees to access the company resources but not have unlimited access to the rest of the network. This creates a kind of virtual private exchange or network. Basically, subscribers that belong to a CUG can communicate only with subscribers of the same group. That applies to calls both to and from a CUG member. The GSM supplementary service closed user group in its basic form restricts users from making any calls outside the CUG and does not allow a user to receive a call from someone outside the CUG. CUG has several options that grant special rights to individual users, like incoming access from non-CUG users or outgoing access to non-CUG users.

Each CUG has an identifier, and a subscriber can be a member of as many as nine different CUGs.

D1, D2 The two GSM 900 networks in Germany. The NDC for D1 is 171, the one for D2 is 172. This information is used in examples throughout this book.

D-interface [GSM 09.02] The interface between VLR and HLR. See Chapter 4.

DCCH [GSM 05.01, 05.02] Dedicated control channel. Generic term to address all bidirectional point-to-point control channels on the Air-interface. An example is the SDCCH.

DCS 1800 Digital Communication System 1800. A GSM system that was ported from the 900 MHz band to the 1800 MHz band. The DCS 1800 has more channels (374), but the protocol and the services are practically identical; only some minor changes to the protocol were made.

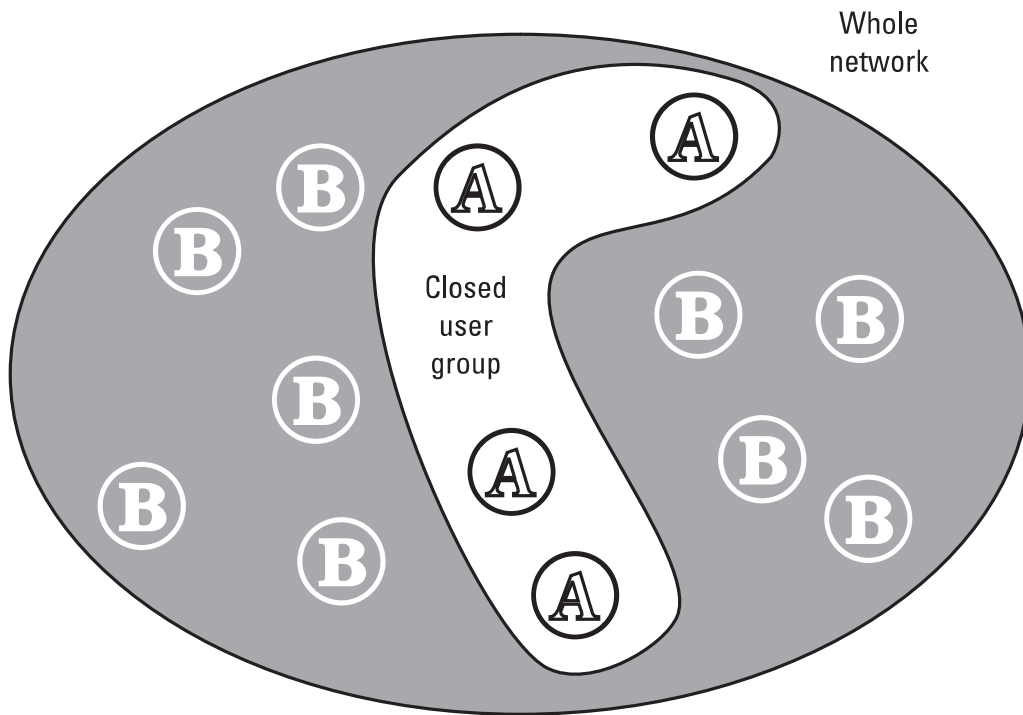


Figure G.24 Closed user group relative to the whole PLMN.

Digit 1 digit = 4 bits = 1/2 byte (see *BCD*).

div A mathematical operator for whole-number division. The result l of a *div* operation is always the whole-number part of the division. n by t , that is, the fraction of the division is discarded. The equation reads:

$$\lambda = v \text{ div } \tau = v/\tau$$

where $\lambda, v \in N_0; \tau \in N$.

Examples are $0 \text{ div } 25 = 0$, $1 \text{ div } 2 = 0$, $5 \text{ div } 3 = 1$, $10 \text{ div } 3 = 3$. A related operation is the *mod* operator.

Diversity Diversity reception is a concept in which the whole receiver path of the TRX module, including the antenna, is implemented multiple times, typically doubled. That allows the signal to reach the receiver via two different paths, and the receiver selects the better of the two signals. In practice, two antennas are mounted rather close to each other. When looking at a radio tower it typically is not possible to tell whether one or two antennas are mounted.

The reason for diversity becomes obvious when we think about an example from everyday life. While a driver is waiting at a stop light and listening to the radio, it frequently happens that the reception quality of the signal degrades. Often it is sufficient to move the car (i.e., the antenna) a very short distance to improve the quality of the reception.

A bad receiver signal at certain spots has the same cause for both radio broadcast and mobile radio, namely, same-channel interference. It is caused (partly) by extinction of the high-frequency signal caused by reflections (e.g., from buildings). This lies in the nature of (electromagnetic) waves, in which two signals with a propagation delay of $l/2$ extinct each other (l = wavelength). For a 900 MHz signal, $l/2$ equals about 1.5m.

With diversity, the TRX demodulates the two signals and forwards them to the low-frequency part. The low-frequency part then decides, based on the quality of the signal, which of the two to process further. Diversity is optional in GSM and hence a decision of the network operator whether or not to deploy it. Cost reduction is the most important factor for a network operator in the decision not to opt for diversity.

DLCI [GSM 08.06, 08.08] Data link connection identifier. An identifier of a DTAP message on the A-interface that identifies which service access point identifier (SAPI) shall be used on the Air-interface. See Chapter 10.

DLR [ITU Q.711–Q.714] Destination local reference. See Chapter 9.

Downlink A direction of signal flow. Used for signals from the network to the mobile station. Table G.7 gives an overview of the frequencies and channels used for uplink and downlink on the Air-interface of GSM 900, DCS 1800, and PCS 1900.

Some time after GSM was put into service, the extended band was introduced to enlarge scarce frequency resources. The extended band was assigned exactly below the original GSM band. The additional channels are numbered from 975 to 1023, which avoids collision with already assigned channel numbers. A number of mobile stations do not support the extended band.

DPC [ITU Q.700–Q.704] Destination point code. Identifier for the destination of an SS7 message (see *MSU*). The length of this identifier differs between ANSI and ITU. The ITU SS7 standard defines the DPC as 14 bits, while the ANSI SS7 standard defines it as 16 bits long. See Chapter 8.

Table G.7
Uplink and Downlink Frequencies of GSM 900, DCS 1800, and PCS 1900

	GSM 900	DCS 1800	PCS 1900
Downlink frequencies	935,2–960 MHz 925,4–935,0 Mhz (extended band)	1805–1880 MHz -/-	1930–1989,6 MHz -/-
Uplink frequencies	890,2–915 MHz 880,4–890,0 Mhz (extended band)	1710–1785 MHz -/-	1850–1909,6 MHz -/-
Channel numbers and number of available channels	1–124 = 124 channels 975–1023 = 49 channels (extended band)	512–885 = 374 channels -/-	512–810 = 299 channels -/-
Formula to convert frequency and channel number	$n = \text{ARFCN} = 1-124$	$n = \text{ARFCN} = 512-885$	$n = \text{ARFCN} = 512-810$
Downlink:	$F(\text{DL}) = (935,2 + 0,2^* (n - 1)) \text{ MHz}$	$F(\text{DL}) = (1805,2 + 0,2^* (n - 512)) \text{ Mhz}$	$F(\text{DL}) = (1930 + 0,2^* (n - 512)) \text{ Mhz}$
Uplink:	$F(\text{UL}) = (890,2 + 0,2^* (n - 1)) \text{ MHz}$	$F(\text{UL}) = (1710,2 + 0,2^* (n - 512)) \text{ MHz}$	$F(\text{UL}) = (1850 + 0,2^* (n - 512)) \text{ MHz}$
Extended Band:	$n = \text{ARFCN} = 975-1023$	-/-	-/-
Downlink:	$F(\text{DL}) = (935,2 + 0,2^* (n - 1024)) \text{ MHz}$	-/-	-/-
Uplink:	$F(\text{UL}) = (890,2 + 0,2^* (n - 1024)) \text{ MHz}$	-/-	-/-

DRX [GSM 03.13/05.02] Discontinuous reception. Used like the DTX as a power saver for the mobile station and to save radio resources. By separating mobile stations into paging groups, a particular mobile station needs to listen to the paging channels (PCH) only in certain multiframes. The transmitter can be switched off in the meantime, in what constitutes the power saving.

DTAP [GSM 04.08, 08.06] See *BSSMAP*.

DTMF [GSM 03.14, 04.08] Dual tone multifrequency. Method to transmit information in an in-band manner over telephone lines by facilitating a combination of two frequencies for every symbol. It distinguishes 12 different symbols. The symbols are the ones found on a telephone set, that is, the numbers 0 through 9 and the symbols * and #. It allows control of processes at the remote end of the connection. As shown in Figure G.25, each key is assigned a unique combination of two frequencies that are created in the telephone set and transmitted when the key is pressed. Today, DTMF is used worldwide for voice mail control, telephone banking, computer-integrated telephony applications, and so on.

GSM supports DTMF for voice connections only in the uplink direction. For GSM, however, no tones are sent over the Air-interface, but messages indicate the beginning and the end of a DTMF tone. When a user presses a button, the ASCII value of the button is sent to the MSC in a `START_DTMF`

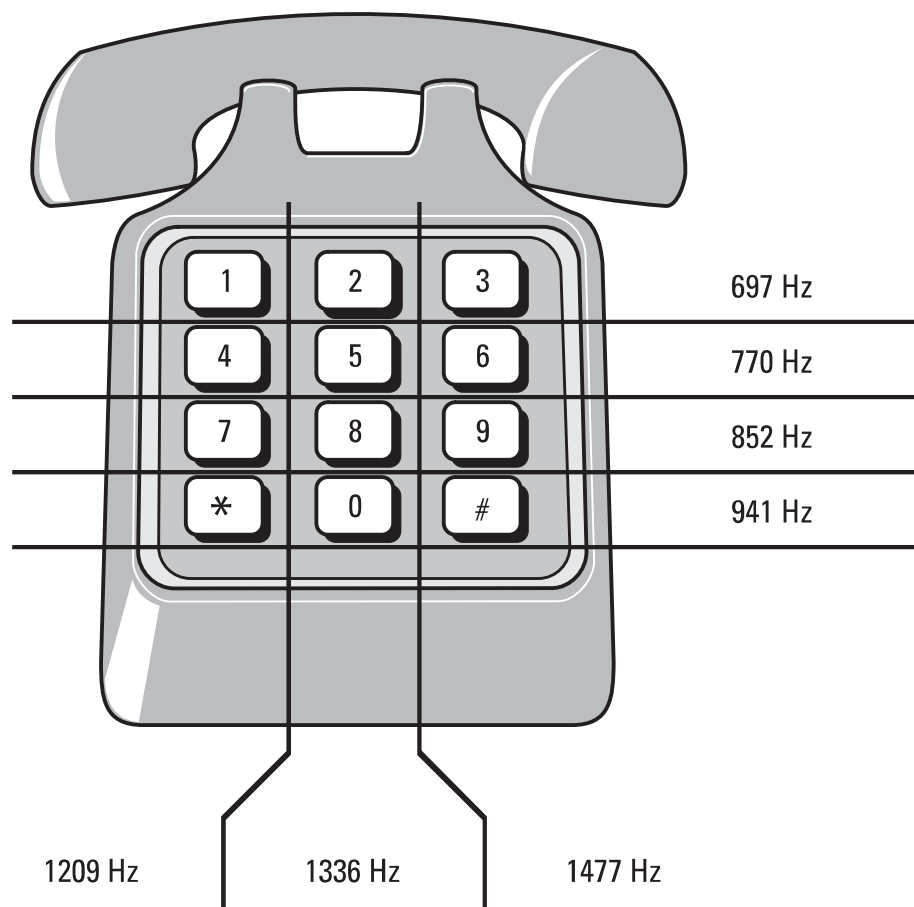


Figure G.25 Key/frequency combinations for DTMF.

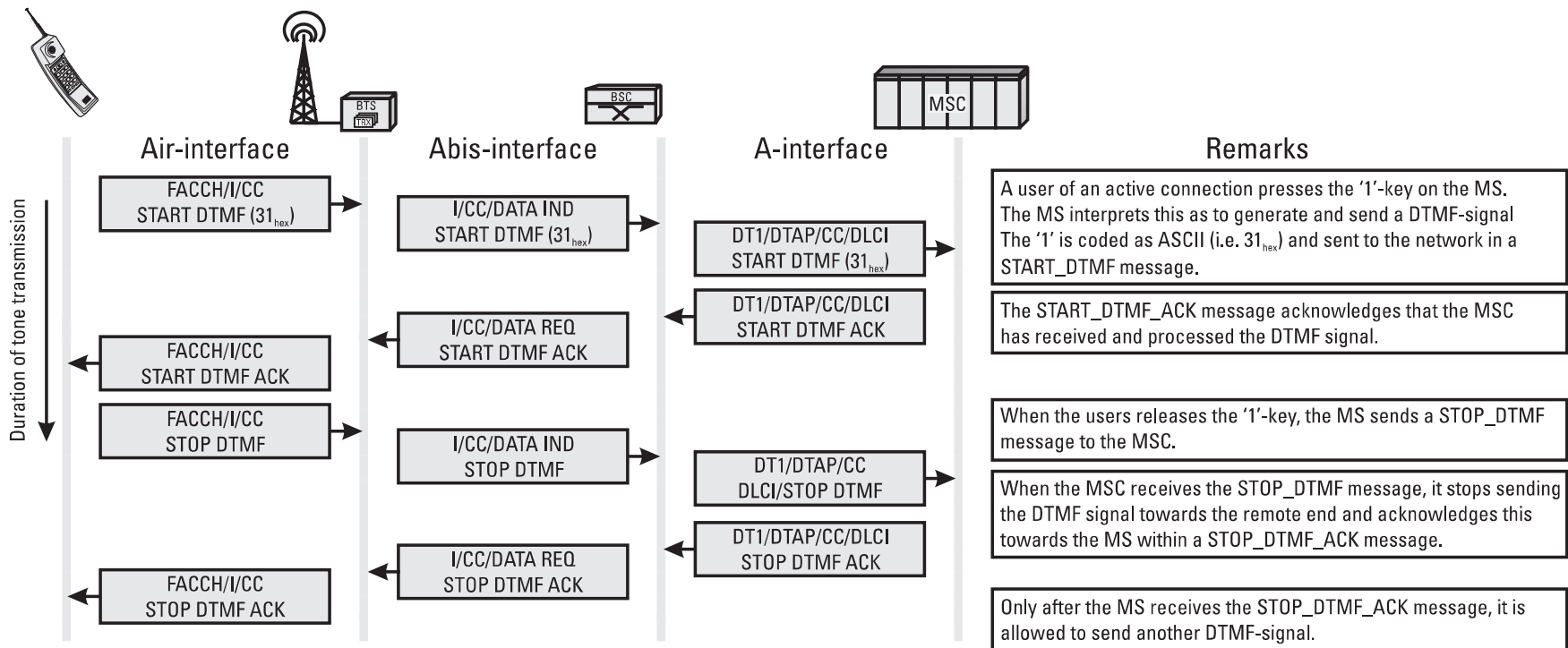


Figure G.26 DTMT-Transmission.

```
DATA INDICATION
Channel Number: Bm + ACCH, TN = 7
Link Identifier
Channel Type: main signaling channel (FACCH or SDCCH)
NA=0: applicable for this message
SAPI 0
L3 Information (Hex): 03 75 2C 31
START DTMF
Keypad Facility = 1
```

Figure G.27 Example of a START_DTMF message.

message. When the button is released, a STOP_DTMF message is generated. The messages are sent in encrypted form on the SACCH or the FACCH. The MSC analyzes the message, generates the frequency combination, and sends the DTMF signal to the remote end. Because the duration of a tone also might be important, the whole process becomes slightly more complex, as shown in Figure G.26.

Figure G.27 is an example of a START_DTMF message in which a user wants to send a 1. The 1 can be found coded as 31_{hex} in the last byte of “L3 Information (Hex).”

DTX [GSM 05.08, 06.12, 06.31, 06.32, 08.60] Discontinuous transmission. During a telephone conversation, typically only one party speaks at a time. At times, no one speaks. It is practical to switch off the Air-interface partly or completely during those silent times until the conversation resumes. One problem to avoid is clipping, that is, the situation when beginnings and ends of words are cut off because the volume of the speech is below a threshold and considered to be silent time. Setting the volume threshold is difficult because different languages have different dynamics, and what appears to be good enough for English may be poor quality for spoken Chinese. The process of detecting silent time and cease transmission is called discontinuous transmission. DTX needs to be distinguished from DRX (discontinuous reception); both methods are independent of each other.

DTX can be activated separately for uplink and downlink. The advantage of using DTX in the uplink direction is the power savings potential within the MS and for both uplink and downlink to reduce interference. One potential problem of DTX is related to background noise. People are so used to it that if it is not there, they assume the connection has been lost, particularly in a mobile conversation. DTX eliminates background noise, so to avoid the impression of a lost connection, artificial noise (called comfort noise) is generated when DTX is active.

With DTX enabled, the BTS or the MS sends only one block of data (456 bits according to channel coding) every 480 ms, which, because of interleaving and depending on the channel type, is transmitted with a variable number of bursts. That allows both sides to still measure the quality of the connection and to adjust the comfort noise if necessary.

Figure G.28 provides an example. After sending speech frames (see under TRAU frame), the MS indicates by a SID frame (SID = silence descriptor) that DTX was activated. A SID frame is a regular speech frame

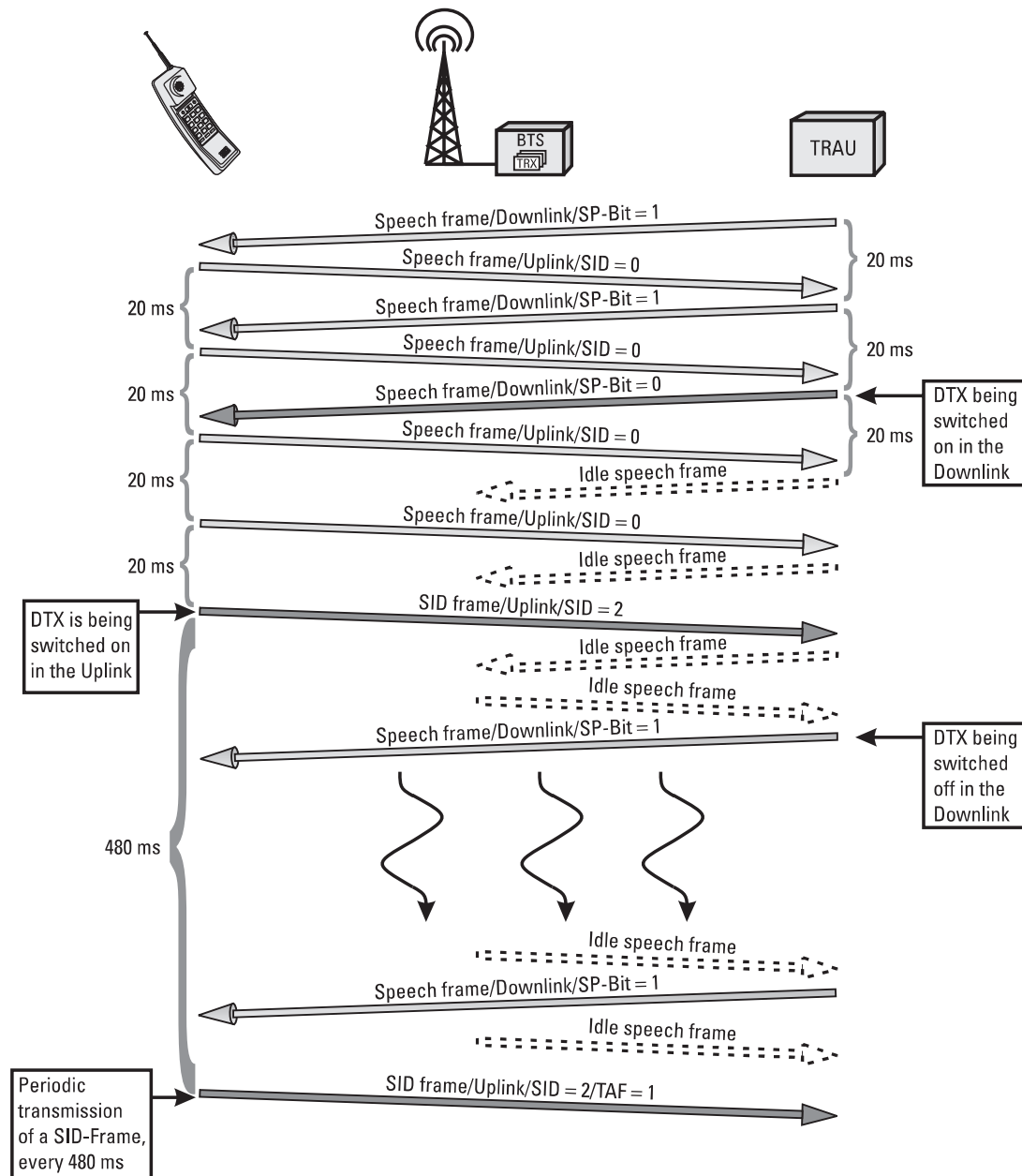


Figure G.28 Activation and details of DTX.

with a 320-bit length, where the SID control bits indicate that DTX was switched on and its data bits allow for the generation of the comfort noise. The TAF bit in the second SID frame from the MS indicates that this packet represents the compulsory frame that has to be sent every 480 ms.

The same applies for the activation of the DTX in the downlink direction. However, the downlink speech frame distinguishes between DTX on and off with the SP bit (speech indicator). This decision is taken by the TRAU.

Note that with active DTX, only the transmission on the Air-interface is turned off. Between TRAU and BTS, however, transmission of idle speech frames (see under TRAU frame) is required. DTX is switched off in the respective direction when one of the connected parties resumes the conversation.

The MSC is always in control of downlink DTX, while the uplink DTX has to be coordinated between BTS and MS. For that purpose, the BCCH/SYS_INFO 3 contains a 2-bit parameter, the DTX indicator, that indicates whether DTX can be applied to the uplink or if it needs to be prohibited.

E-interface [GSM 09.02, 09.10] The interface between MSCs. See Chapter 4, Chapter 11, and Chapter 12.

EIR [GSM 03.02, 03.20, 12.02, 12.03] Equipment identity register. See Chapter 4.

EMI Electromagnetic interference. A critical factor, particularly in a system that uses pulses for transmission purposes. In a TDMA system, like GSM, the transmission occurs only a fraction of the time. Much research has been done in this area so far. The most important result was a potential temperature increase in parts of the head of a GSM-handset user. That is due to the high frequency radiation of a handset that is similar—but to a much lesser extent—to what happens in a microwave oven. This thermal aspect can be reduced by special antenna design, maximum distance between the antenna and the head, and low-power handsets (less than 2W). On the other hand, no certain evidence exists on the nonthermal impact of pulsed high-frequency radiation on the human organism.

It has been proven, however, that GSM handsets may affect electronic components of automobiles. For example, they possibly may activate the airbags, cause the ABS to fail, or cause the ignition system not to work properly. Therefore, it may be dangerous to use a mobile phone in a car without an external antenna. All manufacturers of handsets and all network operators nowadays advise subscribers to refrain from such use.

Another electromagnetic impact of a GSM phone is rather easy to reproduce. Anyone who has ever operated a GSM phone near other electronic

instruments has noticed the low-frequency interference of an active GSM telephone with equipment like TVs, stereo receivers, even fixed network telephone sets. The reason why that can be heard at all lies in the TDMA structure of GSM. As shown in Figure G.29, the transmission energy is radiated in pulses every 4.615 ms. That corresponds to a low frequency of $f = 1/T = 217$ Hz. If that is not completely shielded—and in real life that is never the case—a part of the signal can be picked up by the electronic equipment.

Encryption See *Ciphering*.

ETSI European Telecommunications Standard Institute. European organization responsible for standardization in Europe. It emerged from CEPT in 1988.

Extended band See *Downlink*.

External handover [GSM 05.08] Handover between two cells assigned to two different BSCs. External handover consequently involves two BSCs and possibly two MSCs. (For more details, see Chapter 12; also see *T8* and *synchronized handover*.)

F-interface [GSM 09.02] The interface between the equipment identity register (EIR) and the MSC. More details are provided in Chapter 4.

FACCH [GSM 04.04, 05.01, 05.02] Fast associated control channel. An in-band signaling channel, just like the SACCH, that is associated with an active connection between the MS and the BTS. In contrast to the SACCH, which is sent once per multiframe, the FACCH is used only when no delay is acceptable, that is, if it is not possible to wait for the next SACCH. Then the FACCH is inserted instead of user data. The stealing flag serves to distinguish user data from signaling within a burst. The FACCH can transport 9200 bps in a fullrate channel and 4600 bps in a halfrate channel. (see *N201*, *Burst*.)

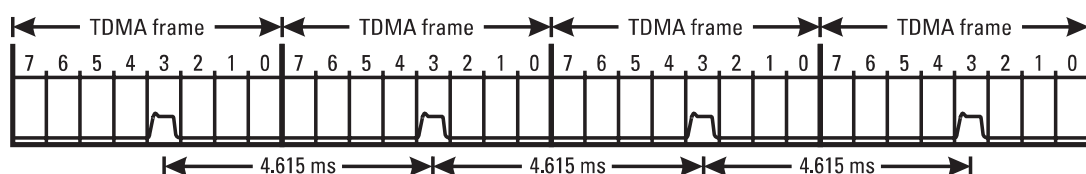


Figure G.29 Low-frequency interference caused by GSM.

FAS [G.711] Frame alignment signal. Term from transmission systems. The FAS is used in a PCM system and transmitted in time slot 0. It allows for synchronization of sender and receiver on the frame structure.

FCCH [GSM 05.01, 05.02] The BTS sends the frequency correction channel (FCCH) on time slot 0 of a BCCH-TRX in frequency bursts (see *Burst*). All 142 data bits are set to zero. Exactly five FCCHs are sent per 51-multiframe. The FCCH allows an MS to identify the frequency of a BTS in GSM. After sending an FCCH, an SCH has to be sent. More details are provided in Chapter 7.

FCS Frame check sequence (FCS). Added to information and control fields of LAPD and SS7 frames. The task of the FCS is the cyclic redundancy check (CRC), which allows Layer 2 to detect transmission errors.

FDMA Frequency division multiple access. Access-sharing technique like TDMA. Multiple access techniques are used to allow a number of users to access a system simultaneously. For that purpose, FDMA divides the frequency space into a multiplicity of frequencies that all can be used at the same time. GSM uses both types of access sharing. For more details, see Chapter 7.

FIB [ITU Q.700–Q.704] Forward indicator bit. The most significant bit (MSB) within the second byte of an SS7 message (FISU, MSU, LSSU). It is used, together with FSN, BSN, and BIB, for error detection during data transmission. See Chapter 8.

Fire code Part of a procedure for data protection during transfer over the Air-interface, used especially for signaling data. See *Channel coding*.

FISU [ITU Q.700–Q.704] Fill-in signal unit. One of three SS7 messages of OSI Layer 2. (The other two are LSSU and MSU.) Figure G.30 shows the format of a FISU. The length indication (LI) element, which in the case of FISUs is always zero, allows distinguishing between FISU, LSSU, and MSU.

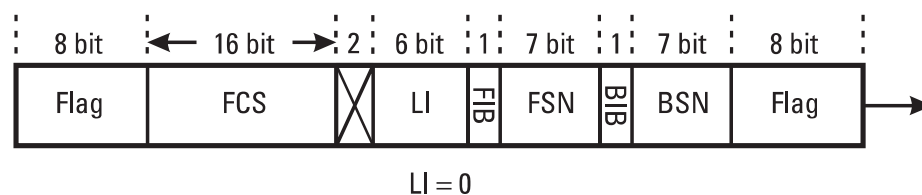


Figure G.30 Format of a FISU.

FN [GSM 05.01/05.02] Frame number. Internal clock of a BTS, to which every MS has to synchronize before the MS can start communicating with the BTS. For that purpose, the BTS broadcasts the current frame number five times for every 51-multiframe over the synchronization channel (see *SCH*).

The FN can take on values between 0 and 2,715,647, where each FN identifies exactly one TDMA frame within a hyperframe. The value 2,715,647 represents the possible number of frames, where $2,715,647 = (26 \cdot 51 \cdot 2048) - 1$. The $- 1$ is necessary, since the count starts with zero. The equation represents the composition of a hyperframe. It consists of 2,048 superframes, each superframe consists of 26 multiframes with 51 TDMA frames or 51 multiframes with 26 TDMA frames. What is transmitted, however, is not the absolute value of the FN, but the relative position of an FN in the frame hierarchy, consisting of 51-multiframe, superframe, and hyperframe. (See also Chapter 7.)

This method of addressing the FN is similar to the way two people tell the time of day. Compare, for example, “The time is 54.900 seconds,” and “The time is 3.15 p.m.” In practice, the FN is sent as a combination of the parameters T1, T2, and T3, what could be brought in the analogy the example hours (T1), minutes (T2), and seconds (T3’) of a clock. The rule is the following:

- T1 (11 bit): Number of the superframe in the hyperframe {0 ... 2,047}; $T1 = FN \text{ div } 1326$, where $1,326 = 51 \times 26$
- T2 (5 bit): Number of the 51-multiframe in the superframe {0 ... 25}; $T2 = FN \text{ mod } 26$
- T3: (6 bit): Number of the TDMA frame in the 51-multiframe {0 ... 50}; $T3 = FN \text{ mod } 51$
- T3’ (3 bit): $(T3 - 1) \text{ div } 10$ out of {0 ... 4}

For T3, only the value of the decade has to be sent, since the synchronization channel is sent exactly five times per 51-multiframe, in fact, always in the position $FN = 1, 11, 21, 31, 41$ (compare Figure G.31). The single digit value, therefore, is redundant and there is no need for its transmission. The value T3’ {0 ... 4} tells the MS exactly which FN in a 51-multiframe is meant and can easily calculate the FN of a 26-multiframe or the absolute value of FN.

Note that this rule applies only to the transmission of FN on the synchronization channel. When the *CHAN_RQD* message is being transmitted, the entire value of T3 has to be sent. That allows the number of the superframe (T1) to be truncated. Indeed, T1’ is used in this case, rather than T1, with $T1' = T1 \text{ mod } 32$. T1’ represents the last five bits of T1. The reason for that is obvious:

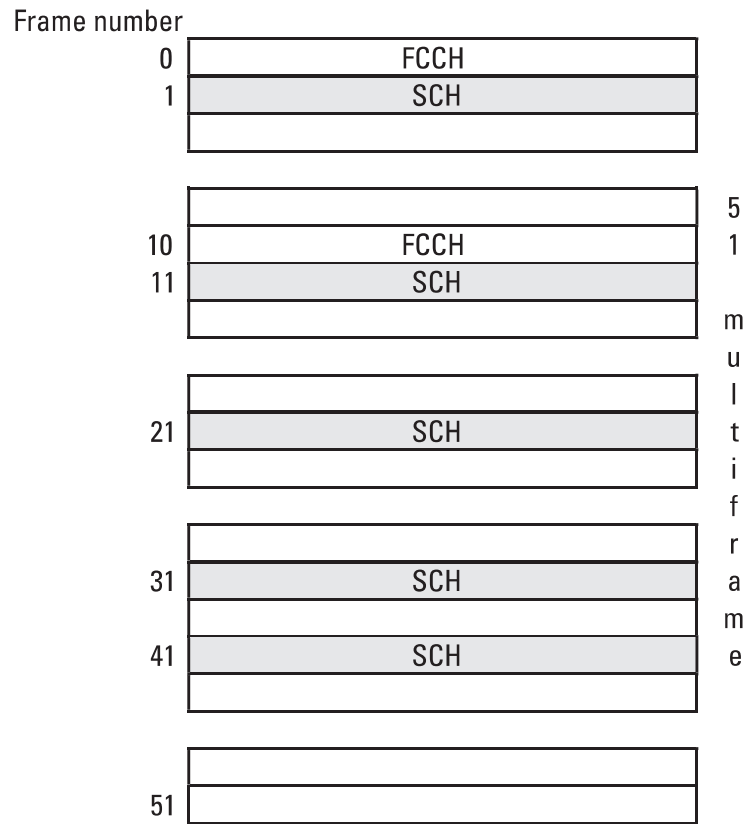


Figure G.31 The fixed position of a synchronization channel in a 51-multiframe.

- First of all, depending on the channel configuration, it is possible to send a RACH, practically anywhere within a 51-multiframe. Thus, T3 cannot be truncated.
- Furthermore, the BSC needs to respond to a CHAN_RQD within seconds. It is therefore not necessary to know the absolute number of the superframe. Knowing only the least significant five bits of the superframe number enables the BSS to uniquely identify and address a single CHAN_RQD message within a time period of $(2^5 - 1) \cdot 6.12s = 189.72s$ (a superframe has a cycle time of 6.12s), which is more than sufficient.

GSM refers to this type of frame number as starting time where *starting time* = $FN \bmod 42432$

Frame Number See *FN*.

Frequency hopping See *HSN*.

Frequency See *Downlink*.

FSN [ITU Q.700–Q.704] Forward sequence number. The sender of an MSU numbers each MSU sent (that is the FSN) and expects an acknowledgment from the receiver. The acknowledgment is sent in the form of the backward sequence number (BSN). See Chapter 8.

G-interface [GSM 09.02] The interface between VLRs. See Chapter 4 and Chapter 11.

G-MSC [GSM 03.02] Gateway mobile switching center. Mobile switching center with an additional functionality that allows a GSM network to interface with other networks. See Chapter 4.

Global title [Q.713] Optional part of the SCCP address. Various formats of the global title exist, but it always contains a routable number, which the SCCP uses to route messages to a network element. See Chapter 9.

GMSK [GSM 05.04] Gaussian minimum shift keying. Method for modulating signals in GSM. It is, as the name suggests, a special form of minimum shift keying (MSK), which belongs to the group of frequency modulation (FM) techniques. The modulated output signal F_O depends on the input signal E , where F_O is switched between the two frequencies $(F_T + f_t)$ and $(F_T - f_t)$. This represents the two (digital) input values $E = 0$ and $E = 1$. Figures G.32 illustrates the MSK modulation for a sequence of input bits. Figure G.32(a) shows the input signal that has to be modulated. The bit sequence in this example is 1110100110101000011. Figure G.32(b) shows the same bit sequence after two consecutive bits have been joined by an exclusive OR (XOR) operation.

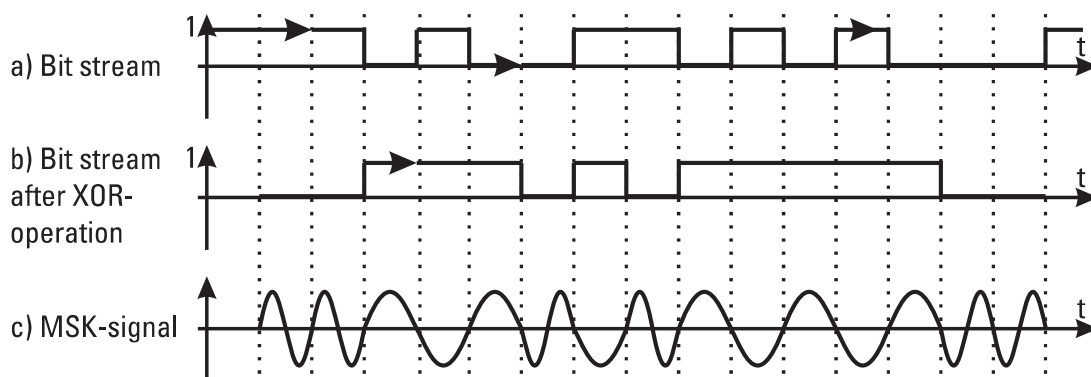


Figure G.32 Generation of an MSK-modulated signal.

Table G.8 shows the corresponding truth table of this operation. To express it in words: When two consecutive bits have the same value, that is, both are 1 or both are 0, the result is 0; when two consecutive bits have different values, the result is 1. Figure G.32(c) and Table G.8 show how the output frequency of the sender depends on the result of the XOR operation.

A disadvantage of MSK is the resulting, relatively wide spectrum of this operation, due to the hard shift between the two frequencies ($F_T + f_t$) and ($F_T - f_t$). It is, however, crucial for every mobile system to use the scarce frequency resources as economically as possible. The GSM community, for that reason, decided not to use MSK; instead, it chose GMSK, which better meets the frequency economy constraint.

GMSK also uses the two frequencies ($F_T + f_t$) and ($F_T - f_t$) but shifts smoothly between the two. Figure G.33 illustrates the process. The bit sequence in Figure G.33(a) is the signal after application of the XOR operation. It represents, electrically speaking, a rectangular-shaped voltage. That voltage is then filtered by a low-pass filter, which smoothes the edges of the rectangle, as shown in Figure G.33(b). The new signal is used as input signal for the modulator. The resulting output frequency is shown in Figure G.33(c.) One can clearly see how the shift between ($F_T + f_t$) and ($F_T - f_t$) occurs more smoothly, which translates into a smaller frequency spectrum, that is, less bandwidth. This positive effect results from filtering the input signal with a Gauss filter with the following parameters

$$B \times T = 0.3$$

where B = 3-dB bandwidth and T = duration of an input bit:
 $T = 577 \text{ ms} / 156,25 \text{ bits} = 3,693 \text{ ms}$.

Table G.8

Truth Table for the Transmission Frequency

Bit ($N-1$)	Bit N	XOR	Frequency
0	0	0	$F_T + f_t$
0	1	1	$F_T - f_t$
1	0	1	$F_T - f_t$
1	1	0	$F_T + f_t$

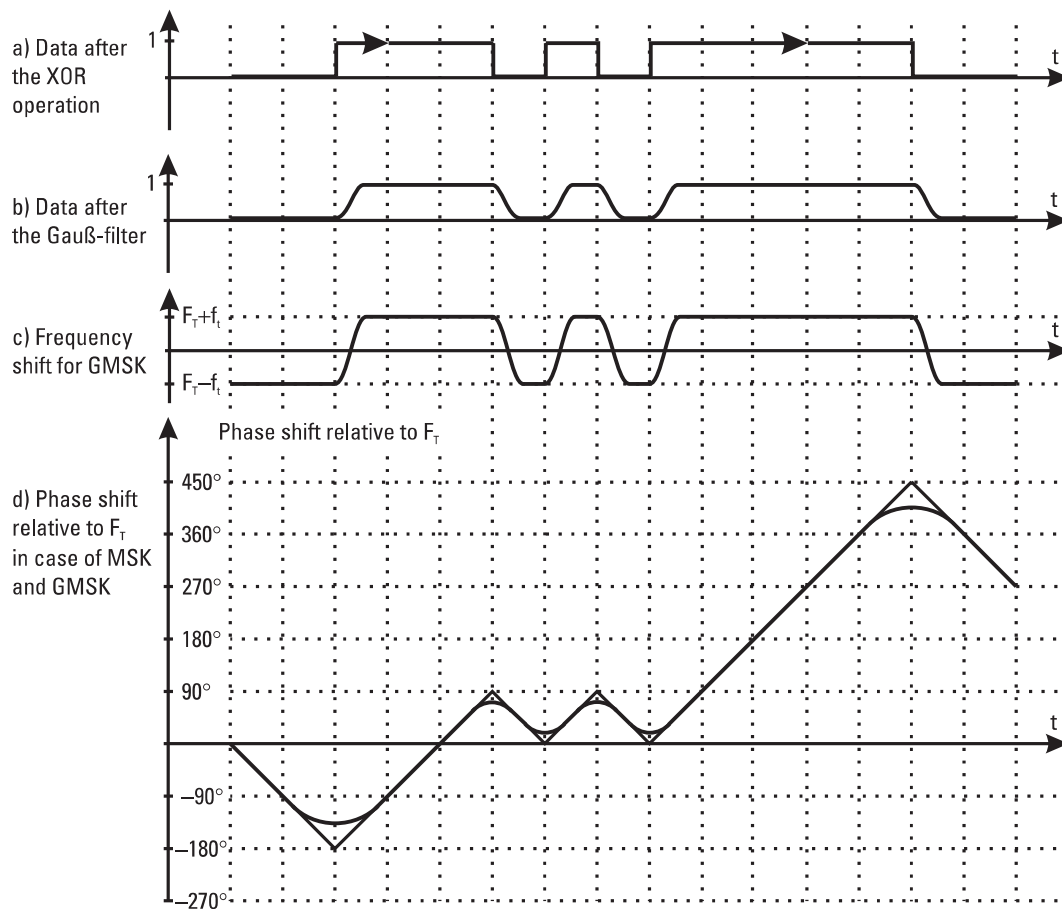


Figure G.33 Frequency chart of GMSK and phase chart of GMSK versus MSK.

From the available data and the index of the modulation $h = 0.5$, the frequency shift, f_t , can be derived. The value $\pm f_t$ indicates the extrema of the frequency, that is, the maximum and the minimum between which the carrier frequency is switched.

The following rule applies:

$$f_t = (\text{data rate} \cdot h) / 2$$

The data rate is determined by the reciprocal value of T (the duration of 1 bit), $1/T = 270.8 \text{ kHz}$.

$$f_t = 270.8 \text{ kHz} \cdot 0.5 \cdot 0.5$$

$$f_t = 67.7 \text{ kHz}$$

An interesting side effect is that since all 142 bits of the frequency correction burst (see *burst*) are coded with a zero value, the transmission frequency of a BTS is not exactly the BCCH frequency but is shifted by exactly 67.7 kHz upward.

The advantages of GMSK can be described as follows: (1) It does not—at least in theory—contain any AM portion, and (2) the required bandwidth of the transmission frequency is an acceptable 200 kHz.

H-interface [GSM 03.02] The interface between the home location register (HLR) and the authentication center (AuC). The H-interface is not standardized, since the AuC is an integral part of the HLR.

Handoff U.S. term for *handover*.

Handover [GSM 04.08, 05.08, 09.10] Operation by which an MS is assigned another traffic channel while involved in a connection. It does not require the cell to change; the two channels can be on the same BTS. See Chapter 12.

Handover number [GSM 03.03, 09.10] A number temporarily assigned to a subscriber in case of a handover between two MSCs, the so-called inter-MSC handover; used to route the call between the two MSCs. The format of this number corresponds to the MSRN.

Handover reference [GSM 04.08] An 8-bit-long parameter that the destination BSC or new BSC randomly assigns for the handover process. The destination BSC sends the value both ways, to the destination BTS and via the new MSC to the originating MSC, which forwards the number, via originating BSC/BTS to the MS. The MS receives its handover reference in an HND_CMD message, which it transmits in an HND_ACC message to the destination BTS. The handover reference is therefore an identifier of the MS at the destination BSC or the new BTS.

HDLC High-level data link control. The general frame format used, for example, by LAPD and SS7. An HDLC frame has, as shown in Figure G.34, a flag at each side, beginning and end, followed by an address field and a control field. The actual data follow the control field. The FCS allows detection of potential transmission errors.

Heading code [Q.704] The message group and message type of an SS7 network management and test message are determined by the heading codes

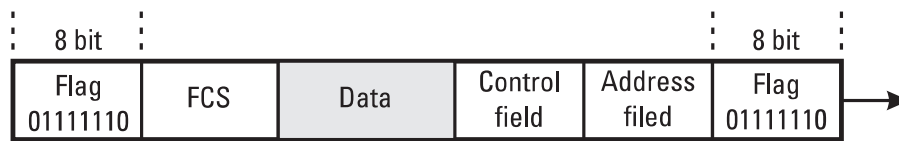


Figure G.34 The HDLC format

0 and 1. This group of messages, for example, COO (change over order) and COA (change over acknowledge), provides information used to bring links into service or to take them out of service, as well as to test and control connections. It is not used, however, to transfer user data.

HLR [GSM 03.02, GSM 03.20, GSM 09.02] Home location register. See Chapter 4.

HLR number [GSM 03.03] The format of an HLR number is the same as for a regular directory number, complying to ITU/T E.164 (see *MSISDN*). Every HLR is assigned a unique address, the HLR number, to enable the SCCP to route messages to the HLR (see also *global title*).

HMI [GSM 02.30] Human-machine interface, formerly called the man-machine interface (MMI). Refers generally to the interface between the human user and any kind of machine (e.g., a personal computer). The keys and the display of the MS are the basic means of a GSM system for this interface, which defines which key combinations activate a certain feature.

HO Handover (see also *Synchronized handover*). See Chapter 12.

HOLD A supplementary service (see *SS*).

HSN [GSM 05.02] Hopping sequence number. One of the following parameters that are necessary to execute frequency hopping.

- Cell allocation (CA). The list of all frequencies (see ARFCNs in ascending order) available in a cell (maximum 64) The CA is part of the BCCH / SYS_INFO 1.
- Mobile allocation (MA). Selection of the frequencies from the CA list that are applicable for the MS and the hopping sequence (maximum 64).
- Hopping sequence number (HSN). A value between 0 and 63 (6 bits without sign) used to control the hopping generator.

- Mobile allocation index offset (MAIO). A value between 0 and 63 (6 bits without sign). The valid range is always equal to the number of frequencies of the MA. The index is different for all MSs that occupy the same MA and the same time slot of a TDMA frame. This results in spreading the mobile stations over the available frequencies.
- Frame number (FN). The frame number or its partial counters (T1, T2, T3) are the variables that change over time for the generation of the hopping sequence.

The parameters MA, HSN, and MAIO are transmitted, for example, in the IMM_ASS-message.

Frequency hopping in a GSM system is referred to as slow frequency hopping because the frequency is constant, that is, the same for the duration of a burst. Fast frequency hopping, in contrast, requires altering of the frequency with every transmitted symbol (bit). The frequency in a GSM system, from the perspective of the mobile station, changes only from TDMA frame to the next TDMA frame, that is, every $8 \cdot 577\mu\text{s}$. The time for a mobile station to adapt to the new frequency, therefore, is $7 \cdot 577\mu\text{s}$. That applies if a synthesizer is available for both uplink and downlink. If only one synthesizer is available for both directions, the time to adjust to the new frequency is reduced to $\approx 4 \cdot 577\mu\text{s}$. The reason is that the mobile station can change only the frequency after the transmission in the uplink is completed (delay of three time slots; see *TA*).

The BTS, on the other hand, has to be capable of changing the frequency from burst to burst. To accomplish that, basically two alternatives are available.

- Baseband hopping. A TRX is divided into a baseband portion (for signal processing) and an HF portion, connected via a switch matrix. The switch matrix is able to connect every baseband signal with every HF signal and knows the hopping sequence of every channel. Uplink and downlink need to be switched separately, because of the known delay of three time slots between them. That results in the baseband signal portion of the TRX on the downlink being connected to a different carrier than for the uplink. The advantage of this alternative is that the HF portion is much easier to implement than for synthesizer hopping. The disadvantage is that it requires a switch matrix and it is possible to hop between only as many frequencies as currently are implemented.
- Synthesizer hopping. With synthesizer hopping, the frequency of the TRX changes from time slot to time slot by reprogramming the frequency of the synthesizer. That requires two pairs of synthesizers, one

pair for the uplink, the other for the downlink. One synthesizer of a pair is always active, while the other prepares for its new frequency, so that each has enough time to adjust to the new frequency. The guard period of a burst is actually used to switch between the synthesizers. Synthesizer hopping is, because of the strict requirements on frequency errors and phase faults in GSM, technically much more demanding than baseband hopping. One major advantage lies in the gained flexibility in network planning, where it is potentially possible to exploit all available frequencies for hopping, independent from the number of carriers that a BTS has.

Mixed configurations of baseband hopping and synthesizer hopping, separated for uplink and downlink, are viable and are deployed. A problem that exists, particularly with older versions of synthesizer hopping, is the potential interference with heart pacemakers (see *EMI*).

Hyperframe [GSM 05.01, 05.02] The hyperframe represents the largest time scale in the GSM frame hierarchy, with a total length of 3 hours, 28 minutes, 53 seconds, and 760 milliseconds. It is composed of 2,048 superframes, which are composed of 1,326 multiframes. See Chapter 7.

Idle-channel measurements [GSM 05.08, 08.58] The TRX permanently performs interference measurements on unused time slots, to determine potential interference on those channels. Interference can be caused by mobile stations or non-GSM systems. The measurements are sent to the BSC in an RF_RES_IND message. The BSC in turn takes the interference measurements into account before assigning a traffic channel.

IMEI [GSM 02.16, 03.03, 03.20] Mobile station equipment identity. Figure G.35 shows the format of the IMEI. In contrast to the IMSI, the IMEI identifies the mobile equipment rather than the subscriber. Another difference to the IMSI is that it is not mandatory for the network operator to query the

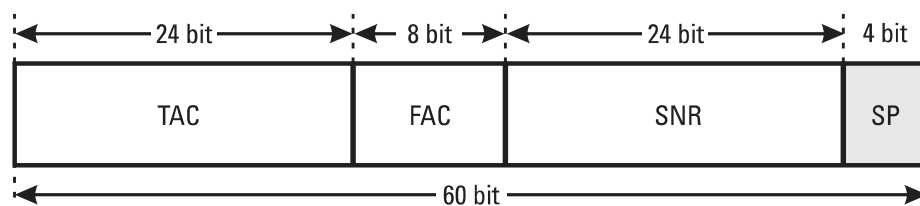


Figure G.35 Format of the IMEI.

IMEI. The purpose of the IMEI is to be a means for passive theft protection. When this functionality is active in a network, the EIR maintains information on stolen mobile equipment in a “black list,” which makes stolen mobile equipment useless. It is even dangerous for a thief to use stolen equipment, since its use reveals the user’s identity, which comes with the SIM, to the network operator. The IMEI comprises the following:

- A 24-bit-long type approval code (TAC). Before any mobile equipment can be brought into service, it has to undergo a test to show that it complies with safety regulations and functionality requirements. This process is called type approval, and the requirements are specified by GSM.
- An 8-bit-long final assembly code (FAC), which identifies the manufacturing facility.
- A 24-bit-long serial number.
- A spare field, currently not used.

Chapter 4 provides more details on the EIR.

IMEISV The IMEISV corresponds to the IMEI plus a software version number (SVN), which can be modified by the manufacturer in case of a software update. The format of the IMEISV is shown in Figure G.36.

IMSI [GSM 03.03, 03.20] International mobile subscriber identity. As identifier for a GSM subscriber, the IMSI is part of the subscriber data stored on the subscriber identity module (SIM) card. The IMSI uniquely identifies one subscription worldwide and is derived from ITU-T Recommendation E.212. Its structure is similar to the ISDN number, which is defined in ITU-T Recommendation E.164. The IMSI is a 15-digit number and is composed of the mobile country code (MCC), the mobile network code (MNC), and the mobile subscriber identification number (MSIN). Note that in GSM, unlike other standards, the MSIN of the IMSI is not used as the subscriber’s telephone

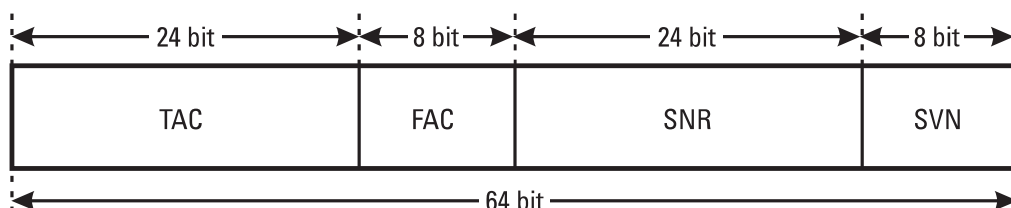


Figure G.36 Format of the IMEISV.

number. To make subscriber tracking more difficult, the IMSI is used only as an identifier when the temporary mobile subscriber identity (TMSI) is not available, e.g., for initial system connections. Figure G.37 shows the format of the IMSI.

IMSI attach/detach [GSM 04.08, 09.02] The BTS permanently broadcasts the parameter ATT in the BCCH / SYS_INFO 3 message. This parameter indicates whether the IMSI attach/detach procedure is required. IMSI detach is a procedure to inform the network that a mobile station will go into an inactive state and thus is no longer available for incoming calls, for example, because of powerdown or because the SIM is removed. The mobile station sends an IMSI_DET_IND message to the network each time it is powered down. The VLR keeps track of that state. The merit of this approach is that it saves radio resources and processing time. The call processing can switch to secondary call treatment, without the need of first sending a PAGING message and then waiting for expiration of the respective timers. Secondary call treatment means initiating call forwarding, voice mail, or simply indicating to the caller that the subscriber is currently not reachable. The complementary operation to IMSI detach is IMSI attach. It indicates to the network that a mobile station is active again. IMSI attach is related to periodic location updating. The location updating procedure is utilized to perform IMSI attach.

Inband signaling The counterpart to outband signaling. Inband signaling describes the situation when control information is transmitted within the traffic channel rather than in dedicated channels for signaling. Examples of outband signaling are SS7, LAPD signaling; examples of inband signaling are FACCH and SACCH (Air-interface).

Incoming call [GSM 04.08, 08.08, 09.02] A call request for a mobile subscriber. Also referred to as mobile terminating call (MTC). See Chapter 12.

Incoming handover [GSM 04.08, 05.08, 08.08, 09.02] During handover, the originating BTS or old BTS that the mobile station is leaving is involved in

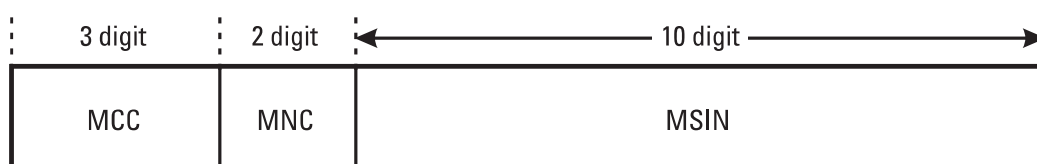


Figure G.37 Format of the IMSI.

an outgoing handover, while the destination BTS or new BTS to which the mobile station is handed over is involved in an incoming handover.

Interleaving [GSM 03.05, 03.50, 05.03] Procedure to distribute or interlace the bits of a channel-coded block (see *channel coding*) onto several bursts. Since channel coding is designed to detect and correct errors on only a relatively few bits, it is the goal of interleaving to prevent complete loss of the information when a whole burst is corrupted. If, for example, a complete burst is lost, but all the others are transmitted without error, only one bit of a larger piece of information is missing and can be restored by the Viterby decoder.

The likelihood of group errors on a radio interface is naturally much higher than errors on single bits. The reason is the effect of fading, which typically is slower than the 270-Kbps transmission rate of the Air-interface.

For transmission of data, the bits are distributed even more than in the case of speech. For data transmission, it is even more important not to lose a single bit, since that could render a complete transmission useless. Speech is not very sensitive to single-bit errors. Propagation delay, on the other hand, is crucial for speech and does not have a very high priority for data connections. The more the bits of one sample are spread over time, the longer the receiver has to wait until all bits for a certain sample have arrived. For data services, that essentially affects only timers of the protocol. This affects the RLP protocol for non-transparent data and the end-to-end protocols of terminal applications for transparent data (GSM 03.05, 03.50).

In a fullrate speech channel, interleaving accounts for a maximum delay is 37.5 ms, while the maximum delay caused by the more intense interleaving in case of a fullrate data channel is 106.8 ms. Only RACH and SCH are transmitted without interleaving. Figure G.38 illustrates interleaving for a fullrate speech channel. The 456 channel-coded bits of block n are divided into 8 subblocks with 57 bits each and then rearranged. Subblocks 0 through 3 of block n are then interleaved with subblocks 4 through 7 of block $n - 1$, while subblocks 4 through 7 of block n are interleaved with subblocks 0 through 3 of block $n + 1$. Initially, subblocks 0 through 3 form the upper half of a burst, while subblocks 4 through 7 form the lower half of a burst. During the subsequent formation of the burst, the bits of the upper half alternately join with the bits of the lower half. Stealing flags are inserted in the middle of a burst.

Internal handover A handover in which the BSC supports the handover procedure without support of the MSC. This is particularly the case for intra-BSC handover and intra-BTS handover. See Chapter 12; also see *T8, external handover*.

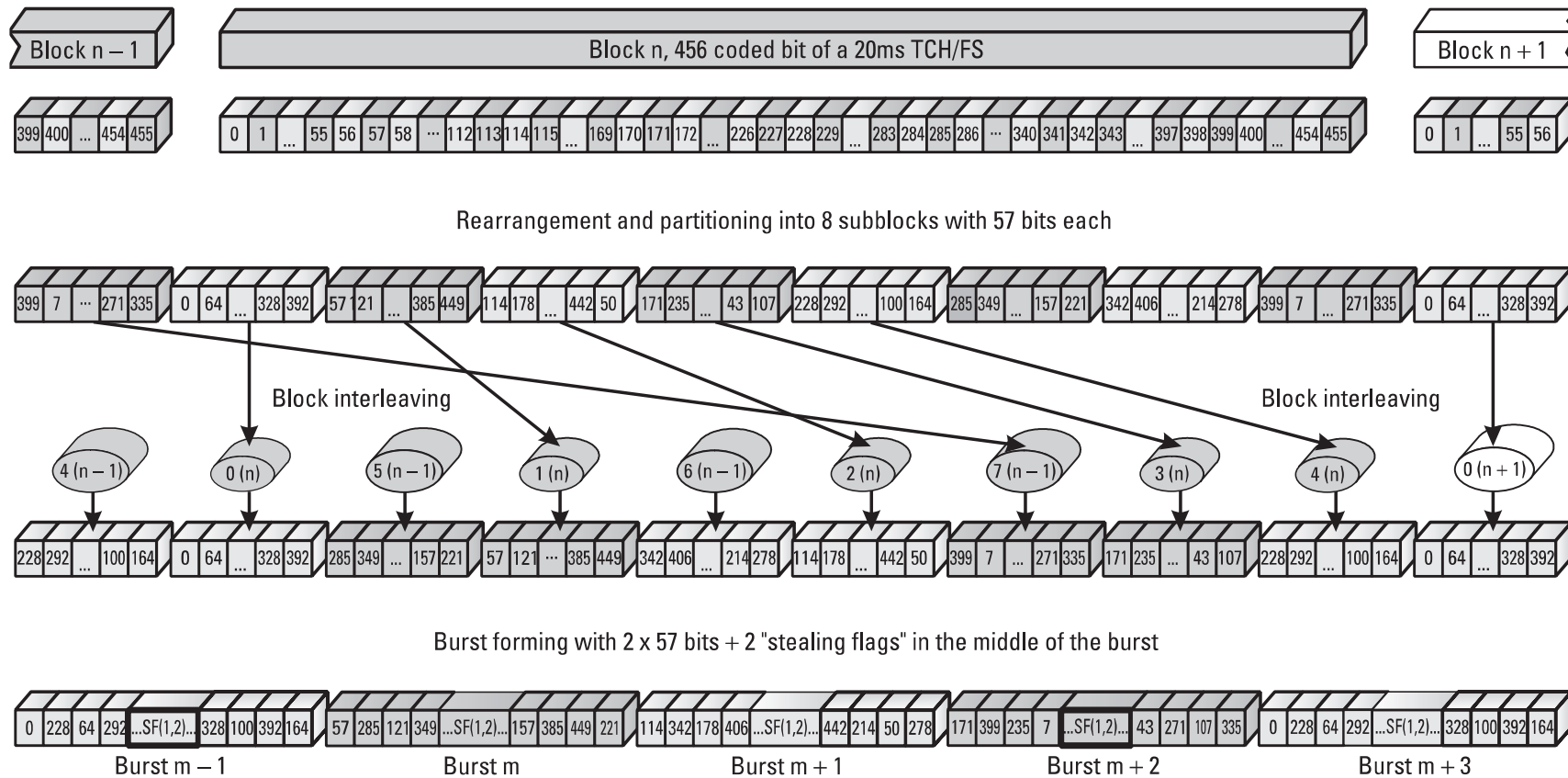


Figure G.38 Interleaving for a fullrate speech channel.

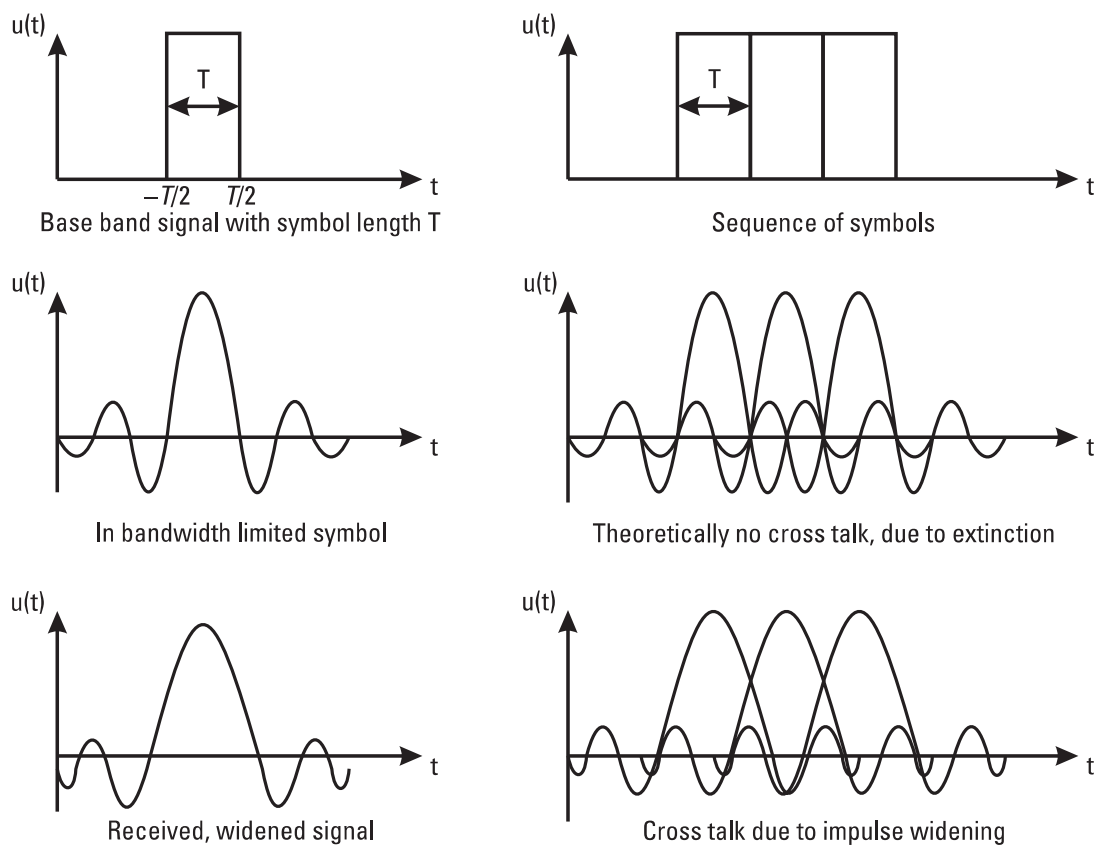


Figure G.39 Intersymbol interference.

Intersymbol interference Intersymbol interference refers to the cross-talk of neighbor cells due to widening of the impulses during transmission and caused by differences in the propagation delay. Figure G.39 illustrates this situation. The left side of the figure, from top to bottom, shows the transformation of a single symbol or impulse. The original signal is presented at the top, the signal after limiting the bandwidth is shown in the middle, and the widened signal after the transmission is shown below. As long as only one symbol is transmitted within the time frame $\pm T$, no negative effect is experienced. The right side, however, shows what can happen if pulses are sent consecutively, one immediately after the other. Without widening, the pulses extinguish each other outside the time frame $\pm T/2$. In case of pulse widening, cross-talk can occur and lead to errors during demodulation.

The reason for intersymbol interference during on-the-Air-interface is that the transmission channel is time variant, that is, it exposes time-dependent characteristics, which the demodulator has to take into account. Another source for intersymbol interference may stem from deviations between the clocks of the sender and the receiver of a signal.

ISDN Integrated Services Digital Network (ISDN).

ISUP [Q.761–Q.766] The ISDN user part. A user of OSI Layers 1 through 3, just like the SCCP. Although no GSM protocol, ISUP is used by the MSC for signaling purposes toward the ISDN.

ITU and ITU-T International Telecommunication Union–Telecommunication Standardization Sector.

IWF [PSTN/ISDN = GSM 09.03, 09.06, 09.07, CSPDN = GSM 09.04, PSPDN = GSM 09.05, 09.06] Interworking function. A subsystem in the PLMN that allows for nonspeech communication between GSM and other networks (see *PSTN*, *ISDN*, *CSPDN*, *PSPDN*). The tasks of an IWF are, in particular, to adapt transmission parameters and protocol conversion. The various IWFs typically are part of the MSC, where only the GMSC has to have IWFs. Physical manifestation of an IWF may be through a modem, which is activated by the MSC, dependent on the bearer service and the destination network. Table G.9 lists which modem types and transmission rates are available for data transmission between PSTN/ISDN and GSM. One can compare these transmission rates with the bearer services of GSM.

K_c [GSM 03.08, 03.20] The parameter K_c is the 8-byte-long cipher key and results from applying the two parameters K_i and RAND to the algorithm A8. Both the BTS and the mobile station use K_c for ciphering.

Table G.9
Valid Modem Types in GSM (According to GSM 09.07)

Network	Modem Type	Transmission Rate
PSTN	V.21	300 baud/synchron
PSTN	V.22	1200 baud/synchron + asynchron
PSTN	V.22bis	2400 baud/synchron
PSTN	V.23	1200/75 baud/asynchron
PSTN	V.26ter	2400 baud/synchron
PSTN	V.32	4800/9600 baud/synchron
ISDN	V.110	300–9600 baud/asynchron

K_i [GSM 03.08, 03.20] The parameter K_i is an individual key that is different for every SIM card. Its value is a number of up to 16 bytes, which is used for authentication (see ciphering). K_i is known only to the SIM card and the AuC/HLR. Since data security and protection from misuse essentially depend on this information being secret, the value of K_i is part of the most secret data of the GSM world. That is the reason why K_i is never transmitted over any interface and is used only within the SIM card and the AuC/HLR (see *A3*, *A5/X*, *A8*, *K_c*).

LAC See *Location area*.

LAI See *Location area*.

LAPB [X.25] Link access protocol B-channel. Described in ITU Recommendation X.25.

LAPD [Q.920, Q.921] Link access protocol D-channel. See Chapter 6.

LI Length indication.

Lm-Channel [GSM 04.03] Lm-Channel is another name for the GSM half-rate channel with a transmission rate of 6.5 Kbps for speech.

LMSI [GSM 03.03] Local mobile subscriber identity. A 4-byte-long parameter that the VLR assigns to a subscriber on a temporary basis. The intention is to expedite queries in the VLR. When the LMSI is assigned, both sides do not only use the IMSI but also the LMSI. Although there is no use for the LMSI in the HLR, except for queries to the VLR, it still must be stored in the HLR. Furthermore, it is required to send the LMSI whenever data between the two databases are exchanged.

Location area [GSM 03.03, 04.08] A location area comprises at least one but typically several BTSs. A location area is defined for the following purpose:

- So a mobile station that changes the serving cell in the same location area does not need to perform a location update;
- So when the network tries to establish a connection to a mobile station, for example, for a mobile terminating call, it is necessary to send only the PAGING message to those BTSs that belong to the current location area of the MS.

Defining a location area, therefore, serves mainly one purpose, to reduce the signaling load. Every BTS broadcasts the location area via the parameter location area identity (LAI) in the messages BCCH/ SYS_INFOS 3 and 4. Even when the MS is involved in an active call, the location area still is communicated to the MS in the SYS_INFO 6 (this is particularly important in a handover). The format of the LAI is shown in Figure G.40. The shaded, one-digit field is a filler (1111_{bin}). It extends the only three-digit MCC to 2 bytes. That is not necessary for the two-digit (1-byte) MNC. The actual location area code (LAC) is four digits long. The LAC is an identifier that can be assigned by the network operator. All values, except 0000_{hex} and FFFE_{hex}, are allowed. Those two values are reserved for cases when the LAI on a SIM has been deleted.

LPD [GSM 04.06] Link protocol discriminator. A 2-bit-long part of the address field of an LAPD_m frame. See Chapter 7.

LSSU [ITU Q.700–Q.704] Link status signal unit. One of three SS7 messages defined in OSI Layer 2 (the others are FISU and MSU). Figure G.41 shows the format of the LSSU. The LSSU is used to indicate error situations when a link is brought into or taken out of service. The figure also shows the possible values of the 3-bit-long status field. The distinction between LSSU, FISU, and MSU is achieved via the length indication (LI) element, which in an LSSU can take only the value 1 or 2. Although the value 2 is explicitly allowed by ITU, only the first byte—or rather the first 3 bits of the status field—are used to carry the actual status information.

LU Location update. See Chapter 12.

MAIO See *HSN*.

Mandatory A term used in standardization to indicate that a specific parameter has to be included in a message. Typically, it also implies the general position that parameter has to be sent, namely, within the mandatory part that typically does not require a specific tag. The opposite term is *optional*.

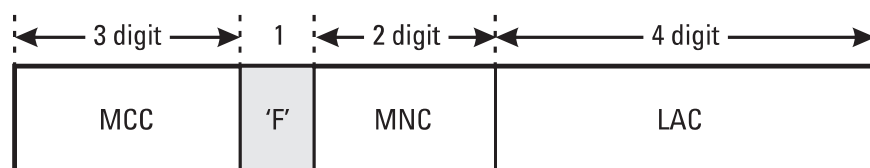


Figure G.40 Format of the LAI.

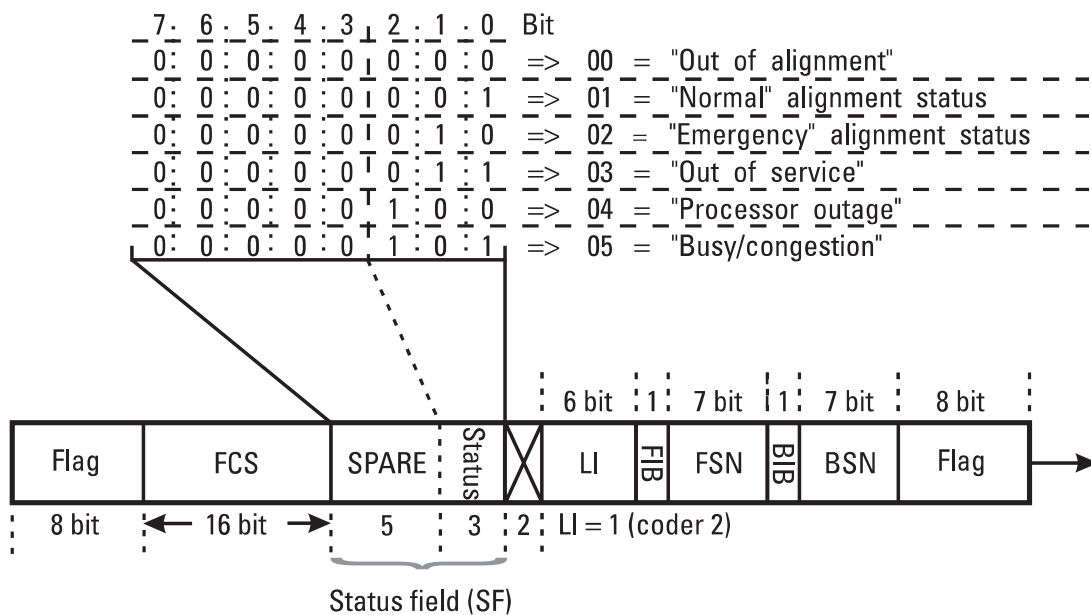


Figure G.41 Format of the LSSU.

MAP [GSM 09.02] Mobile application part. See Chapter 11.

MAX_RETRAN [GSM 05.08] One of the RACH control parameters sent in the BCCH/SYS_INFOS 1-4. MAX_RETRAN indicates how many consecutive times an MS may send the CHAN_REQ message to the BTS. Valid values are 1, 2, 4, and 7.

MCC [E.212] Mobile country code. A three-digit identifier that uniquely identifies a country (not a PLMN). Table G.10 is an extensive list of MCCs (see also *MNC*, *IMSI*).

MEAS_RES and MEAS_REP [GSM 04.08, 05.08, 08.58] BTS and MS measure the signal strength and quality of the received signal during an active connection. The MS periodically sends the measurements in a MEAS_REP message to the BTS (in a SDCCH/SACCH every 470.8 ms; on a TCH/SACCH every 480 ms). The BTS adds the measurements received from the MS to its own measurements and sends the result in a MEAS_RES message to the BSC. These measurements serve as input data for the BSC to perform the power control function and handover decision. Chapter 12 gives an example that shows how to decode a MEAS_RES message.

The measurements during an active connection should not be confused with the idle-channel measurements, which the TRX performs while time

slots are not used. These results are periodically reported to the BSC in an RF_RES_IND message.

MM [GSM 04.08] Mobility management. A user protocol between the mobile station and the network switching subsystem (NSS), for which the base station subsystem (BSS) is transparent. The messages defined in MM allow for roaming and security functions (see *authentication*) in GSM.

MNC [GSM 03.03] Mobile network code. A two-digit identifier used (like the 3-bit-long NCC) to uniquely identify a PLMN (see also *MCC*, *IMSI*, *NCC*).

Table G.10
Mobile Country Codes

Country	MCC	Country	MCC
Afghanistan	412	Albania	276
Algeria	603	American Samoa	544
Angola	631	Antigua and Barbuda	344
Argentina	722	Australia	505
Austria	232	Azerbaijan	400
Bahamas	364	Bahrain	426
Bangladesh	470	Barbados	342
Belgium	206	Belize	702
Benin	616	Bermuda	350
Bolivia	736	Botswana	652
Brazil	724	British Virgin Islands	348
Brunei	528	Bulgaria	284
Burkina Faso	613	Burma	414
Burundi	642	Cambodia	456
Cameroon	624	Canada	302
Cape Verde	625	Cayman Islands	346
Central African Republic	623	Chad	622
Chile	730	China	460
Colombia	732	Comores	654

Table G.10 (continued)

Country	MCC	Country	MCC
Congo	629	Cook Islands	548
Costa Rica	712	Croatia	219
Cuba	368	Cyprus	280
Czech Republic	230	Denmark	238
Germany	262	Djibouti	638
Dominica (Commonwealth of the)	366	Dominican Republic	370
Ecuador	740	Egypt	602
El Salvador	706	Equatorial Guinea	627
Estonia	248	Ethiopia	636
Faroe Islands	288	Fiji-Islands	542
Finland	244	France	208
French Antilles	340	French Polynesia	547
Gabun	628	Gambia	607
Georgia	282	Ghana	620
Gibraltar	266	Greece	202
Greenland	290	Grenada	352
Guam	535	Guatemala	704
Guernsey (England)	234	Guiana (French)	742
Guinea	611	Guinea-Bissau	632
Guyana	738	Haiti	372
Honduras	708	Hong Kong	454
Hungary	216	Iceland	274
India	404	Indonesia	510
Iran	432	Iraq	418
Ireland	272	Isle of Man (England)	234
Israel	425	Italy	222
Ivory Coast	612	Jamaica	338
Japan	440 + 441	Jersey (England)	234
Jordan	416	Kenya	639
Kiribati	545	Korea (North)	467
Korea (South)	450	Kuwait	419
La Reunion	647	Laos	457
Latvia	247	Lebanon	415

Table G.10 (continued)

Country	MCC	Country	MCC
Lesotho	651	Liberia	618
Libya	606	Lithuania	246
Luxembourg	270	Macao	455
Madagascar	646	Malawi	650
Malaysia	502	Maldives	472
Mali	610	Malta	278
Mauritania	609	Mauritius	617
Mexico	334	Monaco	212
Mongolian Republic	428	Montserrat	354
Morocco	604	Mozambique	643
Namibia	649	Nauru	536
Nepal	429	Netherlands	204
Netherlands Antilles	362	New Caledonia	546
New Zealand	530	Nicaragua	710
Niger	614	Nigeria	621
Norway	242	Oman	422
Pakistan	410	Panama	714
Papua New Guinea	537	Paraguay	744
Peru	716	Philippines	515
Poland	260	Portugal	268
Puerto Rico	330	Qatar	427
Reunion	647	Romania	226
Russia	250	Rwandese Republic	635
San Marino	292	Sao Tome and Principe	626
Saudi Arabia	420	Senegal	608
Seychelles	633	Sierra Leone	619
Singapore	525	Slovakia	231
Slovenia	293	Solomon Islands	540
Somalia	637	South Africa	655
Spain	214	Sri Lanka	413
St. Kitts and Nevis	356	St. Lucia	358
St. Pierre and Miquelon	308	St. Vincent and the Grenadines	360
Sudan	634	Suriname	746

Table G.10 (continued)

Country	MCC	Country	MCC
Swaziland	653	Sweden	240
Switzerland	228	Syria	417
Taiwan	466	Tanzania	640
Thailand	520	Togo	615
Tonga	539	Trinidad and Tobago	374
Tunisia	605	Turkey	286
Turks and Caicos Islands	376	UAE	424
UAE/Abu Dhabi	430	UAE/Dubai	431
Uganda	641	Ukraine	255
United Kingdom	234 + 235	Uruguay	748
USA	310 – 316	Uzbekistan	250 + 434
Vanuatu	541	Venezuela	734
Vietnam	452	Virgin Islands	332
Wallis and Futuna Islands	543	Western Samoa	549
Yemen/Arab. Republic	421	Yemen/People's Republic	423
Yugoslavia	220	Zaire	630
Zambia	645	Zimbabwe	648

MOC Mobile originating call. See Chapter 12.

mod Mathematical operator that uses only the remnant of a division without fraction. The result λ of a $(\nu \bmod \tau)$ operation is always an integer value of the division ν over τ . The equation reads:

$$\lambda = \nu \bmod \tau = \nu - \tau \cdot (\nu \operatorname{div} \tau)$$

where $\lambda, \nu \in N_0, \tau \in N$. Examples are $3 \bmod 6 = 3$; $10 \bmod 3 = 1$; $10 \bmod 2 = 0$ (see also *div*).

MoU Memorandum of Understanding. Worldwide forum for GSM network operators.

MPTY A supplementary service (see *SS*).

MS Mobile station. See Chapter 2.

MSC Mobile switching center. See Chapter 4.

MSC number [GSM 03.03] The format of the MSC number corresponds to that of an ordinary directory number (see *MSISDN*). Every MSC has its own routable number that allows the SCCP (see *global title*) to address messages to the MSC.

MSISDN [GSM 03.02, 03.12] Mobile subscriber ISDN. The directory number of a mobile subscriber. Note that it is possible for one subscriber to have several MSISDNs in parallel on one SIM. The different MSISDNs are used to address different services, for example, one number for voice, another number for fax. The format of the MSISDN is shown in Figure G.42.

Example: 49 171 5205787 is the directory number of a subscriber to the D1 network in Germany. The country code (CC) identifies a country or region (e.g., 49 for Germany, 1 for the United States); the national destination code (NDC) identifies the PLMN (e.g., 171 for the operator D1); and the subscriber number (SN) is a unique identifier within the PLMN.

MSK Minimum shift keying. A modulation technique (see *GMSK*).

MSRN [GSM 03.03] Mobile station roaming number. A temporary identifier, used for mobile terminating calls, to route a call from the gateway MSC to the serving MSC/VLR. The serving MSC/VLR is the MSC/VLR in which area the subscriber currently roams. The VLR assigns the MSRN when a request for routing information is received from the HLR. The MSRN is released after the call has been set up. Figure G.43 shows the format of an MSRN. The MSRN is used solely to route an incoming call and contains no information to identify the caller or the called party. See Chapter 12.

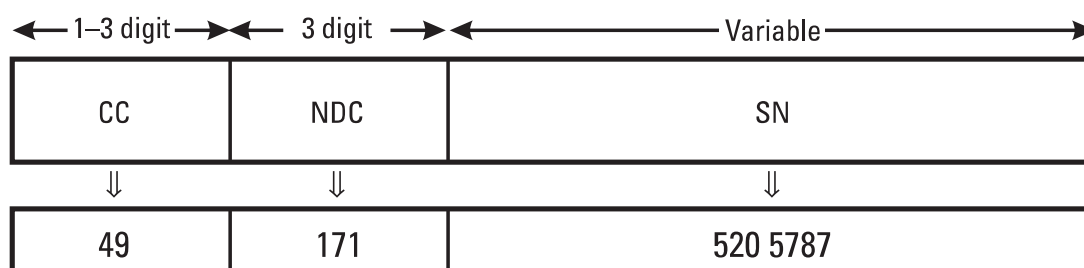


Figure G.42 Format of the MSISDN.

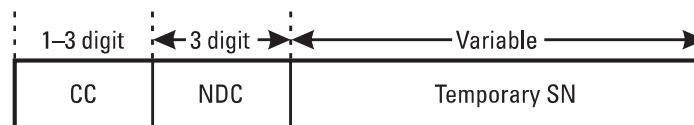


Figure G.43 Format of an MSRN.

The MSRN contains the following codes: the country code (CC) is the prefix of a country or region (e.g., 44 is the United Kingdom); the national destination code (NDC) identifies the PLMN (e.g., 172 is the D2 operator of Germany); and the temporary subscriber number (temp. SN) is assigned by the serving MSC/VLR of the called subscriber.

MS_TXPWR_MAX [GSM 05.08] Parameter that describes the maximum output power that an MS may use on a traffic channel of the serving cell.

MS_TXPWR_MAX_CCH [GSM 04.08, 05.05, 05.08] Parameter that describes the maximum output power that an MS may use on a random access channel (RACH). This parameter is sent to the MS in the BCCH/SYS_INFOS 3 and 4.

MSU [ITU Q.700–Q.704] Message signal unit. One of three SS7 messages defined in OSI Layer 2 (the others are FISU and LSSU). Figure G.44 shows the format of the MSU. The MSU is used for any kind of data transfer. The distinction between the various SS7 user parts (ISUP, SCCP, etc.) is made via the service information octet (SIO). The signaling data is carried in the signaling information field (SIF). The distinction between LSSU, FISU, and MSU is achieved via the length indication (LI) element, which in case of an MSU is always greater than 2. See Chapter 8.

MTC Mobile terminating call. See Chapter 12.

MTP [ITU Q.700–Q.704] Message transfer part. Part of SS7 that covers OSI Layers 1 through 3. Three messages are defined for the MTP: FISU, LSSU, and MSU. See Chapter 8.

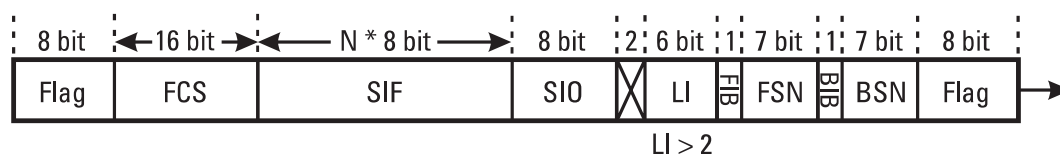


Figure G.44 Format of an MSU.

Multidrop A serial or ring configuration of BTSs on the Abis-interface. See Chapter 6.

Multiframe [GSM 05.01, 05.02] Two types of multiframe have to be distinguished in the frame hierarchy of GSM: the 26-multiframe, with a length of 120 ms, and the 51-multiframe, with a length of 235.8 ms. As the name suggests, the 26-multiframe is composed of 26 TDMA frames, while the 51-multiframe comprises 51 TDMA frames. Every TDMA frame comprises eight single bursts. In traffic channels, the 26-multiframe provides the absolute frame number (see *FN*), while the 51-multiframe provides the respective information in signaling channels.

Multiparty A supplementary service (see *SS*).

N200 [GSM 04.06 for LAPD_m, Q.921 for LAPD] A counter for the maximum number of retransmissions on the Abis- or Air-interface. It defines how often one message can be retransmitted before the Layer 2 connection is torn down. For the Abis-interface, this value is 3 ($N200 = 3$). For the Air-interface, N200 can take on different values, depending on the channel type. For the Air-interface, it is necessary to distinguish between N200, which is the parameter for Layer 2, and RADIO_LINK_TIMEOUT, which is the respective tear down criterion of Layer 1. Table G.11 lists the values of N200 on the Air-interface.

N201 [GSM 04.06 for LAPD_m, Q.921 for LAPD] A counter for the maximum number of octets in the information field of the LAPD/LAPD_m frames on the Abis- or Air-interface. The value of N201 on the Abis-interface is 260 ($N201 = 260$). The value for the Air-interface depends on the channel type. It has to be noted that the overall maximum length of a frame for signaling data is restricted, due to physical limitations (see *channel coding, GMSK*), to 23 octets or 184 bits. See Chapter 7. Table G.12 lists the values of N201 on the Air-interface.

N(R) and N(S) [Q.920, Q.921] Counters for forward error correction that indicate that a frame was received, N(R), or sent, N(S), respectively. Both counters are used by the LAPD and LAPD_m protocol to acknowledge I-Frames (only) on the Air-interface and the Abis-interface. See Chapter 6.

NCC [E.164, GSM 03.03] Network color code. The 3-bit-long code that identifies the PLMN. This parameter is part of the BSIC and is broadcast in the synchronization channel (see *SCH, burst*).

Table G.11

Values of N200 on the Air-interface

Channel Type	N200
SACCH	5
SDCCH	23
FACCH (fullrate)	34
FACCH (halfrate)	29

Table G.12

Values of N201 on the Air-interface

Channel Type	N201
SACCH	18
SDCCH, FACCH	20
BCCH, PCH, AGCH	23

NDC [E.164, GSM 03.03] National destination code. Part of an ISDN number as defined by ITU-T in Recommendation E.164. Typically, the NDC addresses an area. It may, however, also be used to address a service, just as the NDC 800 addresses free phone service in the United States. In Germany, the NDCs 171 and 172 are used to address the two GSM 900 operators.

Neighbor cell All BTSs that are considered to be potential handover candidates for a given BTS. Each BTS (see *serving cell*) needs to inform all active and inactive mobile stations in its area about the BCCH frequencies of its neighbor cells. That is taken care of by the neighbor cell information within the BCCH/SYS_INFO 2 (for inactive mobiles) or BCCH/SYS_INFO 5 (for active mobiles).

Note that a handover can be performed into only those cells listed in the neighbor cell description of a BTS. If suitable or necessary neighbor cells are not listed, handover into such a cell is not possible, and the call drop rate (for drops during outgoing handover) will increase.

Nonsynchronized handover See *Synchronized handover*.

NSS Network switching subsystem. Generic term for the network elements in a PLMN that are not radio related. Hence, parts of the NSS are the mobile switching center (MSC), the home location register (HLR), the visitor location register (VLR), and the equipment identity register (EIR). See Chapter 4.

Ny1 [GSM 04.08] The maximum number of repetitions of a PHYS_INFO message during an asynchronous handover (see *T8, T3105*).

OACSU [GSM 04.08] Off-air call setup. Used to save radio resources by the late assignment of a traffic channel. In fact, no traffic channel is assigned before the called party takes the call. Without OACSU, the ASS_CMD message for the TCH assignment follows directly after CALL_PROC (for MOC) or after CALL_CONF (for MTC) (Figure G.45). Note that at this time no traffic channel is needed, because ringing or the creation of a ringback tone can be achieved without traffic channel.

With OACSU, the TCH gets assigned only when the called party actually takes the call and starts talking. Consequently, the scarce traffic channel resources experience, on average, a lower busy duration. This is particularly effective for short or unsuccessful calls. The drawback is that the user-to-user connection is not instantly available when the call is answered. Hence, no conversation is possible for a short period of time. GSM maintains that that time period is less than 1 second in 95% of all cases.

Octet 1 octet = 1 byte = 8 bit.

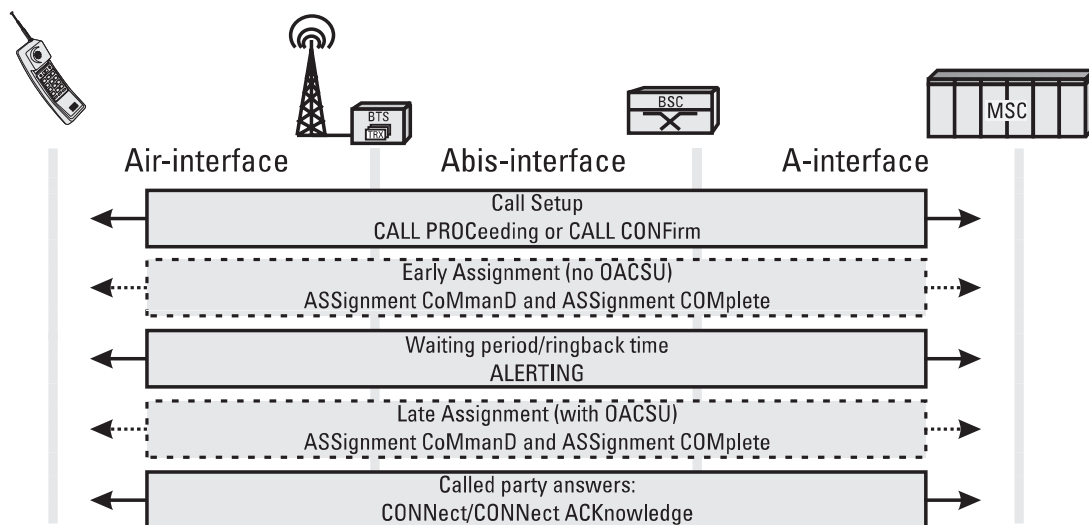


Figure G.45 Channel assignment with and without OACSU.

OML [GSM 08.59] Operation and maintenance link. See Chapter 6.

OPC [Q.700–Q.704] Originating point code. Code that identifies the sender of an MSU. The ITU SS7 standard defines the OPC as a 14-bit code, while the ANSI SS7 standard defines it as a 16-bit code. The OPC is carried in the routing label, together with the DPC and the SLS. See Chapter 8.

OSI Reference Model Open System Interconnection Reference Model. Defined by ITU in Recommendation X.200 as a means to facilitate communication between different systems. It contains general agreements on the communication among network elements. The basic underlying idea is to separate a communication process into seven largely independent layers. See Chapter 5.

OSS Operation subsystem. Other name for the operation and maintenance center (OMC).

Outband signaling See *inband signaling*.

Outgoing call A call initiated by a mobile station, also referred to as a mobile originating call (MOC).

Outgoing handover See *incoming handover, synchronized handover*, Chapter 12.

PABX Private automatic branch exchange.

PAD [GSM 09.05] Packet assembler/disassembler (Figure G.46). Required when a connection is routed from the PLMN to a PSPDN, either directly or via the PSTN.

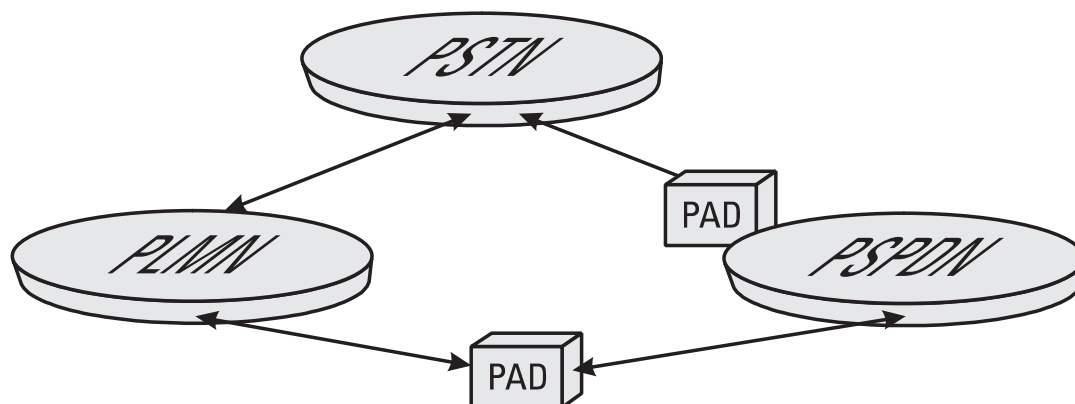


Figure G.46 Definition of the packet assembler/disassembler.

Paging group [GSM 05.02] Mobile subscribers are categorized into paging groups, to allow for discontinuous reception (see *DRX*), which extends the working time of a mobile's battery. Being assigned to a particular paging group, a mobile station needs to listen for an incoming call only every BS_PA_MFRMS 51 multiframe within a defined paging channel block (see Chapter 7). The IMSI and BS_CC_CHANS are necessary for the mobile station to calculate its paging group. BS_CC_CHANS indicates how many time slots of the BCCH frequency are reserved for common control channels (see *CCCH*).

The paging group itself (corresponding to the number of the paging channel block) is calculated as follows:

$$\text{Paging group } (0 \dots n-1) = [\text{IMSI mod } 1000) \text{ mod } (\text{BS_CC_CHANS} \times n)] \text{ mod } n$$

where n = number paging channel blocks.

PCH [GSM 05.01, 05.02] Paging channel. The transmission rate per PCH block is 782 bps. See Chapter 7.

PCM Pulse code modulation.

PCS 1900 Personal Communication System 1900 (PCS 1900). PCS 1900 is not a standardized system but refers to a collection of mobile systems that operate in the 1900 MHz band in the United States. One of these systems is a derivative of GSM or DCS 1800. Other standards are CDMA/IS-95 and TDMA/IS-136.

PD [GSM 04.08] Protocol discriminator. See Chapter 7.

PDU [X.200–X.209] Protocol data unit. A term from the OSI Reference Model that refers to a data area in a message. The data area comprises application data and control information or coding information for the application data. PDU is used in the transaction capabilities application part (TCAP) as a generic term to address the dialog part and the component part or the content of these parts, respectively. For TCAP, the application protocol data unit (ADPU) is also used to address these areas. See *TCAP* and *MAP*.

PHS Personal Handy Phone System. An inexpensive Japanese standard for wireless communications in urban areas.

PIN [GSM 02.17] Personal identification number. A four- to eight-digit number that provides limited protection against unauthorized use. The PIN can be changed by the user and is stored on the SIM. The PIN is optional and can be disabled. When enabled, the PIN needs to be entered at powerup. When the wrong PIN is entered three consecutive times, the SIM goes into a blocked mode, and only the PIN unblocking key (PUK) can release the SIM. See Chapter 2.

PLMN Public land mobile network. A PLMN is the GSM, DCS, or PCS network of an operator within a country. The network color code (NCC) identifies a PLMN within a country.

PMR Private mobile radio. An inexpensive variant to provide mobile service. Several standards for PMR exist. Generally, PMR provides limited functionality and limited privacy. PMR uses simplex transmission, that is, only one party of a call can be on the air at a time.

Power class [GSM 05.05] In GSM, BTSs and mobile stations are classified and available in different power classes. The mobile station indicates its power class during every connection setup to the network. Most mobile stations belong to classes 4 and 5 (handheld). Mobile stations with higher output power typically are meant to be installed in cars or used for stationary applications.

Table G.13 lists the power classes for mobile stations and BTSs of GSM, DCS 1800, and PCS 1900.

Power control [GSM 05.05, 05.08] GSM requires that every mobile station is subject to power control. For the BTS, on the other hand, power control is optional. Depending on the quality of a connection, the BSC will request the BTS and the mobile station to adjust their output power. The purpose of power control is to minimize interference with other channels and to increase the working time of the battery.

The BSC informs the BTS via the Abis-interface within a BS_POWER_CON message of the output power to be used (Figure G.47). Only if necessary, the BSC will send an MS_POWER_CON message to the BTS to initiate an adjustment of the output power of the mobile station. This new output power level is forwarded to the mobile station within the Layer 1 header of the next SACCH to be sent. Note that one SACCH is sent to the mobile station every 480 ms, always telling the mobile station the current output power.

The maximum power is called P_n . Starting from there, the output power may be reduced in steps of 2 dB. Power control on the BTS side allows

Table G.13
Power Classes in GSM, DCS 1800 and PCS 1900

	GSM		DCS1800		PCS1900	
Class	MS (W/dBm)	BTS (W/dBm)	MS (W/dBm)	BTS (W/dBm)	MS (W/dBm)	BTS (W/dBm)
1	-/-	320/55	1/30	20/43	1/30	20/43
2	8/39	160/52	0,25/24	10/40	0,25/24	10/40
3	5/37	80/49	4/36	5/37	2/33	5/37
4	2/33	40/46	-/-	2,5/34	-/-	2,5/34
5	0,8/29	20/43	-/-	-/-	-/-	-/-
6	-/-	10/40	-/-	-/-	-/-	-/-
7	-/-	5/37	-/-	-/-	-/-	-/-
8	-/-	2,5/34	-/-	-/-	-/-	-/-
Micro (M1)	-/-	0,25/24	-/-	1,6/32	-/-	0,5/27
Micro (M2)	-/-	0,08/19	-/-	0,5/27	-/-	0,16/22
Micro (M3)	-/-	0,03/14	-/-	0,16/22	-/-	0,05/17

```

MS POWER CONTROL
Channel Number: Bm + ACCH, TN = 2

MS Power: 05h = +33 dBm

BS POWER CONTROL
Channel Number: Bm + ACCH, TN = 3

BS Power: 03h = Pn - 6 dB

```

Figure G.47 MS_POWER_CON and BS_POWER_CON messages from an Abis trace file.

reduction of the output power by 30 dB in 15 steps, while the output power of the MS can be reduced between 20 dB and 30 dB, depending on the standard (GSM, DCS1800) and the power class of the MS. Figure G.47 is an example of the two messages that are used for power control. While the MS_POWER_CON message always uses an absolute value, the BS_POWER_CON message always uses a relative value ($P_n - X$).

Note that all downlink channels of the BCCH-TRX have to permanently use the maximum output power P_n , since the BCCH is serving as a beacon and

reference for the neighbor cell measurements of the mobile stations. Figure G.48 shows an example of a TRX where a variety of output power levels are used on the different channels. The channels TS 1 and TS 6 of this example are not in use.

Table G.14 provides the coding and the related output power for mobile stations in GSM and DCS1800/PCS1900. There is also a minimum output power below which a mobile station may not transmit. That value is 5 dB_m for GSM and 0 dB_m for DCS 1800/PCS 1900.

Presynchronized handover See *synchronized handover*.

Preprocessing [GSM 08.58] An optional functionality whereby the BTS evaluates its own measurement results and those from the mobile station. In this case, the BTS forwards a so-called PREPRO_MEAS_RES to the BSC only once in a while rather than sending MEAS_RES messages every 480 ms. Obviously, preprocessing should relieve the BSC from this task.

Primitive All parameters of TCAP that are “atomic,” that is, that cannot be further partitioned, are called primitives. See Chapter 11. Furthermore X.200 (definition of the OSI Reference Model) defines primitives as messages that are exchanged between vertical layers of the OSI Reference Model (Layer N and Layer $(N+1)$). See Chapter 5.

Pseudo-synchronized handover See *synchronized handover*.

PSTN Public switched telephone network.

PUK [GSM 02.17] PIN unblocking key. A 10-digit code stored on the SIM, which in contrast to the PIN, cannot be altered by the user. The PUK unblocks a SIM that was blocked because someone entered a wrong PIN three consecutive times.

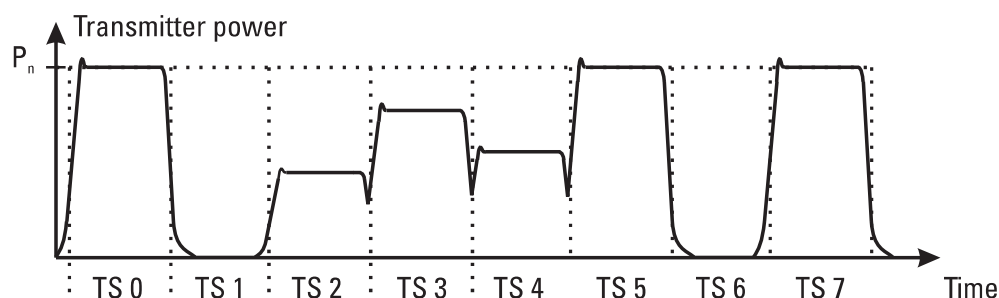


Figure G.48 Power control in the graph “Power over time.”

Table G.14

Hex-Codes for the Output Power of an MS, as used in the MS_POWER_CON Message

Code	GSM	DCS 1800/PCS 1900
0	39	30
1	39	28
2	39	26
3	37	24
4	35	22
5	33	20
6	31	18
7	29	16
8	27	14
9	25	12
0A	23	10
0B	21	8
0C	19	6
0D	17	4
0E	15	2
0F	13	0
10	11	0
11	9	0
12	7	0
13	5	0
14	5	0
15	5	0
16	5	0
17	5	0
18	5	0
19	5	0
1A	5	0
1B	5	0
1C	5	0
1D	5	36
1E	5	34
1F	5	32

RACH [GSM 05.01, 05.02] Random access channel (RACH) is an uplink common control channel (CCCH) that the MS uses to send a connection request to the BTS. The access burst (see *burst*) is always used for the transmission of the RACH. The only two messages that are sent on the RACH are CHAN_REQ and HND_ACC, with a net data length of 8 bits and a transmission rate of 34 bps.

Radio_Link_Timeout See *Radio link failure*.

Radio link failure [GSM 04.08, 05.08] Summary of the various conditions under which the connection over the Air-interface has to be regarded as terminated. Two possibilities need to be distinguished:

- **Radio Link Failure, Layer 1.** The most frequent reason for the declaration of a radio link failure on Layer 1 is simply the incapacity to decode the SACCH [RADIO_LINK_TIMEOUT] times. This definition applies to both uplink and downlink. For SACCHs that cannot be read, the channel decoder sets the BFI flag to 1. The parameter RADIO_LINK_TIMEOUT can be set per BTS and is broadcast in the BCCH / SYS_INFO 3. When a radio link failure on Layer 1 is detected on a dedicated channel (see *TCH* and *SDCCH*), the BTS sends a CONN_FAIL message with cause 1 = radio link failure to the BSC. The BSC consequently sends a CLR_REQ message cause 1 = radio interface failure to the MSC to indicate the connection loss and to release the resources. Figure G.49 shows this relation.
- **Radio (data) link failure, Layer 2.** The criteria for radio link failure on Layer 2 are similar to those for Layer 1. When an MS or a BTS sends a Layer 2 frame (I-frame, SABME-frame, etc.) as often as indicated in N200 without receiving a response, Layer 3 receives an error indication that requests release of that channel (Figure G.50). An ERR_IND message cause 1 = timer T200 expired (N200 + 1) times is sent to the BSC to release the channel. The BSC then performs the channel release procedure. This results frequently in a radio link failure on Layer 1, due to the fact that the radio link is so bad that the SACCH cannot be decoded anymore.

RAND [GSM 03.08, 03.20] Random number. As the name suggests, a number that the AuC picks on a random basis. The RAND range is up to $2^{128} - 1$ and has a length of 16 bytes. The network sends RAND in an AUTH_REQ message to the MS for authentication and ciphering.

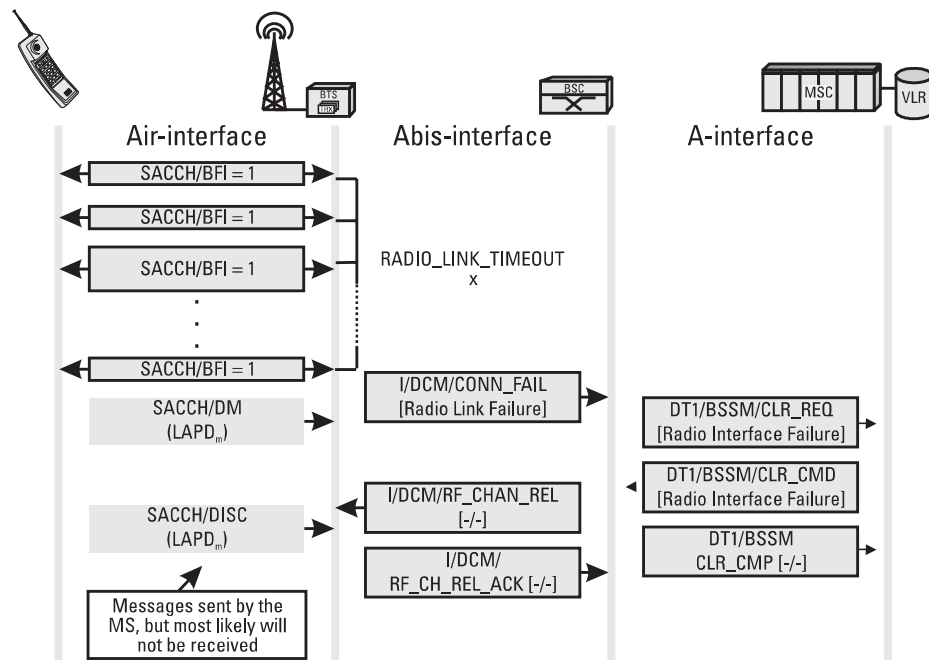


Figure G.49 A radio link failure, Layer 1.

RPE-LTP [GSM 06.10] Regular pulse excitation-long-term prediction. Procedure used by GSM to compress speech data from 64 Kbps to 13 Kbps in a fullrate channel and to 6.5 bps for a halfrate channel. This function is applied on both sides, the MS and the TRAU.

Roaming In the context of mobile communications, the ability of a subscriber to move around and change the location with or without an active connection. Wide-area roaming, perhaps internationally, distinguishes a mobile communications network like GSM from all wireless services.

Routing label [Q.700–Q.704] A 32-bit-long sequence within an MSU, consisting of the destination point code (DPC), originating point code (OPC), and signaling link selection (SLS) (Figure G.51). The routing label is used for message routing and is part of the signaling information field (SIF). See Chapter 8.

RSL Radio signaling link. Signaling channel on the Abis-interface between TRX and BSC. The signaling channel between BTS and BSC to convey information related to O&M is correspondingly referred to as OML.

RSZI [GSM 03.03] Regional subscription zone identity. Code that restricts the service area for a particular subscriber by restricting the roaming capability within a PLMN. The RSZI consists of a country code (CC), the network

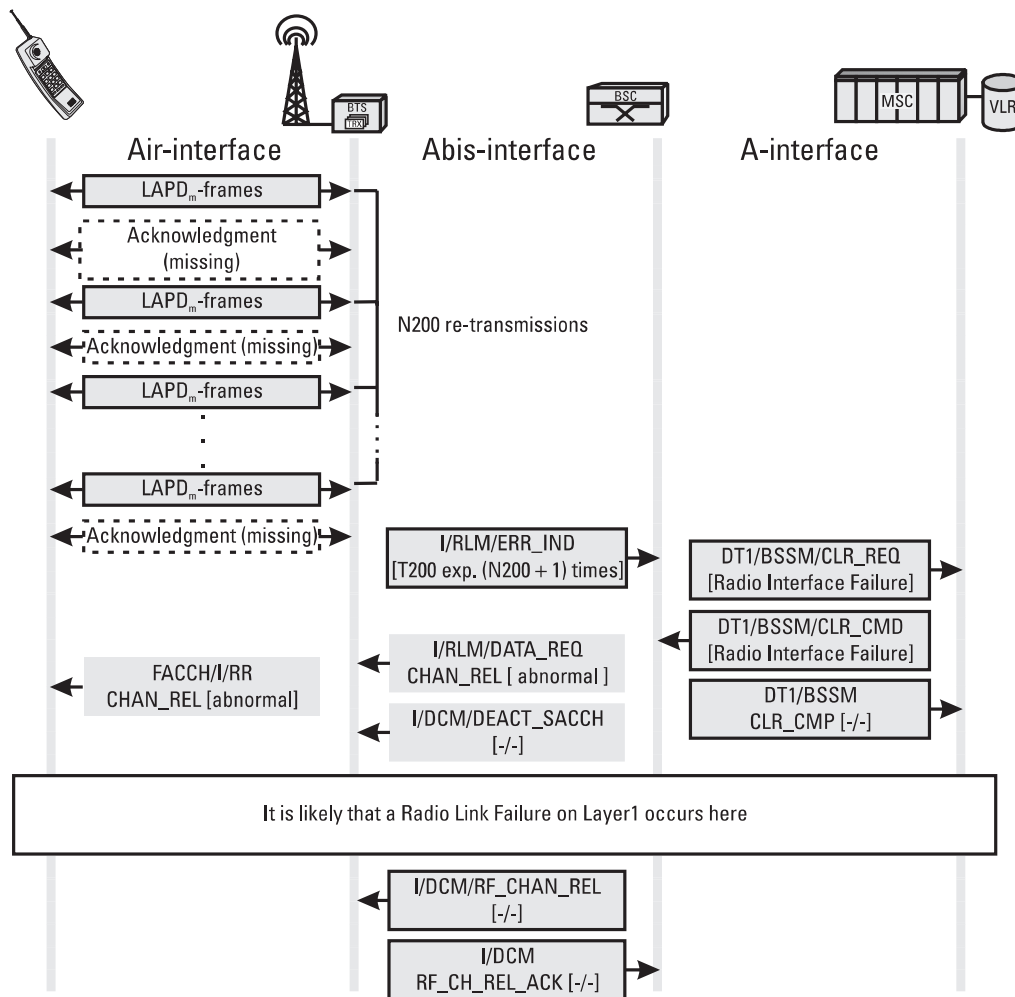


Figure G.50 Message flow when a radio link failure on Layer 2 occurs.

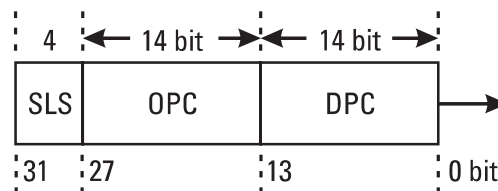


Figure G.51 Format of the routing label.

destination code (NDC), and a zone code (ZC). RSZIs can be assigned to a subscriber on a per-PLMN basis to indicate the allowed service areas of a PLMN for that subscriber. Figure G.52 is an example of an RSZI for a subscriber to the D2 network in Germany.

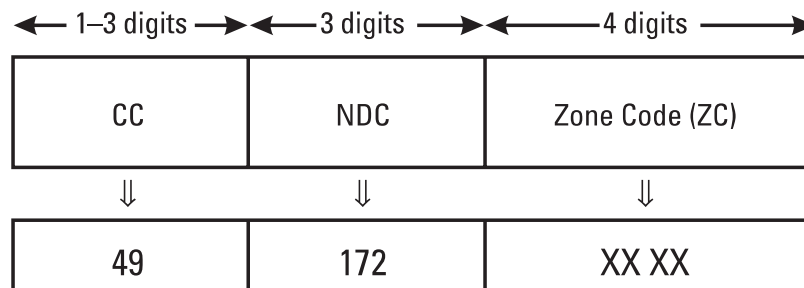


Figure G.52 Format of the RSZL (CC = 49, for Germany; 172 = D2 network).

RXLEV [GSM 05.08] RXLEV provides the results of the measurement of the receiving level on the Air-interface. These measurements are performed independently by the MS and the BTS. The BTS measures the receiving level for an active connection. The MS measures the receiving level of that BTS, where an active connection exists (serving cell) plus the receiving level of the neighbor cells indicated in the SYS_INFO 2. The values of both RXLEV and RXQUAL are sent to the BSC in a MEAS_RES/MEAS_REP, as basis for a decision by the BSC on power control or handover. It has to be distinguished between values with active DTX (SUBSET) and values without DTX (FULL or ALL). (See Chapter 12.) RXLEV values are coded the same way for uplink and downlink. A 5-bit-long, binary coded RXLEV value can directly be converted into a receiver-level dB_m. The procedure outlined in Table G.15 is applicable.

RX_LEV_ACC_MIN [GSM 05.08] Indication of the minimum receiving level that an MS has to receive from a BTS for that BTS to be a candidate as serving cell. Typical values are around –100 dB_m. Every BTS broadcasts this parameter in the BCCH / SYS_INFOS 3 and 4.

Table G.15
Conversion of RXLEV

RXLEV	Receiving Level (dB _m)
0	< –110
1–62	–(111 – RXLEV) through –(110 – RXLEV) (level range)
63	> –48

RXQUAL [GSM 05.08] RXQUAL values, like the ones for RXLEV, are relevant for the decision of a BSC on power control and handover. They indicate the bit error rate that was measured on the Air-interface. The bit error rate can be determined by facilitating the training sequence (see *TSC*). The current values of RXQUAL for an active connection can be tracked in the MEAS_RES/MEAS_REP messages by using a protocol analyzer on the Abis-interface. Values with active DTX (SUBSET) have to be distinguished from values without DTX (FULL or ALL).

RXLEV values are coded the same way for uplink and downlink and are 3 bits long, which allows for a range of 0 through 7. Coding of RX_QUAL is shown in Table G.16.

SACCH [GSM 04.04, 05.01, 05.02] Slow associated control channel (see also *FACCH*). The inband control channel assigned to the TCH or the SDCCH. Every 26th burst of a TCH or every 51st burst of an SDCCH is an SACCH. The consequence is that exactly one SACCH is sent per multiframe. Figure G.53 illustrates the format of the SACCH for uplink and downlink. The transmission rate is 391 bps when the SACCH is assigned to the SDCCH. When assigned to the TCH, the transmission rate is 383 bps.

SAPI [Q.920, Q.921, X.200] Service access point identifier. See Chapter 6.

SCH [GSM 04.08, 05.01, 05.02] Every BTS broadcasts the synchronization channel (SCH) in time slot zero of the BCCH-TRX. The SCH contains the absolute value of the frame number (see *FN*) of a BTS, which is time

Table G.16
Conversion of RXQUAL in Bit Error Rates

RXQUAL	Bit Error Rate	Assumed BER
0	BER < 0,2 %	0,14 %
1	0,2 % < BER < 0,4 %	0,28 %
2	0,4 % < BER < 0,8 %	0,57 %
3	0,8 % < BER < 1,6 %	1,13 %
4	1,6 % < BER < 3,2 %	2,26 %
5	3,2 % < BER < 6,4 %	4,53 %
6	6,4 % < BER < 12,8 %	9,05 %
7	BER > 12,8 %	18,1 %

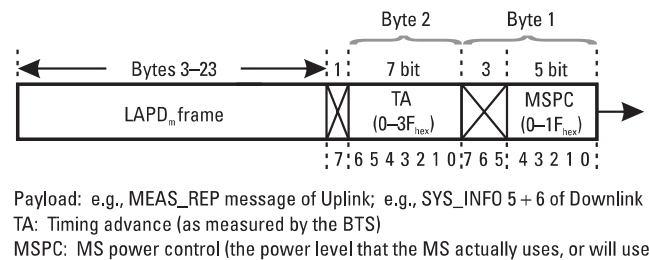


Figure G.53 Format of the SACCH.

dependent, and the base station identity code (see *BSIC*) for an initial rough identification of the cell. The SCH has a length of 25 bits and is sent in the synchronization burst.

SCCP [Q.711–Q.714] Signaling connection control part. Defined in OSI Layers 3 and 4. The SCCP is a user of the SS7-MTP 3 and is used by GSM on almost all NSS interfaces, including the A-interface. See Chapter 9.

SDCCH/4 and SDCCH/8 [GSM 05.01, 05.02] Standalone dedicated control channel. Used for uplink and downlink of the Air-interface to transmit signaling data for connection setup and location update (LU). The transmission rate is 779 bps. The distinction between SDCCH/8 and SDCCH/4 refers to the channel configuration on the Air-interface. An SDCCH/8 channel configuration can never be realized on TS 0 of the BCCH-TRX. The available bandwidth is, because of the BCCH that occupies part of the bandwidth there, not sufficient to allow for that. TS 0 of the BCCH-TRX can be used for, at maximum, one SDCCH/4 channel configuration with four SDCCH sub-channels. See Chapter 7.

Serving cell The BTS where the MS is actually booked on and from which the MS receives BCCH information.

SFH Slow frequency hopping (see *HSN*).

SI [Q.700–Q.704] Service indicator. A 4-bit-long parameter within an MSU that indicates the user part (SCCP, ISUP, etc.). See Chapter 8.

SID [GSM 06.31, 6.41] Silence descriptor. A 2-bit-long parameter that indicates whether a TRAU frame in the uplink is a SID frame (SID = 2) or a regular speech frame (SID = 0). A SID frame contains only data for the purpose of producing comfort noise (see *DTX*) but no speech information.

SIF [Q.700–Q.704] Signaling information field (see also MSU). The maximum length of a SIF amounts to 272 bytes. See Chapter 8.

SIM [GSM 02.17, 11.11] Subscriber identity module. See Chapter 2 (see *PIN*, *PUK*).

SIO [Q.700–Q.704] Service information octet. Used in SS7 messages to distinguish between national and international messages, as well as between the various SS7 user parts (see *MSU*); 8 bits long. See Chapter 8.

Skip indicator See *Transaction identifier*.

SLC [Q.700–Q.704] Signaling link code. Part of the routing label of SS7 management and test messages. It is located at the same place as the SLS field of other SS7 messages and is 4 bits long. The SLC can be used to identify the SS7 connection when a management or test message is sent (SLS = 0, if nothing is defined). The SLC field is not used for load sharing.

SLR [Q.711–Q.714] Source local reference. See Chapters 9 and 13.

SLS [ITU Q.700–Q.704] Signaling link selection. Part of the routing label of SS7 Messages. This 4-bit-long parameter is used to balance load on SS7 connections. See Chapter 8.

SMG When the standardization work on GSM started, it was carried out by a group called Groupe Spécial Mobile (GSM). When more and more countries worldwide became interested in GSM, it was decided to change the name of the group to Special Mobile Group (SMG). At the same time, the meaning of GSM was changed to Global System for Mobile Communications. SMG is the standards body responsible for all GSM specifications. SMG is a technical committee of ETSI.

SMS [GSM 03.40] Short message services. A GSM service that allows small text messages to be sent to and from a mobile station. It is similar to a paging service integrated in the MS but is two-way.

SMS gateway MSC [GSM 03.02] See *SMS interworking MSC*.

SMS interworking MSC [GSM 03.02] The interface functionality for short messages from the SMS service center toward the mobile station is performed by a special MSC, called SMS gateway MSC. Routing messages in the opposite

direction, from the mobile station to the SMS service center, is done by another MSC, called the SMS interworking MSC. Figure G.54 illustrates the tasks of the two types of MSCs.

SMSCB Short message service cell broadcast. See *CB*.

SPC [Q.700–Q.704] Signaling point code. An identifier in SS7 to specify the address of a network element, for example, that of a BSC. SPC is the generic term for originating point code (OPC) and destination point code (DPC). See Chapter 8.

SRES [GSM 03.08, 03.20] Signed response. Used to verify the identity of an MS. SRES, which is 4 bytes long, is calculated by the MS by applying K_i and RAND to the algorithm A3 (see *Ciphering*).

SS [GSM 02.04, 04.10, 04.80] Supplementary services. Telecommunications services that supplement or modify a basic service. This terminology is used by GSM and ISDN. Examples of supplementary services are call forwarding and multiparty call.

In addition to those SSs that GSM 02.04 lists, there exists another category of supplementary services, the unstructured supplementary services (USSs). USSs give mobile stations and the network the capability of exchanging PLMN-specific text messages up to 80 bytes long. The text messages are called unstructured supplementary services data (USSD). This allows the network operator to offer proprietary features to its subscribers. USSD can be created on the MS side, by means of the HMI/MMI keys.

Table G.17 lists and explains all current GSM supplementary services.

SS7 [Q.700–Q.704] Signaling system number 7 (SS7). See Chapter 8.

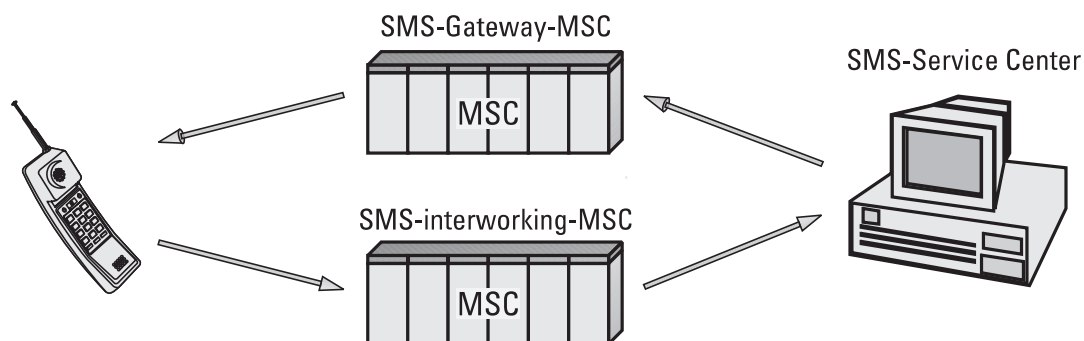


Figure G.54 The task of the SMS gateway MSC and the SMS interworking MSC.

Table G.17
GSM Supplementary Services

Acronym	GSM	SS-Code (Hex)	SS Name	Explanation
CLIP	02.81	11	Calling Line Identification Presentation	The number of the calling party is sent to the MS of the served subscriber for display.
CLIR	02.81	12	Calling Line Identification Restriction	The number of the served subscriber is restricted from being displayed at the called party's terminal.
COLP	02.81	13	Connected Line Identification Presentation	The number of the called party that the call is connected to is sent to the MS of the served subscriber for display.
COLR	02.81	14	Connected Line Identification Restriction	The actual number of the served subscriber, when answering a call, is restricted from being displayed at the calling party's terminal.
CFU	02.82	21	Call Forwarding Unconditional	A number to which all incoming calls will be redirected that has to be registered.
CFB	02.82	29	Call Forwarding on Mobile Subscriber Busy	Incoming calls will be redirected to a previously registered number when the MS is in a busy state.
CFNRy	02.82	2A	Call Forwarding on No Reply	Incoming calls will be redirected to a previously registered number when the MS does not answer within a specified time. The served subscriber may adjust the <i>No Reply Timer</i> .

Table G.17 (continued)

Acronym	GSM	SS-Code (Hex)	SS Name	Explanation
CW	02.83	41	Call Waiting	When the MS is in the busy state, Call Waiting indicates to the served subscriber that a second call came in.
HOLD	02.83	42	Call Hold	This allows the served subscriber to put a call on hold.
MPTY	02.84	51	Multi Party Service	MPTY allows the served subscriber to establish a conference call with up to 5 peer parties.
CUG	02.85	61	Closed User Group	CUG allows restriction of the communications capabilities to a limited number of parties. Several options exist to allow for incoming and outgoing access to parties outside the CUG. A subscriber can be member of up to ten Closed User Groups
AoCI	02.86	71	Advice of Charge (Information) (AoCI)	AoCI is the information level of AoC. It allows a MS to calculate a fairly accurate estimate of the call charges that will incur, by means of the <i>AoC parameters</i> that the MS receives at call set up. For MOC, these parameters are sent in a Facility element of a CON message, for the MTC (roaming charges) in a FACILITY message, which directly follows the CON message.
AoCC	02.86	72	Advice of Charge (Charging) (AoCC)	The same principle applies for the charging level of AoC, as for AoCI. The difference is the added requirement on accuracy. It is possible to limit the total amount of charges. When this limit is reached, an existing call is dropped and new calls are not accepted. AoCC can be used for pre-paid services.
BAOC	02.88	92	Barring of All Outgoing Calls	The subscriber is not able to place an outgoing call.
BOIC	02.88	93	Barring of Outgoing International Calls	The subscriber is not able to place outgoing international calls.

Table G.17 (continued)

Acronym	GSM	SS-Code (Hex)	SS Name	Explanation
BOIC-exHC	02.88	94	Barring of Outgoing International Calls except those directed to the Home PLMN Country	The subscriber is not able to place outgoing international calls, except to the country where the home PLMN is.
BAIC	02.88	9A	Barring of All Incoming Calls	The subscriber is not able to receive calls.
BIC-Roam	02.88	9B	Barring of Incoming Calls when Roaming Outside the Home PLMN Country	The subscriber is not able to receive calls when roaming outside the country where the home PLMN is (to prevent charges for international roaming).
USS	02.90	F0 - FF	Unstructured Supplementary Services	This allows a network operator to offer PLMN specific, i.e., non-standardized Supplementary Services.

SSF [Q.700–Q.704] Subservice field. A term from SS7. The 4-bit-long SSF is part of the MSUs, and its sole content is the network indicator (NI), which allows for national messages to be distinguished from international ones. The SSF is also part of the service information octet (SIO). See Chapter 8.

SSN [Subsystem Number Q.711 through Q.714, Send Sequence Number GSM 04.08] Subsystem number. Identifies the actual user of an SCCP message. Examples of SSNs are the BSSAP (see *BSSMAP*) and MAP. See Chapter 9. Also abbreviation for send sequence number (SSN), which relates to bit number 6 of the octet that indicates the message type of GSM messages on the Air-interface.

Stealing flag [GSM 05.03] The stealing flag is 1 bit long and is part of the normal burst. Stealing flags embrace the training sequence (see *TSC*). They are used in the uplink and downlink direction to indicate whether and which bits of a traffic channel are used (stolen) to carry signaling information (see *FACCH*). Stealing of bits to send signaling information on the traffic channel (see TCH) may become necessary when the MS or the BTS have to immediately send signaling data but the SACCH is not available.

Examples of control data are the HND_CMD, CON, and the DISC messages. Note that 456 bits (four bursts) are necessary to transfer such a message, completely. The stealing flag was introduced in order not to lose four consecutive bursts for traffic data. Actually, a signaling message is divided into eight packets with 57 bits each and then transmitted in eight consecutive bursts. Only the even-numbered bits are used to carry signaling data in the first four bursts, while only the odd-numbered bits are used for signaling in the last four bursts (i.e., 5 through 8). That allows use of the remaining 57 bits per burst to carry traffic data (Figure G.55).

STP Signaling transfer point. A node within a SS7 network. The STP does not only process SS7 messages, it also relays them to other SS7 network elements (Figure G.56). Basically, every SS7 network element could be used as an STP, too. See Chapter 8.

Subchannel [GSM 05.01, 05.02] For the SDCCH and for the halfrate traffic channel, a single Air-interface channel with 13 Kbps can be divided into subchannels. In halfrate, one channel simply is divided in half, that is, two subchannels, while in SDCCH up to eight subchannels can be configured on a single 13-Kbps channel. See Chapter 7.

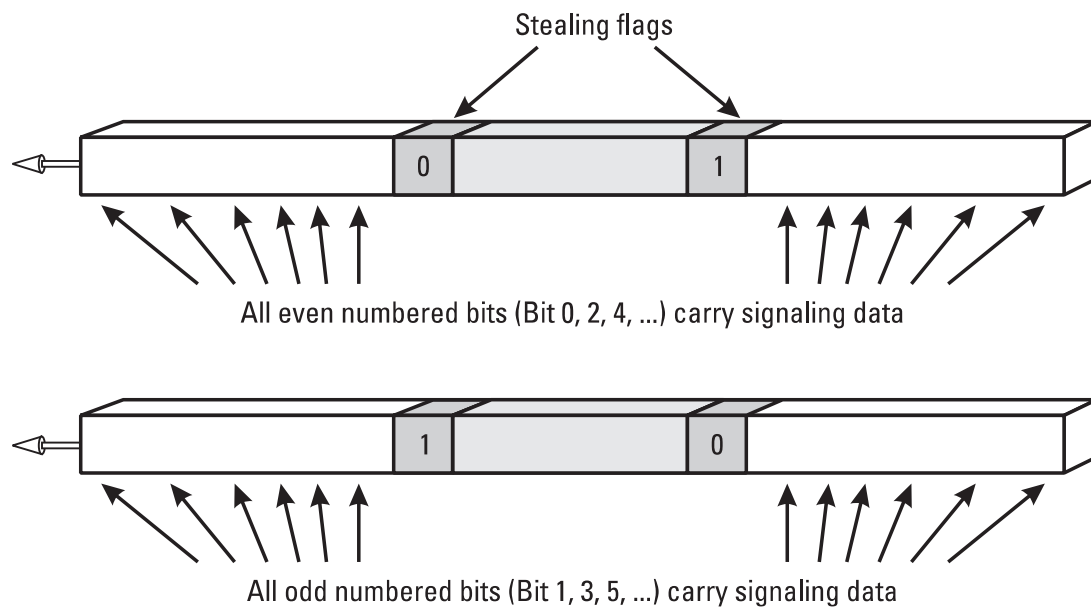


Figure G.55 The stealing flag.

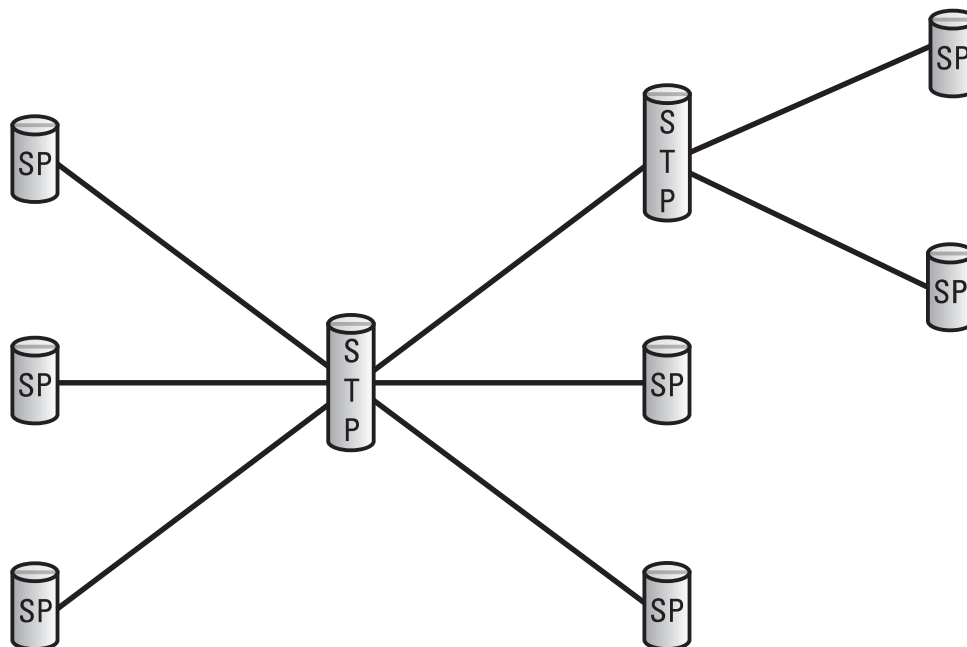


Figure G.56 The STP relay in the SS7 network.

Subscriber An entity that subscribes to telecommunications services. A subscriber can be a natural person or a legal entity. GSM does not distinguish between the subscriber and the user of a service.

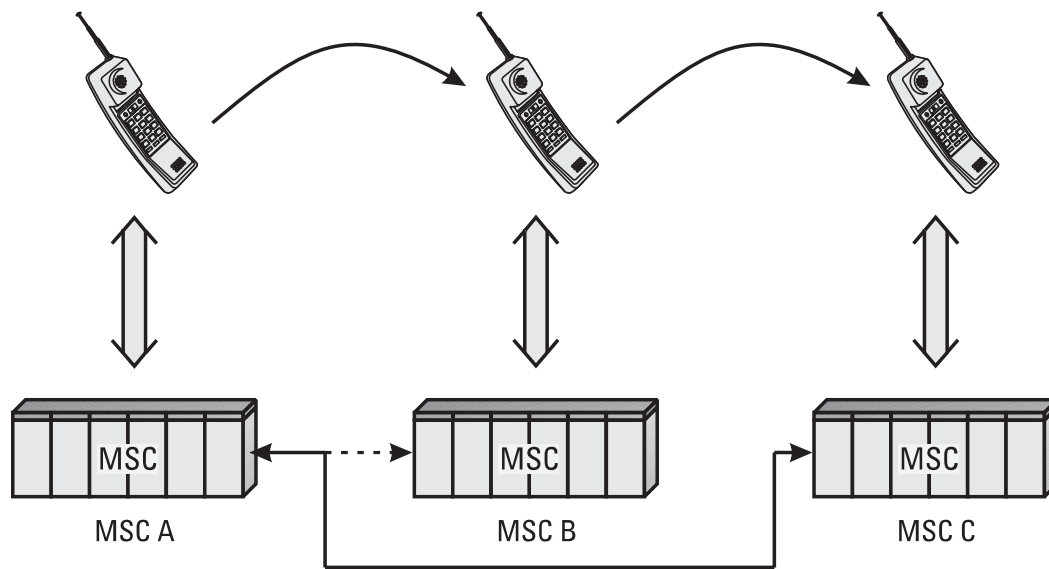


Figure G.57 Intersystem and subsequent handover.

Subsequent handover [GSM 09.10] Situation in which an inter-MSC handover occurs more than once for a single connection. MSC A hands the call to MSC B, later the call is handed over to MSC C or back to MSC A (Figure G.57). Since MSC A is always in charge of such a connection, the scenario for the second or third handover is different from the first one. For that reason, the term *subsequent handover* was introduced. See Chapter 12.

SUERM [Q.700–Q.704] Signal unit error rate monitor. Part of Layer 2 of an SS7 network element. The number of faulty signal units received subsequently or within a certain time period is monitored. When a defined threshold is passed, for example, 64 subsequent faulty signal units have been received, an error indication is issued to Layer 3, and the SS7 connection is taken out of service.

Superframe [GSM 05.01, 05.02] A superframe consists of twenty-six 51-multiframes or fifty-one 26-multiframes and has a length of 6.12s. See Chapter 7.

Supplementary services See *SS*.

Synchronization channel See *SCH*.

Synchronized handover [GSM 04.08] All BTSs that are finely synchronized can perform a so-called synchronized handover. Fine synchronization means

that the starting times and the ending times of all time slots are identical for the synchronized cells. That is not the case when the two BTSs are not finely synchronized. Compare in Figure G.58 the channel structure of BTS 1, BTS 2, and BTS 3. While BTS 1 and BTS 3 are finely synchronized, BTS 2 operates independently.

Now let's assume that a handover is to be performed from BTS 1 to BTS 3. In general, the distance from the MS to BTS 1 and to BTS 3 will be different. Of course, that results in different propagation delays of the signal from BTS 1 to the MS, compared to the time the signal takes from BTS 3 to the MS. Based on that difference, the MS is able to calculate the distance to BTS 3 and to adjust its timing advance (see *TA*) for a handover from BTS 1 to BTS 3. Consequently, it is not necessary for BTS 3 to send PHYS_INFO messages to the mobile station.

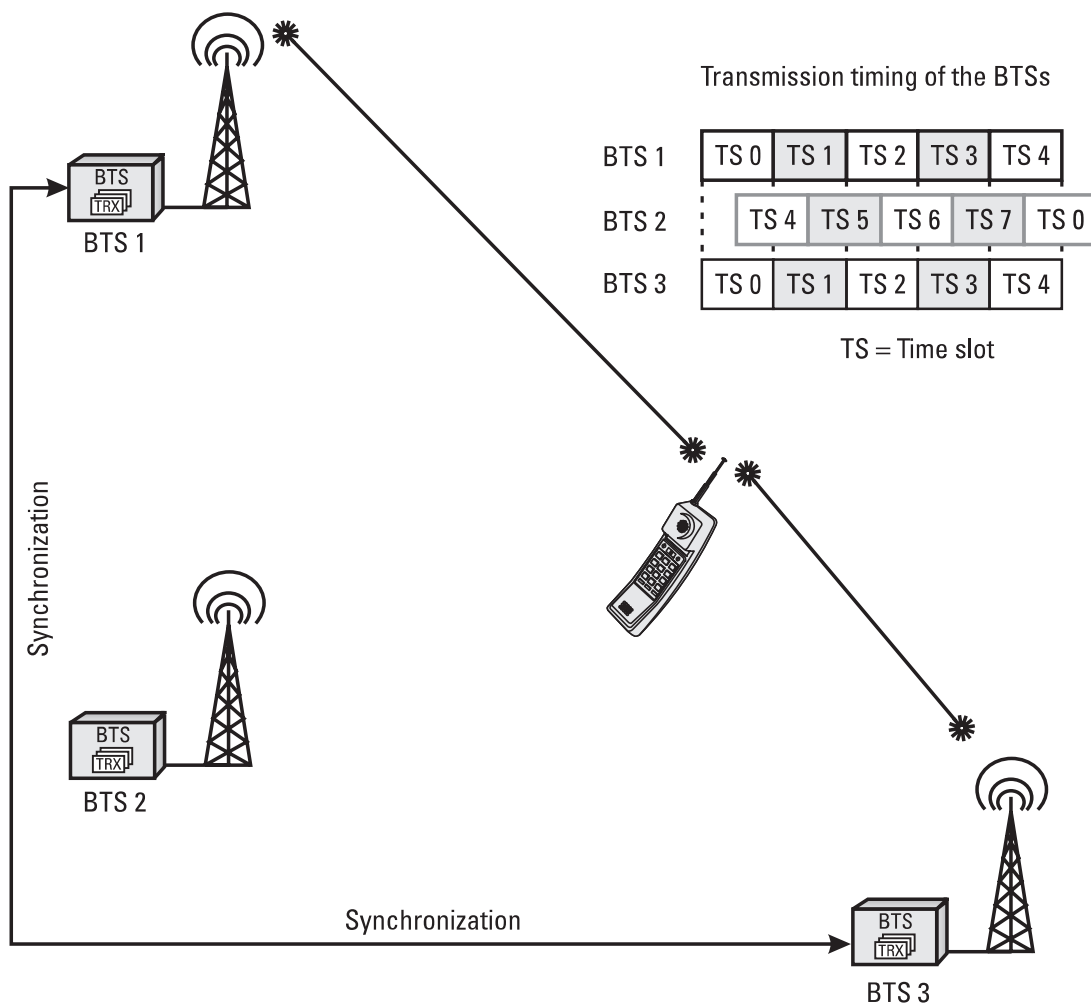


Figure G.58 Synchronized BTSs.

This possibility does not exist for a handover from BTS 1/BTS 3 to the nonsynchronized BTS 2. Only a nonsynchronized handover is possible in this case and requires BTS 2 to send PHYS_INFO messages during the handover, for the MS to adjust the TA.

GSM has defined two more handover types, the pseudo-synchronized and the presynchronized handover. The pseudo-synchronized handover requires the MS to predetermine the time offset between BTS 1 (active cell) and BTS 2 (destination cell) from the neighbor cell measurements. The MS sends the resulting MEAS_REP messages to BTS 1 or, more precisely, to the BSC. These data reflect the view of the MS, only. Another condition for pseudo-synchronized handover is that BTS 1 needs to know exactly how much earlier or later the destination cell (BTS 2), relative to BTS 1, actually transmits. With that information and with the results of the measurements from the MS it is possible for BTS 1 to calculate the distance between MS and BTS 2 and, hence, the TA that the MS has to preset when being handed over to BTS 2. BTS 1 sends the TA value to be used in an HND_CMD message to the MS. For the MS, pseudo-synchronized handover is an optional feature, and its availability is indicated to the BSC in the mobile station classmark during call setup.

A presynchronized handover requires the same behavior from the MS as a synchronized handover. The BTS does not send a PHYS_INFO message and the MS uses either the value requested in the HND_CMD message or a standard TA, with a value of 1, when the HND_CMD message does not contain any value for TA.

SYSTEM Information 1–8 See BCCH SYS_INFOS 1–4.

T7 [GSM 08.08] Timer T7 is a timer of the BSC that indicates the minimum time interval between two HND_RQD messages for the same connection (Figure G.59).

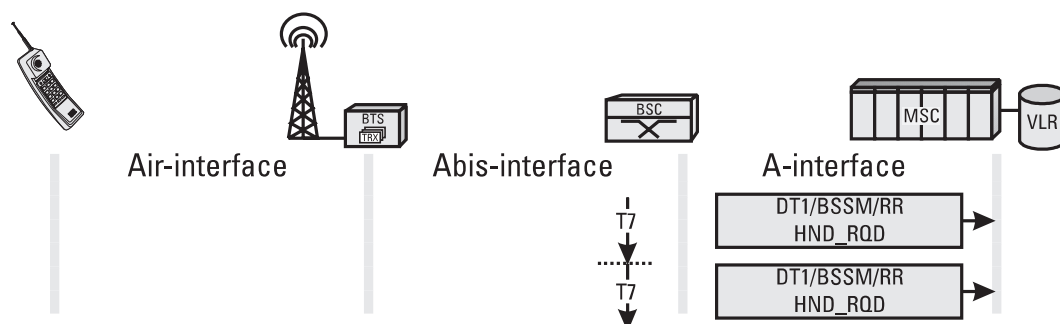


Figure G.59 Timer T7 in the BSC.

T8 [GSM 08.08] A timer of the “old” BSC that indicates the waiting period during an external handover between transmission of the HND_CMD message and either the positive acknowledgment of a handover by the MSC (CLR_CMD) or the negative acknowledgment by the MS (HND_FAI). The old BSC releases the connection with a CLR_REQ message (cause 0 = radio interface message failure) in case T8 expires, before any of these messages is received. See Figure G.60.

T10 [GSM 08.08] A timer of the BSC that supervises the waiting period between emission of an ASS_CMD message and the according acknowledgment by the MS (Figure G.61). The BSC sends an ASS_FAIL cause: radio interface message failure to the MSC, if the timer expires during a TCH assignment, without an ASS_COM message or an ASS_FAI message being received from the MS.

If, during intra-BTS handover, an HND_CMD message instead of the ASS_CMD message is used for the assignment of the new traffic channel, the BSC sends CLR_REQ cause: radio interface message failure to the MSC, instead of the ASS_FAIL message.

T200 [GSM 04.06, Q.921] Timer used by LAPD and LAPD_m. The sender of a frame expects to receive acknowledgment for that frame within the time specified by T200. T200 starts when a message is sent. If no acknowledgement is received within T200, the frame may be retransmitted as many times as specified by N200, before the connection is released.

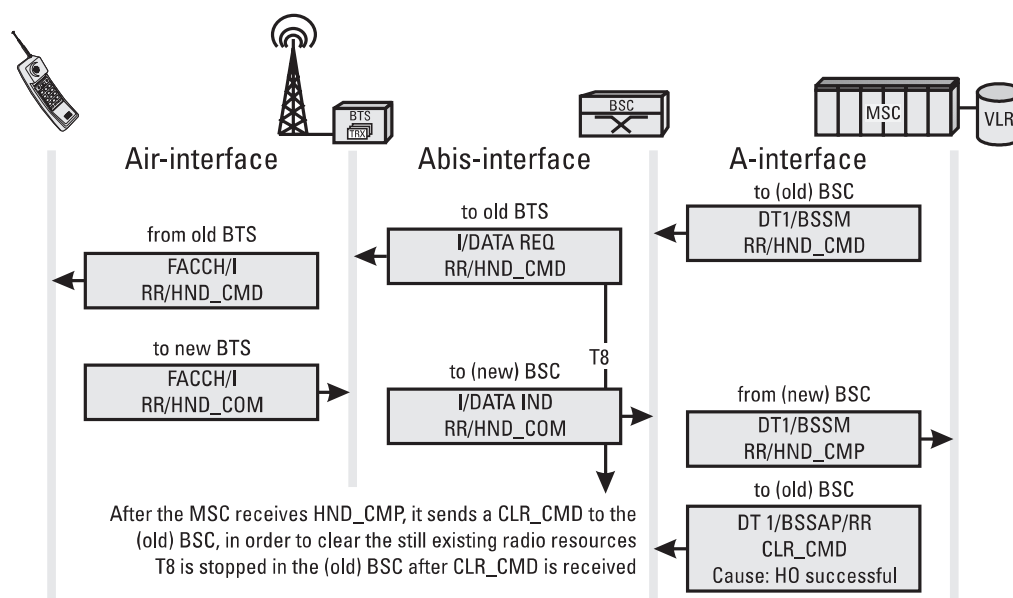


Figure G.60 The task of timer T8.

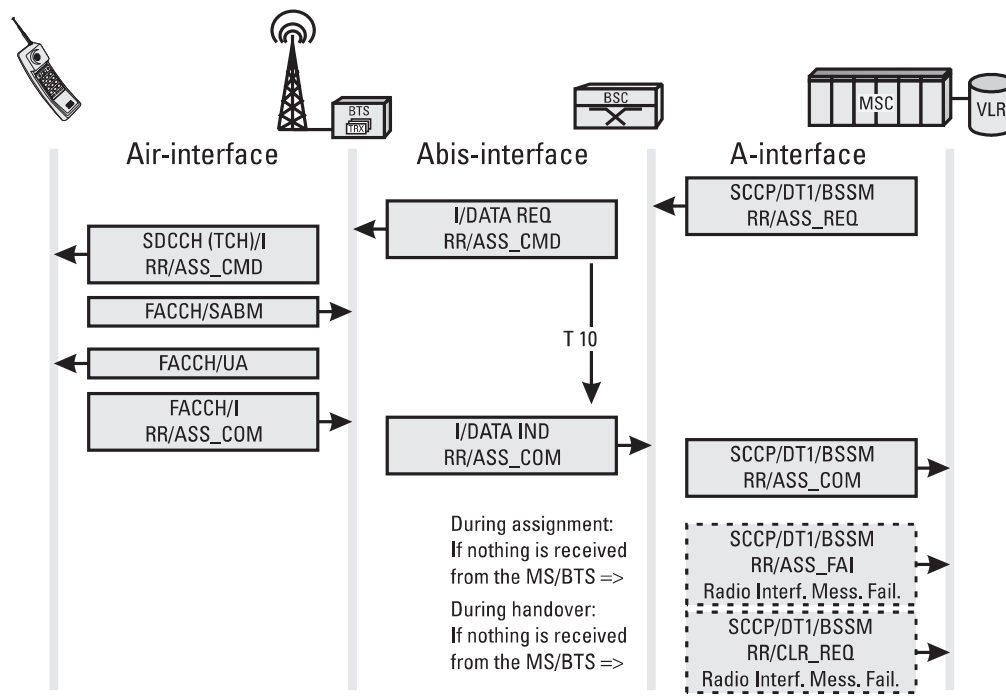


Figure G.61 Timer T10 during the TCH assignment.

T3105 [GSM 04.08] A timer of the BTS that defines the time between transmission of two consecutive PHYS_INFO messages.

T3212 [GSM 04.08] A timer of the mobile station or the SIM. The value of T3212 specifies the time interval for periodic location updating.

TA Timing advance. The agreement in a GSM system is for the MS to send its data three time slots after it received the data from the BTS. The BTS then expects the bursts from the MS in a well-defined time frame. This prevents collision with data from other mobile stations. The mechanism works fine, as long as the distance between MS and BTS is rather small. Increasing distance requires taking into account the propagation delay of downlink bursts and uplink bursts. Consequently, the mobile station needs to transmit earlier than defined by the “three time slots delay” rule. The information about how much earlier a burst has to be sent is conveyed to the mobile station by the TA. The TA is dynamic and changes in time. Its current value is sent to the mobile station within the layer 1 header of each SACCH. In the opposite direction, the BTS sends the current value for TA within the MEAS_RES messages to the BSC (e.g., for handover consideration). The farther the MS is away from the BTS, the larger is the required TA. Figure G.62 illustrates the relation between distance and TA.

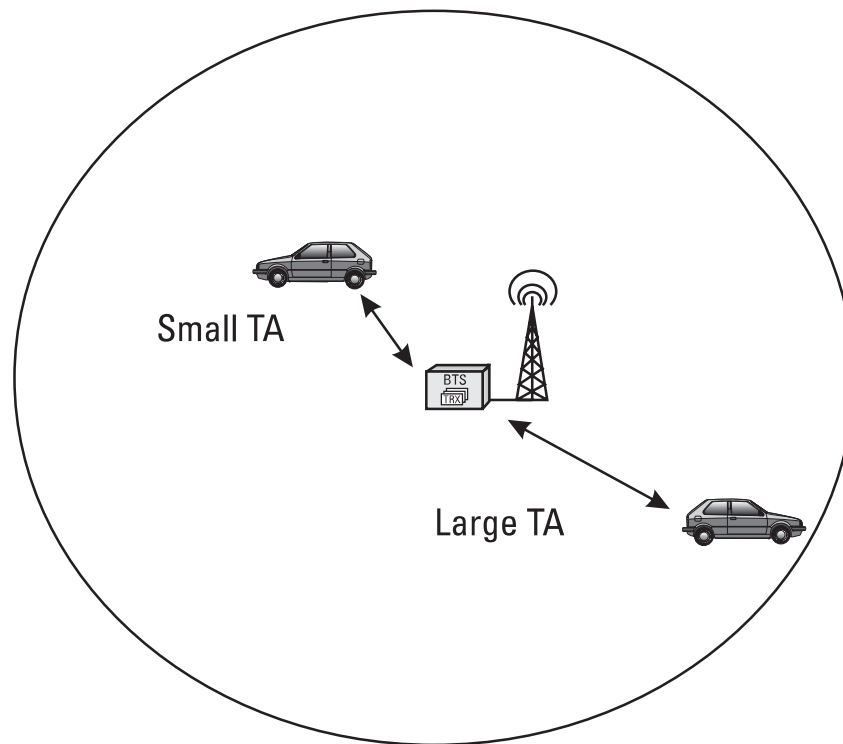


Figure G.62 The dependency of TA from the distance.

Using the TA allows the BTS to receive the bursts from a particular MS in the proper receiver window. The BTS calculates the first TA when receiving a RACH and reports the value to the BSC. TA can take any value between 0 and 63, which relates to a distance between 0 km and 35 km. The steps are about 550 m ($35 \text{ km}/63 \approx 550 \text{ m}$). With respect to time, the different values of TA refer to the interval $0 \mu\text{s}$ through $232 \mu\text{s}$, in steps of $48/13 \mu\text{s}$. It is important to note that this value of TA represents twice the propagation delay. Figure G.63 illustrates the effect of TA by an example in which a connection is active on TS 1.

TAF [GSM 07.01, 07.02, 07.03] Terminal adaptation function. Function that supports the mobile station in setting up data connections.

TAG [Q.773] Indicates parameter types within TCAP and MAP. The term stems from ASN.1. See Chapter 11.

Tail bits See *Burst*.

TCAP [Q.771, Q.772, Q.773] Transaction capabilities application part. See Chapter 11.

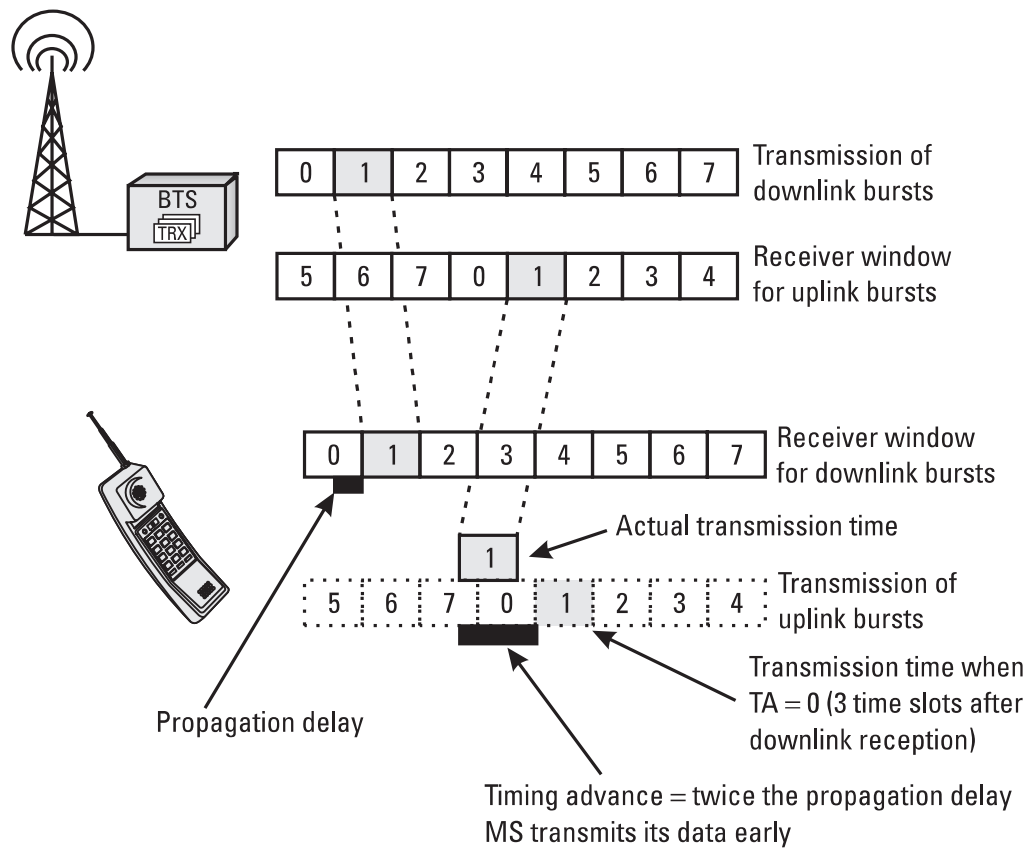


Figure G.63 Adjusted transmission time due to TA.

TCH [GSM 05.01, 05.02, 05.03] Traffic channel. GSM uses the following types of TCHs (see Table G.18).

Table G.18
The TCHs in GSM

Abbreviation	Remark
TCH/FS	Fullrate speech traffic channel
TCH/HS	Halfrate speech traffic channel
TCH/F9.6	9.6-Kbps fullrate data traffic channel
TCH/F4.8	4.8-Kbps fullrate data traffic channel
TCH/H4.8	4.8-Kbps halfrate data traffic channel
TCH/F2.4	2.4-Kbps fullrate data traffic channel
TCH/H2.4	2.4-Kbps halfrate data traffic channel

TDMA Time division multiple access. See *FDMA*.

TEI [Q.920, Q.921] Terminal endpoint identifier. Used by the LAPD protocol in connection with the SAPI to specify the destination of a message. See Chapter 6.

Teleservice A telecommunications service that a GSM operator offers to its customers (subscribers). While for a teleservice all seven OSI layers are specified, the related bearer services require only Layers 1 through 3. A bearer service forms, from a physical point of view, the lower layers of a teleservice. From a standardization point of view, they belong, however, to different categories. Table G.19 lists the Teleservices of GSM.

TI Transaction identifier.

Timing advance See *TA*.

TMSI [GSM 03.03] Temporary mobile subscriber identity. Used to identify a mobile subscriber, like the IMSI. Unlike the IMSI, however, the 4-byte-long TMSI has only temporary significance. The VLR assigns a TMSI upon location registration for confidentiality purposes, so it is not required to transfer the IMSI over the Air-interface frequently. Assignment and use of the TMSI is only possible with active ciphering. The TMSI can take any value, except FF FF FF FF_{hex}. This value is reserved in case the SIM does not contain a valid IMSI.

TN Time slot number.

Table G.19
Teleservices in GSM

Teleservice	Code	Description
Speech	11	Regular telephone service
	12	Emergency calls
Short Message Services	21	SMS/(MT/PP)
	22	SMS/(MO/PP)
	23	Cell broadcast (CB)
Fax	61	Speech + fax/group 3
	62	Fax/group 3

Training sequence code See *TSC*.

Transaction identifier [GSM 04.07, 04.08] Parameter used by CC (call control) Layer 3 messages. Note that RR messages and MM messages do not need a transaction identifier and therefore fill its position with the skip indicator (always 0000_{bin}).

The purpose of the TI is to distinguish among simultaneous connections (transactions) of one mobile station. See Chapter 7.

TRAU Transcoding rate and adaptation unit. See Chapter 3

TRAU frame [GSM 08.60] In fullrate channels, every TRAU frame is 320 bits long. In halfrate channels, both 160 bits and 320 bits are possible. One has to distinguish four different types of TRAU frames:

- The speech frame is used to transfer voice. The payload is 260 bits for fullrate and 112 bits for halfrate.
- The O&M frame to transfer O&M data between BTS and TRAU. The BTS acts in this case only as a relay for the BSC, for which these data are actually destined or where they are generated (264-bit O&M data for both fullrate and halfrate).
- The data frame carries 252 bits of payload in fullrate and 126 bits in halfrate, but no voice.
- The idle speech frame for quiet times between BTS and TRAU with active DTX.

TS Time slot.

TSC [GSM 05.02] Training sequence code. Code positioned in the middle of every burst, independent from the direction uplink or downlink. The dummy burst and the frequency correction burst are both exceptions from this rule and do not contain a TSC. The length of the TSC depends on the burst type. The TSC can be of fixed format or be assigned (there are eight TSC formats) (Figure G.64).

- Synchronization burst (see *Burst*): predefined TSC with 64 bits.
- Access burst: predefined TSC (synchronization sequence) with 41 bits.
- Normal burst: dynamic TSC with 26 bits; can be independently assigned for common control channels (see *CCCH*) and dedicated

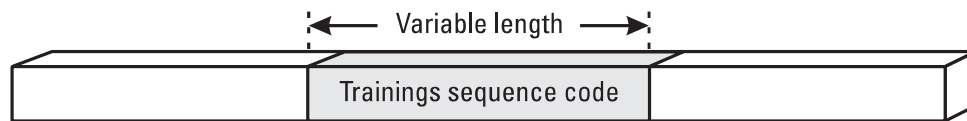


Figure G.64 The TSC.

channels (see *TCH*, *SDCCH*). Which of the eight TSCs is used for CCCHs, is determined by the base station color code (see *BCC*). Assignment of the TSC for dedicated channels takes place in the IMM_ASS message, the ASS_CMD message, and the HND_CMD message.

Since the content of the TSC is known on both sides, it can be applied as a reference that enables the receiver to conclude on possible bit errors of the entire burst. Depending on the grade and type of error, either the original data can be restored or the whole burst will be discarded. The bit error rate that was determined by means of the TSC is the basis for the RXQUAL information of the MEAS_RES messages and the MEAS_REP messages.

Triplet Generally refers to three related things. Used in GSM in relation to security features, where it refers to SRES, RAND, and K_c .

TRX Transmission/reception unit. Generic term for both the high-frequency and low-frequency modules that perform signal processing in the BTS. Some of the tasks of the TRX are channel coding/decoding, ciphering/deciphering, and GMSK modulation/demodulation. See Chapter 3.

TX_Integer [GSM 05.08] Parameter transmitted in the RACH control parameters in the BCCH / SYS_INFO 1–4. TX_Integer indicates the maximum number of RACH time slots that a mobile station has to wait after an unsuccessful BTS access before another CHAN_REQ can be sent. See Chapter 7.

In those cases, the MS selects a random number R , with

$$0 \leq R \leq TX_Integer$$

and waits R TDMA frames before the CHAN_REQ messages is sent again (see MAX_RETRAN).

μ -law See *A-law*.

Um-interface The GSM-specific term for the Air-interface.

UMTS Universal Mobile Telecommunication System (UMTS). A third-generation mobile telecommunication system currently being discussed by SMG as an evolutionary step of GSM. The goals of UMTS are similar to those of the Future Public Land Mobile Telecommunication System (FPLMTS).

Uplink The direction of a signal from the mobile station toward the network. See *Downlink*.

User parts The various applications of the MTP (SS7). Examples are the SCCP and ISUP. See Chapters 8 and 9.

USSD [GSM 02.90] Unstructured supplementary service data (USSD). In addition to the supplementary services, which are defined by GSM 02.04, GSM has defined the concept of the unstructured supplementary services (USSs). USSs allow the network operators to offer PLMN-specific supplementary services to their customers with a rather short time to market. USSs can be implemented in the MSC, the VLR, or the HLR. For the USSs, some MAP messages have been predefined that allow data packages of up to 80 bytes to be sent. The data packages are referred to as USSD. The subscriber is capable of entering USSD at the mobile station via the HMI.

VAD [GSM 06.32] Voice activity detector. A unit in the BTS and the MS that determines whether or not voice activity prevails. If there is no voice signal, it will be switched to DTX mode.

VLR [GSM 03.02, 12.02, 12.03] Visitor location register. See Chapter 4.

VLR number [GSM 03.03] An identifier for the VLR that corresponds to that of a regular ISDN number or directory number (see *MSISDN*). Every VLR has a unique VLR number that is used to address messages to the VLR via the SCCP.

About the Author

Gunnar Heine received his Ph.D. in Communications Technology from the University of Wilhelmshaven. In 1991, he began his career as a system engineer of GSM for ALCATEL SEL in Germany. Heine was responsible for the integration and troubleshooting of the just commissioned GSM systems both in Germany and internationally. In 1996, Gunnar Heine was sent to the United States to take over the position of Director of Technical Support for ALCATEL Mobile Switching. After 7 1/2 years with ALCATEL, he has returned to Germany and is currently the VP of Technology Management for HanseNet GmbH in Hamburg.

Index

- A-format frame, 102, 105
- A-interface, 27, 168, 277, 280
 - base station subsystem application part, 173–84
 - dimensioning, 171–73
 - error analysis, 287–91
 - error analysis in BSS, 296–302
 - error messages, 291–96
 - signaling analysis, 280–82, 285
- Abisinterface, 19, 25, 26–27, 44, 277, 280
 - BTS/BSC connection, 52–55
 - channel configurations, 51–52
 - error analysis, 287–91
 - error analysis in BSS, 296–302
 - error messages, 291–96
 - layer 2, 56–71, 81–83
 - layer 3, 71–86
 - protocol stack, 55–56
 - service, bringing into, 87
 - signaling analysis, 280, 282–84, 286
- ABORT message, 221
- Abstract Syntax Notation
 - number 1, 45, 189, 193, 194
- Access grant channel, 95–100
- ACCH. *See* Associated control channel
- Acknowledged message, 57
- Address field, 60, 83, 102, 104, 105
- Addressing
 - Signaling System Number 7, 130–33
 - transaction capabilities application part, 186–88
- AGCH. *See* Access grant channel
- Air-interface, 19, 27, 28, 44, 63, 71, 75, 279
 - channel configuration, 97–100
 - interleaving, 100–1
 - layer 2 signaling, 101–6
 - layer 3 signaling, 107–23
 - logical-channel connection, 94–100
 - physical vs. logical channel, 94
 - structure, 89–94
- ALCATEL, 34
- AM. *See* Amplitude modulation
- Amplitude modulation, 90
- APDU. *See* Application protocol data unit
- Application layer, 46
- Application protocol data unit, 189
- Architecture, 3–4
- ASN.1. *See* Abstract Syntax Notation
 - number 1
- Assignment failure
 - message, 292–94, 298–300
- Associated control channel, 102
- AuC. *See* Authentication center
- Authentication center, 32–33
- B-format frame, 102, 105
- B-interface, 34, 37, 51, 214
- Backward indicator bit, 127, 135–38

- Backward sequence number, 127, 133–38
- Base station controller, 5–6, 25–27, 61, 73, 130, 172–73, 227
 - connection to BTS, 52–55, 87
 - handover, 257, 260–62
- Base station range, 3
- Base station subsystem, 6, 29–30, 174
 - error analysis, 280, 287, 296–302
 - location update, 227–31
 - mobile originating call in, 233, 235–40
 - mobile terminating call in, 244–50
- Base station subsystem application
 - part, 153–54, 169, 173–76, 285
- Base station subsystem management
 - application part, 173–75
 - message decoding, 183–184
 - message types, 176–183
- Base transceiver station, 5, 17, 19–25, 61, 64, 72–73, 75, 91, 171, 227, 287
 - clock module, 21–22
 - configurations, 22–25
 - connection to BSC, 52–55, 87
 - handover, 251, 254, 257–59
 - input/output filters, 22
 - operations and maintenance, 20
 - transmitter/receiver, 20
- Bbis-format frame, 102
- BCCH. *See* Broadcast common control channel
- Begin message, 201, 221
- BIB. *See* Backward indicator bit
- Binary data, 285
- Bit, 9
- Bit error rate, 296
- Black list, 38
- Broadcast common control
 - channel, 95–100
- BSC. *See* Base station controller
- BSN. *See* Backward sequence number
- BSS. *See* Base station subsystem
- BSSAP. *See* Base station subsystem application part
- BSSMAP. *See* Base station subsystem management application part
- BTS. *See* Base transceiver station
- Burst, 90–91
- Burst segmentation, 105
- Call control, 7, 17, 44, 104, 107–10, 118–23, 174, 263, 267
- Called-party address, 159, 162–65
- Call handling error, 21–22
- Calling-party address, 159, 162–65
- Call release, 10
- Call setup, 10
- CaPA. *See* Calling-party address
- CBA. *See* Change back acknowledge
- CBCH. *See* Cell broadcast channel
- CBD. *See* Change back declaration
- CC. *See* Call control; Connection confirm
- CCCH. *See* Common control channel
- CCH. *See* Control channel
- CCM. *See* Common channel management
- CDMA. *See* Code division multiple access
- CdPA. *See* Called party address
- Cell broadcast channel, 95–100
- Cell identity, 22
- Cellular network, 3–4
- Central module, base station controller, 27
- CEPT. *See* Conference Européenne des Postes et Télécommunications
- Change back acknowledge, 148
- Change back declaration, 148
- Change over acknowledge, 148
- Change over order, 140, 148
- Changeover procedure, 140–41
- Channel coding, 105
- Channel mapping, 91
- Channel number, 75
- Checksum, 44
- CI. *See* Cell identity
- Ciphering, 91
- Class field, 191
- Clear request message, 291–92, 297–98
- Clear-to-send signal, 43
- Clock module, 21–22, 91
- CNP. *See* Connection not possible message
- CNS. *See* Connection not successful message
- COA. *See* change over acknowledge
- Code division multiple access, 2, 89
- Coding, transaction capabilities application
 - part, 189–98

- Collocated base transceiver station, 24–25, 54
- Command/response bit, 61, 62, 102, 106
- Common channel management, 55, 75
- Common control channel, 75
- Component portion, 205–8
- Compression. *See* Speech compression/decompression
- Computer port, 43
- Conference Européenne des Postes et Télécommunications, 2
- Connect message, 201
- Connection confirm, 161, 167
- Connection failure message, 294–95
- Connectionless service, 154–56, 165–66, 186, 285, 287
- Connection non successful message, 149
- Connection not possible message, 149
- Connection-oriented service, 154–56, 165–66, 285–86
- Connection refused message, 161
- Connection request message, 161, 167
- Connection successful message, 149
- Consistency check, 57, 64
- Constructor, 191–93, 197
- Control channel, 10, 94, 286
- Control field, 62, 67, 69, 83
- COO. *See* Change over order
- CR. *See* Connection request
- C/R bit. *See* Command/response bit
- Credit parameter, 165
- CREF. *See* Connection refused message
- CSS. *See* Connection successful message
- CTS signal. *See* Clear-to-send signal
- D-channel, 10, 55–57
 - See also* Data Link Access for D-Channel
- Database, base station controller, 27
- Data form 1, 161, 168
- Data link connection, 149
- Data link connection identifier, 175
- Data link layer, 43–44
- Data type octetstring, 194
- DCCH. *See* Dedicated control channel
- DCM. *See* Dedicated channel management
- DCS 1800. *See* Digital Cellular System 1800
- DECT. *See* Digital enhanced cordless telecommunications
- Dedicated channel management, 55, 75
- Dedicated control channel, 102
- Destination local reference, 154–56, 166–68, 189, 285
- Destination point code, 131–32
- DeTeMobil software, 280–84
- Dialog control, 198–99
 - structured vs. unstructured, 198, 201, 220–23
- Dialog portion, 198, 203–4
- Dialog unit, 201–2
- Digital Cellular System 1800, 2
- Digital Enhanced Cordless Telecommunications, 2
- Dimensioning, 171, 173
- Direction dependency, 211–12
- Direct transfer application part, 173–75
- Disconnected-mode frame, 56, 68
- Disconnect frame, 56, 69
- Discontinuous transmission, 29, 255–56
- DLC. *See* Data link connection
- DLCI. *See* Data link connection identifier
- DLR. *See* Destination local reference
- DM frame. *See* Disconnected-mode frame
- Downlink, 73, 94–95, 97–98, 102
 - synchronization, 93–94
- DPC. *See* Destination point code
- Drivetest, 275–76
- DT 1. *See* Data form 1
- DTAP. *See* Direct transfer application part
- DTMF. *See* Dual-tone multifrequency
- DTX. *See* Discontinuous transmission
- Dual-tone multifrequency, 17
- Duplex service, 90
- EA field-bit. *See* Extension address field-bit
- ECA. *See* Emergency change over acknowledge
- ECO. *See* Emergency change over order
- EIR. *See* Equipment identity register
- EL-bit, 104
- Emergency change over order, 148
- End message, 208, 210, 221
- End-of-optional-parameter, 158, 165
- End-to-end addressing, 163

- End-to-end data control, 44–45
- EO. *See* End-of-optional-parameter
- Equipment check, 227, 233
- Equipment identity
 - register, 7, 31, 37–38, 185, 227, 233
- Error analysis
 - in base station subsystem, 296–302
 - general information, 287–91
 - important messages, 291–96
- Error detection/correction, 43–44, 133–38
- Error indication message, 296
- ETSI. *See* European Telecommunications Standard Institute
- European Telecommunications Standard Institute, 2
- Exchange-identification frame, 57, 70
- Extension address field-bit, 61, 102
- F-bit. *See* Final bit
- FACCH. *See* Fast associated control channel
- Fast associated control channel, 95–100
- FCCH. *See* Frequency correction channel
- FCS. *See* Frame check sequence
- FDMA. *See* Frame division multiple access
- FIB. *See* Forward indicator bit
- Fifty-one multi-frame, 91–92, 97–99
- Fill-in octet, 105–6
- Fill-in signal unit, 127, 130, 134, 137–38
- Final bit, 62
- Fine synchronization, 22
- FISU. *See* Fill-in signal unit
- Fixed mapping, 51–52
- Flag parameter, 60, 105
- Format field, 191
- ForwardAccessSignaling service, 213
- Forward indicator bit, 127, 135–38
- Forward sequence number, 127, 133–38
- Frame check sequence, 43–44, 60, 63, 82, 102, 105, 127, 133, 137
- Frame hierarchy, 90–93
- Frame length indicator, 104
- Frame-reject frame, 57, 69–70
- Frequency allocation, 3
- Frequency correction channel, 95–100
- Frequency division multiple access, 89–91
- Frequency hopping, 20–21
- FRMR. *See* Frame-reject frame
- FSN. *See* Forward sequence number
- Fullrate channel, 28–29, 90
- Gateway mobile switching center, 36, 251
- Gaussian minimum shift keying, 17, 20, 43, 90
- Global System for Mobile Communication, 1–3
 - architecture, 3–4
 - subsystem overview, 4–7
- Global title, 162–63
- GMSK. *See* Gaussian minimum shift keying
- Gray list, 38
- GSM. *See* Global System for Mobile Communication
- H-interface, 32
- Halfrate channel, 28–29
- Handoff, 251
- Handover, 21, 24, 27, 36
 - analysis, 255–56, 294
 - external, 260
 - inter-MSC, 263, 267–69
 - intra-BSC, 257, 260–62
 - intra-BTS, 257–59
 - intra-MSC, 260, 263–66
 - measurement of BTS/MS, 251, 254
 - subsequent, 267, 270–72
 - synchronized/nonsynchronized, 22, 24, 91–93, 256–57, 261, 263
- HDLC. *See* High-level data link control
- Heading code, 142
- Hexadecimal data, 285
- HF. *See* High frequency
- High frequency, 43
- High-level data link control, 43, 56
- HLR. *See* Home location register
- HMI. *See* Human-machine interface
- Home location register, 5–6, 31–35, 130, 185, 202, 205, 221, 244
- Human-machine interface, 20, 86
- Hyperframe, 91, 93
- I-frame, 66–67, 71
- Idle frame number, 97
- Idle phase, 64, 67
- IEI. *See* Information element identifier

- IMEI. *See* International mobile equipment identity
- IMSI. *See* International mobile subscriber identity
- Inactivity test, 162
- Inband signaling, 10, 29
- Information element identifier, 175
- Information field, 105
- Input filter, 22
- Integrated Services Digital Network, 34, 56, 108
- Interfaces, network switching subsystem, 31–32
- Interference, 3, 53, 279
- Interleaving, 100–1, 105
- International mobile equipment identity, 7, 18, 37–38, 227, 234
- International mobile subscriber identity, 191–92, 202, 205, 227
- International Telecommunications Union, 1, 45, 46, 51, 56, 61, 63, 139, 153, 158, 164, 186, 189, 194
- International Telecommunications Union Telecommunication Standardization Sector, 10, 198
- Interworking function, 36, 40
- Invoke component, 205
- IS-95 standard, 89
- ISDN. *See* Integrated Services Digital Network
- ISDN user part, 36, 125, 128, 130, 153, 233, 251
- ISUP. *See* ISDN user part
- IT. *See* Inactivity test
- ITU. *See* International Telecommunications Union
- ITU-T. *See* International Telecommunications Union Telecommunication Standardization Sector
- IWF. *See* Interworking function
- Japan, 3
- LAPD. *See* Link Access Protocol for D-channel
- “Leap,” layer, 47
- Least significant bit, 194
- Length indicator, 196–98
- LFU. *See* Link forced uninhibit
- LIA. *See* Link inhibit acknowledgment
- LID. *See* Link inhibit denied
- LIN. *See* Link inhibit signal
- Line topology, 54
- Link Access Protocol for D-channel, 10, 26, 43–44, 55–57, 211
- frame concept, 56–57
- frame types, 64–70
- layer 2 signaling, 101–6
- layer 3 signaling, 107–23
- message decoding, 70–71
- message parameters, 60–70
- modulo 128 vs. modulo 8, 57–59, 63–64
- vs. LAPDm, 105–6
- Link Access Protocol for D-Channel modified, 101–6, 296
- Link failure, 141–42
- Link forced uninhibit, 150
- Link inhibit acknowledgment, 150
- Link inhibit denied, 150
- Link inhibit signal, 150
- Link local inhibit test, 150
- Link remote inhibit test, 151
- Link status signal unit, 127–28, 130, 132, 134
- Link uninhibit acknowledgment, 150
- Link uninhibit signal, 150
- LLT. *See* Link local inhibit test
- LMSI. *See* Local mobile subscriber identity
- Local error code, 205, 207
- Local mobile subscriber identity, 221–22
- Local operation code, 213–20
- Location update, 45, 227–32
- Logical channel configuration, 94–100
- vs. physical channel, 94
- LRT. *See* Link remote inhibit test
- LSB. *See* Least significant bit
- LSSU. *See* Link status signal unit
- LU. *See* Location update
- LUA. *See* Link uninhibit acknowledgment
- LUN. *See* Link uninhibit signal

- M-bit, 104
- Management message, 142–51
- Mandatory fixed part, 158
- Mandatory variable part, 158
- MAP. *See* Mobile application part
- MAP-CLOSE service, 213
- MAP-DELIMITER service, 212
- MAP-NOTICE service, 213
- MAP-OPEN service, 212
- Mapping, logical channel, 95–100
- MAP-U-ABORT service, 213
- ME. *See* Mobile equipment
- MEAS_REP analysis, 256
- MEAS_RES analysis, 255
- Message discriminator, 73, 75
- Message representation, 10–12
- Message signal unit, 127–30, 134–38, 156
- Message transfer, 135–38
- Message transfer part, 44, 126–27, 153
- Message types
 - air interface, 109–13
 - base station subsystem management
 - application part, 176–84
 - connection principle, 167–69
 - radio link management, 75–80
 - signaling connection control
 - part, 161–67
 - Signaling System
 - Number 7, 127–30, 148–51
 - transaction capabilities application
 - part, 198–200
- Microprocessor, 39
- MM. *See* Mobility management
- Mobile application
 - part, 153, 163–65, 185, 205, 208–9, 285
 - application communication, 220–23
 - local operation codes, 214–20
 - services, 211–14
 - user communication, 209–11
- Mobile application part application, 211
- Mobile equipment, 227
- Mobile originating call, 45, 108, 233–43
- Mobile services switching center, 6
- Mobile station, 5, 14, 17–18, 75, 109
 - handover measurement, 251, 254
- Mobile station roaming number, 244
- Mobile subscriber identification
 - number, 192, 193
- Mobile subscriber ISDN, 244
- Mobile switching center, 6, 31, 34–37, 75, 130, 137–38, 169, 171–73, 185, 227
 - gateway, 36, 251
 - handover, 260, 263–69
 - visitor location register, 36–37
- Mobile terminating call, 45, 244–53
- Mobility management, 7, 17, 44, 104, 108–18, 174
- MOC. *See* Mobile originating call
- Modularization, 39
- Most significant bit, 194
- MS. *See* Mobile station
- MSB. *See* Most significant bit
- MSC. *See* Mobile switching center
- MSIN. *See* Mobile subscriber identification number
- MSISDN. *See* Mobile subscriber ISDN
- MSRN. *See* Mobile station roaming number
- MSU. *See* Message signal unit
- MT. *See* Message type
- MTC. *See* Mobile terminating call
- MTP. *See* Message transfer part
- Multiframe, 91, 97–99
- MYC. *See* Mobile terminating call
- National destination code, 244
- NDC. *See* National destination code
- Network indicator, 130
- Network layer, 44
- Network management, Signaling System
 - Number 7, 138–51
- Network switching
 - subsystem, 31–32, 109, 153, 185, 285
 - location update, 227, 232–33
 - mobile originating call in, 233, 242–43
 - mobile terminating call in, 244, 251–53
 - signaling analysis, 280
- NI. *See* Network indicator
- N(R). *See* Receive sequence number
- N(S). *See* Send sequence number
- NSS. *See* Network switching subsystem

- O&M module. *See* Operations and maintenance module
- OACSU. *See* Off-air call setup
- Octetstring, 194
- Off-air call setup, 226
- OMC. *See* Operations and maintenance center
- OML. *See* Operation and maintenance link
- OPC. *See* Originating point code
- Open System Interconnection Reference Model, 7, 39–40
 - advantages, 42–43
 - comprehension issues, 46–49
 - data types, 41
 - information processing, 42
 - layer 2, Abis-interface, 56–71
 - layer 3, Abis-interface, 71–86
 - layered architecture, 40–41, 43–46
 - protocol stack, 55–56
- Operation and maintenance link, 83–85
- Operations and maintenance
 - center, 22, 27, 72, 276–78
- Operations and maintenance link, 83–86
- Operations and maintenance
 - module, 20, 83–86
- Optional part, 158
- Originating point code, 130–32
- OSI Reference Model. *See* Open System Interconnection Reference Model
- Outage, 140–41
- Outband signaling, 10
- Output filter, 22
- Overload, 67, 89–90, 139–40
- Paging channel, 95–100
- P-bit. *See* Polling bit
- PC. *See* Problem code
- PCH. *See* Paging channel
- PCM. *See* Pulse code modulation
- PC parameter. *See* Protocol class parameter
- PCS 1900. *See* Personal Communication System 1900
- PD. *See* Protocol discriminator
- Peer-to-peer protocol, 41, 209
- Personal Communication System 1900, 2
- Personal Handy Phone System, 2–3
- P/F bit. *See* Polling/final bit
- PHS. *See* Personal Handy Phone System
- Physical channel, 94
- Physical layer, 43
- PLMN. *See* Public land mobile network
- Point code, 130
- Pointer, 158
- Point-to-point connection, 105
- Polling bit, 62–63
- Polling/final bit, 62, 106
- Polling process, 64
- Power control input parameters, 254
- Presentation layer, 45–46
- Primitive, 191–93, 211, 221
- Problem code, 208–9
- Protocol analyzer, 276–79, 287
- Protocol class parameter, 154, 165–66
- Protocol discriminator, 107, 184
- Protocol measurement, 44
 - operations and maintenance center, 276–78
 - protocol analyzer, 278–79
 - tools, 275–76
- Protocol stack, 55–56
- PSTN. *See* Public switched telephone network
- Public land mobile network, 18, 32
- Public switched telephone network, 125
- Pulse code modulation, 9–10, 43, 171
- Pulse code modulation clock, 21
- QOS. *See* Quality of service
- Quality of service, 53, 100–1, 275–76
- RACH. *See* Random access channel
- Radio interface failure, 292
- Radio interface message failure, 292
- Radio link management, 55, 75
 - message types, 75–80
- Radio resource management, 108–10
- Radio signaling link, 73–74, 84
- RAND. *See* Random number
- Random access channel, 95–100
- Random number, 33
- RC. *See* Release cause
- RCT. *See* Route set congestion test
- Ready-to-send signal, 43
- Receive-not-ready frame, 56, 67–68

- Receive-ready frame, 44, 56, 63–64, 66–67, 86, 104, 263
- Receive sequence number, 63, 67–68, 135
- Refusal cause, 166
- Regular pulse excitation-long term prediction, 28
- Reject component, 208–9
- Reject frame, 56, 67–68
- Release cause, 166
- Release complete, 161, 169
- Released message, 161, 169
- Return cause, 166
- Return error component, 205
- Return result component, 205, 208
- RF. *See* Refusal cause
- Ring topology, 54–55
- RLC. *See* Release complete
- RLM. *See* Radio link management
- RLSD message. *See* Released message
- RNR. *See* Receive-not-ready frame
- Route set congestion test, 151
- Route set test, 140–41, 149
- Routing, message, 130–33
- RPE-LTP. *See* Regular pulse excitation-long term prediction
- RR frame. *See* Receive-ready frame
- RR management. *See* Radio resource management
- RSL. *See* Radio signaling link
- RST. *See* Route set test
- RT. *See* Return cause
- RTS signal. *See* Ready-to-send signal
- S-bit, 75
- SABM frame. *See*
- Set-asynchronous-balance-mode frame
- SABME frame. *See* Set-asynchronous-balance-mode-extended frame
- SACCH. *See* Slow associated control channel
- SAPI. *See* Service access point identifier
- SCCP. *See* Signaling connection control part
- SCH. *See* Synchronization channel
- SDCCH. *See* Standalone dedicated control channel
- Sectorized base transceiver station, 24–25, 54
- Segmentation, packet, 44
- Segmenting/reassembling, 166
- Send receive number, 104–5, 127
- Send sequence number, 63, 67–68, 104–5, 127, 135
- Sequencing/segmenting, 166
- Serial configuration, 52–55
- Service access point
 - identifier, 58, 60–61, 71–73, 84, 102, 104, 175
- Service indicator, 130
- Service information octet, 128–29, 139, 156
- Session layer, 45
- Set-asynchronous-balance-mode
 - frame, 46–47
- Set-asynchronous-balance-mode-extended
 - frame, 56, 68, 87, 105
- Short-message service, 18, 71, 104, 107
- SI. *See* Service indicator; Status indication
- SIB, 128–29
- SIE, 129, 132
- SIEMENS, 34, 280
- SIF. *See* Signaling information field
- Signaling technology performance/
 - uses, 8–10
- Signaling analysis, 280
 - automatic, 280–84
 - manual, 284–85
- Signaling connection control
 - part, 27, 125–26, 128, 130, 133, 173–74, 185–87, 189, 196, 211
 - connection identification, 285–87
 - message format, 156–58
 - message types, 158–67
 - tasks, 153–56
- Signaling information field, 130, 156
- Signaling link selection, 130–31, 301
- Signaling link test acknowledge, 151
- Signaling link test
 - acknowledgment, 132, 134
- Signaling link test message, 132, 134, 151
- Signaling point, 125–26, 128, 130, 139–41
- Signaling point
 - code, 130, 132, 159, 162, 164, 285
- Signaling System Number 7, 10, 27, 44, 125–26, 173, 185–86, 251

- error detection/correction, 133–38
- message routing, 130–33
- message transfer part, 126–27
- message types, 127–30
- network management, 138–51
- Signaling transfer point, 125–26, 128, 130, 139–41, 187
- Signed response, 33, 300–1
- SIM. *See* Subscriber identity module
- SIN, 129, 132
- SIO. *See* Service information octet
- SIOS, 128–29, 132
- Skip indicator, 108
- Slow associated control
 - channel, 95–100, 256
- SLR. *See* Source local reference
- SLS. *See* Signaling link selection
- SLTA. *See* Signaling link test
 - acknowledgment
- SLTM. *See* Signaling link test message
- SMG. *See* Special Mobile Group
- SMS. *See* Short-message service
- Source local reference, 154–56, 166, 167, 189, 285
- SP. *See* Signaling point
- SPC. *See* Signaling point code
- Special Mobile Group, 2–3
- Speech compression/decompression, 28–29
- S/R. *See* Segmenting/reassembling
- SRES. *See* Signed response
- SS. *See* Sequencing/segmenting;
Supplementary services
- SS7. *See* Signaling System Number 7
- SSA. *See* Subsystem allowed
- SSF. *See* Subservice field
- SSN. *See* Subsystem number
- SSP. *See* Subsystem prohibited
- SST. *See* Subsystem status test
- Standalone dedicated control
 - channel, 95–100, 105, 251, 294
- Star configuration, 52, 55
- Status indication, 128
- STP. *See* Signaling transfer point
- Subscriber identity module, 5, 13–17
 - ID-1, 13, 15
 - plug-in, 13, 15
- Subscriber identity module card, 300
- Subservice field, 130
- Subsystem allowed, 162
- Subsystem number, 60, 159, 162, 164, 166–67
- Subsystem overview, 4–7
- Subsystem prohibited, 162
- Subsystem status test, 162
- Superframe, 91
- Supervisory frame, 57, 63, 104
- Supplementary services, 71, 107, 123
- Switch matrix, 26
- Synchronization channel, 91–94, 95–100
- Synchronized handover, 22, 24, 91–93
- T-bit, 73, 75
- TA. *See* Timing advance
- TAG field, 190–91, 193–95, 196–98
- TCAP. *See* Transaction capabilities
 - application part
- TCE. *See* Terminal control element
- TCH. *See* Traffic channel
- TDMA. *See* Time division multiple access
- TEI. *See* Terminal endpoint identifier
- Telephone system applications, 40
- Terminal control element, 26–27
- Terminal endpoint identifier, 61, 102, 105
- Testing, network, 138–51
- Test message, 142–43, 147–51
- Test mobile station, 18
- TFA. *See* Transfer allowed
- TFC. *See* Transfer controlled
- TFP. *See* Transfer prohibited
- TFR. *See* Transfer restricted
- TI. *See* Transaction identifier
- Time division multiple access, 89–91, 96
- Time-division multiplexing, 9–10
- Time slot, 90, 93, 100, 277
- Timing advance, 24, 93–94
- TRA. *See* Traffic restart allowed
- Traffic channel, 94, 251, 286
- Traffic restart allowed, 141, 151
- Transaction capabilities application
 - part, 45, 130, 153–54, 185–86, 285
 - addressing, 186–87
 - coding, 189–98
 - GSM messages, 198–208

- Transaction capabilities application
 - part (continued)
 - internal structure, 187–89
- Transaction capability application
 - part, 45, 130
- Transaction identifier, 108–9, 184
- Transcoding rate and adaptation
 - unit, 6, 28–30, 171, 294
- Transfer allowed, 141
- Transfer controlled, 140, 150
- Transfer prohibited, 140, 141, 148
- Transfer restricted, 140, 149
- Transmitter/receiver, 17, 19–21, 52–53, 61, 286, 302
- Transport layer, 44–45
- TRAU. *See* Transcoding rate and adaptation unit
- TRX. *See* Transmitter/receiver
- TS. *See* Time slot
- Twenty-six multi-frame, 91–92
- UA frame. *See* Unnumbered acknowledgment frame
- UDT message. *See* Unit data message
- UDTS. *See* Unit data service
- UI frame, 56, 63, 68–69, 71
- Umbrella cell configuration, 22–24
- UMTS. *See* Universal Mobile Telecommunication System
- Unacknowledged message, 57, 58
- Unit data message, 158, 161, 186, 189, 196
- Unit data service, 161
- Universal Mobile Telecommunication System, 3
- Unnumbered-acknowledgment
 - frame, 57, 69, 105
- UpdateLocation service, 213–14
- Uplink, 29, 73, 94–95, 97, 102, 109, 256
 - synchronization, 93–94
- UPU. *See* User part unavailable
- Urban area, 53
- User part unavailable, 151
- Virtual connection, 156
- Visitor location register, 5, 6, 31–37, 163, 185, 202, 214, 221, 227, 244
- VLR. *See* Visitor location register
- White list, 38
- X-bit, 75
- XID. *See* Exchange-identification frame