# 5

# Second Generation

The second generation (2G) cellular networks were designed as digital instead of analog. The main purpose of the digitalization was to minimize the bandwidth needed for a voice channel to support wide deployment of mobile phones. The emerging digital technologies provided a means to improve the quality of the voice connection by making the voice traffic resilient against any disturbances on the radio channel. Security could also be enhanced by encrypting the digital radio signals. An additional benefit of digital transmission was that it also enabled a straightforward way of transporting data over the cellular network without digital-analog conversions.

## 5.1 GSM

### 5.1.1 Standardization of Second Generation Cellular Systems

The first generation (1G) analog mobile systems were deployed nationally. By the mid-1980s, the concept of mobile telephony had proven to be a viable one. The first generation mobile telephony market covered advanced business users and staff who worked far from their office environments with fixed phones. Mobile telephony supported superior reachability of their users on the road. There were still a few major problems to solve. First of all, being national systems, the mobile telephone networks did not support international travelers, except Nordic Mobile Telephone (NMT) in Scandinavia. Second, the analog networks could not be scaled up for larger numbers of users, as their spectral efficiency was just too low. Further, their terminals were expensive and heavy. When electronic components become smaller, the first hand-portable mobile phones were introduced, which indicated that mobile telephony might also have potential for the consumer market in addition to the business market.

**Global System for Mobile Communications (GSM)** was born as a pan-European cellular system standard [1]. GSM became the leading 2G cellular system. The original aim of GSM standardization was to create a single mobile phone system to cover the whole of Europe. This would be achieved by getting telephone operators in different European countries to deploy compatible GSM systems and creating international **roaming** contracts between the operators. The following goals were defined for the standard:

- Provide network elements and mobile stations compliant to the GSM standard for a large market area. Due to the economies of scale, this was expected to decrease the cost of equipment and network deployment as the initial research and development cost would be shared by a very large number of customers.
- Enable a single GSM user to use the mobile station and GSM subscription in different countries while traveling within Europe.

*Converged Communications: Evolution from Telephony to 5G Mobile Internet*, First Edition. Erkki Koivusalo.
© 2023 The Institute of Electrical and Electronics Engineers, Inc. Published 2023 by John Wiley & Sons, Inc.
Companion website: www.wiley.com/go/koivusalo/convergedcommunications

- Enable connecting a voice call to the GSM user regardless of which country the user is located in and which operator network the phone is currently using. Such a roaming service is provided by the visited operator, which has made a roaming agreement with the home network operator of the user.
- Optimize the usage of radio frequencies reserved for GSM channels and provide the user with high-quality and secure voice and data services.
- Provide services that would be compatible with the fixed public switched telephone network (PSTN) network, especially with the Integrated Services Digital Network (ISDN) standards, which emerged in the 1980s parallel to GSM standardization.
- Enable development of different types of mobile stations such as portable phones, vehicle-based stations, and modems attached to computers.
- Support maritime usage of mobile stations.

GSM standardization was started in 1982, and the service was deployed commercially the first time a decade later, in 1991. The standardization work was started by a new committee of European Conference of Postal and Telecommunications Administrations (CEPT), called GSM (Groupe Spécial Mobile). In 1989, the GSM standardization was moved to a new standardization forum, European Telecommunications Standards Institute (ETSI), which was established in 1988. Currently, the GSM standards are maintained by the 3rd Generation Partnership Project (3GPP) standardization forum. In 3GPP, the GSM radio access network standards are referred to with a new acronym, GERAN (GSM EDGE Radio Access Network), which covers both GSM and Enhanced Data rates for Global Evolution (EDGE) technologies, part of the GSM evolution.

In the beginning of the 1990s, networks compliant to GSM specifications were opened first within Europe, but soon such networks were deployed also on other continents, especially Asia and Australia. In 2008, there were GSM networks in over 200 countries, and the total number of GSM subscribers exceeded 3 billion. At the time of this writing in 2022, GSM networks are still widely supported for low-price entry level phones, building network coverage to sparsely populated areas and supporting telephony for users roaming abroad.

GSM standards had three phases of evolution:

- GSM phase 1 standard was frozen in 1991. The standard specified GSM voice calls, **short messaging service (SMS),** and basic supplementary services, such as call forwarding and network roaming. GSM air interface and SMS were novelties for GSM, but the GSM core network specifications for voice call support were largely based on existing circuit switched technologies such as digital exchanges and the SS7 protocol stack. GSM extended SS7 protocols to cover areas relevant for cellular networks, such as mobility and radio resource management. This made it possible for the vendors to use their existing digital exchange products to support GSM just with additional software packages [2].
- GSM phase 2 standard was frozen in 1995. This version of the standard provided an extended set of supplementary services, such as conference calls, call hold, call waiting, and originating identification presentation (rendering the number of the caller on the GSM phone of callee). Additionally, the specification defined how GSM could be used for transporting data or telefaxes.
- GSM phase 2+ standards were completed by 1997. The release 96 version of the standard specified the **high-speed circuit switched data (HSCSD)** service, and the release 97 version introduced packet switched data support on GSM networks with the **general radio packet service (GPRS)**.

The structure and functions of the GSM system are described in the GSM specifications of ETSI, later adopted by 3GPP. There are more than a hundred technical specifications in the original GSM specification library. The original ETSI GSM specifications are divided into different standard series according to their topics, as follows:

- TS GSM 01: General, GSM terminology and abbreviations
- TS GSM 02: Services provided by GSM system
- TS GSM 03: The functions of GSM network and general descriptions of those

- TS GSM 04: GSM radio interface and protocols
- TS GSM 05: The physical layer of GSM radio interface
- TS GSM 06: Voice coding algorithms used for GSM
- TS GSM 07: Terminal adaptors for mobile station
- TS GSM 08: Interfaces and protocols between GSM base station and mobile switching center (MSC)
- TS GSM 09: Interconnection between GSM network and fixed PSTN network
- TS GSM 11: GSM SIM card, equipment, and type approval of GSM devices
- TS GSM 12: Operation, maintenance, and charging in GSM networks

The listed standardization series covers all GSM standards up to 3GPP standard release 99. This release was the last of the 3GPP releases with a name that referred to the target year for completing the release. During the 1990s, 3GPP tried to produce a set of standards every year, but soon it turned out that completing the standards release within the target year was too challenging. After completing releases 97, 98, and 99, 3GPP published its fourth standards release, named Rel-4. From 3GPP Rel-4 onwards, the GSM standardization series was renumbered. The number of the new standardization series was its original number plus 40; thus, numbers in the range 41–52 were allocated for GSM specifications. Two additional standardization series, 33 and 55, were created for information security aspects.

In addition to these technical standards, the GSM operators had their own agreements, which aim at harmonizing the commercial aspects of joint usage of GSM networks. This agreement framework, known as GSM Memorandum of Understanding (MoU), covers the following topics:

- Deployment of GSM networks
- Telephone numbers used in GSM networks
- Tariffs and pricing of GSM services

### 5.1.2 Frequency Bands Used for GSM

The following frequency areas were reserved globally for GSM systems:

- GSM 900
  - The original GSM 900 standard specified two 25 MHz bands for GSM:
    - Frequency band 890–915 MHz for uplink channel from the mobile station to the base station
    - Frequency band 935–960 MHz for downlink channel from the base station to the mobile station
  - Each of those bands is divided into 125 subbands. GSM dedicates a subband for one single mobile station for only a short period of time known as a GSM timeslot (or burst) and uses a frequency hopping scheme to renew subband allocations for every timeslot. The subbands are numbered as 0 . . . 124.
  - In the later version of the GSM standard, both the uplink and downlink bands were extended with 10 MHz additional bandwidth to the lower end of the original band. These additional bands were divided into 50 subbands, which were numbered as 974 . . . 1023.
- GSM/DCS 1800:
  - DCS 1800 standard was created in the years 1990–1991 and allocated two new 75 MHz bands for GSM:
    - Frequency band 1710–1785 MHz for uplink channel from the mobile station to the base station
    - Frequency band 1805–1880 MHz for downlink channel from the base station to the mobile station
  - Each of those bands is divided into 375 subbands.

Additional GSM 1900 and 850 bands were used in North America, where the global GSM bands were already used for other systems. After the 4G LTE (long-term evolution) technology required more bandwidth than was initially available, the higher GSM frequency bands have in many cases been reallocated from GSM to LTE networks [2].

### 5.1.3 Architecture and Services of GSM Systems

#### 5.1.3.1 GSM Services

The GSM Phase 2 system provides the following services:

- Voice calls within the GSM network or with the fixed PSTN/ISDN network
  - Ordinary voice calls between two subscribers
  - Emergency calls to a local emergency center
- **Short message service (SMS)** between GSM mobile stations. The short message was specified as a message of a maximum 160 characters, written with the keypad of the mobile phone. The short message is forwarded to its recipient via the short message center within the GSM network. In the later versions of the specification, the upper limit of the message length was relaxed, and more advanced ways were specified to deliver different types of content than only plain text.
- Transport of Telefax messages according to International Telecommunications Union (ITU)-T standard T.30 [3]
- Data transport using GSM connection with a maximum speed of 9600 bps toward other data networks:
  - Digital connection from a GSM mobile station to a modem in the edge of the GSM network. The modem converts the data to analog format compatible with PSTN modems, to provide connectivity from a GSM mobile station to a PSTN modem service.
  - Digital connection from a GSM mobile station to the digital ISDN network and an ISDN terminal.
  - Digital connection from a GSM mobile station to a packet switched public data network (PSPDN) and its terminals. The connection to the packet data network can be set up in different ways, either directly or via the fixed telephone network (PSTN or ISDN) using an equipment called packet assembler and disassembler (PAD). The PAD takes care of needed conversions of the packet and circuit switched data (CSD).
  - Digital connection between two GSM mobile stations that use the same GSM network.
- **Supplementary services** related to the voice call. GSM users may make use of the supplementary services by defining how the network shall process incoming or outgoing calls. GSM Phase 2 has the following supplementary services:
  - Presentation of the calling number or connected number [4]
  - Transferring an ongoing call to another party [5]
  - Forwarding the call to another number in different cases such as no answer or the called phone is busy, powered off, or out of the network coverage [6]
  - Queuing of the incoming call and call waiting indication [7]
  - Putting the call on hold, for instance, if the user wants to answer another call or discuss with others before continuing the call [7]
  - Barring of outgoing or incoming calls based on conditions defined for the user's subscription, such as barring of all outgoing calls or barring of international calls [8]
  - Charging indication [9]
  - Multiparty conference calls [10]
  - Closed user groups, which allow any calls between the members of the group but none outside of the group [11]
  - Unstructured supplementary service data (USSD) with which operators can build their own supplementary service messages for operator proprietary services [12]

The availability and pricing of these services for the user depend on the cellular operator as well as user's subscription type. Also, the features supported by the mobile station may limit the supplementary services available. GSM teleservices are briefly listed in 3GPP TS 02.03 [13].

#### 5.1.3.2 GSM System Architecture

GSM system architecture and interfaces were defined in 3GPP TS 03.02 [14]. GSM architecture description was later incorporated to the 3GPP multi-RAT (radio access technology) architecture specification TS 23.002 [15].

The GSM system consists of the following parts, shown in Figures 5.1 and 5.2:

- **Mobile equipment (ME),** which may be a mobile phone or a GSM modem attached to a computer. A GSM mobile phone consists of a radio modem (transmitter and receiver); antenna, microphone, and loudspeaker; display and keypad; and a battery power source. GSM modems typically consisted of a low-level digital signal processing (DSP) unit and an application-specific integrated circuit (ASIC) for higher-level L1 signal processing. Compared to the earlier first-generation phones, the major difference was the smaller size of hand-portable phones, which was achieved with the great progress of electronics and battery technology throughout the 1990s. Such progress also made it possible to introduce separate application microprocessors to the phones, to run software for more advanced applications and user interface functions. When equipped with a SIM card, the mobile equipment is called a **mobile station (MS).**
- **Subscriber identity module (SIM),** which is a smart card used to identify the service subscription of a user. A GSM phone has a SIM card holder. When the card is put into the holder, the contact points on the surface of the card touch the SIM connectors of the phone, allowing the phone to exchange data with the card. The card stores secret data related to subscriber **authentication**. There is also some processing power on the SIM card to run the authentication algorithms and some small applications created with a SIM application toolkit (SAT). SAT was used to create some operator-specific UI applications, but more recently its main purpose has been to support remote update of configuration data within the phone or on the SIM card. While a GSM phone is switched off, the SIM card stores certain pieces of state information (such as the location area and frequencies used in the cell before switch-off) needed when the phone is powered on once again. The SIM card has also limited amount of memory capacity to store phonebook entries or short messages. The SIM card is separate from the mobile station to allow the user to switch the phone while keeping the subscription or change the subscription while keeping the phone. The SIM card can be protected against unauthorized use with a personal identification number (PIN) code, which the user is asked to enter when powering on the phone. The SIM card specification can be found from 3GPP TS 42.017 [16].

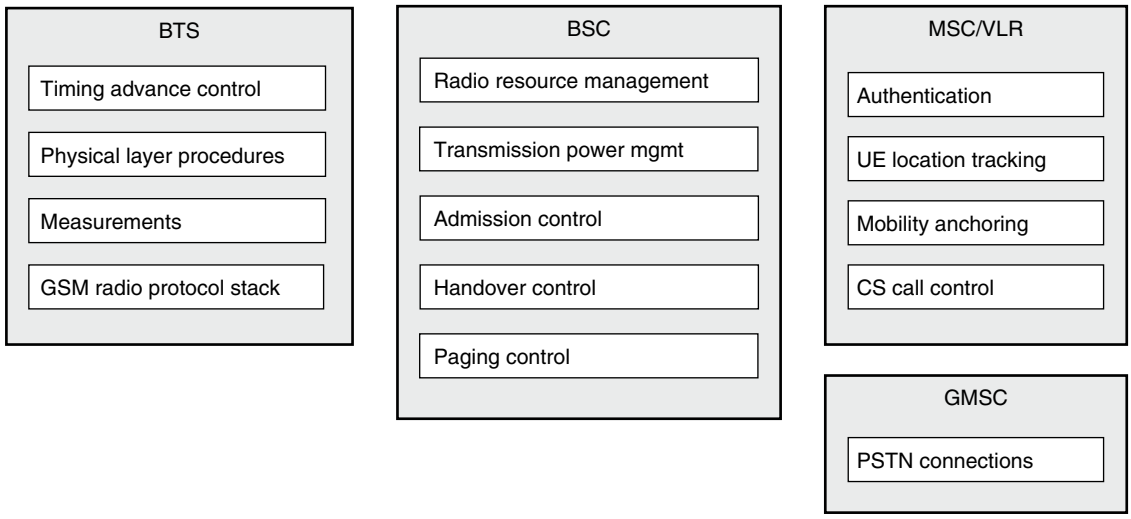


**Figure 5.1** Functional split between GSM network elements.

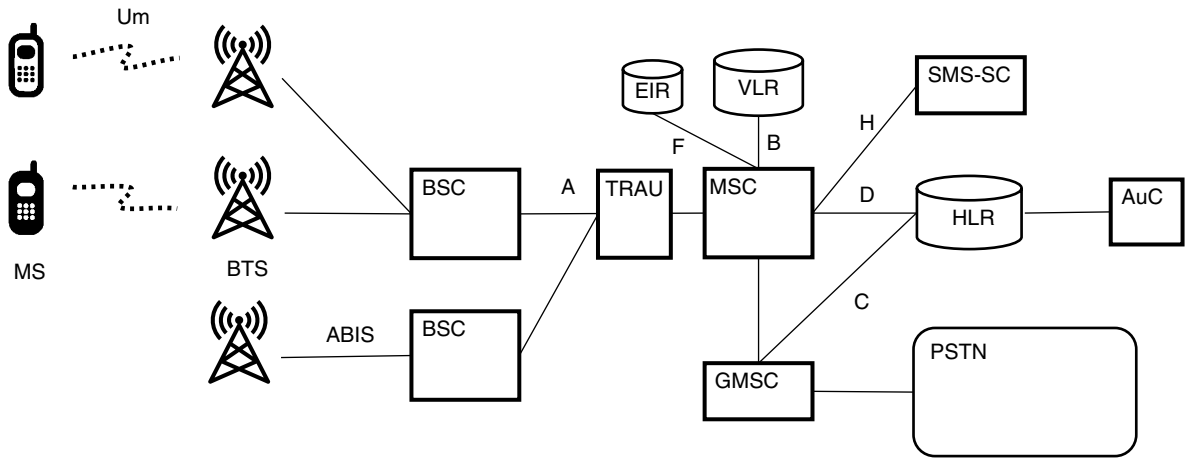


**Figure 5.2** Architecture and interfaces of the GSM system.

- **Base transceiver station (BTS)** is a GSM base station that has radio transmitters, receivers, and the antennas serving the GSM cell. GSM BTS may have 1–16 different **transceivers (TRX)**. A transceiver has a transmitter and receiver working together as a pair. Additionally, BTS has a computer system controlling the BTS functions and a telecommunications link toward the base station controller (BSC). BTS functionality is described in 3GPP TS 48.052 [17]. GSM base stations have the following tasks:
  - Modulation, multiplexing, binary coding, and encryption of transmitted GSM radio signals.
  - Demodulation, demultiplexing, decoding, and decryption of received GSM radio signals in order to retrieve the digital data sent by the mobile stations.
  - Managing GSM radio frequencies, frame structures, and synchronization.
  - Recognizing **random access** requests from mobile stations.
  - Managing **timing advance** of the mobile stations camping in a GSM cell. The correct time of a GSM mobile station for sending GSM bursts depends on its distance from the BTS. When a mobile station is far from the cell tower, the BTS tells it to send it bursts earlier so that they would arrive at the BTS exactly within the expected timeslot at the BTS.
  - Measuring the signals sent by mobile stations and providing the measured values to BSC.
- **Base Station Controller (BSC)** is a network element that controls and coordinates functions of multiple base stations and connects those base stations to the MSC. BSC functionality is elaborated in 3GPP TS 48.002 [18] and TS 48.052 [17]. GSM BSCs have the following tasks:
  - Allocation of radio channels for voice calls. The BSC controls the channel allocation for all the base stations connected to the BSC. The radio channel is allocated as a defined frequency hopping sequence for successive GSM bursts, starting from a given timeslot of the GSM frame.
  - Handover of the call between two base stations when the mobile station is moving. The BSC uses measurements from a number of candidate base stations to select the best one to serve the mobile station for an active GSM call.
  - Management of the transmission power of base stations and the mobile stations served by the base stations.
  - Management of the telecommunications links toward the MSC.
- **Transcoder and rate adapter unit (TRAU)** is a piece of equipment used to convert the 16 bps (or less) voice coding used in GSM systems to the 64 kbps PCM signal used in the fixed PSTN network and vice versa. For downstream, TRAU multiplexes four GSM speech channels into a single 64 kbps timeslot toward the base

station. The GSM standards assume that TRAU would be a part of the BSC, but in practical implementations TRAU is located as close to the MSC as possible, in order to minimize the transmission capacity needed between the BSC and the MSC.

- **Mobile switching center (MSC or** mobile telephone exchange [**MTX**]**)**: GSM MSC takes care of routing and switching calls between mobile phones. GSM MSCs perform the following tasks:
  - Routing and connecting mobile originated and mobile terminated calls, and calling the phone (paging) located under certain BSC when an incoming mobile terminated call arrives for the GSM phone.
  - Control of the call handover if the handover is done between two base stations controlled by two different BSCs.
  - Participating in the location management and user authentication in GSM network when the mobile station registers to the GSM network service.
- **Interworking function (IWF)** is a piece of equipment used to adapt the GSM data connection with an external data network.
- **Gateway mobile MTX (GMSC)** is a special MSC that has to find out which MSC is currently serving a mobile station, which would receive a mobile terminating call attempt. The GMSC connects the mobile terminating call to the right MSC. GMSCs connect the calls to PSTN and control echo cancelers used between PSTN and PLMN due to the long speech coding delay [19].
- **Home location register (HLR)** is a database used in GSM network to permanently maintain information about subscribers, services available for them, related settings, and other GSM networks, which the subscriber is entitled to use. The HLR also knows which MSC/VLR (visitor location register) currently serves the subscriber. HLR ensures that the subscriber information is copied to only one single VLR database at any moment.
- **Visitor Location Register (VLR)** is a database used by a single MSC to store subscriber information about those users who are currently camping on any base station connected to that MSC. The VLR database knows the current location area of the user and has a copy of HLR subscriber data as needed to connect calls to the subscriber. Copying the data from HLR to VLR reduces traffic between MSC and HLR while the MS is located under the area managed by MSC. In cases where the user is roaming abroad, the serving MSC and VLR do not belong to the home network of the user but to the visited network. MSCs in both home and visited network must interact to connect calls to or from the roaming users.
- **Authentication center (AuC)** is a server that permanently stores the secret data used to authenticate users of GSM network. The AuC exchanges authentication data with HLR and VLR databases when a GSM phone with SIM card is powered on and it registers to the GSM network. The AuC also stores the encryption keys used to secure the data sent over the radio interface.
- **Equipment identity register (EIR)** is a database that stores information about the GSM mobile stations. Each mobile station is identified by its unique International Mobile Equipment Identity (IMEI) code. The EIR knows IMEI codes of stolen phones so that they can be blocked for GSM network access.
- **Short message service serving center (SMS-SC)** is a server that forwards GSM short messages between mobile stations. SMS-SC is able to temporarily store the message if the destination mobile station is not reachable or is switched off. The message will be sent when the MS becomes reachable again.
- **SMS-gateway** refers to two types of gateways that contribute to forwarding of short messages:
  - SMS-GMSC has the task to find out under which MSC the target mobile station camps and thereafter forwards the short messages to that MSC.
  - SMS-IWMSC has the task of forwarding the short messages to the SMSC of the short message destination, when the SMS endpoints have different home networks.
- **Billing center (BC)** is a database used for collecting the billing data.
- **Operations and maintenance center (OAMC)** is the GSM network management system.

GSM network has the following subsystems:

- **Mobile station (MS)** is the GSM phone and the SIM card inside of it.
- **Base station subsystem (BSS)** covers BSCs and the base stations controlled by them.
- **Network and switching subsystem (NSS)** has MSCs and the related databases such as HLR, VLR, AuC, EIR, and SMS-SC.
- **Operations and support subsystem (OSS)** is the GSM network management system supporting the following functions:
  - Subscriber management
  - Configuring the network and its parameters
  - Measuring and following up network performance
  - Supervision of different error situations in the network

GSM standards define named **interfaces** between different network elements. Detailed standardization of those interfaces is necessary to make it possible to build networks with elements from different vendors so that those elements are able to interoperate. The most important interfaces of the GSM system, shown in Figure 5.2, are as follows:

- Um: Radio interface between mobile station and base station
- Abis: Telecommunications interface between GSM base station and BSC
- A: Telecommunications interface between BSC and the MSC
- B: Interface between MSC and the VLR database
- C: Interface between GMSC and HLR database
- D: Interface between MSC/VLR and HLR databases
- E: Interface between two MSCs that contribute setting up connections to a certain mobile station, for instance, in an inter-MSC handover scenario
- F: Interface between MSC and EIR database
- G: Interface between two VLR databases
- H: Interface between MSC and SMS-SC
- I: Interface between MSC and mobile station

A standard **protocol stack** is defined for most of these interfaces. The stack is used to pass signaling messages or user data between network elements over the interface. The radio interface relies on protocols specified only for the GSM network while the protocol stacks used on other interfaces are extensions of the stacks defined in ISDN and SS7 protocol specifications. GSM standards also specify how the protocols interoperate when signaling messages are forwarded over a chain of interfaces that use different protocol stacks.

It is worth noting that this interface list corresponds to the traditional GSM architecture. After 3G UMTS was deployed, another option was introduced to connect GSM BSS to Serving GPRS Support Node (SGSN) and MSC via the Iu interface that was used also by 3G RNC (Radio network controller). Both of those architectures are depicted in 3GPP TS 23.002 [15] and the related two protocol stack architectures in TS 23.060 [20].

The following different types of identifiers have been defined in 3GPP TS 23.003 [21] for the GSM subscriber and mobile station:

- **International mobile subscriber identity (IMSI)** is a unique and permanent identifier of a GSM subscriber and the home network. Every SIM card has its own IMSI code, which is different from IMSI codes of other SIM cards.
- **Temporary mobile subscriber identity (TMSI)** is a temporary identifier given for a GSM user by the MSC, which currently serves the subscriber. TMSI is used in the clear text messages sent over the radio interface between the mobile station and the GSM network. TMSI is used to hide the real identity of the user for any third parties who might listen to those messages.

- **International Mobile Equipment Identity (IMEI)** is a unique permanent identifier of the mobile equipment. IMEI is used to block a stolen GSM mobile station from accessing GSM networks and also to ensure that every mobile station model connecting to the network has received a type approval. IMEI code consists of the following parts: the type approval code, the factory which has manufactured the mobile station, and the serial number of the device.
- **Mobile station ISDN number (MSISDN)** is the telephone number of the mobile station (or rather its SIM card) used for creating circuit switched voice or data connections. The international number format has a country code, area or network code, and the subscriber number within the network. The IMSI is a permanent property of the SIM card, but the MSISDN telephone number can be changed if the subscriber wants to have a new telephone number for any reason.
- **Mobile station roaming number (MSRN)** is an ISDN number granted by the VLR to a mobile station when there is a mobile terminated call attempt for the station. The MSRN identifies the mobile station and the MSC currently serving it. The MSC/VLR that has reserved the MSRN number is able to associate the MSRN to the IMSI code of the subscriber. Other MSCs use the MSRN number to route the MT call to the current serving MSC.

Additionally, GSM specifications define the following two identifiers related to the location of the mobile station in the network:

- **Cell global identity (CGI):** Globally unique identifier of a GSM cell and the corresponding base station.
- **Location area identity (LAI):** Identifier for a set of cells under a single MSC. The mobile station shall send a location update message to the network when it moves from one location area to another.

#### 5.1.3.3 GSM Functions and Procedures

GSM system specifications cover three functional areas of interaction between the GSM mobile station and the network:

- **Radio resource management (RR)** for managing the radio connections between a mobile station and the MSC. The RR procedures are not focused on GSM air interface alone. Instead, they also cover interfaces between and among the base station, BSC, and MSC irrespective of the specific transmission technology used on those links. The main tasks of radio resource management are the following:
  - Allocating radio channels between a base station and those mobile stations that have circuit switched GSM connections and releasing the allocated radio channels after disconnecting the circuits.
  - Handover of a circuit switched call between two base stations when the mobile station moves from a cell to another.
  - **Power control** to minimize the transmission power used by mobile and base stations while keeping the quality of received radio signals within predefined limits. The power control mechanism has two purposes: to minimize the power consumption and minimize interference between mobile stations in different cells. Power saving is important for both the operator and the subscriber. Operators want to minimize the base station electricity bills and subscribers want to maximize the idle and talk time for a single charge of the battery.
  - Adjusting timing of **GSM bursts** sent by mobile stations to synchronize them to the frame structure of the base station. **Timing advance** commands align the reception time of bursts from mobile stations to the common timeslot structure from the base station perspective, regardless of the distance of the mobile stations from the base station.
- **Mobility management (MM),** which covers the following tasks:
  - Tracking the location of a mobile station. The main task of the mobility management is to keep the network aware of the location area (and related cells) within which the mobile station should be paged for any incoming mobile terminated calls.

**Table 5.1** Functional areas of GSM.

| | RR | MM | CM |
|---|---|---|---|
| Mobile station | Request radio resources, adjust the transmission power and timing, handovers | Camp to a GSM cell, send location updates | Initiate MO calls, answer MT calls, send and receive short messages |
| Base station | Give commands for timing advance, generate GSM radio frames | – | – |
| Base station controller | Select the base station and radio channel for the mobile station, power control, handover between base stations under a single BSC | – | – |
| Network and switching subsystem(MSC, VLR, HLR, SMSC, AuC) | Handovers between two BSCs | Location information management, user authentication | Connect calls and forward SMS to and from mobile stations |

  - Actions related to cell selection (and reselection when an idle mobile station is moving) by both mobile station and the network.
  - **Security management (SM),** which covers authentication of GSM subscriber and encryption of the traffic sent over radio interface. The information security of the GSM system covers both traffic encryption over the GSM radio interface and hiding the location of the user within the network.
- **Communication management (CM)** takes care of call control, forwarding of short messages, and management of supplementary services. Call control means routing, switching, setup, and release of circuit switched calls.

The devices defined for GSM architecture have the responsibilities described in Table 5.1 related to these three functional areas.

The GSM system elements communicate with each other with signaling protocols to exchange needed pieces of information to perform these tasks. GSM specifications define a set of signaling protocols to be used over the interfaces between the network elements. 3GPP TS 29.010 [22] describes GSM communication procedures and mapping of parameters between messages of different protocols used in the communication path over multiple interfaces.

#### 5.1.3.4 GSM Protocol Stack Architecture

GSM was designed to use layered protocol stacks following the open systems interconnection (OSI) model, according to 3GPP TS 44.001 [23].

On the link layer of Um radio interface, the signaling messages are transported over LAPDm protocol, which is a member of the high-level data link control (HDLC) protocol family. Within the BSS, the link layer uses LAPD protocol, which is another variant of HDLC protocol. Connections between and within NSS up to BSC use the message transfer part (MTP), SSCP, and TCAP protocols of SS7 protocol family [24]. Links between BTS, BSC, and NSS elements are run either over cables or fixed microwave radio links.

GSM radio resource control (RRC) protocol is used over the radio interface between BSC and MS for radio resource management. The BSC uses TS 48.058 [25] protocol to control BTS radio resources. NSS uses base station subsystem management part (BSSMAP) and MAP/E protocols for radio resource management.

Mobile station and MSC are the endpoints for mobility and communication management protocols MM and CM, which are members of the direct transfer application part (DTAP) protocol family. BSS only forwards

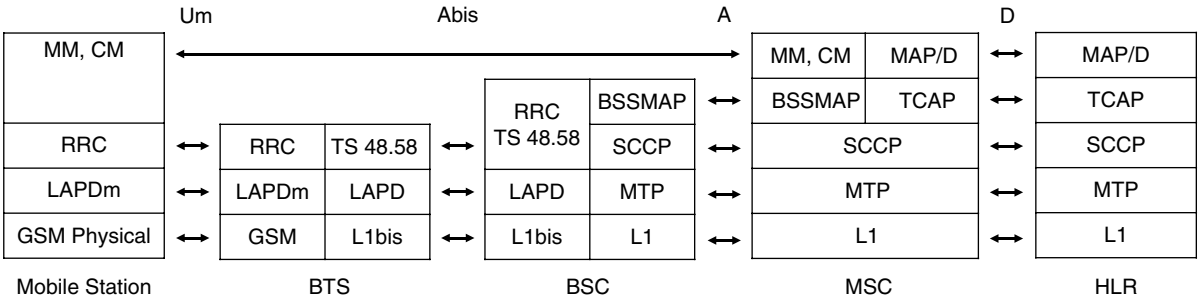


**Figure 5.3** GSM control plane signaling protocols.

messages belonging to these protocols but does not participate in the actual communication. In NSS, the VRL uses SS7 MAP/D protocol to discuss with the HLR database.

The GSM control plane (Figure 5.3) and user plane protocol stacks are further described in 3GPP TS 43.051 [26] and TS 48.008 [27]. For the description of radio resource management, location management, and communication management, please refer to Section 5.1.3.3.

### 5.1.4 GSM Radio Interface

The interface between the GSM mobile station and base station is called GSM **radio interface** or **air interface**. On the lowest physical layer of the radio interface, the GSM protocol stack has GSM radio channels.

GSM radio interface is specified in the 45-series of 3GPP specifications, such as these:

- TS 45.001 [28]: General description covering, for instance, GSM frame structures
- TS 45.002 [29]: Multiplexing and mapping of logical to physical channels, frequency hopping parameters
- TS 45.003 [30]: Channel coding
- TS 45.004 [31]: Modulation
- TS 45.005 [32]: Transceiver requirements
- TS 45.008 [33]: Power control, measurements, cell reselection
- TS 45.009 [34]: Link adaptation

#### 5.1.4.1 Modulation and Multiplexing

GSM uses two different approaches combined for multiplexing radio channels of multiple users over the shared radio media, as seen in Figure 5.4.

1) **Time division multiple access (TDMA):** The GSM frame of 4.62 ms is divided into eight timeslots, 577 µs each. The full-speed voice channel of a mobile station uses only one single timeslot for each GSM frame. In other words, a frame supports eight mobile stations at a time. The uplink timeslots are delayed by three slots compared to the downlink, allowing the devices some time to switch between reception and transmission.
2) **Frequency division multiple access (FDMA):** Each base station divides its available GSM radio band to subbands or radio frequency (RF) physical channels of 200 kHz. The subband is used by one single mobile station for the duration of one timeslot. The GSM cell uses one frequency band for transmission and another for reception. The distance between adjacent uplink and downlink RF channels allocated for one mobile station are always 45 MHz. The specific RF channel pair is identified with its absolute radio frequency channel number (ARFCN). The adjacent cells do not use the same subbands to avoid any intercell interference.

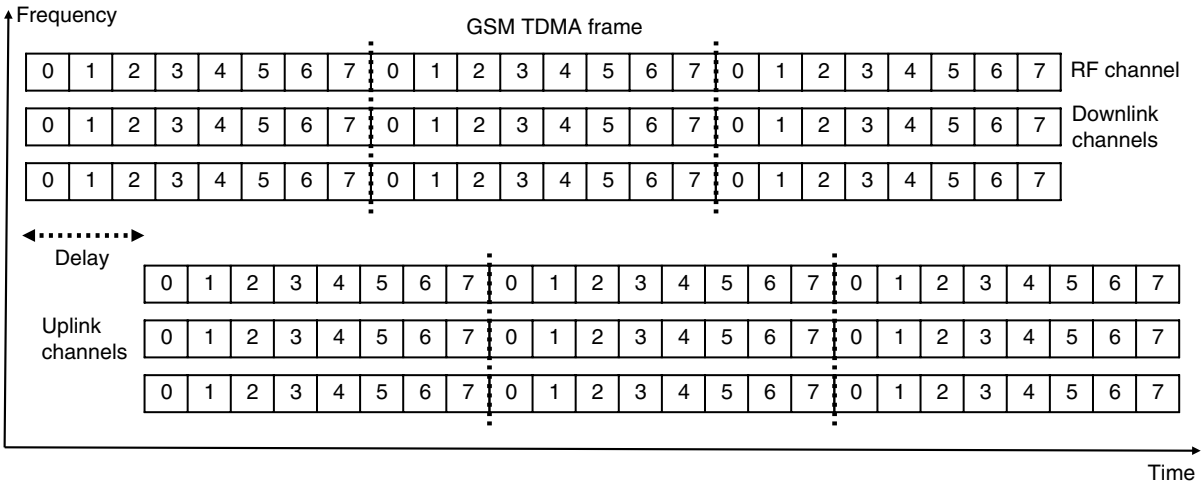


**Figure 5.4** Multiplexing on GSM radio interface. *Source:* Adapted from 3GPP TS 05.02 [35].

Transmission done within one timeslot and subband of the GSM radio interface is called a **burst**. The modulation method for the GSM radio signal is called **gaussian minimum shift keying (GMSK)**, defined in 3GPP TS 45.004 [31]. GMSK is a mathematically complex modulation method where the frequency of transmitted signal is chosen as a function of multiple bits sent after each other. The value of 1 bit in theory impacts a GMSK modulated signal until its end, but in practice the impact is noticeable in the signal generated for transmitting three sequential bits. The benefit of GMSK modulation is that the transmission power is focused to a rather narrow band, which makes it possible to divide the GSM bandwidth to many 200 kHz RF physical channels.

One GSM cell can in theory use 31 subbands, but in practice a cell typically has up to 16 RF channels. The RF channels are reallocated between served mobile stations for every timeslot. Thus, GSM uses frequency hopping radio technology where the mobile station changes its frequency for every burst it sends and receives, once for a GSM TDMA frame. The mobile station knows the RF channels it shall use for its timeslots based on its frequency hopping sequence according to the HSN and Mobile allocation index offset (MAIO) parameters that the MS gets from BSC, as described in Section 5.1.4.4. The hopping sequences are defined in such a way that two mobile stations will never use same RF channel of a cell simultaneously.

As can be seen in Figure 5.5, the TDMA frames of downlink and uplink are not aligned, but there is a difference of three timeslots between them. When a mobile station is given with a channel assigned to timeslot TN3, the transceiver of the station has 1154 ms (two timeslots) to switch between the transmit and receive modes and to tune itself to the correct RF channel.

The number of simultaneous calls within GSM cell is approximately eight times to the number of 200 kHz RF channels allocated to the cell. In practice, the number of simultaneously served mobile stations within the cell is slightly less since certain radio channels are used as shared channels on which common information related to the cell and GSM network, such as **system information** messages, are broadcast to all the mobile stations within the cell. System information messages provide the mobile stations with common network and cell specific parameter values.

#### 5.1.4.2 Frame Structure and Logical Channels

The GSM mobile station has multiple information flows toward the network. To support those flows, a number of logical channels have been defined for the GSM air interface in 3GPP TS 44.003 [36].

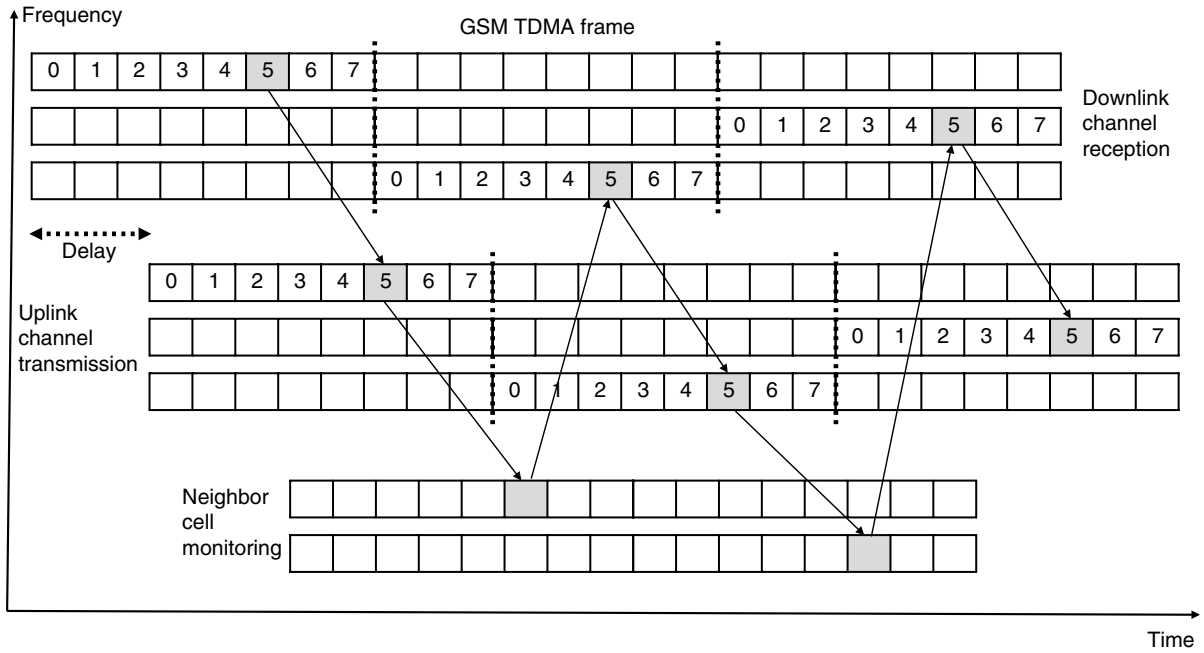


**Figure 5.5** GSM frequency hopping scheme used by mobile station. *Source:* Adapted from 3GPP TS 05.02 [35].

GSM logical channels are as follows:

1) Shared channels used by all mobile stations camping on the cell
   - Broadcast channels (BCH) used by the base station to send commonly used information to all mobile stations within the cell.
     - Frequency correction channel (FCCH): Channel used to transport a fixed sine wave within its every burst. When searching a GSM cell, the mobile station tries to find such a burst pattern in the time-frequency space as used for GSM. After detecting an FCCH burst, the mobile station is able to recover the clock frequency, timeslot boundaries, and the radio frequency used for BCH channels. This enables the mobile station to recognize the synchronization channel (SCH) of the cell.
     - Synchronization channel (SCH): Bursts sent on the SCH help mobile stations to detect the frame structure as transmitted by the base station. After the mobile station has successfully received SCH bursts, it is synchronized to both the timeslot and frame structure of the cell and is thereafter able to decode other channels.
     - Broadcast control channel (BCCH): Channel used to broadcast GSM system information messages to all mobile stations within the cell, to provide them with information about the network, and various control parameter values such as these:
       - The name of the network operator, which is used for the operator selection algorithm of the mobile station
       - The location area to which the cell belongs
       - The frequencies used by the cell
       - The frequencies used by the BCH channels of adjacent cells
       - Information of the common control channel (CCCH) and cell broadcast channel (CBCH) timeslot configuration

- Common control channels (CCCH) are in shared use of all mobile stations within the cell, but without a broadcast mechanism. Only one mobile station may use an uplink channel at a time, and the messages on the downlink channel have the destination mobile station address.
  - Paging channel (PCH): Channel on which the network sends paging messages to a mobile station to notify it about an incoming mobile terminated call. The paging message is sent in all the cells of that location area where the mobile station has most recently sent a location update message.
  - Random access channel (RACH): Channel used by the mobile station to request a dedicated radio connection to initiate a mobile originated call, send a short message, or a location update message.
  - Access grant channel (AGCH): Channel on which the network tells the mobile station about a dedicated radio channel granted to the MS.
- Cell broadcast channel (CBCH): Channel on which special short messages can be broadcasted to all mobile stations synchronized to the GSM cell.

2) Voice or data channels dedicated to one single mobile station
   - Traffic channel (TCH): Voice channel dedicated to one single mobile station at a time. TCH can also be used for CSD transport, depending on the application.
     - TCH/F – full-speed voice channel, which provides 13 kbps speed for voice and 12, 6, or 3.6 kbps speed for data connections.
     - TCH/H – half-speed voice channel, which provides 7 kbps speed for voice and 6 or 3.6 kbps speed for data connections.
3) Signaling channels dedicated for one single mobile station
   - Dedicated control channels (DCCH): Channels used to transport control information between GSM network and one mobile station.
     - Slow associated control channel (SACCH): Bidirectional channel allocated to a mobile station capable of slow exchange of signaling messages. The transmission speed of this channel is on the average sufficient for two messages per second. Mobile stations measure signals received from neighboring GSM cells and use SACCH to inform the network about the measurement results. The network sends timing advance and power control commands to mobile stations over SACCH. It is possible to use SACCH also for transporting short messages.
     - Fast associated control channel (FACCH): Channel allocated to a mobile station capable of fast exchange of signaling messages. FACCH is not a separate channel in the GSM frame structure but it uses the capacity of a TCH channel when no voice or data is sent over that TCH. FACCH is used at the opening and closing phases of TCH when transport of user data over the TCH is not yet started or is already finished. Every burst of a TCH has 2 bits, which tell if the timeslot belongs to the FACCH or whether the TCH carries user data or voice.
     - Standalone dedicated control channel (SDCCH): Channel which the network may allocate to a mobile station when no other user data than short messages have to be transported or for call setup signaling prior to the traffic channel has been allocated for the call. SDCCH is typically used when the mobile station only needs to send signaling messages, such as location updates or messages related to call transfer. The transmission speed of SDCCH is one-eighth of the TCH/F.

Each of the above-mentioned radio channels are implemented as a set of bursts repeating in defined intervals in the GSM TDMA frame structure cycle of eight timeslots, as shown in Figure 5.6.

The bursts sent by mobile stations located at different distances from the base station shall still be received at the base station as aligned to the frame structure of the base station and its timeslots. As propagation of radio signal over distance takes a small amount of time, the base station asks those mobile stations that are farther away to send their bursts a bit earlier compared to the stations closer to the base station, in order to compensate the transmission delay. This timing advance command is sent on SACCH.

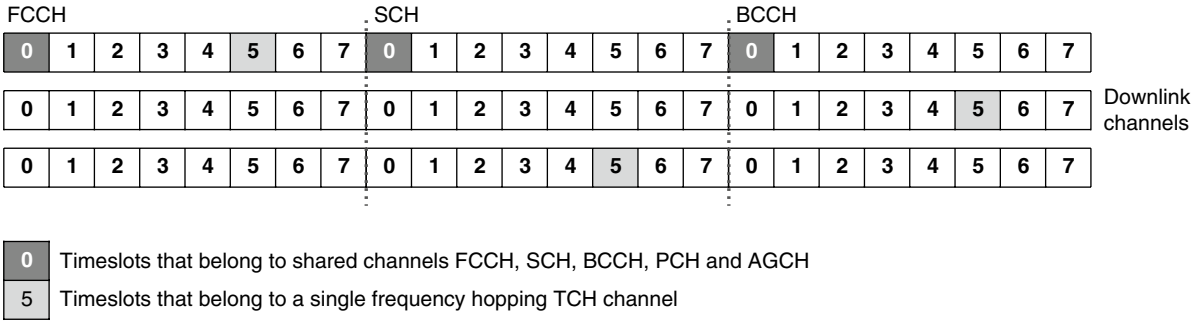


**Figure 5.6** Allocation of GSM physical channels over GSM frame structure. *Source:* Adapted from 3GPP TS 05.02 [35].

The logical channels are mapped to physical channels of GSM frames and RF channels with mechanisms defined in TS 44.004 [37] and 45.002 [29]. The mapping of GSM logical radio channels to GSM timeslots is defined using a concept of GSM **multiframe** and rules about which RF channels the logical channel may use.

- **Shared channels** BCH and CCCH: These channels are transported over one single GSM RF channel of the cell, using the BCCH beacon frequency. No frequency hopping is used. The physical channel mapping of this C0 RF channel is defined within a multiframe consisting of 51 successive TDMA frames, eight timeslot each. The shared channels are transported in the first timeslot TN0 of the TDMA frame. The RACH channel consists of uplink TN0 bursts from the mobile station to the base station. Mapping of the shared downlink channels to TN0 bursts from the base station to the mobile station is as follows:
  - FCCH and SCH channels are composed of one burst per 10 frames in timeslot TN0. Within the multiframe, the first TN0 burst of TDMA frame #0 belongs to FCCH and second TN0 burst of frame #1 to SCH.
  - BCCH is transported in TN0 bursts of frames #2–#5.
  - PCH and AGCH use the rest of the TN0 bursts of the multiframe (except those carrying FCCH or SCH bursts), either up to burst #19 or to the end of the multiframe, depending on the capacity reserved for these channels in the cell. These channels can be divided into multiple subchannels so that the mobile station must listen to only one single subchannel and save its battery while other subchannels are being used. This mechanism specified in 3GPP TS 43.013 [38] is called GSM discontinuous reception (DRX). The mobile station can deduce the subchannel it shall listen to from its own IMSI code.
  - In a cell with large capacity, the structure of the shared channels can be mapped also to other timeslots TN2, TN4, and TN6. Exceptions to this are the FCCH and SCH used for cell synchronization, which may appear only at TN0.
- **Dedicated channels** TCH and DCCH: These channels may be mapped to any RF channel of GSM cell. Frequency hopping is used. The channel structure is defined within a multiframe consisting of 26 successive TDMA frames, eight timeslots each:
  - TCH/F use the bursts #0–#11 and #13–#24 for the timeslot allocated to mobile station. The related SACCH uses bursts #12 and #25. The second burst is not used for GSM transmission, and the mobile station may use it to listen to frequencies used by adjacent cells for their shared channels.
  - TCH/H uses every other timeslot of bursts #0–#11 and #13–#24. The related SACCH uses either burst #12 or #25 of the timeslots used for TCH/H.
- The dedicated SDCCH signaling channel: SDCCH and the associated SACCH may be mapped to any RF channel of the cell. The channel structure is defined within a multiframe consisting of 102 successive frames: SDCCH uses two groups of four bursts within the multiframe of 102 frames (see Figure 5.7). The SACCH related to this channel uses one group of four bursts within the same multiframe. Within the multiframe a total of 12 bursts are needed to carry these two channels for a mobile station. These bursts may be mapped to a timeslot

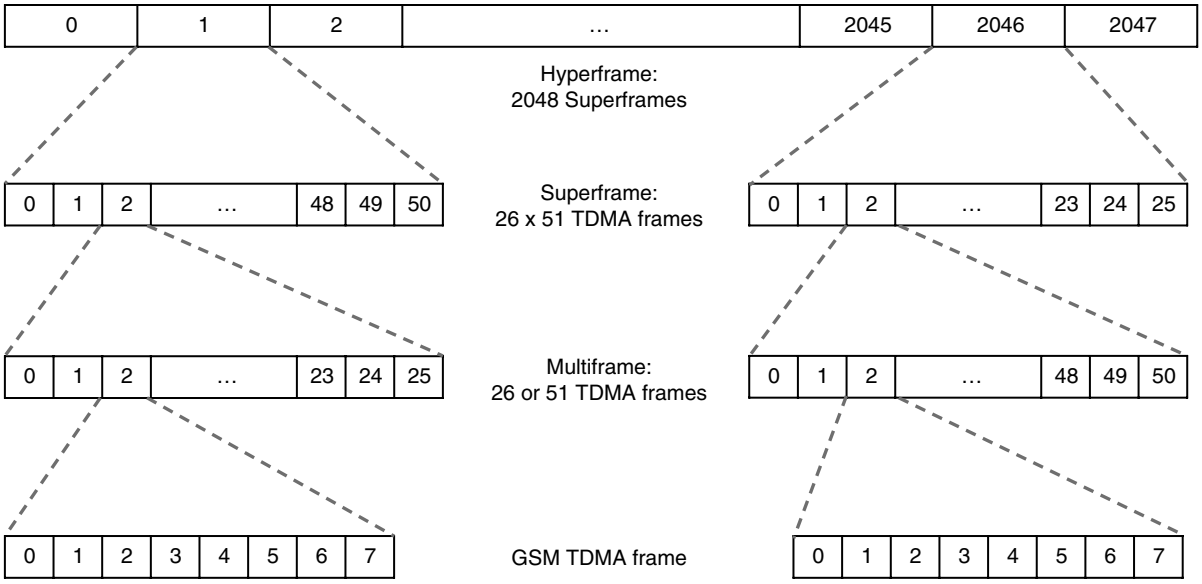


**Figure 5.7** The multiframe structure of GSM radio interface.

that does not carry any other channels or unused TN0 timeslots when PCH and AGCH do not use any timeslots after TN0 #19 of the multiframe.

The lengths of multiframes defined for shared and dedicated channels are different to ensure that a mobile station actively engaged for voice or data connection could measure and detect the synchronization channels of adjacent cells. The fact that the multiframes have different sizes prevents the case in which the burst belonging to the synchronization channel would always overlap with the timeslot the mobile station is using for its traffic.

#### 5.1.4.3 GSM Bursts and Channel Coding

As mentioned in Section 5.1.4, the nominal length of a GSM timeslot is 577 μs. In the beginning and end of the burst, there is a period of 30 ms to ramp the transmission power up and down. Taking that into account, it is possible to send a maximum 148 bits of information within a single burst. The internal structure of the burst depends on the type of the radio channel to which the burst belongs to [28] (see Figure 5.8):

1) On the FCH channel, F-bursts are sent, which contain 148 zero bits. After GMSK modulation, the signal is pure sine wave. The purpose of such a burst is to be very easily recognizable so that a mobile station can easily detect the FCH channel and can thereafter calibrate its own clock frequency to the frequency of sine wave of the F-burst as sent by the base station. The leading and trailing edges of the sine wave burst indicate the boundaries of timeslots within the GSM frame.
2) On the SCH channel, S-bursts are sent with the following structure:
   - In the middle of the burst, there is a predefined constant string of 64 bits called a training sequence. This sequence enables the mobile station to recognize the S-burst and adjust its receiver to compensate for any signal distortion on the radio channel.
   - Both in the front of and right after the training sequence, the burst has 39 bits that describe the BSIC code of the cell and the TDMA frame number.
   - In both ends of the burst, there are three zero bits.
3) On the RACH channel, the length of the burst is only 87 bits. This burst is short because the mobile station that sends a random access burst has not yet received a timing advance command. As the station does not know

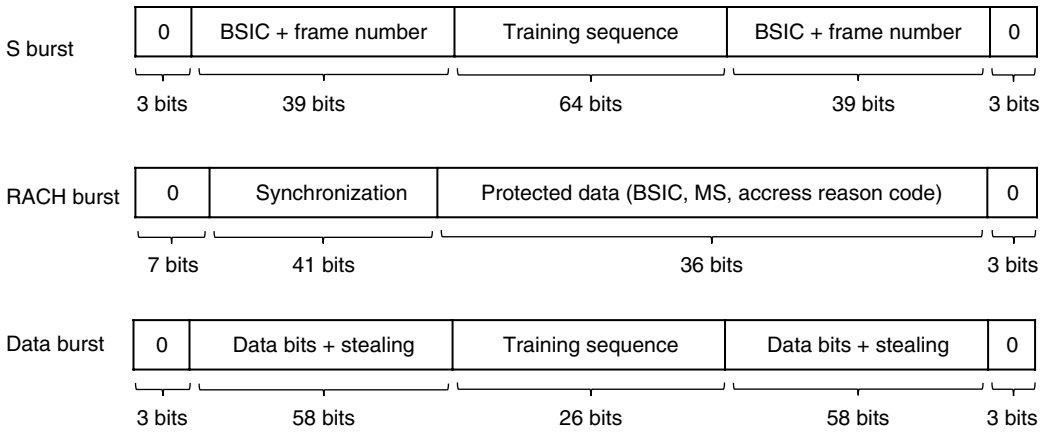


**Figure 5.8** GSM transmission burst types.

how far it is from the base station, usage of a short burst aims at ensuring that the whole burst can be received by the base station within one timeslot. The structure of a random access burst is as follows:

- There are 7 zero bits in the beginning and 3 zero bits in the end of the burst.
- Right after the leading zero bits, the burst has 41 bits with a constant predefined synchronization bit sequence.
- Thereafter, the burst carries 36 bits of protected data. This bit sequence is derived from 8 bits of information, protected with 6 parity bits added bitwise with 6 bits of BSIC code. The result is encoded with 1/2 convolutional code to produce the transmitted data bit sequence. The 8 information bits contain a random bit sequence for identifying the mobile station and a reason code for its random access attempt.

4) Bursts sent on other channels have the following structure:
   - In the middle of the burst there are 26 bits with constant predefined training sequence, helping the receiver to adjust itself to compensate for any distortion over the radio channel.
   - On both sides of the training sequence, there is 1 stealing bit and 57 bits of user data, such as encoded voice. The total number of data bits per burst is 114. Stealing bits are used to distinguish control and data bursts. When the stealing bit is set, the burst belongs to the FACCH rather than the TCH channel.
   - There are 3 zero tail bits in both ends of the burst.

GSM **channel coding** process is used to make transmission of voice and data tolerant against transmission errors. The channel coding process specified in 3GPP TS 45.003 [30] consists of the following steps:

- Block coding
- Convolutional coding
- Interleaving
- Burst generation

In the channel coding process, the user data bitstream to be transmitted is divided into data bursts in the following manner:

1) The bit stream is divided into fixed-size blocks for further processing.
2) Each block is encoded to protect the data against transmission bit errors. The encoding increases the redundancy of data so that the size of the block can be doubled from its original size. Encoding increases the number of data bits in two ways:
   - A cyclic redundancy check (CRC) may be calculated over and added to the original block. The CRC checksum enables the receiver to detect and correct single bit errors.

- The bit sequence of the block can be used to generate a convolutional forward error correction code. Convolutional code may be created from the original bit sequence by combining it with exclusive-or operation with copies of the same bit sequence shifted with one or multiple bit positions. It is also possible to calculate multiple different convolutional codes from the same bit sequence and combine selected bits of each code for the bit stream to be transmitted. In this way, any single bit in the original bit sequence impacts the value of multiple bits transmitted. When decoding the received bit sequence, the redundancy within it helps the receiver to calculate the most probable original data block.

3) The encoded data block is split into shorter blocks, each of which can be transmitted within a burst. A burst may carry either one such block or parts of multiple interleaved blocks for further robustness against transmission errors.

In block coding, the 260 bits from the voice codec are divided into three different priority classes:

- Class I-A of 50 bits protected by 3-bit CRC
- Class I-B of 132 bits not protected by CRC
- Class II of 78 bits

The class I bits are then provided to a convolutional coder while class II bits are provided directly to the interleaver. In a convolutional coder the class I bits are protected with a forward error correction method, which expands the number of transmitted bits to two or three times the number of information bits. After GSM convolutional encoding, 1 information bit affects 4 transmitted bits. The strongly protected class I-A bits carry the most important parameters for voice reproduction, such as higher-order bits of the filter parameters [2].

When the bits generated by convolutional encoder are combined with class II bits, a bit sequence of 456 bits is provided to the interleaver. Those 456 bits can be carried by four GSM bursts, each containing 114 information bits. The basic **interleaving** process is performed as follows: At first the interleaver divides the 456 bits to eight subblocks of 57 bits, so that bits from every group of 8 bits are put to its own subblock. For instance, the first subblock gets bits 1, 9, 17, . . ., 449 of the original sequence. GSM burst is able to carry two of these subblocks. Further on, the bits carried in the GSM burst may be also interleaved to achieve a second level of interleaving.

This kind of channel coding method makes the transmission robust against typical short disturbances on the radio path affecting some narrow areas of frequency. Even if a single burst is corrupted, the convolutional coding can be used to reconstruct the original data bit stream without any retransmissions. The drawback of channel coding is the additional delay caused by both convolutional coding and interleaving processes. The receiver must wait for all the bursts over which the original stream of 260 bits has been spread, before giving the decoded bits to the voice decoder.

GSM standards specify the details of convolutional coding and interleaving processes separately for each type of radio channel and bit rate used. The ways differ from each other in the following respects: the length of the original and encoded blocks, the exact way of calculating the convolutional code, usage of a separate checksum, how the bit stream is divided into bursts, and how multiple blocks of encoded data are interleaved to a single burst.

#### 5.1.4.4 GSM Frequency Hopping

GSM base stations use one single fixed RF channel for the shared BCH and CCCH logical channels. As frequency hopping is not used for the shared channels, the base station has no need to inform mobile stations about its hopping patterns. Also, the cell search algorithm of the mobile station is kept simple as both FCCH and SCH channels stay on a single frequency.

GSM uses **frequency hopping** for TCH, DCCH, and SDCCH dedicated to one mobile station. In frequency hopping, the mobile station changes its operating frequency (subband) always for a new burst, like that shown in Figure 5.5. As the TDMA frame of GSM carries eight different timeslots, the frequency hopping is done per frame so that the frequency is changed for every complete frame. The frequency hopping method has many goals. At first it

decreases the effect of any disturbance source impacting a specific narrow frequency area. It also minimizes interference between two GSM calls running simultaneously. Finally, frequency hopping decreases fading of a channel caused by any obstacles on the radio path, since the impact of an obstacle depends on the radio frequency used.

The frequency hopping sequences given to different mobile stations within a cell must satisfy the following two properties:

- No two mobile stations may use the same RF channel at the same time. Otherwise, their bursts would clash with and corrupt each other.
- To support a maximum number of voice calls per cell, the hopping sequences used in parallel must allocate every available timeslot of every RF channel of a cell to the dedicated channels. There should be no unused available timeslots on any RF channel that a mobile station is unable to use.

The mobile station and base station derive the frequency hopping sequences with a function defined in GSM specifications. This function uses the following three parameters as its input:

- The hopping sequence number (HSN) identifies 1 of the 64 different hopping patterns to be used for picking subchannels for every new burst of the multiframe.
- MAIO defines the RF subchannel, which is used for the first burst of the hopping sequence. The hopping sequence starting times are synchronized within the GSM superframe structure of the cell.

The parameter values are allocated so that every cell has its own value for HSN. Every transceiver of the cell has its own MAIO value, so the MAIO defines one single physical channel per timeslot of the GSM frame. The impact of these parameters to the frequency hopping sequence is as follows:

- Two sequences with different HSN will use the same frequency in 1/n timeslots where n is the number of frequencies used for the timeslot. In practice, this means that two GSM calls in different cells will interfere with each other only occasionally for a single burst.
- Two sequences with the same HSN but different MAIO never use the same frequency for the same timeslot. This means that two calls within a GSM cell will never interfere with each other.

The mobile station learns the value of the HSN parameter and frequencies used by the cell from the system information messages that the BTS sends on the BCCH channel. When a new dedicated channel is given to the mobile station, the BTS tells the MS the values of MAIO and the timeslot number to be used for the channel. Equipped with those pieces of information, the MS knows how to apply the frequency hopping sequence to the given subchannels.

### 5.1.5 Signaling Protocols between MS and GSM Network

#### 5.1.5.1 LAPDm Protocol

The link layer protocol used on DCCH signaling channels is called LAPDm. The LAPDm protocol transports upper layer signaling messages between the mobile station and base station. LAPDm is specified in 3GPP TS 44.005 [39] and TS 44.006 [40].

LAPDm is a variant of HDLC, which was described in Chapter 3, Section 3.1.33.1. The frame structure of LAPDm has been optimized to take advantage of the synchronization and error correction mechanisms of the GSM physical layer. The biggest differences between LAPDm and HDLC protocol are as follows:

- The LAPDm protocol frame is not delimited by start and end markers. Instead, it has been defined that the LAPDm frame is always 23 octets, which is the length of blocks transported on DCCH channels. Depending on the specific channel (SACCH, FACHH, or SDCCH), such a block is transported either within four or eight GSM bursts. In the latter case, the block is interleaved with either the previous or next block. If the size of the upper

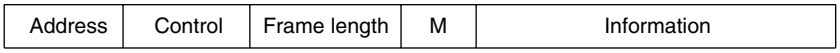


**Figure 5.9** Structure of LAPDm frame.

layer message is longer than what fits in one LAPDm frame, the LAPDm protocol segments the upper layer message before transmission and reassembles it after receiving the related LAPDm frames.

- Unlike the HDLC frame, the LAPDm frame does not contain a cyclical redundancy check since the data block sent over the radio interface is protected by mechanisms of the GSM physical layer. The LAPDm protocol uses the information provided by the GSM physical layer to decide if the LAPDm frame needs to be retransmitted. Retransmissions are not used at all for time critical data, such as radio signal measurements, which only have value over a very short lifetime.
- Size of the LAPDm window for unacknowledged message is one.
- LAPDm protocol does not use flow control commands.

The LAPDm frame shown in Figure 5.9 consists of the following fields:

- Address of one octet tells if the frame is used for signaling messages (service access point identifier [SAPI] 0) or short messages (SAPI 3).
- Control field, which tells the type of the frame that has the same structure as defined for HDLC.
- The length of LAPDm frame together with the more-bit used for segmentation and reassembly function.
- Information field, which contains the upper layer data to be transported over the link.

#### 5.1.5.2 RIL3 Protocols

Three different GSM radio interface layer 3 (RIL3) signaling protocols are used over the radio interface between the mobile station and GSM network. These protocols are members of the DTAP protocol family of SS7:

- RIL3-RR or RRC: radio resource control
- RIL3-MM: mobility management
- RIL3-CC: call control

The RIL3 protocols for MM and CC and the related procedures are specified in 3GPP TS 24.008 [41], and the protocols and procedures for RRC are specified in TS 44.018 [42].

Most of the messages of any RIL3 protocols use the same common frame structure shown in Figure 5.10. This structure consists of the following fields:

- Protocol discriminator as either RR, MM, CC, or some other value defined for other services.
- Transaction identifier, which is used in RIL3-CC protocol to match the response message to the corresponding request message. In the other two protocols, a skip indicator with value 0 is used to indicate that the transaction identifier is not used.
- Message type, which tells the purpose of the message and determines how the rest of the message shall be interpreted.
- The mandatory parameters of the message, which depend on the message type. Since the message type defines also the order and lengths of those mandatory parameters, the message itself contains only the values of those parameters in the predefined order.

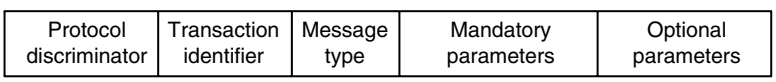


**Figure 5.10** Generic structure of RIL3 protocol frame.

- The optional parameters of the message. For these, the message contains at least the parameter name and value if the length of the parameter is fixed in the specification. For variable length parameters, the message uses the type-length-value (TLV) pattern where the parameter is encoded to the message with three fields: the name of the parameter, the length of its value field, and the value itself.

RIL3 protocol messages are transported over the GSM air interface as payload of the LAPDm link layer protocol.

### 5.1.6 Signaling Protocols of GSM Network

#### 5.1.6.1 Layer 1

Connections between BTS, BSC, and MSC are provided as 64 kbit DS0 channels over E1 or T1 data links. See 3GPP TS 48.004 [43] and TS 48.054 [44]. In addition to signaling, the main purpose of these channels is to carry voice circuits. A single BTS may not need all the channels of an E1 link, but just a subset of them to support the needed voice connections.

#### 5.1.6.2 Layer 2

Signaling messages are transported between the GSM base station and BSC over Abis interface within a dedicated 64 kbit channel. The LAPD link layer protocol is used to carry the signaling messages, as specified in ISDN standards.

RIL3 protocol messages for mobile station are transported as payload of LAPD protocol frames over the Abis interface. Additionally, the LAPD protocol is used to transport base station control messages, which are specified in 3GPP TS 48.058 [25]. The functionality of LAPD protocol is described in TS 48.056 [45].

#### 5.1.6.3 Layer 3

Layer 3 commands between BTS and BSC are defined in 3GPP TS 48.058 [25]. These commands are used to manage GSM channels, radio links, and BTS TRX units.

#### 5.1.6.4 SS7 Protocols

GSM MSC specifications were based on the existing specifications for fixed network switches. Because of that, MSC uses the SS7 protocol stack when communicating with BSC or other switching centers, whether mobile or fixed.

The original GSM design for protocol layers 1–3 was based on delivering MTP protocols of SS7 stack over the E0 channels of the E1 link. In the A interface, the signaling messages between BSC and MSC were transported within a dedicated 64 kbit E0 channel. The link layer protocol is the MTP2 as specified for SS7. In the network layer, the signaling messages are carried with MTP3 and SCCP protocols. The MTP3 protocol is used to manage the chain of links between MSC and BSC and carry the SCCP protocol messages. For detailed descriptions of these SS7 protocols, please refer to *Online Appendix B.1*.

While GSM networks evolved, 3GPP introduced another SS7 over IP (or SIGTRAN) option to replace the traditional MTP protocols of SS7 with an IP-based stack. In this option, point-to-point Ethernet over fiber links (see Chapter 3, Section 3.1.1) are used at the physical and link layer to replace E1 links and MTP1. The functionalities of MTP layers 2 and 3 are replaced in a SIGTRAN solution with the following stack:

- IP protocol is used on the network layer to support SS7 message routing.
- SCTP is used on the transport layer to support reliable transport of signaling messages between endpoints. See Chapter 3, Section 3.3.6 for further details.
- MTP3 User Adaptation Layer (M3UA) protocol was defined to emulate the MTP3 service interface toward the upper layer SS7 protocols, such as SCCP. M3UA is an adaptation layer between the SCTP transport protocol and the original SS7 protocols as specified on top of MTP3.

At the time of this writing, GSM networks being deployed are already relying on the IP option so that the operators can maintain just a single IP-based transport network for all types of their cellular networks.

The SCCP protocol is used as follows:

- The control commands from the MSC to the BSC are transported with SCCP class 0 connectionless service.
- The signaling messages for a specific mobile station are transported to the BSC with SCCP class 2 connected service. The MSC sets up a new SCCP connection for the mobile station when it has to send messages related to a handover or receive location update messages from the mobile station. The lifetime of the connection is limited to the execution of the related procedures.

As its payload the SCCP protocol carries messages of one the following two upper layer protocols:

- BSSMAP: signaling messages between MSC and BSC as specified in 3GPP TS 48.008 [27].
- DTAP: RIL3 signaling messages between MSC and mobile station, forwarded over the BSC.

The SS7 protocol stack is used also for the interfaces B to H within the NSS subsystem. The difference to interface A to the BSS is that within the NSS subsystem the MAP protocol is used as the topmost protocol of the stack. There are many variants of the MAP protocol specified for GSM, called MAP/B to MAP/I, where the letter after the slash means the GSM interface over which the MAP subprotocol is used. MAP protocol is specified in 3GPP TS 29.002 [46].

Within the NSS, the protocols underlying the MAP are as follows:

- SCCP protocol is used to route messages to the correct GSM network element, using SCCP class 0 connectionless service.
- TCAP protocol messages are carried as the payload of SCCP.
- MAP/x protocol messages are carried as the payload of the TCAP protocol. These messages may contain either control information between GSM network elements or signaling messages for the mobile station.

There is no frame structure defined for the MAP protocol. Instead, the frame structure defined for the TCAP protocol is used for MAP. The MAP messages are defined as GSM specific operations (with operation-specific information elements) to be transported within the TCAP protocol frame. The names of MAP messages used later in this book refer to the operation codes used within the corresponding TCAP message.

### 5.1.7 Radio Resource Management

Management of radio resources aims at maximizing the number of GSM users that can be served at the network coverage area with the frequency band given. A dedicated GSM radio channel is reserved for a mobile station only for the duration of the voice or data call. To minimize power consumption and interference, GSM mobile stations should use cells with which they have the best radio connectivity. All this is achieved by the GSM radio resource management.

Radio resource management is the main task of the BSC. The MSC participates in radio resource management only at a handover between two different BSCs or MSCs.

#### 5.1.7.1 GSM Radio Channel Assignment

The GSM mobile station has two different modes related to its state of the network connectivity and usage of radio channels:

1) **Idle mode:** The mobile station in the idle mode has not yet been allocated with any dedicated channels.
2) **Dedicated mode:** The mobile station in the dedicated mode has been allocated with a dedicated channel, such as TCH or SDCCH. The station uses the dedicated channel for signaling, voice, or data call. The station

granted with TCH also uses either slow or fast DCCH for signaling. In addition to using these channels, the mobile station may periodically listen to the FCCH and SCH of any nearby GSM cells to prepare itself for a possible handover between cells.

After being switched on, a GSM mobile station gets into the idle mode as follows: The mobile station searches a GSM network. The station detects the frequencies and frame structures of GSM cell by finding its FCCH and SCH bursts. After **synchronizing** itself to the cell, the station starts to listen to SYSTEM INFORMATION messages sent on the BCCH and CBCH. Eventually, the mobile station starts listening to the paging requests sent on the PCH. The mobile station in idle mode can also send a **random access request** on the RACH channel to request a dedicated channel. The network grants the dedicated channel over AGCH, causing the mobile station to move from idle to dedicated mode.

If the mobile station enters the dedicated mode for a voice or data call, it is granted with a TCH. The TCH is connected to the anchor MSC of the GSM core network, to connect the call to the remote endpoint. In the dedicated mode, the mobile station always has a dedicated signaling channel. If a TCH has been granted, the signaling channel is either SACCH or FACCH. Without TCH, the standalone SDCCH signaling channel is used. In the dedicated mode the signaling channel is connected to the BSC, but the controller is able to forward signaling messages between the mobile station and MSC. As the protocol stacks are different in the interfaces between BSC – MSC versus BSC – MS, the BSC does all the necessary conversions between protocols used on different layers of the stacks.

The mobile station transfers from the idle mode to the dedicated mode over the access procedure, which can be performed due to the following reasons:

1) To initiate a call or send a short message.
2) To receive a call or short message. In this case, the mobile station performs the access procedure after the network has paged the mobile station.
3) To send a location update message.

The following two procedures are depicted in Figure 5.11. The GSM network pages a mobile station for a mobile terminated call as follows:

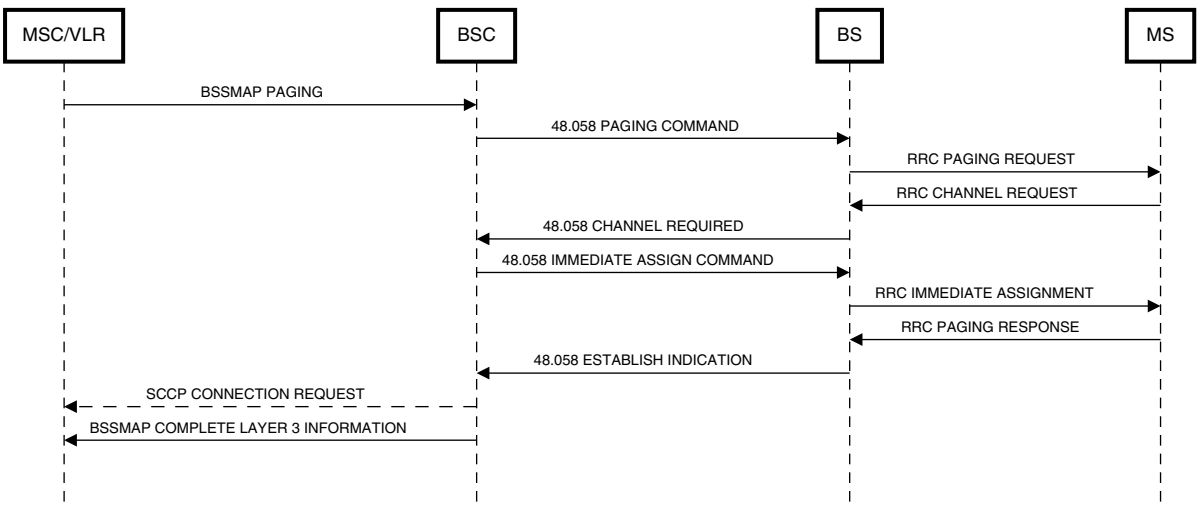


**Figure 5.11** Paging and opening of dedicated channel for GSM MT call.

1) The GMSC, which routes the call attempt to the user, asks the location of the user's mobile station from the HLR database. The HLR tells the GMSC which MSC/VLR currently serves the user.
2) The GMSC sends a connection request to the MSC/VLR switching center, which sends a BSSMAP PAGING message to the BSC serving the user's location area. The message tells the BSC the IMSI identifier of the called user and the user's location area as known by the HLR.
3) The BSC sends a 48.058 PAGING COMMAND message to all the base stations of the location area. This message tells the TMSI identifier of the user and the PCH subchannel used by the mobile station when using DRX.
4) The base station sends an RRC PAGING REQUEST message to the given PCH subchannel to reach the MS. This message contains the TMSI identifier of the called user.

When the mobile station has received a paging request or when the user initiates a call, a random access procedure for acquiring the dedicated channel is performed as shown in Figure 5.11:

1) The mobile station sends a single RACH burst (also known as RRC CHANNEL REQUEST) to the base station. The burst contains only 8 bits of protected information about
   - The reason of the channel request: answering to a mobile terminated call, mobile originated call, emergency call, or location update. Based on the reason, the network can decide whether to accept or reject the request and choose the type of dedicated channel to be provided when accepting the request.
   - A random bit sequence with which the mobile station may recognize the response from the network. When multiple mobile stations try a random access procedure incidentally over the very same RACH burst, there is a collision and the network does not necessarily receive either of the requests. When the mobile station does not receive any response, it shall repeat its access request after a random period.
2) The base station forwards the received access request to the BSC, accompanied with an initial estimate of the transmission delay between the mobile station and base station. The BSC reserves a dedicated channel for the mobile station and informs both the base station and the mobile station about it. With the RRC IMMEDIATE ASSIGNMENT message that the BSC sends to the MS, the BSC tells the MAIO and timeslot number parameters used for hopping sequence control as well as the transmission power and timing advance to be used on the dedicated channel.
3) The mobile station opens a LAPDm signaling link to the base station and sends a request message, the type of which is specific to the reason to go into dedicated mode: MT or MO call, location update, or MS switch off. In case of an MT call, the request type is RRC PAGING RESPONSE.
4) The base station echoes the received request back to the mobile station, which can now compare the received message to the one it has sent. If two mobile stations happened to send the same 8-bit sequence in their random access bursts, only one of them now gets its own request returned. This completes the content resolution process, after which only one of the mobile stations continues using the dedicated channel.
5) The base station forwards the request from the mobile station to the BSC, which sets up a new SCCP protocol connection to the MSC and informs the MSC about the request. The MSC can now authenticate the user and start encryption on the dedicated channel as described in Section 5.1.8.2.

For further details about the messages used in these procedures and various options for the UE to open radio connection, please refer to *Online Appendix I.2.1*.

If the network or the cell suffers from overload, the network may stop the mobile station from sending further random access requests in the following two ways:

- The base station may send an RRC IMMEDIATE ASSIGNMENT REJECT message on AGCH channel. This message denies the mobile station to try out random access during a given period.
- The network may send a request on BCCH channel, which tells a predefined group of mobile stations to not try out random access for any other reason than an emergency call.

#### 5.1.7.2 Changing Channel Type or Data Rate

After the MS has been assigned with a dedicated GSM channel, the network can later change the parameters or the type of the channel in one of the following ways:

1) Change the type of the dedicated channel (SDCCH, TCH/H, or TCH/F). A typical case is that the mobile station was initially given only with a standalone signaling channel but later the mobile station requests a TCH for a voice or data call.
2) Change the bit rate or other parameters of the circuit switched TCH data channel.

Changing the channel type or data rate is done as follows:

- The MSC initiates the change with the BSSMAP assignment request procedure toward the BSC to describe the new characteristics of the dedicated connection.
- Procedures within the BSS depend on whether the channel type is changed or not.
  - To change data rate or other parameters of the channel, BSC uses 48.058 mode modify procedures toward the base station and the RRC channel mode modify toward the mobile station.
  - To change the type of the channel and simultaneously other necessary connection parameters, BSC uses 48.058 channel activation procedures toward the base station and the RRC assignment toward the mobile station.

The process for changing the type of the dedicated channel is a bit more complex than the process for changing other parameters. When the channel type is changed, the signaling is also moved from the old to the new channel. The BSC does not release the old channel until it has received a message from mobile station over the new channel. That message confirms that the new channel has been successfully taken into use. In any error case, the mobile station can stay on the old channel and avoid loss of the connection.

For further details about the messages used in these procedures, please refer to *Online Appendix I.2.2*.

#### 5.1.7.3 Releasing GSM Radio Channel

When a call has been finished or location update has been performed, the anchor MSC will tear down the connection toward the mobile station and release any resources reserved for it. The MS goes back to idle mode. The release procedure is performed as shown in Figure 5.12:

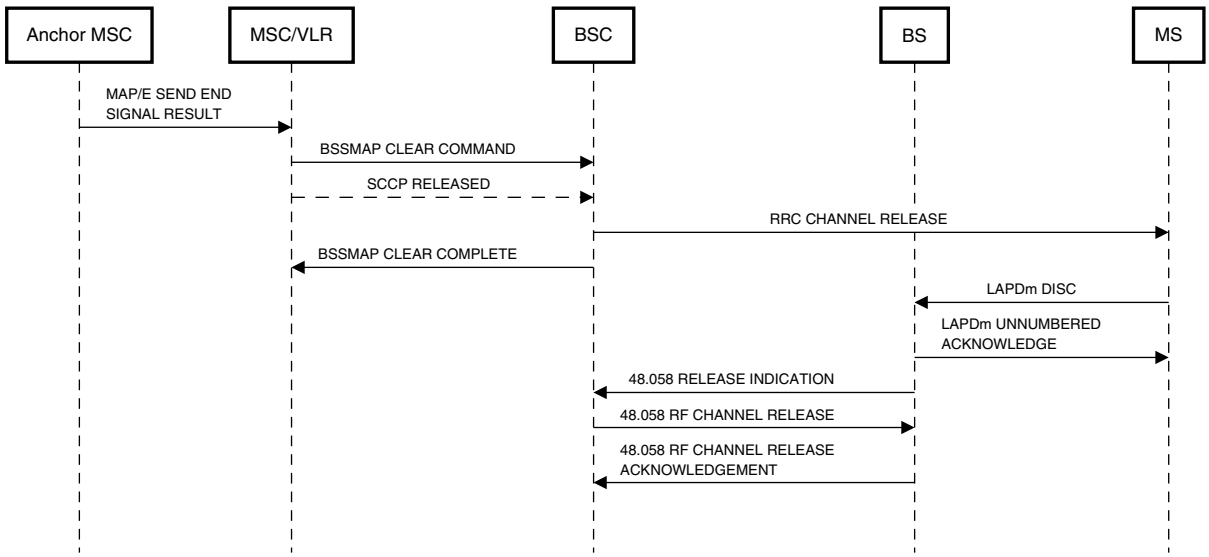


**Figure 5.12** GSM connection release.

1) If the anchor MSC does not directly control the serving BSC, the anchor MSC sends a MAP/E SEND END SIGNAL RESULT message to the MSC connected to the BSC. The anchor MSC releases its circuit switched connections to the mobile station.
2) The MSC which is currently serving the mobile station contacts the BSC and triggers teardown of the SCCP connection. The BSC sends an RRC CHANNEL RELEASE message to the mobile station and releases the SCCP connection toward the MSC after responding to the MSC.
3) The mobile station disconnects the LAPDm signaling link toward the base station. Thereafter, the base station and the BSC release the channels used for the mobile station.

For further details about the messages used in these procedures, please refer to *Online Appendix I.2.3* (Figure 5.12).

### 5.1.8 Security Management

Security mechanisms have been defined in GSM specifications for two different purposes:

- Authentication of the user to ensure that the calls are routed to correct recipients and that the right user is charged for the GSM services used.
- Encryption of the data over the radio interface so that no third parties could eavesdrop on the communication or learn the location of a GSM subscriber.

GSM security architecture and functions are defined in 3GPP TS 03.20 [14].

#### 5.1.8.1 Security Algorithms

GSM specifications define the framework for GSM security but not the detailed algorithms used for security key derivation or encryption. The algorithm specifications were left as a task for the industry, including the network operators and security software vendors.

Both user authentication and data encryption are based on a secret user-specific **master key** Ki, which is stored to two places: the SIM card of the subscriber and the AuC of the network. The Ki key is never exposed outside of these two entities.

Authentication of the subscriber is done and encryption started when a dedicated channel is opened for a location update or a circuit switched call. Consequently, the lifetime of encryption keys and authentication credentials is the same as the lifetime of the dedicated channel. The SIM card and the AuC derive the encryption keys and credentials based on the secret master key Ki and a random number RAND, the latter of which is sent from the network to the mobile station when opening a dedicated channel.

- During the user authentication process, the mobile station uses values of Ki and RAND for algorithm A3 to calculate the SRES authentication code to be returned to the network. The A3 algorithm was not specified in the original GSM specifications, but it was left to be defined by each service provider (or SIM card vendor). The same instance of A3 algorithm shall be used on both SIM card and at AuC.
- The encryption key Kc is calculated with algorithm A8, which is not specified in GSM standards.

The encryption of transported data is done with the A5/1 algorithm, which is defined in the GSM MoU agreement between GSM operators. This algorithm uses the encryption key Kc and the number of the frame being encrypted to produce bit sequences S1 and S2, each 114 bits. The S1 and S2 sequences are used to encrypt and decrypt transported frames. A later version of A5/3 was added in 2002 to support longer frames of GPRS and EDGE networks, described in Sections 5.2 and 5.3. Initially, the security level of the initial GSM security algorithms used was deemed, sufficient but while the processing power of devices increased, it eventually became possible to crack the encryption with reverse engineering and raw brute force trial-and-error approaches.

#### 5.1.8.2 Security Procedures

The MSC/VLR gets the authentication credentials – RAND and corresponding SRES – from the HLR within a MAP/D INSERT SUBSCRIBER DATA message. The MSC/VLR authenticates the subscriber by sending a RIL3-MM AUTHENTICATION REQUEST message to the mobile station. The request contains one of the RAND numbers received from the HLR. The mobile station responds with an authentication response message that contains the SRES code calculated by the SIM against the given RAND. If the SRES number received from the HLR and stored to the VLR database for the used RAND matches with the SRES number received from the mobile station, the authentication is completed successfully.

Encryption is started on a dedicated channel following carefully designed steps to ensure that corruption of any message at a critical moment would not break the connection. This process is as shown in Figure 5.13:

1) The MSC activates encryption by sending a BSSMAP CIPHER MODE COMMAND to the BSC. This message tells which encryption mode to use.
2) The BSC sends a 48.058 ENCRYPTION COMMAND to the base station. This message contains an RRC CIPHERING MODE COMMAND to be forwarded to the mobile station.
3) The base station starts decrypting the information sent by the mobile station on the dedicated channel. The base station then sends an RRC CIPHERING MODE COMMAND message in clear text to the mobile station. If reception of this message fails, the base station continues sending the message until it finds the mobile station to have started traffic encryption on the dedicated channel.
4) After receiving the ciphering mode command, the mobile station starts encryption of the transmitted traffic and decryption of the received traffic from the base station. As the base station does not yet encrypt its traffic, the signaling connection from the network to the mobile station is temporarily lost. The mobile station sends an encrypted RRC CIPHERING MODE COMPLETE to the base station.
5) When the base station receives the first encrypted message and is able to decrypt it, the base station starts to use encryption also for transmitted messages. The base station forwards the RRC CIPHERING MODE COMPLETE message from the MS to the BSC.
6) In the end, the BSC sends a BSSMAP CIPHER MODE COMPLETE message to the MSC. This message tells the MSC that the encryption was successfully taken into use (Figure 5.13).

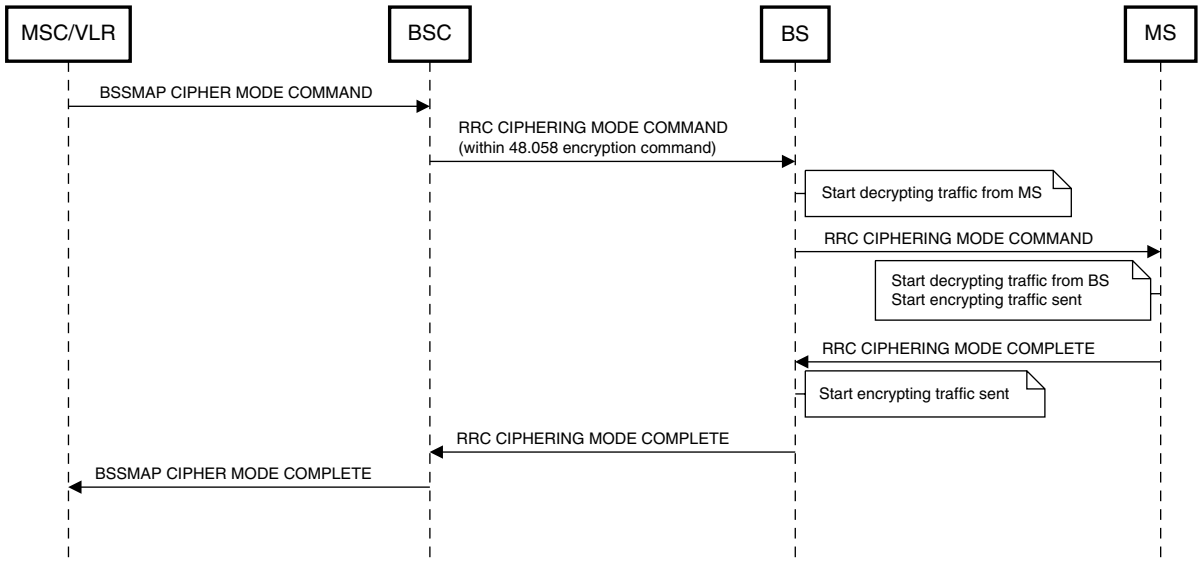


**Figure 5.13** Starting GSM encryption.

#### 5.1.8.3 Hiding The Identity of the User

To prevent external parties from finding out the location of a certain GSM subscriber within the network coverage area, any signaling messages sent without encryption should not contain the IMSI identifier of the subscriber. As GSM encryption is user-specific, the user identity shall be told in the signaling messages before encryption can be started. To solve this dilemma, GSM specifications use a temporary user identity TMSI in cleartext signaling messages. The TMSI is allocated to the mobile station by the MSC after performing subscriber authentication once. The TMSI identifier contains a temporary identifier of the mobile station and the identifier of the location area under the MSC. If the mobile station changes its location area, the new MSC can find it from the old TMSI of the location update message from which the MSC got the IMSI code behind the TMSI. The new MSC sends a MAP SEND PARAMETERS message to the old MSC. After being returned with the user's IMSI, the new MSC can allocate a new TMSI code for the mobile station, to be used under its new location area.

### 5.1.9 Communication Management

#### 5.1.9.1 Mobile Originated Call

To initiate a voice call, the GSM user selects the called number and presses the "send" button of the phone. The mobile station performs random access to get a dedicated TCH channel for the call. After a dedicated signaling channel has been opened, the voice call is set up as shown in Figure 5.14:

1) The mobile station sends a RIL3-MM CM SERVICE REQUEST message to the MSC with random access procedures described in Section 5.1.7.1. This request contains the TMSI identifier of the subscriber and the reason code for requesting a dedicated channel.

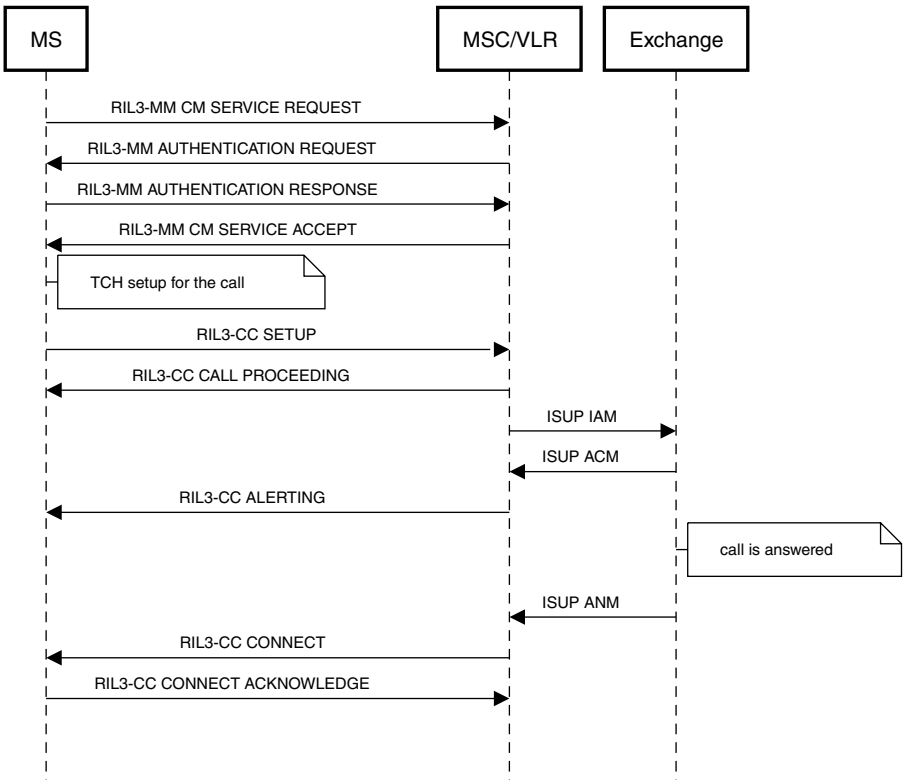


**Figure 5.14** GSM MO call setup.

2) The MSC may thereafter authenticate the user as described in Section 5.1.8.2. After performing the authentication, the MSC may change the channel type as TCH and start encryption on it. Finally, the MSC sends a RIL3-MM CM SERVICE ACCEPT message to the mobile station.
3) The mobile station sends a RIL3-CC SETUP message that contains the telephone number of the callee and some information about the call type (voice or data call). The MSC checks if the request is acceptable and figures out the switching center via which the call must be connected toward the callee. If the MSC accepts the setup request, it sends a RIL3-CC CALL PROCEEDING message to the mobile station and an ISDN user part (ISUP) IAM message to the other switching center to get the call connected.
4) When the MSC eventually receives an ISUP ACM message from the other switching center indicating the target phone to be ringing, the MSC sends a RIL3-CC ALERTING message to the mobile station.
5) When the callee eventually answers the call, the MSC is informed about it with an ISUP ANM message. At this point, the MSC sends a RIL3-CC CONNECT message to the calling mobile station, which responds the MSC with a RIL3-CC CONNECT ACKNOWLEDGE message. Now transport of digitally encoded voice can be started over the dedicated TCH channel and the circuit switched connection established (Figure 5.14).

The MSC may also reject the call due to a number of reasons while the call is being set up:

- The MSC may send a RIL3-MM CM SERVICE REJECT message as a response to the RIL3-MM CM SERVICE REQUEST message, for instance, if subscriber authentication fails.
- The MSC may send a RIL3-CC RELEASE COMPLETE message as a response to the RIL3-CC SETUP message, for instance, if there are no available timeslots for the TCH or if the user is not entitled to call the specific number. The latter case may be due to an agreement with the operator to block calls to expensive service numbers or due to the subscriber activating a call barring supplementary service.
- The MSC may send a RIL3-CC DISCONNECT message after the RIL3-CC CALL PROCEEDING message, for instance, if the called phone cannot be reached, the phone is busy, or if the callee does not simply answer soon enough. After receiving the RIL3-CC DISCONNECT message, the mobile station shall send a RIL3-CC RELEASE message to get a RIL3-CC RELEASE COMPLETE back from the MSC.

#### 5.1.9.2 Mobile Terminated Call

A mobile terminated call is connected to a GSM mobile station as shown in Figure 5.15:

1) The MSC which serves the caller sends an ISUP IAM message, which is routed to the GMSC center of the callee's home network, based on the called MSISDN telephone number. The GMSC has the task to figure out the location of the called phone and continue routing the call setup request toward the right MSC/VLR. The GMSC contacts the HLR to get the MSRN for the subscriber. The HLR knows which MSC/VLR currently serves the subscriber and contacts the MSC to get an MSRN allocated to the subscriber. The HLR forwards the received MSRN number to the GMSC, which uses the information from it to route the ISUP IAM message to the correct MSC/VLR. In the forwarded message, the subscriber is identified with the MSRN number rather than the originally used MSISDN number.
2) When the MSC/VLR receives the IAM message, it sends a BSSMAP PAGING message to the BSC serving the mobile station. With that message, the MSC/VLR requests the BSC to page the mobile station. After being paged and granted with a dedicated channel, the mobile station sends an RRC PAGING RESPONSE to the BSC, which now correlates the RRC message with the paging request. The BSC opens an SCCP connection toward the MSC/VLR, which then sends a RIL3-CC SETUP message toward the mobile station. The mobile station confirms the call and requests a specific type of TCH channel for it. The MSC can thereafter change the type of the existing dedicated channel as described in Section 5.1.7.2.
3) The mobile station starts ringing and sends an alerting message to the MSC/VLR, which informs the calling switching center about the callee being alerted. When the subscriber answers the call, the mobile station sends a RIL3-CC CONNECT message to the MSC/VLR, which informs the calling exchange over ISUP. The digitally

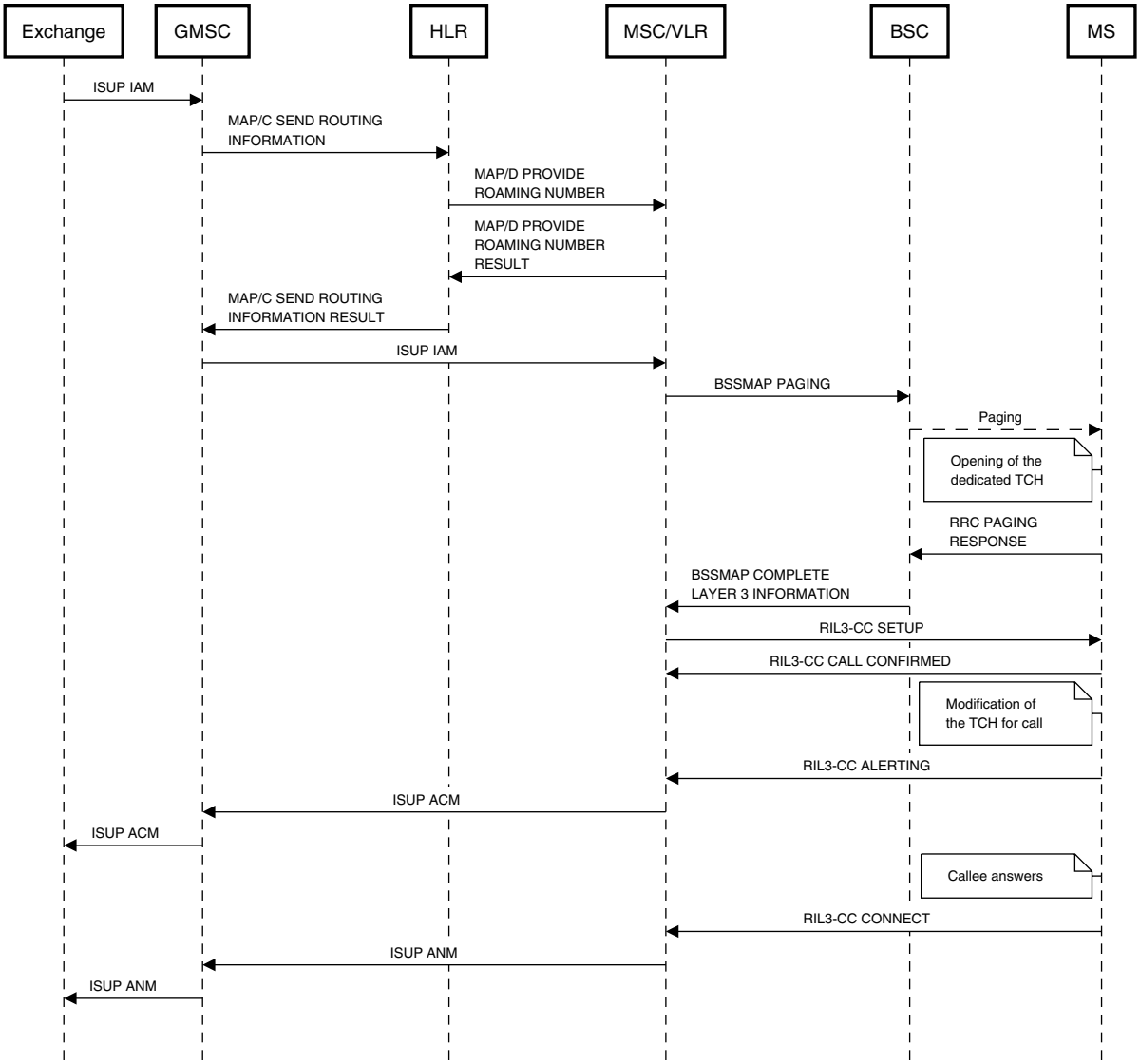


**Figure 5.15** GSM MT call setup.

encoded voice can now be transported over the established circuit switched connection and the dedicated TCH channel assigned to the mobile station.

For further details about the messages used in these procedures and MSRN identifier, please refer to *Online Appendix I.2.4* (Figure 5.15).

#### 5.1.9.3 Call Release

An ongoing call is terminated as follows:

1) When the user of the mobile station ends the call, the mobile station sends a RIL3-CC DISCONNECT message to its MSC. The MSC then sends an ISUP RELEASE message to the other switching center. The call ends and the circuit switched connection is torn down.

2) At the remote end, the mobile station receives a RIL3-CC DISCONNECT message from its MSC.
3) The DISCONNECT message causes its receiver to send a RIL3-CC RELEASE message, which is acknowledged with a RIL3-CC RELEASE COMPLETE message. This message concludes the three-way call termination handshake process.

#### 5.1.9.4 Other Communication Management Functions

The following functions of GSM system are also part of the communications management:

- Changing the channel type between a voice and data call, when necessary. The mobile station initiates the change by sending a RIL3-CC MODIFY message to the MSC, which will change the channel type as described in Section 5.1.7.2.
- Putting the call on hold and removing it from hold with the help of a RIL3-CC HOLD and a RIL3-CC RETRIEVE message.
- Supporting dual-tone multifrequency (DTMF) tones from the keypad of the mobile station. Dual frequency tones would be a rather exceptional use case for GSM voice codecs, causing extra complexity for them. Because of this, DTMF tones are not sent over GSM as audio but instead with signaling messages RIL3-CC START DTMF and RIL3-CC STOP DTMF.
- Managing supplementary services. The mobile station uses MAP/I protocol messages, such as ACTIVATE, REGISTER, or INVOKE, to manage supplementary service settings in the HLR database. These messages are sent within a RIL3-CC protocol messages, such as a RIL3-CC FACILITY message. Other RIL3-CC message types may also be used if the mobile station has also some other needs for using RIL-CC protocols at the same time that it is modifying supplementary service states. GSM supplementary service procedures are defined in TS 23.081 [4] – 23.096 [47], and TS 24.010 [48] provides a generic view about supplementary service control procedures.

### 5.1.10 Voice and Message Communications

#### 5.1.10.1 Voice Encoding for GSM Circuit Switched Call

Voice is transported in digital form over GSM radio connections. GSM systems use several types of **voice codecs** to convert analog voice waveforms to digital formats. The basic process of voice digitalization is the same as used for PCM: taking frequent samples from the voice acoustic waveform captured with a microphone, encoding the values of those samples to digital numbers, sending the numbers to the remote end where they are used to reproduce the sound with a loudspeaker. While the basic PCM is a simple approach to run this process, it is not an optimal way to do the job. A PCM stream requires relatively high data rate of 64 kbps. Further on, the PCM quantization process filters out the frequencies above 4 kHz, so its sound reproduction properties are far from perfect. Better outcome and lower bitrates can be achieved with vocoding techniques, which utilize the specific characteristics of human voice. Vocoding works by dividing a continuous voice waveform to segments of a few tens of milliseconds, matching the segments against predefined voice models, trying to adjust the chosen model with the segment using parameters of the model, and eventually transmitting the resulting parameters to other end where the voice can be reproduced by decoder with the help of models locally stored as codebooks.

A number of standard algorithms have been specified for digital encoding of voice to meet the following goals:

- The audio shall be reproduced well and close enough to the original sound. What is "well enough" is typically measured with **mean opinion score (MOS),** where a number of listeners would rate the quality of audio samples played. Each sample would then get an average score indicating its perceived quality. To reach high MOS score, the voice encoding and decoding process should retain most of the information from the form of the original analog electrical signal from the microphone, regardless of the frequencies within the sound wave.
- The encoded voice stream should need a minimal bit rate to maximize the number of voice connections for a given radio bandwidth.

- Voice encoding and decoding processes must not cause significant latency for interactive end-to-end voice transport.
- The voice codec implementation should consume minimal resources of the GSM phone. Compared to the modern smartphones, GSM phones of the 1990s were really minimal computing platforms. The voice codec software had to work only with a very small amount memory and processing power.

Voice is transported between the GSM mobile station and the TRAU transcoding element in one of the digital formats defined in the GSM standards. The TRAU takes care of conversions between the GSM digital voice encoding and the 64 kbps PCM voice encoding used in fixed PSTN networks. Since the TRAU is typically located at an MSC site, the compact GSM voice encoding methods save transmission capacity within the whole GSM BSS rather than air interface only. Even if the links between GSM base stations and MSC/TRAU would be standard E0 channels used for PCM voice, the GSM network can multiplex four 16 kbps voice connections into one E0 channel. This multiplexing structure is removed at the TRAU so that a single 64 kbps E0 channel from the MSC toward the fixed PSTN or another PLMN mobile network is occupied by a single voice call only.

The GSM phase 1 standard TS 06.10 [49] defined the GSM Full Rate voice codec, which uses regular pulse excitation-long-term prediction (RPE-LTP) encoding algorithm, depicted diagrammatically in Figure 5.16. This algorithm generates a 13 kbits bitstream that can be transported over a GSM full-speed dedicated channel TCH/F. The latest version of its specification can be found from TS 46.010 [50].

The RPE-LTP algorithm groups the taken voice samples to segments of 20 ms. At first, PCM encoding is applied to the samples to encode them into digital form. Thereafter, the digitalized samples are analyzed and encoded

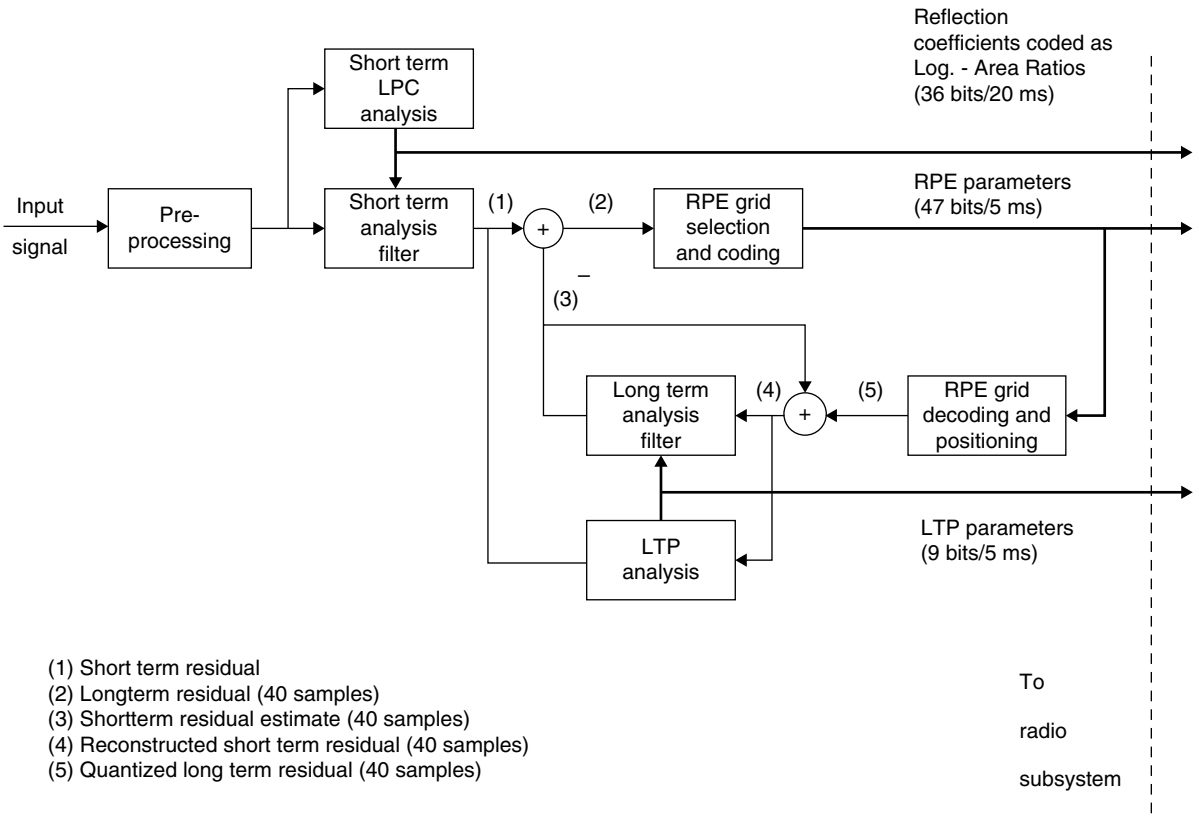


**Figure 5.16** Simplified block diagram of the RPE – LTP encoder. *Source:* 3GPP TS 06.10. Fair use.

with code excited linear prediction (CELP) filtering technology for transmission. For samples taken in 20 ms, the algorithm generates data blocks of 260 bits, to carry dynamic parameters and values created during the encoding process for CELP filters to reconstruct the voice. The CELP technology uses the following approach for voice modeling:

- The vibration produced by human vocal cords can be described by two components: frequency and amplitude. Because the frequency and amplitude of human voice do not typically change very quickly in some unexpected way, it is possible to predict the frequency and amplitude values of the next sample by extrapolating values of a few earlier samples. This approach is called linear prediction coding (LPC).
- The tongue and lips of the speaker modify this basic vibration produced by vocal cords and cause certain non-linear changes to it. CELP technology uses a codebook to encode such changes typical to human voice. Each code of the codebook means a certain waveform pattern. When encoding a voice sample, the codec uses such code of the codebook which makes the voice synthesizer to reproduce voice waveform very close to the original one.

The data blocks encoded with RPE-LTP then carry data about differences of amplitude and phase between voice samples and codebook codes for generating specific voice synthetization waveforms. The amount of encoded data bits is optimized with the long-term prediction (LTP) technique. The stream produced by an LPC filter contains a periodically repeating component, which can be removed from transmitted blocks by the long-term prediction approach. In the receiving end, the removed component can be algorithmically reproduced, rather than using additional data bits to transport the information.

The TCH/F data rate of 16 kbps covers the 13 kbps RPE-LTP bitstream and the following types of additional data items:

- Indicator of the voice codec type used
- Timing and synchronization data of the voice frames
- Currently used DTX mode (ON/OFF)

The **discontinuous transmission (DTX)** method can be used to optimize GSM voice transport. The phone uses **voice activity detection (VAD)** technique to enable DTX. On a typical voice conversation, only one of the parties speaks at a time, so at every moment of the call the voice channel to one of the directions is idle. When the user does not speak, instead of sending voice blocks every 20 ms, the phone sends samples encoded from the background noise more infrequently. Only 0.5 kbps bitrate is needed to send such comfort noise samples to avoid the remote user believing that the voice channel has been dropped. Since GSM uses bidirectional TCH, the DTX method does not save any air interface or transport capacity but it has the following other benefits:

- Longer effective voice call time with one battery charging cycle
- Minimization of the interference level of the GSM system

The GSM phase 2 standard TS 06.20 [51] defined the GSM Half Rate voice codec using vector sum excited linear prediction (VSELP) algorithm. VSELP generates a 6.5 kbps bitstream that can be transported over the half-speed dedicated channel TCH/H. VSELP is a variant of the CELP algorithm with an improved way of using codebooks. The GSM 06.20 VSELP codec generates a block of 112 bits every 20 ms. The latest version of the specification can be found from TS 46.020 [52].

GSM Enhanced Full-Rate (EFR) is a codec evolved from the original GSM Full Rate coded. GSM EFR uses the algebraic code excited linear prediction (ACELP) technique, which is able to use a very large codebook. GSM FER produces a 12.2 kbps bitstream. As further enhancement, the AMR encoding defined for 3G networks as described in Chapter 6, Section 6.1.11.1 has been used also in GSM networks with GSM Phase 2+ release 99.

The full and half rate speech processing functions are currently described in 3GPP technical specifications TS 46.001 [53] and TS 46.002 [54], respectively.

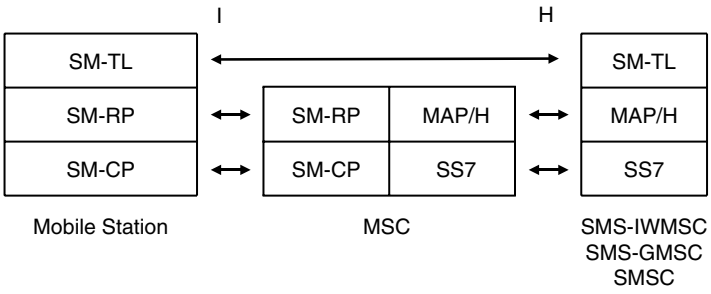


**Figure 5.17** GSM short message protocols.

#### 5.1.10.2 Short Messages

As described earlier, short messages are transmitted between GSM mobile stations and base stations on SACCH or SDCCH, over the SAPI3 link of the LAPDm protocol. The following nested protocols and layers specified in 3GPP TS 23.040 [55] and TS 24.011 [56] are used to transport short messages between a mobile station and the MSC:

- The Short Message Control Protocol (SM-CP) supports sending one SM-RP message between the MS and the MSC. The SM-CP also supports message acknowledgments and retransmissions.
- The Short Message Relay Protocol (SM-RP) provides the MSC with the SMSC address and reference number to identify a specific short message among multiple ones in transit. The SM-RP implements the protocol service for the SM-RL layer.

There are two layers related to SMS service, as shown in Figure 5.17:

- The short message relay layer (SM-RL) protocol provides support for transporting short messages within SM-TL packets between mobile stations and an MSC. The SM-RL RP message contains the addresses of the SMSC short message center and the mobile station between which the SM-TL message is relayed. The MSC uses the SMSC address to communicate with the correct SMSC with the MAP/H protocol.
- The short message transfer layer (SM-TL) protocol provides support for sending and receiving one short message or SMS receiver report at the time. The SM-TL protocol is run between the mobile station and the SMS center or gateway. The SM-TL uses SMS reference numbers to identify short messages within parallel SM-TL transactions.

Between the mobile station and the base station, the above-mentioned protocol messages are carried by the LAPDm protocol while the LAPD protocol is used between the base station, BSC, and MSC on the link layer. Between the MSC and SMS-gateway, the SS7 protocol stack is used. The MSC exchanges SM-TL messages with the gateway or SMSC over MAP/H protocol.

Sending a short message from a mobile station to another is done as shown in Figure 5.18:

1) The mobile station sends the short message within a SM-TL SMS-SUBMIT message. This message is encapsulated into a SM-RL RP-MO-DATA message sent to the MSC.
2) The MSC forwards the SM-TL short message to an SMS-IWMSC, which routes the message to the correct SMSC based on the MSISDN number of the short message recipient. The SMSC sends the short message to the SMS-GMSC that serves the SMS recipient.
3) The SMS-GMSC sends a MAP/C SEND ROUTING INFO FOR SHORT MESSAGE request to the HLR of SMS recipient. The HLR returns the address of the MSC/VLR that currently serves the SMS recipient. The SMS-GSMC sends the short message onwards to the MSC/VLR, which forwards the short message to the destination mobile station and receives back an SMS reception acknowledgment.

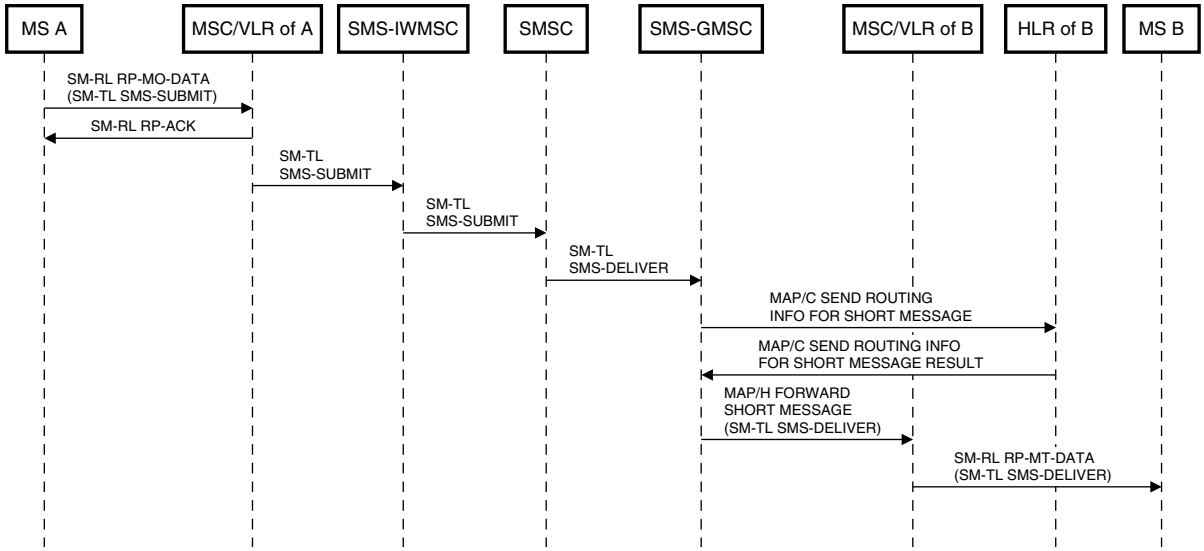


**Figure 5.18** GSM SMS.

For further details about the messages used in these procedures, please refer to *Online Appendix I.2.5* (Figure 5.18).

If the mobile station of the SMS recipient is not reachable, either the HLR or MSC returns a negative acknowledgment to the SMS-GMSC for its MAP request. This causes the SMS-GMSC to inform the SMSC about the MS status. In such a case, the SMSC stores the short message so that it can be sent to the MS once it becomes reachable. The fact that there is a short message waiting for the MS is also stored into the HLR.

Later on, the mobile station registers back to the GSM network by sending a location update message to the MSC. The MSC checks if the mobile station has changed its location area. If it has, the MSC sends a MAP/D UPDATE LOCATION to the HLR; otherwise, it sends a MAP/D NOTE MS PRESENT to the HLR. As the HLR now becomes aware that the mobile station is reachable again, the HLR sends a MAP/C ALERT SERVICE CENTER message to the SMS-GMSC, which informs the SMSC accordingly. The SMSC completes the delivery of short message to the mobile station as described above.

### 5.1.11 Data Connections

#### 5.1.11.1 Circuit Switched Data

Support of circuit switched GSM data has become obsolete with the introduction of packet switched GPRS technology, which is described in Section 5.2.3. The description of GSM CSD methods within Section 5.1.11 has only historical value. If the reader is not interested in such aspects of GSM evolution, the whole section could be skipped.

The original GSM Phases 1 and 2 standards supported only CSD over a single GSM TCH channel. The options for data transmission rate were 300, 600, 1200, 2400, or 9600 bps with a dedicated half- or full-speed channel. These data rates were on par with the data rates of early analog modems used within PSTN. When faster modem types were introduced in the 1990s, GSM CSD data rates fell behind.

The GSM Phase 2+ standards defined a new approach to reach higher data transmission rates up to 57.6 kpbs. GSM HSCSD used up to four GSM full- speed channels for a single data connection. The 144CC encoding method produced 14.4 kbps bitrate per timeslot; hence, 57.6 kbps rate could be reached with four timeslots. HSCSD is specified in 3GPP TS 22.034 [57] and TS 23.034 [58].

As described earlier, a GSM TDMA frame consists of eight timeslots. While voice call uses one single timeslot only, HSCSD reserves two to four timeslots from the GSM frame for a data connection. If more than two timeslots are used, the radio modem of the mobile station must be capable of simultaneous transmission and reception. It is also possible to reserve different numbers of timeslots asymmetrically for uplink versus downlink or change the number of the used timeslots dynamically while data is transported over the connection. The data streams transported over different timeslots are combined to a single stream at either the BSC or IWF. From the merging point onwards, the whole data stream is transported over a single 64 kbps E0 timeslot available in PSTN. The BSC must be able to perform a cell handover simultaneously for all the timeslots belonging to a single HSCSD data connection.

When setting up a HSCSD connection, a mobile station describes the needed transmission capacity and acceptable channel coding methods in a RIL3-CC SETUP message sent to the MSC. The MSC confirms the transmission resources reserved within the RIL3-CC CALL PROCEEDING message sent back to the mobile station. The BSC reserves the needed timeslots from the base station and sends an RRC ASSIGNMENT COMMAND message to the mobile station. After taking the reserved timeslots into use, the mobile station sends an RRC ASSIGNMENT COMPLETE message to the BSC to confirm the setup of the HSCSD channel.

#### 5.1.11.2 Data Connectivity to External Data Networks

GSM data services have been designed to provide data connections from GSM mobile stations to external data networks. User data transport between two GSM mobile stations was an exceptional case, which the GSM standards do not specifically consider.

The data service provided by GSM was evolved from ISDN, which was specified on parallel with GSM in the 1980s. The aim was to support compatibility between GSM and ISDN so that both of those types of terminals could be connected to the same remote endpoints. When GSM was specified, it was expected that ISDN networks would gradually replace the traditional circuit switched PSTN networks. However, that did not eventually happen due to the strong adoption of IP packet-based technologies from the 1990s onwards. The main differences between ISDN and GSM come from the properties of GSM air interface:

- The transmission speed of one full-speed voice channel in GSM is just one- fourth of the 64 kbps speed as used for the basic rate ISDN transport channel.
- The transmission latencies are longer in the GSM network compared to the ISDN network.

As GSM has primarily been specified for voice, data adapters must be used on both the ends of the GSM connection. Adapters convert data formats as used on the external data networks and local computers connected to GSM terminals to formats usable over the GSM channel. The two types of adapters specified for GSM can be implemented as separate devices or functions of the mobile station or another GSM network element:

- Terminal adaptation function (TAF): An adapter connected to or inside of the mobile station, used to convert the data stream from a computer or telefax into a format used over the GSM channel.
- IWF: An adapter used at the edge of the GSM network to convert the data from a GSM channel to a format of an external data network.

The GSM data channel transports both the user data and adapter control data between the TAF and IWF functions. From the perspective of a GSM data user, the TAF and IWF functions are like external data modems used over traditional PSTN PCM audio channels.

Original GSM specifications defined a number of adaptation function types to interconnect GSM data with different types of external networks commonly deployed in the 1980s:

1) Connecting a GSM data flow to an audio modem via traditional fixed PSTN telephone network. During the 1980s and 1990s, audio modem connections to modem pools of universities and enterprises were the most common networking use cases for users of fixed PSTN networks. GSM was also expected to provide

connectivity between the audio modems at customer premises and behind the PSTN network. The setup used two conversion points: TAF was used to adapt the signal from the user's computer to the GSM channel and IWF to adapt the signal from the GSM channel to a PSTN PCM audio link of 64 kbps. In the original GSM specification, it was defined that IWF had to provide modem functionality as specified by CCITT for 300–9600 bps transmission speeds. The GSM connection between TAF and IWF adapters had to be able to transport both the user data and the control information between the remote data modem and the local computer connected to TAF over a serial interface. GSM adapters took care of conversions between synchronous GSM connections and asynchronous modem connections in cases where the clock frequency used for modems did not match with the GSM clock frequency.

2) Transmission of a telefax over a GSM connection to reach a remote telefax equipment connected to the PSTN network. Analog modems were also used for delivering telefaxes transported over the PSTN. At the mobile station, the TAF adapter shall be connected to a separate fax adapter when using an external telefax equipment with an integrated analog modem. In such a setup, the fax adapter and TAF would convert the audio signal from telefax to digital GSM format. A more straightforward setup would be to use telefax equipment with an integrated GSM mobile station rather than an integrated audio modem. Telefax data is transported over GSM to the IWF, which converts the data with its audio modem to the form used by remote telefax equipment.
3) Connecting GSM digital data to digital ISDN network. As the GSM channel speed is smaller than that of ISDN channel, a transmission rate adapter (RA) as specified in ITU V.110 is used for such a connection.
4) Connecting GSM data to a circuit switched public data network (CSPDN). The data connection is set up from the GSM network to CSPDN either directly or via the ISDN network. The mobile station uses the X.21 protocol for connecting to the CSPDN, while the GSM network uses a standard X.30 mechanism for transmission rate adaptation.
5) Connecting GSM data to a public X.25 packet data network (PSPDN):
   - Analog modems were used to create connections to X.25 packet data networks over PSTN. In the packet data network, the connection was supported using either a packet assembler disassembler (PAD) device, which composes the packets with X.28 protocol, or a packet handler (PH), which only forwards packets following the X.32 format from the mobile station to the packet data network.
   - The connection to the packet data network was created over the ISDN network using the X.32 protocol toward a packet handler in the PDN.
   - The connection to the packet data network was created directly from the GSM network so that the user does not need to select a telephone number within PSTN or ISDN networks for PDN connection. The communication between the mobile station and a PDN is done using either X.28 or X.32 protocols.

#### 5.1.11.3 Data Transport within the GSM Network

Two different modes have been specified for GSM CSD transport: transparent and non-transparent:

- Transparent (T) mode could be used for real-time data flows with reasonable tolerance for errors. Transparent mode does not use error correction or retransmissions, but it provides a fixed transmission rate and latency. Data from upper layer protocols is transported as such over transparent mode connection.
- Non-transparent (NT) mode uses RLP protocol, which supports error checking and retransmission of corrupted data. The retransmission mechanism causes some variable delay for the data stream. To maximize the capacity available, the non-transparent mode may even drop upper layer error checksums from the packets and use only its own error correction mechanisms. Non-transparent mode was supported only for the following two upper layer protocols understood by TAF and IWF:
  - Asynchronous character-oriented protocol, where there is start and end bits around each character
  - LAPB protocol used in the context of X.25 packet networking

The RLP protocol of non-transparent mode was specified in 3GPP TS 24.022 [59]. RLP protocol is a variant from the HDLC protocol. RLP segments the upper layer protocol frames to blocks of 200 or 536 bits. Checksum is calculated for

each block, and it can be used either for controlling retransmissions or forward error correction. The size of an RLP frame is either 240 or 576 bits, and it contains user data, checksum, and frame sequence number. The RLP frame has no frame start or end markers as the length of RLP block matches with a GSM block used at the radio interface.

Both the transparent and non-transparent mode rely on a variant of V.110 [60] protocol originally specified for ISDN. V.110 had the following responsibilities:

1) Adapt any asynchronous character-oriented data stream to synchronous GSM connection by delaying the transmission or removing some extra end bits with RA0 function.
2) Transport the clock frequency of the original data stream over the synchronous GSM connection. While GSM clock frequency is different from the one of the original data stream, V.110 uses specific commands used to adjust the clock phase of the receiver.
3) Pass modem control signals over GSM connection from a computer to the IWF with RA1' function.
4) Perform any needed rate adaptation for data streams between 600 and 9600 bps.

### 5.1.12 Mobility Management

#### 5.1.12.1 PLMN and Cell Selection

According to GSM standards, a GSM network is operated by one single GSM service provider, within the territory of one country. GSM networks are identified with their **public land mobile network (PLMN)** IDs. Every GSM subscriber has a home network, which is the network of the operator that provides the GSM subscription and a SIM card for the subscriber. GSM subscribers are allowed to roam in GSM networks of other GSM operators and use the services of such visited networks, according to the roaming contracts between the operators. Every GSM operator has roaming partners practically in every country where GSM is deployed. In this way, GSM subscribers can use their GSM mobile stations in all the countries with GSM network support, if the subscription type just allows international roaming.

To enable roaming, the service providers have to provide the following inter-operator technical and administrative services:

- Exchange of subscriber information between networks
- Exchange of mobile station location information between networks
- Exchange of charging information between networks
- Definition of the services provided in the visited network, including support and tariffs

Network roaming may cause additional charging for the subscribers, settled between the home and visited operators. In the early days of GSM, the roaming charges were significant, but within Europe the EU regulation later pushed roaming tariffs down.

At the switch-on, a GSM mobile station starts GSM network selection process to enter the idle mode. The MS measures radio signals on the GSM frequency bands:

- To find those GSM PLMN networks that provide coverage at the location of the mobile station and select one of them for camping.
- To select the best cell of the chosen GSM network, providing the strongest radio signal for the mobile station. After choosing the cell, the mobile station makes a location update and registers itself to the location area of the cell.

There are a few partly contradictory requirements for the **cell search** and PLMN selection procedure:

- The mobile station should find and select the PLMN network as quickly as possible.
- The network search should not consume too much battery.
- The mobile station shall select the home network of the subscriber whenever under its coverage.

GSM network and cell selection process has the following steps:

1) After the mobile station is turned on, it starts searching FCCH and SCH of GSM cells. The mobile station starts the search over those frequencies it has used in its most recent home network access. Those frequencies cover the ones used by the most recently camped cell and its neighbor cells. If the mobile station is not able to find the home network in these frequencies, it shall continue the home network search by scanning all GSM frequencies supported by the mobile station. If the mobile station finds a GSM synchronization channel on these frequencies, it shall synchronize itself to the cell, measure the strength of the received radio signal, and listen to cell selection parameters sent on the BCCH channel. For each cell found, the mobile station calculates a special value called C1 based on the received BCCH parameter values, strength of the cell's radio signal, and the maximum transmit power of the mobile station. The mobile station initially camps on a cell with the biggest C1 value.
2) If the mobile station did not find home network cell on any frequency band, it can consider camping to a GSM cell of any other network found during the scan. The mobile station may select one of these networks either automatically or ask the user to select the network. The used method is chosen according to the mobile station settings.
   - Mobile stations using automatic selection check the found networks against two different lists stored to the SIM card:
     - Networks which have blocked access attempts earlier.
     - Networks which the home network provider or subscriber would prefer using when home network is not available. Among the available networks, the one with the highest preference on this list is chosen, which has not blocked an earlier access attempt.
   - In the manual search, the mobile station shows its user a list of networks found, except the ones which have earlier blocked an access attempt. The user can then pick the preferred network from that list.
3) After the network has been selected, the mobile station accesses a cell of that network. The mobile station listens to its BCCH to learn the frequencies used by the neighboring cells of the network. The mobile station then performs measurements for these cells and calculates the C1 values for them. Mobile station camps to the cell with the biggest C1 value.

After selecting the cell, the mobile station continues listening to the BCCH channel and starts listening to paging messages on the PCH channel. In idle mode, the mobile station also goes on measuring the neighboring cell frequencies learned from the BCCH channel SYSTEM INFORMATION TYPE2 messages. The purpose of continuing the measurements is to find out if the C1 values of other cells would suggest cell reselection, for instance, when the station is moving. Each cell sends a cell-specific value for the CELL_SELECT_HYSTERESIS parameter on its BCCH. This value is subtracted from the C1 value calculated for the cell when the mobile station does not yet use that cell. This adjustment is not done for the C1 value of the currently used cell. The hysteresis mechanism is to get the mobile station to slightly prefer its current cell and avoid unnecessary cell reselections when being close to the edge of two cells.

If the mobile station moves completely out of the GSM network coverage area, the mobile station starts to search for any other GSM network, as it does after being switched on. If no other network is found, the mobile station will periodically repeat the search over all the supported frequency areas until the network is found or the mobile station is switched off.

#### 5.1.12.2 Location Update

After selecting the cell, the mobile station must tell the network its identity and location. The network responds to the mobile station, whether it is allowed to use all the GSM services of the network or only the emergency

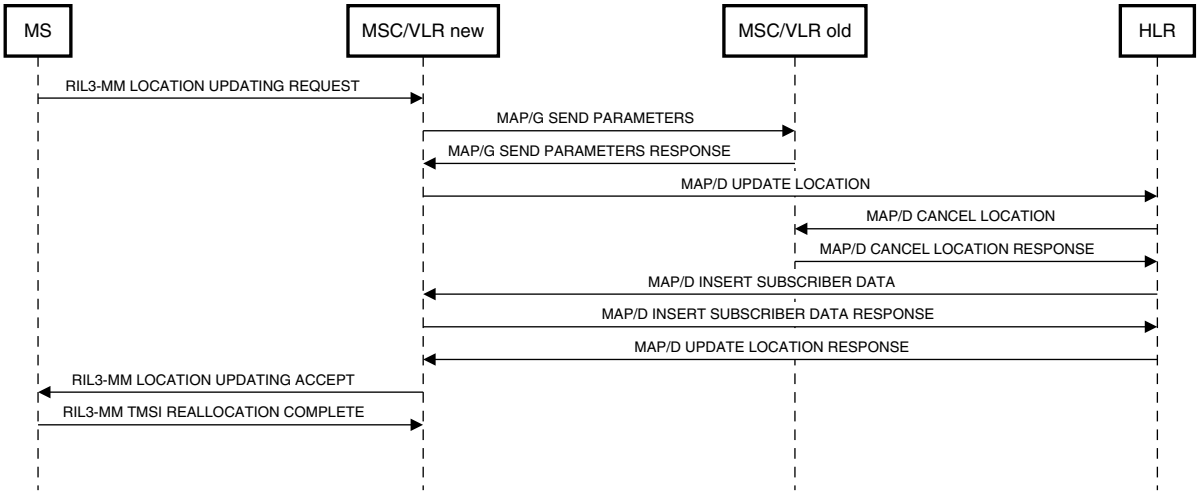


**Figure 5.19** GSM location update.

call. In the latter case, the mobile station and its user must decide whether to stay in this network or camp to another network for full services. The location update procedure is performed as shown in Figure 5.19:

1) The mobile station requests a dedicated channel for the location update, as described in Section 5.1.7.1. After acquiring a dedicated standalone signaling channel, the mobile station sends a RIL3-MM LOCATION UPDATING REQUEST message. The message contains the TMSI code, which the mobile station earlier received from the MSC.
2) The MSC checks the old location area of the MS as encoded to the TMSI code. If the area belongs to another MSC, the new MSC/VLR sends a MAP/G SEND PARAMETERS message to the old MSC to retrieve the IMSI code of the user. The new MSC updates the location of the subscriber to the HLR of the subscriber's home network. If the MSC belongs to a visited network, the HLR checks if the subscriber has the right to use that network and returns the result to the new MSC. If the HLR accepts the new network, it stores the new location area and the new serving MSC/VLR to its subscriber location database and requests the old MSC/VLR to remove all data related to the subscriber from its VLR database. In the end, the HLR responds to the new MSC/VLR that the location update has been completed.
3) The new MSC/VLR may allocate a new TMSI code for the subscriber and send it to the mobile station within the location accept message. The new MSC/VLR stores into its database the state of the mobile station as reachable. The new MSC/VLR gets from the HLR the necessary subscriber security parameter values, such as encryption keys Kc, RAND random numbers, and the corresponding SRES authentication codes used to authenticate the user.

For further details about the messages used in these procedures and the case when the HLR rejects the new location, please refer to *Online Appendix I.2.6* (Figure 5.19).

If the mobile station has not changed its location area since it was turned off, the MSC/VLR already has the subscriber's authentication credentials when receiving the new location update message. If the location area has been changed, MSC/VLR gets the authentication credentials within a MAP/D INSERT SUBSCRIBER DATA message from the HLR. The MSC/VLR can thereafter authenticate the subscriber and start traffic encryption as described in Section 5.1.8.2. For further details about subscriber data stored in different network entities, please refer to 3GPP TS 23.008 [61].

The mobile station must regularly, at least once a day, send a location update message to the GSM network even if the location area has not been changed. The purpose of this is to ensure that both HLR and VLR databases of

the network have the accurate location information of the mobile station regardless of any possible error situation. The mobile station in the idle mode may perform cell reselection as described in Section 5.1.12.1. Cell reselection triggers the mobile station to send a location update if the new cell belongs to another location area than that of the previously used cell.

When the mobile device is being switched off, the station sends a RIL3-MM IMSI DETACH message to the MSC to inform it about the upcoming switched off state. After receiving this message, the MSC stores to its VLR database the new state of the user as unreachable and informs the HLR about the same.

#### 5.1.12.3 Handover in Dedicated Mode

In mobile networks, there are many conditions that cause a mobile station to lose its connection to a base station. If the station has an ongoing call, handover of the call between GSM base stations can be used to avoid call drop. The main reasons for handover decision are as follows:

1) When the mobile station moves farther away from the serving base station, its radio connection to the cell weakens. On the other hand, the movement may bring the mobile station closer to another base station and improves the quality of radio signal received from that cell. The call can be handed over between these cells when the radio connection to the new base station improves over the currently used connection. After the handover, the mobile station may use smaller transmission power to reduce the interference level of the network.
2) The used radio connection may experience very quick degradation if the radio signal is attenuated by an obstacle that suddenly appears between the MS and BTS. This may happen due to the mobile station itself moving behind an obstacle or other objects, like vehicles moving to positions where they block the signal. In such a case, an immediate handover would be needed to avoid the call being dropped.
3) When a cell experiences high load, there may be more mobile stations trying to camp on a cell and initiate calls than what the cell is able to support. In such a case, the GSM network may decide to hand over some of the ongoing calls to another nearby cell to balance the load between cells. The drawback of handovers done for load balancing is that the mobile stations are handed over to cells against which they do not have optimal radio connectivity. This causes the mobile stations to increase their transmission power, causing increase of interference level in the GSM network.

The GSM mobile station and base station measure frequently the quality of received signals to find out when handover would be either useful or necessary to maintain a call. Handover decision is made by the BSC or MSC based on the measurement data from the mobile station and base station. The measurement and handover decision process consists of the following steps:

1) The base station measures the error ratio and power loss of the dedicated channel.
2) The mobile station measures also the error ratio and power of the dedicated channel from its perspective. Additionally, during the idle unused timeslots, the mobile station measures power from all the BCH channels of any neighboring cells. To find out the frequencies of neighboring cells for measurement, the mobile station checks the SYSTEM INFORMATION TYPE2 messages sent over the BCCH of its own cell. The mobile station may also get more detailed information over its dedicated SACCH signaling channel about how the measurements should be performed.
3) The mobile station delivers its measurement data to the base station at most twice a second within the RRC MEASUREMENT REPORT messages sent over the active SACCH. In the RRC message, the mobile station tells the measured frequencies, measured signal quality values, and the BSIC codes detected on the SCH of the measured cells. This BSIC code identifies the measured cell to the network.
4) The base station forwards the measurement data to the BSC in a 48.058 MEASUREMENT REPORT message. The data is sent either as received from MS or pre-processed to minimize the traffic between the base station and BSC.

5) The BSC and MSC together know the load level of the cells under the BSC. When making handover decisions, the BSC takes into account all the above-mentioned data points as well as the maximum transmission power supported by each of the mobile stations.

Based on the measurement results, the BSC can send **power control** commands either to the base station or mobile station. Power control aims to ensure that neither of the stations would use any more transmission power than necessary, still keeping the quality of radio connections in acceptable levels. The BSC can send a 48.058 BS POWER CONTROL message to a base station for controlling its transmission power. The same message can also give the base station an order to adjust the power control parameter value sent to the mobile station over the SACCH.

When the quality of measured radio signals become significantly better for any other cell than the currently serving cell, the network may make a handover decision for the call. The main steps of handover process in GSM system are as follows:

1) The network (either a BSC or MSC) reserves dedicated channels for the mobile station into a new target cell.
2) The network creates new circuit switched connections from the MSC to the new base station, chosen as the target BTS of the handover.
3) The network instructs the mobile station to connect to the new cell and take the reserved dedicated channels into use, simultaneously releasing the channels used earlier with the old cell.
4) After the handover, the network releases the radio channels and corresponding circuit switched connections of the old cell, which is no longer used by the mobile station.

Depending on the relation of the old and new cells, there are three types of handovers in GSM as shown in Figure 5.20:

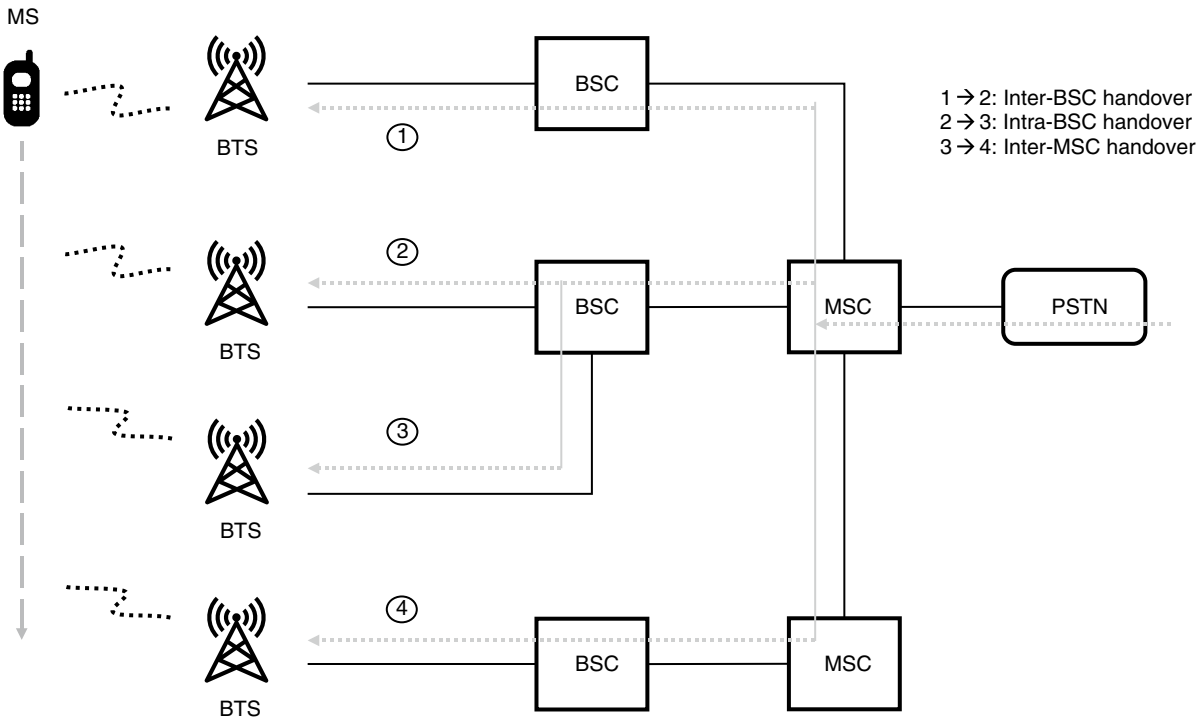


**Figure 5.20** Different types of GSM handover.

- **Intra-BSC handover**, where both the old and the new cell are controlled by the same BSC.
- **Inter-BSC handover**, where old and new cells are controlled by two different BSCs connected to a single MSC. In this case, the currently serving BSC requests the MSC to perform handover to the new cell, as identified with its Cell ID and location area code LAC.
- **Inter-MSC handover**. If the handover is done between base stations under two different MSCs, the originally used MSC stays in control of the call until the call is released. That MSC is called **anchor MSC,** which maintains the call and collects the related charging data. The anchor MSC finds the other MSC based on the LAC code of the new cell, as given by the currently serving BSC.

In each of these cases, from the mobile station point of view the handover process looks the same. The mobile station receives a handover command from the network and moves to the new cell accordingly. The difference is in the steps needed to prepare for the handover in the network side. In the Intra-BSC case, the serving BSC can handle the handover autonomously with the base stations controlled by the BSC. In other cases, the involved BSC and MSC nodes must communicate with each other and allocate a new path for the voice signal between network elements before the handover command is sent to the mobile station. GSM handover procedures are described in 3GPP TS 23.009 [62].

The steps of GSM Inter-BSC **handover procedure** are as shown in Figure 5.21:

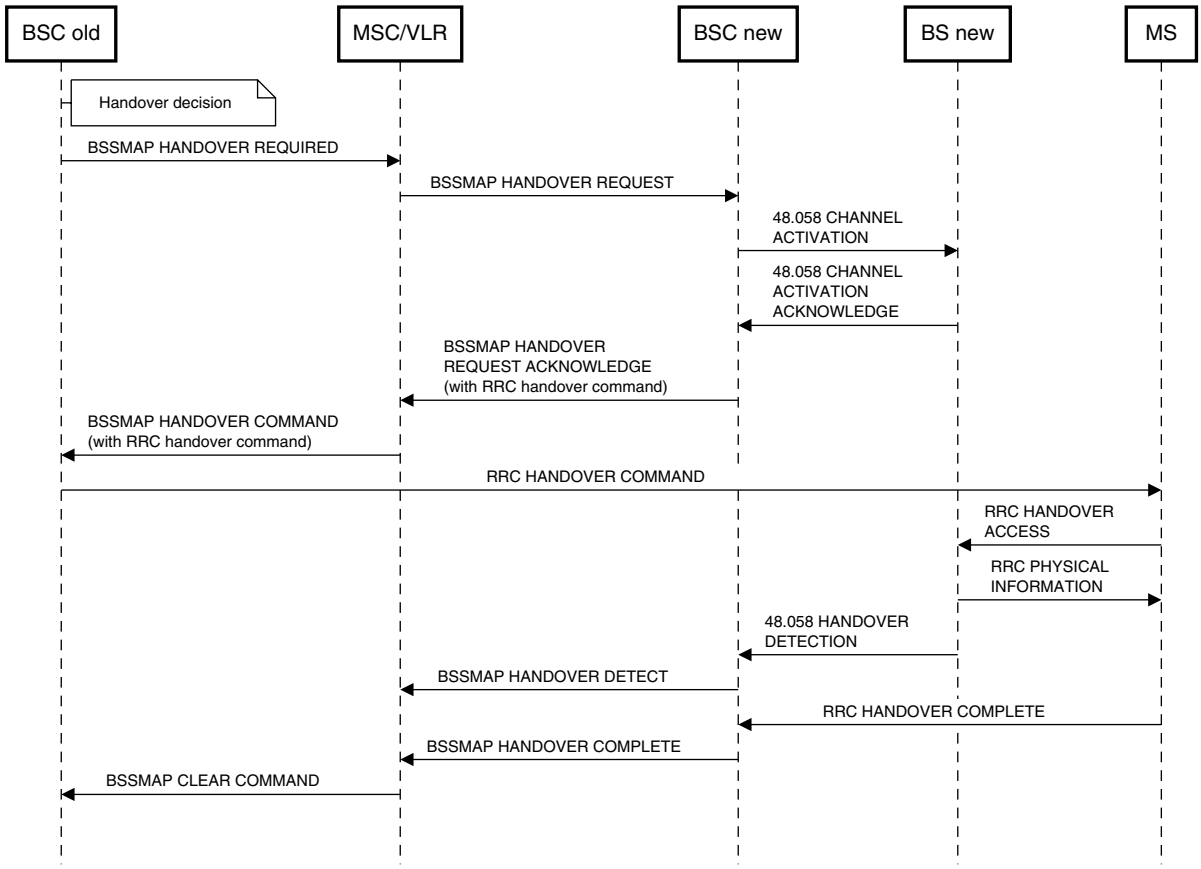


**Figure 5.21** Inter-BSC handover under the anchor MSC.

1) The old BSC, which currently serves the mobile station, makes the handover decision. If the BSC itself does not control the target base station of the handover, the BSC sends a BSSMAP HANDOVER REQUIRED message to its currently serving MSC to inform it about the handover decision. The MSC sets up a new signaling connection control part (SCCP) connection to the new BSC, which is in control of the target cell. The MSC sends a BSSMAP HANDOVER REQUEST message to the new BSC.
2) The new BSC reserves dedicated radio channels and activates them at the target base station. The new BSC composes an RRC HANDOVER COMMAND for the mobile station and sends this RRC message to the MSC within its BSSMAP response message. The MSC establishes thereafter the needed circuit switched connections toward the new BSC. The MSC sends a handover command to the old BSC, which forwards the RRC message from the new BSC to the mobile station.
3) The mobile station learns the BSIC code and SCH channel frequency of the target cell from the RRC HANDOVER COMMAND. The message also describes the new dedicated channels, gives the MS an 8-bit handover reference number, and indicates whether synchronized or non-synchronized handover method shall be used. With the synchronized method, the message may also give a new timing advance value to be used for the target cell.
4) The mobile station connects to the target cell and starts right away receiving traffic over the new dedicated channels. The mobile station also sends RRC handover access bursts with the handover reference number over the dedicated channel to confirm the successful setup of the connection to the new cell.
5) After receiving access burst from the mobile station, the target base station sends a handover detection message to its BSC. The new BSC confirms the handover to the MSC so that the MSC can redirect the circuit switched connections from the old cell to the new one. Eventually, the mobile station declares the handover as complete so that the MSC can release any pending connections to the old cell.

For further details about the messages used in these procedures and the case when the old and new BSCs are connected to different MSC/VLRs, please refer to *Online Appendix I.2.7* (Figure 5.21).

## 5.2 General Packet Radio Service

### 5.2.1 Standardization of General Packet Radio Service

When the GSM network services were evolved further in the 1990s, the focus shifted from voice to data transport. The Internet became a major driver for data consumption, and engineers faced the need of transporting packet switched data efficiently over the GSM network. Packet switched data was earlier used in fixed networks for business purposes, but with the Internet it gradually became a mainstream consumer service for accessing email and browsing the Web. Fixed Internet access and GSM voice were forces behind the telecommunications boom of the 1990s, but the pressure increased for providing also mobile Internet access over proven GSM networks. Unfortunately, GSM mobile stations only supported CSD access, which is quite inefficient for transporting bursty packet data. Worse, GSM data service provided only symmetric and small data rates.

Even if the CSD connections enjoy benefits such as constant latencies, guaranteed bitrates, and no need in network level addressing in data packets, the rigid circuits waste capacity when used for Internet traffic. The typical packet data traffic pattern is highly variable. For instance, Web browsing mixes short periods of high-rate downlink data rate transport with long idle periods while the user is digesting the data. The traffic is also asymmetric as only small hypertext transfer protocol (HTTP) queries are sent an uplink while the big responses arrive by downlink. The GSM circuit switched connection wastes capacity for idle periods and slows down the high-rate data bursts, which exceed the constant bitrate of the connection. In theory, it would be possible to release the GSM data circuit for the idle periods, but this would cause extra delay and signaling load for releasing and reopening connections over the data consumption session.

To solve these problems, a new approach was used for GSM data transmission and its resource reservation. With the new GPRS service, the network dynamically reserves one or multiple GSM timeslots for the data channel as long as there is data to be transported and releases them when there is nothing to be sent [63]. The essential improvement compared to the circuit switched model is the dynamic, quick, and lightweight allocation of GSM timeslots for the radio channel to follow the pattern of user data packet flow. Compared to the long setup time of circuit switched end-to-end connection, activating an existing GPRS link can be done much quicker. While no data is transported, GPRS does not use network transmission capacity, which makes GPRS suitable for "always-on" and bursty IP connectivity. The GPRS system is also able to allocate different numbers of timeslots to uplink versus downlink when the use case requires asymmetric data rates. It is important to note that GPRS was not just a new way of using GSM air interface, but it introduced a completely new core network and protocol stack designs as well. In practice, both the network and mobile stations had to support separate CS voice and PS data systems, just sharing a common air interface L1 structure. Designing GPRS on top of GSM was a major operation for ETSI-driven standardization. Complete GPRS service description can be found from 3GPP TS 22.060 [64], which was published as part of GSM Phase 2+ release 98.

When the GPRS solution was being specified, there were a few competing packet switched protocols in common use within the fixed networks:

- Internet protocol IP
- X.25 packet data protocol for public packet switched networks
- Other vendor specific protocols

The GSM packet data transport solution was designed as generic to support all such protocols. Due to that, the solution was called **General Packet Radio Service (GPRS)**. When GPRS was eventually deployed after some years of specification, research, and development, the IP protocol had already become dominant. GPRS support for other protocols has not been widely used. In retrospect, it might be claimed that it would have been wiser to optimize GPRS for IP traffic rather than to create a protocol-independent general packet radio system.

The first GPRS networks entered commercial use around 2000, when the first GPRS mobile stations (or handsets) became available. The mobile stations were GPRS-enabled mobile phones, network cards that could be installed to computers, or personal digital assistant (PDA) devices supporting GPRS packet data connections. Typical GPRS use cases were multimedia messages (MMS), email, limited Web browsing capabilities, and using GPRS mobile station as a data modem for a portable computer.

GPRS is specified in 3GPP standardization series 40–55 and 21–35. These standards cover both the GSM voice system and the GPRS system as its extension. The most important GPRS specific 3GPP technical specifications are as follows:

- TS 22.060: GPRS service description – concepts and requirements
- TS 23.060. GPRS service description – functions and architecture
- TS 43.051: General description of GPRS protocols
- TS 43.064: General description of GPRS radio interface
- TS 44.060: Radio link control/Media Access Control (RLC/MAC) protocols
- TS 44.064: Logical link control (LLC) protocol
- TS 44.065: Subnetwork dependent convergence protocol (SNDCP) protocol
- TS 29.060: GPRS tunneling protocol (GTP) protocol
- TS 48.018: BSS GPRS protocol

GPRS mobility management (GMM) and session management (SM) procedures and messages are specified in 3GPP TS 24.008 [41].

At the time of this writing, GPRS has become a niche technology. Compared to newer cellular data systems, such as LTE, GPRS has many disadvantages: small bitrates, high latencies, and low spectral efficiency. GPRS and

its EDGE enhancement are still supported in GSM networks for certain embedded devices that occasionally transfer only a small amount of non-time critical data.

### 5.2.2 Architecture and Services of GPRS System

GPRS network architecture and functionality is specified in 3GPP TS 23.060 [20].

#### 5.2.2.1 GPRS System Architecture

The key constraint for GPRS design was reuse of existing GSM equipment and frequency bands. Consequently, GPRS uses GSM radio interface but manages the allocation of physical channels differently than the circuit switched GSM. An existing GSM network can be upgraded to support GPRS for all or a subset of its cells. Deployment of GPRS means the following activities for the network operator:

- Connecting new packet switched GPRS network elements to a GSM core network
- Software updates for base stations and BSCs to support GPRS
- Software updates for HLR, VLR, EIR, and AuC to support the additional parameters and information as used for GPRS

The GPRS network assigns a packet switched **tunnel** for each packet data flow of a GPRS mobile station, to carry the upper layer packet data protocol messages to the edge of GPRS network. The tunneling mechanism was designed to be able to transport different types of packet data protocols over the GPRS infrastructure. GPRS introduced a new mechanism, referred as **packet data protocol (PDP) context**, to manage the packet data protocol flows and related tunnels. The network sets up PDP contexts according to connectivity requests received from GPRS mobile stations. A mobile station sends a connectivity request toward a specific external **packet data network (PDN)** identified by its **access point name (APN)**. The request also defines the type of packet data protocol used. When receiving such a request the GPRS network creates a PDP context, assigns a packet data protocol address for the mobile station, and creates tunnels needed for routing and transporting the packets between the mobile station and the PDN. It must be noted that the tunnel routes the data packets only toward the correct destination PDN network, but to route packets to their ultimate destinations each packet must contain both source and destination addresses, such as IP addresses. These addresses are also used to map packets to the correct GPRS tunnels within the GPRS network.

The following types of network elements (see Figure 5.22) were added to GSM architecture to support GPRS (see 3GPP TS 03.02 [65] for further details):

- **Serving GPRS Support Node (SGSN)** with the following tasks:
  - Tracking the location of GPRS mobile stations and their GPRS service states within the GPRS tracking area managed by SGSN.
  - Querying the HLR database for GPRS subscriber authentication credentials and other subscription details to perform authentication and authorization when a mobile station attaches to the GPRS service.
  - Maintaining mappings of PDP contexts, GPRS tunnels, mobile stations and Gateway GPRS support nodes (GGSNs), which belong together.
  - Forwarding of packets between Packet Control Unit (PCU) and GGSN nodes via GTP tunnels.
  - Encryption of the packet data transported between the SGSN and mobile station.
- **Gateway GPRS Support Node (GGSN)** with the following tasks:
  - Management of PDP contexts and GTP tunnels to connect mobile stations to external packet data networks such as the Internet or an X.25 PSPDN.
  - Routing packets between external packet networks and SGSNs serving GPRS mobile stations. The GGSN is an edge router of the GPRS network. The GGSN routing mechanism is based on a database of PDP contexts, corresponding tunnels, and packet data protocol addresses.

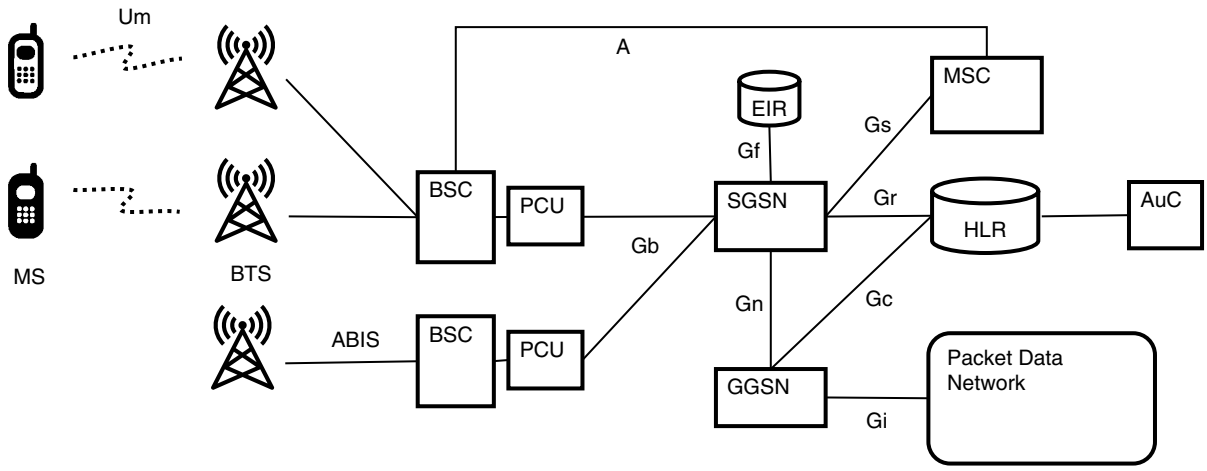


**Figure 5.22** Architecture and interfaces of GPRS system.

- Forwarding packet data between mobile stations and external packet networks within GTP tunnels between GGSN and SGSN nodes.
- Assigning IP addresses for the PDP contexts and performing possible network address translation between the private IP address reserved for the mobile station and a public IP address owned by the GGSN, visible to the external networks.

- **Packet Control Unit (PCU)** is a function that forwards packet switched data from/to BSC to the SGSN of the GPRS network. The PCU segments long LLC frames into shorter RLC frames and takes care of both flow control and retransmissions. The PCU creates, supervises, and releases packet-switched calls. Toward the air interface, the PCU manages assignment of timeslots for both uplink and downlink GPRS data flows. A PCU can be implemented as part of a base station or BSC, or it may have its own dedicated PCU support node device connected to the BSC over the $A_{gprs}$ interface.

GPRS core networks can be divided into the following parts:

- **The GPRS backbone** network connects the SGSN and GGSN devices within the operator network.
- **The Inter-PLMN GPRS backbone** or **IP roaming exchange (IPX)** network connects the SGSN of the visited network to the GGSN of the user's home network. This setup, known as home routing, is used to support users roaming abroad. Home routing allows the roaming user to exchange packet data with external packet data networks over the home GGSN, while being served by an SGSN of the visited network.

Like GSM specifications, GPRS specifications also define the interfaces as reference points between GPRS network elements. The GPRS network interfaces shown in Figure 5.22 are

- Gb: Interface between BSC/PCU and SGSN.
- Gs: Optional interface between SGSN and MSC.
- Gn: Interface between two GSN (either SGSN or GGSN) nodes, which belong to the same network
- Gp: Interface between SGSN and GGSN in different networks. This interface enables GPRS roaming where the SGSN is in a visited network and the GGSN in the home network.
- Gi: Interface between GGSN and external packet data network.
- Gf: Interface between SGSN and EIR.
- Gc: Interface between GGSN and HLR database. Gc interface may be omitted when the SGSN takes care of all necessary communication with the HLR.

- Gr: Interface between SGSN and HLR database, relying on the MAP protocol and an underlying SS7 stack.
- Gd: Interface between SGSN and MSC serving a SMSC.

GPRS mobile stations have been divided into three categories as follows:

- Type A stations are able to use GPRS data and GSM circuit switched voice connections simultaneously. This is enabled by the dual transfer mode (DTM) support in the network with which the circuit and packet switched timeslots do not overlap.
- Type B stations are not capable of simultaneous use of GPRS and GSM services. When starting a GSM voice call, the station automatically suspends its GPRS data connection. The data connection is reactivated after the voice call is closed.
- Type C stations let the user choose whether to use the device for GSM voice call or GPRS data. When used for GPRS data, the station is not even able to receive incoming GSM voice calls.

The service provided by the GPRS system does not depend only on the type of the mobile station but also the network operation mode. The networks supporting operation mode I are able to page the mobile stations for incoming mobile terminated calls while GPRS data is being transported. Mode II networks can page the mobile station for calls only when the GPRS functionality of the station is in the idle state.

3GPP standards specify 29 different **multislot classes** of GPRS mobile stations. The classes differ by the number of timeslots that can be used for a GPRS connection and whether simultaneous GPRS uplink and downlink data transfer is supported. The number of GPRS timeslots for a GPRS channel determine the maximum data rate of the GPRS device. Actual data rate depends also on the type of channel coding used on the radio interface. Maximum data rates of 70–150 kbps can be reached when using four to eight timeslots of a GSM TDMA frame for a single connection.

GPRS defines another packet temporary mobile subscriber identity (P-TMSI) identifier for the subscriber, in addition to the TMSI code as defined for GSM. P-TMSI is a code given by the SGSN to the subscriber located within the area controlled by the SGSN. P-TMSI is used in signaling messages sent as cleartext over radio interface between the mobile station and the network, like how the TMSI code is used for GSM.

#### 5.2.2.2 GPRS Functions and Procedures

GPRS radio resource management takes care of allocation of GSM timeslots for GPRS data connections. GPRS extends GSM communication management with packet data **session management**. Session management is used to prepare the packet data connectivity by reserving a packet data protocol address for the mobile station and setting up GTP tunnels for transporting packet data flows through the GPRS network. The GGSN sets up its routing configuration so that any packets from the external packet data network toward the reserved address are routed to the tunnel toward the mobile station. These activities are performed at the **PDP context** activation. The concept of PDP context means pieces of configuration data shared between the GGSN, SGSN, and GPRS mobile station about the GPRS connection to the MS. The PDP context covers details of the packet data protocol and addresses used, the connected packet data network, the user data flows, and the GTP tunnels established to carry those within the GPRS network.

GMM is an extension of GSM mobility management MM. The main differences between MM and GMM are related to the mobility management states and accuracy of tracking the location of the mobile station:

- GPRS uses three mobility management states for the mobile station. When GPRS data transfer is going on, the mobile station is in ready state. In addition to idle and ready states, GPRS introduced the standby state. In the standby state, the mobile station is attached to GPRS service and has an active PDP context waiting for any new data to be transported. The network is able to initiate GPRS data transfer to a mobile station which is in the standby state by moving it to ready state. Also, the mobile station is able to move itself to ready state to transmit packet data. After the data has been transported or there is a long enough pause in the transport, the mobile station moves back to the standby state.

- For mobile station location tracking, the GPRS system uses a concept of **GPRS routing area (RA)**. Like the GSM location area, a GPRS routing area consists of a set of cells within which the mobile station may move without updating its location to the network. A routing area is always a subset of a GSM location area. The GPRS network tracks the mobile stations in ready state in the accuracy of a single cell and stations in standby mode within a routing area. Each routing area has a unique ID called routing area identifier (RAI).

Routing areas were introduced to balance the signaling traffic between the GPRS location messages and paging messages sent within a routing area. GSM and GPRS systems need areas of different sizes mainly because the GPRS system shall be capable of quicker and more frequent activation of the packet data connections compared to the GSM system with infrequent but potentially long circuit switched calls.

GMM consists of the following functions:

- GPRS attach and GPRS detach with which the mobile stations enter and leave the GPRS service. When attaching to GPRS, the mobile station informs the network of its location and capabilities so that the network can contact the mobile station when needed.
- Mobile station location updates in terms of a GPRS routing area, a GSM location area, and a cell. The accuracy of the location information stored into the network depends on the state of the GPRS service for the tracked mobile station. The location is tracked in the accuracy of a single cell while GPRS data is being transferred. Otherwise, when the mobile station is attached to GPRS service, its location is tracked in the accuracy of a routing area. Without GPRS attach, the network tracks the GSM location area of the mobile station.

#### 5.2.2.3 GPRS Protocol Stack Architecture

GPRS protocol stack for Um and Gb interfaces is described in 3GPP TS 43.051 [26], and TS 23.060 [20] defines the complete GPRS protocol stack architecture. GPRS user plane protocol stacks shown in Figure 5.23 carry user data flows between the MS and GGSN.

The link layer of GPRS radio connection is divided into two protocols, MAC and RLC. These protocols, run between the base station and mobile station, multiplex the data flows and perform error correction over the radio interface. The base station subsystem GPRS protocol (BSSGP) takes care of similar link layer tasks between the base station and SGSN. The topmost LLC protocol of the link layer is used between the mobile station and SGSN for features such as encryption, flow control, and error correction. The SNDPC protocol is run between mobile station and SGSN on top of LLC. The main task of SNDPC is compression of the data to minimize the needed radio interface transport resources.

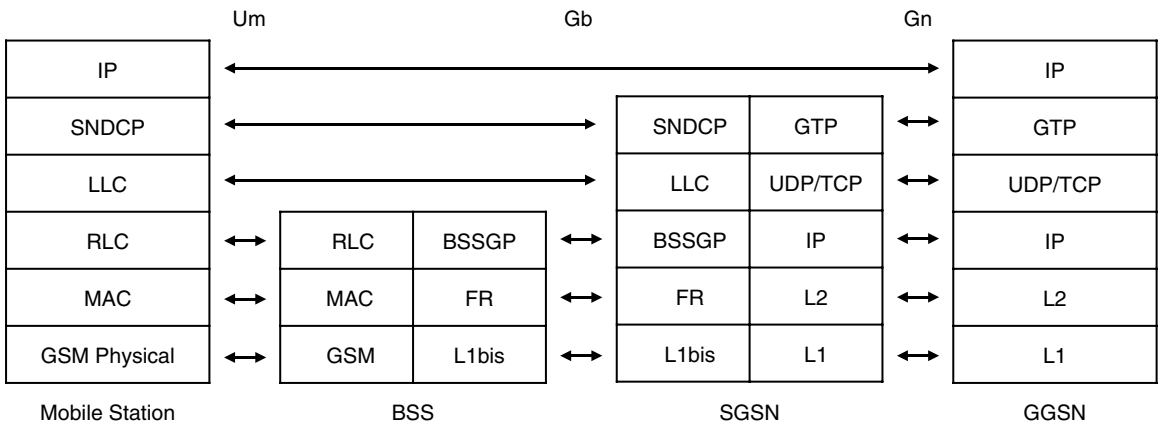


**Figure 5.23** GPRS packet system user plane protocols.

The TCP/IP protocol stack is used to transport data between the SGSN and GGSN nodes. GTP tunneling protocol is the topmost protocol of the TCP/IP stack. The tunneling mechanism enables transporting of different packet data protocols (such as IP or X.25) over GPRS to/from the access points provided by GGSN toward external packet data networks.

Signaling between the SGSN and MSC is done with the SS7 protocols such as MTP, SSCP, TCAP, and MAP. Those protocols are used for GPRS in the same way as for GSM.

### 5.2.3 GPRS Radio Interface

Overview of the GPRS radio interface can be found from 3GPP TS 43.064 [66].

#### 5.2.3.1 GPRS Radio Resource Allocation

The basic characteristics of GPRS radio interface come from the GSM air interface, which GPRS partly reuses but with certain extensions. Both the systems use shared TDM/FDM multiplexing and the common TDMA frame structure to support both GSM and GPRS services. The GPRS service uses the timeslots of the underlying GSM network. Individual bursts within the timeslots are used for both GSM and GPRS traffic. The base station can divide its timeslots between GSM and GPRS services either in a fixed way or dynamically based on the network load. In the latter case specific timeslots may be used for either of these services, depending on the instantaneous capacity demand per service.

The network grants GPRS transmission resources for a GPRS mobile station dynamically as **temporary block flows (TBF)**, based on the transmission needs that the MS has indicated to the network after a GPRS random access procedure. A mobile station may have one or multiple TBFs allocated. The uplink TBFs are separate from downlink TBFs, since the resource allocation is often asymmetric. Typically, more resources are granted to the downlink TBF than to the uplink TBF. A TBF has two dimensions for the dynamic resource allocation:

- GPRS packet data channel (PDCH)
- GPRS radio block

As we know, the GSM TDMA frame has eight timeslots. A PDCH is one of those timeslots allocated for GPRS traffic. Thus, the cyclic GSM frame structure may carry a maximum of eight PDCHs when none of the timeslots are used for voice. In the frequency space, PDCH uses the same frequency hopping scheme as a GSM TCH. The TBF allocated to the mobile station is linked to 1–5 PDCHs of a GSM frame. The number of PCDH resources that the mobile station can use simultaneously depends on the multislot class of the station and varies between 4 and 5 for downlink and 1–4 for uplink.

The basic unit of GPRS radio resource allocation is a group of four bursts used to carry one GPRS RLC/MAC protocol frame over a single PDCH channel. This group is called an **RLC data block**. Each of the four bursts of the RLC data block is carried within its own GSM TDMA frame, using the same timeslot number allocated for the PDCH. The **GPRS radio block** is a group of four consecutive GSM frames, capable of transporting eight RLC data blocks – one per timeslot (or PDCH).

GPRS has its own multiframe structure over the GSM TDMA frames. The GPRS 52-multiframe consists of 52 GSM frames, or rather two GSM 26-multiframes. GPRS multiframe has 12 GPRS radio blocks and four GSM frames that do not belong to any GPRS radio block. Frames 12 and 38 are used for timing advance calculations, while frames 24 and 51 can be used for measuring neighboring cells. Up to eight mobile stations may be multiplexed to one PDCH so that only one of those stations can use the PDCH within a radio block. Within the next GPRS radio block, the same PDCH may be assigned to another mobile station. Thus, when a mobile station gets a PDCH assigned to it, the station may not use that PDCH continuously but only within those radio blocks where the PDCH is allocated to that station (see Figure 5.24). For each radio block, the network indicates to which mobile station (and its TBF) the PDCH belongs.

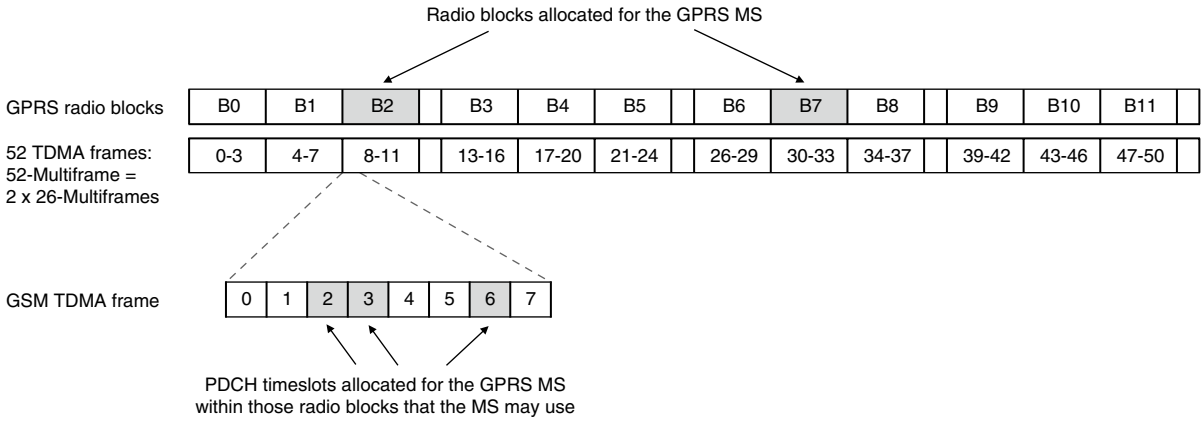


**Figure 5.24** PDCHs and radio blocks allocated to the GPRS mobile station within the GPRS multiframe.

**A temporary block flow (TBF)** is the temporary allocation of PDCH timeslots within a number of non-consecutive GPRS radio blocks for a mobile station. As its name indicates, the allocation of TBF is not permanent, and thus it is bound in time for a number of radio blocks. When the mobile station has to send or receive user data over GPRS, the network grants the station with one or multiple PDCH timeslots for as many radio blocks needed until the data transport has concluded. Thereafter, the TBF allocation is released. For bidirectional traffic, a TBF is allocated for either of the directions. The TBF is identified by a **temporary flow identifier (TFI)**. At the allocation of uplink TBF, the network gives the mobile station an **uplink state flag (USF)** value separately for each allocated PDCH. For that PDCH, the USF value uniquely identifies one mobile station among those eight stations or less multiplexed to the same PDCH.

While allocation of PDCHs for a TBF is fixed when the TBF is created, the same does not apply to the allocation of radio blocks. GPRS uses a few different mechanisms to indicate the mobile station when the assigned PDCH(s) of a radio block belongs to the MS. One of those mechanisms is used for downlink and others for uplink. The four timeslots of one PDCH within a radio block carry a single RLC protocol frame. The downlink RLC frame header contains the TFI of the TBF to which the frame belongs to. The mobile station reads all the RLC headers of downlink PDCHs of its downlink TBF. When the header contains the TFI of its own TBF, the mobile station reads the complete RLC protocol frame that was sent on that PDCH over the radio block. The uplink radio block allocation of PDCH can be indicated to the mobile station in the following ways:

1) Fixed allocation. When the TBF is created, the network sends the mobile station a bit map per PDCH indicating those radio blocks in which the PDCH belongs to the mobile station. A single bit of the map tells if the PDCH can or cannot be used in the radio block corresponding to the bit. The sequence of bits of the map means the consecutive radio blocks after the TBF start time, one bit per radio block. If the mobile station still has more data to send when the radio blocks described within the bit map have been transmitted, the mobile station may request the network to send a new bitmap for additional radio blocks.
2) Dynamic allocation. The network manages the radio block allocation between mobile stations dynamically, one radio block at a time. The MAC header sent with the RLC block contains a USF, which identifies the mobile station that may use the PDCH in the next uplink radio block. The USF has eight possible values, each indicating a specific mobile station multiplexed to that PDCH. With extended dynamic allocation, the network may use a single USF to assign several timeslots for mobile station with a high multislot class.

In the network side, the allocation is managed by the PCU. For downlink, the PCU allocates as many blocks as needed for the downstream traffic. For uplink, the PCU allocates blocks based on the requests received from

mobile stations. The uplink MAC header has a countdown field indicating the number of radio blocks needed to complete the data transfer. The original design of GPRS was to release the uplink TBF when the countdown reaches the value zero. With the extended uplink TBF method, the TBF is maintained until the expiry of an idle timer to reduce delay and overhead if the uplink transmission continues in a few seconds. Creation of a new TBF typically takes longer than half a second, so the extended uplink tries to avoid such kinds of delays for traffic patterns with potentially short idle periods, such as Web browsing. When the browser retrieves a Web page, it typically needs to send multiple HTTP requests after each other, as described in Chapter 3, Section 3.6. Each of those requests is sent separately but very soon after each other, so the extended uplink TBF method may keep the TBF alive long enough to retrieve a complete page.

#### 5.2.3.2 GPRS Logical Channels

The GPRS mobile station uses the FCCH and SCH of the GSM frame structure to synchronize itself to the GSM frame cycle. Additionally, GPRS mobile station listens to SYSTEM INFORMATION TYPE13 messages sent on the BCCH. These messages tell the mobile station how it can find the packet broadcast control channel (PBCCH) channel providing more information about the GPRS service and its shared channels in the cell. If the cell does not support the PBCCH channel, the additional information is given directly in the SYSTEM INFORMATION TYPE13 message.

The following logical channels were originally defined for GPRS:

1) Shared signaling channels used by all GPRS mobile stations camping in a cell:
   - Packet broadcast control channel (PBCCH): The channel on which six different types of PACKET SYSTEM INFORMATION messages are broadcast within the cell. These messages provide mobile stations with information about the GPRS network and various parameter values used to control mobile station functionality, such as
     – How PCCCH logical channels are mapped to PDCH channels of the cell
     – The number of information bits the mobile stations shall add to their PACKET CHANNEL REQUEST messages
   - Packet common control channels (PCCCH) are in shared use of all mobile stations within the cell, but without broadcast mechanism. Only one mobile station may use an uplink channel at a time, and the messages on the downlink channel have the address of the destination mobile station.
     – The packet paging channel (PPCH) on which the network sends a paging message to a mobile station for either incoming packet data or a circuit switched voice call. Paging messages are sent in all the cells that belong to the routing area (RA) where the mobile station has most recently sent a routing area update message. Like the GSM PCH channel, the GPRS PPCH channel can be divided into multiple subchannels for DRX. When using DRX, the mobile station has to listen to only one of the PPCH subchannels and save its battery the rest of the time.
     – The packet random access channel (PRACH) on which the mobile station can request itself a dedicated channel for packet switched data transport.
     – The packet access grant channel (PAGCH) is used by the network to inform the GPRS mobile station about the dedicated GPRS TBF allocations for packet data traffic channel (PDTCH) data and packet associated control channel (PACCH) signaling channels.
     – The packet notification channel (PNCH) used by the network to send PTM-M message to a group of GPRS mobile stations. This message is used to inform the mobile stations about point-to-multipoint packet data arriving to the members of the group.
2) Packet data channels dedicated to a single mobile station
   - Packet data traffic channel (PDTCH) is used to transport packet switched user data. The PDTCH channel consists of the PDCH timeslots within radio blocks allocated to the mobile station.

3) Signaling channels dedicated to a single mobile station
   - Packet associated control channel (PACCH) is used to transport signaling messages between the network and a single mobile station. The PACCH channel is used for packet resource requests and assignment messages, packet data acknowledgments, and power control commands. The PACCH may be used to notify mobile stations about incoming circuits switched calls, when the network supports such an operation mode. The TBF resource allocation of the mobile station is divided between PDTCH and PACCH. The payload type field of the MAC headers sent with the RLC block tells if the block carries PDTCH user data or PACCH signaling.
   - Packet timing control channel (PTCCH) to which GPRS mobile stations send uplink bursts to allow the base station to determine the timing advance needed by the mobile station. The network sends the timing advance commands to the mobile stations on the downlink of the PTCCH channel.

According to the original specifications, the GPRS network was able to multiplex the following combinations of logical channels to a single PDCH over the GPRS multiframe:

1) PBCCH + PCCCH + PDTCH + PACCH + PTCCH
2) PBCCH + PCCCH
3) PCCCH + PDTCH + PACCH + PTCCH
4) PDTCH + PACCH + PTCCH

In other words, one PDCH timeslot (in 52 consecutive GSM frames) could carry many types of signaling channels together with a dedicated packet data channel. Multiplexing of the logical channels to the PDCH is done in the following way: Among the available combinations of logical channels to be multiplexed to the PDCH, one is chosen. Each of the channels in the combination is granted with a certain fraction of the 52 PDCH bursts of the multiframe. The channels are mapped to the sequence of 52 bursts in the order as stated above for each of the four multiplexing options. To limit impact of short disturbances on the radio channel, the sequence of 52 PDCH bursts for logical channel multiplexing is defined in a very specific way, instead of just concatenating the bursts in the order of TDMA frames transmitted. As described earlier, the GPRS multiframe consists of 52 GSM TDMA frames, grouped to 12 GPRS radio blocks B0–B11 of four frames. The four GSM frames that do not belong to any GPRS radio block are used for the PTCCH. PDCH bursts of the radio blocks are used for the other channels. The bursts of different radio blocks are concatenated to one contiguous stream of bursts with the following order of radio blocks: B0, B6, B3, B9, B1, B7, B4, B10, B2, B8, B5, and B11.

As an example, we use the PDCH to which the following logical channels have been multiplexed according to option 4: PDTCH (ten radio blocks B0, B6, B3, B9, B1, B7, B4, B10, B2, and B8), PACCH (two blocks B5 and B11), and PTCCH (four individual GSM frames, one after each group of three radio blocks). In this case, the PDCH timeslots of the multiframe are divided between the logical channels as follows:

- PDTCH: frames 0–3, 26–29, 13–16, 39–42, 4–7, 30–33, 17–20, 43–46, 8–11, 34–37
- PACCH: frames 21–24, 47–50
- PTCCH: frames 12, 25, 38, 51

While 3GPP has evolved GSM and GPRS specifications, the packet broadcast and common control channels PBCCH and PCCCH have been deprecated. Their services have been merged with the GSM broadcast and common control channels BCCH and CCCH. The latest versions of TS 44.018 [42] say: “Independently of what is stated elsewhere in this and other 3GPP specifications . . . the network shall never enable PBCCH and PCCCH.” This is due to optimizing the service. These GPRS channels were eventually deemed redundant to GSM broadcast and common channels, so it was decided to merge those to simplify the system. Consequently, from the above-mentioned four specified logical channel combinations for PDCH, only options 3 and 4 are still deployed.

**Table 5.2** GPRS coding schemes.

| | PDCH data rate (kbps) | Coding ratio (%) | Coding method |
|---|---|---|---|
| CS-1 | 8 | 50 | A checksum of 40 bits is added to the 181 bits of RLC/MAC frame and the three USF bits. The result is encoded with 1/2 convolutional code. |
| CS-2 | 12 | 66 | A checksum of 16 bits is added to the 268 bits of RLC/MAC frame and the 6 precoded USF bits. The result is encoded with 1/2 convolutional code and thereafter predefined 132 bits are removed (puncturing). |
| CS-3 | 14.4 | 75 | A checksum of 16 bits is added to the 312 bits of RLC/MAC frame and the 6 precoded USF bits. The result is encoded with 1/2 convolutional code and thereafter predefined 220 bits are removed (puncturing). |
| CS-4 | 20 | 100 | A checksum of 16 bits is added to the 428 bits of RLC/MAC frame and the 3 USF bits. Thereafter, precoding is applied to USF bits to generate a sequence of 12 bits. |

#### 5.2.3.3 GPRS Channel Coding and Transmitter Design

GPRS uses the same methods for dividing the user bit data stream to bursts as GSM. However, GPRS supports the four **coding schemes** as in Table 5.2 to generate a sequence of 456 bits from RLC/MAC frame, to be carried as an RLC data block within the four PDCH bursts of a GPRS radio block:

Note that the PDCH data rate means the data rate for using one timeslot per GPRS frame. The full data rate of GPRS connection is the PDCH data rate multiplied with the number of PDCHs (timeslots) used per GSM TDMA frame. As can be seen in the table, the size of the RLC/MAC frame is different in these encoding methods. The CS-4 coding method provides the highest bit rate for traffic tolerant to errors or delay due to retransmissions. CS-4 is typically used over channels with good radio signal quality. CS-1 minimizes the latency since the strong forward error correction reduces the need for any retransmissions.

The **coding ratio** is number of original data bits compared to the user data bits used in the transmission. Coding schemes with smaller coding ratio are more robust against transmission errors as 1 user data bit is encoded with multiple redundant bits. Coding ratio can be adjusted with the puncturing technique, where some of the data bits in fixed bit positions are not sent at all. The receiver adds 0 bits to these positions and then applies convolutional decoding. If the punctured bit was 1 rather than 0, then these bits would appear to the decoder as bit errors. Puncturing increases effective data rates but decreases efficiency of the forward error correction. Puncturing ratios are chosen to find a reasonable balance between those.

The sequence of 456 bits generated in the channel coding process is interleaved to four bursts of the radio block with GSM interleaving methods. The structure of the burst sent on the PDTCH channel is the same as used on GSM TCH channel. The stealing bits of the burst are used in GPRS to indicate the coding scheme used for the burst. The burst sent on the PRACH channel had the same structure as a burst on the GSM RACH channel. Figure 5.25 shows the block diagram of GPRS transmitter.

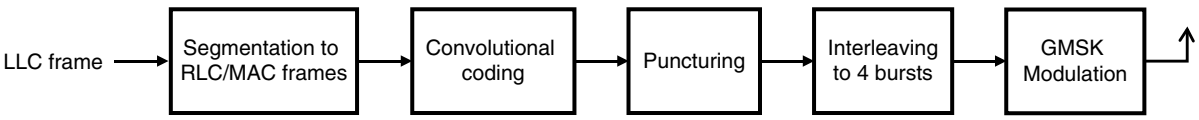


**Figure 5.25** GPRS transmitter design.

### 5.2.4 Protocols between MS and GPRS Network

#### 5.2.4.1 MAC Protocol

**GPRS medium access control (MAC)** protocol takes care of multiplexing PDTCH data channel and PACCH signaling channel to the PDCH channel allocated to the mobile station. The GPRS MAC protocol is specified in 3GPP TS 44.060 [67] for mobile stations that use traditional GSM A/Gb interfaces and in 3GPP TS 44.160 [68] for those that rely on the Iu interface, which was introduced originally for UMTS but reused later also for GPRS.

Uplink and downlink GPRS MAC frames use different structures and header fields as shown in Figure 5.26. The uplink MAC frame sent by the mobile station has the following fields:

- Payload type tells if the frame contains the user data (PDTCH) or signaling (PACCH).
- Countdown value (CV) is the number of radio blocks still needed for the TBF. This value is decreased after each radio block transmitted. The network uses this value to check the number of radio blocks to be allocated before releasing the TBF.
- Stall indicator tells if the RLC transmit window of the mobile station is able to move or not.
- Retry bit tells if the mobile station has sent a CHANNEL REQUEST message only once or multiple times during its most recent random access attempt.
- Payload data is inside of the uplink MAC frame, which is an RLC frame.

The downlink MAC frame sent by the base station has the following fields:

- Payload type tells if the frame contains the user data (PDTCH) or signaling (PACCH).
- Relative reserved block period (RRBP) indicates the mobile station the radio block uses for RLC/MAC PACKET CONTROL ACKNOWLEDGE messages or other PACCH channel signaling.
- Supplementary/polling (S/P) bit tells if the mobile station shall send the acknowledgment on the radio block identified by RRBP or not.
- USF tells which of the mobile stations listening to this timeslot may use the next uplink radio block for its transmission.
- Payload data is inside of the downlink MAC frame, which is an RLC frame.

#### 5.2.4.2 RLC Protocol

**GPRS Radio Link Control (RLC)** protocol transports LLC protocol frames between the base station and mobile station. It additionally has the task to segment the LLC frames to blocks that fit into a single radio block and reassembly of those frames on the receiving end of the link. As a result of the segmentation process, a single RLC frame may contain only a fraction of a single LLC frame, or it may have the end of one LLC frame and the start of the next one. After channel coding, the length of one RLC/MAC frame equals the length of four GPRS bursts. Thus, one GPRS PDCH can carry the frame within a single radio block. GPRS RLC protocol is specified in 3GPP TS 44.060 [67].

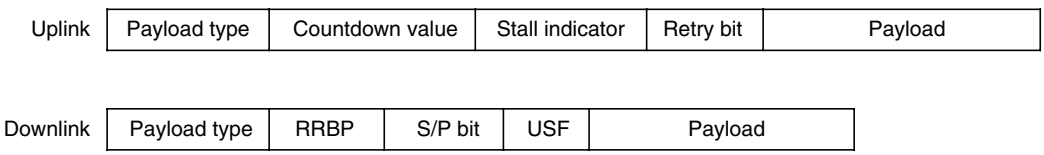


**Figure 5.26** Structures of GPRS MAC uplink and downlink frames.


**Figure 5.27** Structures of GPRS RLC uplink and downlink data frames.

RLC protocol uses one of the following modes for transporting the frames:

- Acknowledged mode is where the received frames are acknowledged and retransmitted if the frame was corrupted on the radio path. A retransmission window of 64 frames is used so that transmission of new frames stops only when no acknowledgments are received for 64 consecutive frames. The acknowledge message tells the sequence number of the frame up to which all frames have been successfully received. Retransmission of a frame can be requested with a negative acknowledgment. While RLC data frames are transmitted over the PDTCH channel, RLC acknowledgments are sent on the PACCH.
- Non-acknowledged mode is without any RLC level retransmissions. The transmission delay of RLC frames over radio interface is fixed, but the transmission is less reliable than in the acknowledged mode.

The RLC mode used is chosen when the mobile station requests the network to allocate a new packet data protocol context (PDPC) for it.

Like MAC frames, the uplink and downlink RLC have different structures, as shown in Figure 5.27. The uplink RLC frame has the following fields:

- Packet flow identifier (PFI) indicator (PI) bit tells if the frame has PFI fields.
- Temporary flow identifier (TFI) is the identifier of the TBF to which the RLC block belongs. The TBF identifies the mobile station that has sent the frame.
- Temporary logical link identifier (TLLI) indicator (TI) bit tells if the frame has a TLLI field.
- Block sequence number (BSN) is the sequence number of the RLC block.
- There are one or multiple records, each of which describes a fraction of an LLC frame within the RLC frame payload:
  - Length indicator (LI) is the number of octets of the LLC frame.
  - More (M) bit tells if the payload has a fraction of another LLC frame.
- Temporary logical link identifier is the identifier of LLC protocol link between the mobile station and SGSN.
- Packet flow identifier.
- Payload of the uplink RLC frame carrying the LLC fragments.

The downlink RLC data frame has the following fields:

- Power reduction (PR) tells if the mobile station shall adjust its transmission power for upcoming radio blocks.
- TFI is the identifier of the TBF to which the RLC block belongs. The TBF identifies the mobile station that will receive the frame.
- Final block identifier (FBI) bit identifies if this RLC block is the last one sent on the downlink to the mobile station. The downlink TBF is released right or soon after the network sets this bit.
- BSN is the sequence number of the RLC block.
- There are one or multiple records, each of which describes a fraction of an LLC frame within the RLC frame payload:
  - LI (length indicator) is the number of octets of the LLC frame.
  - M (more) bit tells if the payload has a fraction of another LLC frame.
- The payload of the downlink RLC frame carries the LLC fragments.

The downlink RLC signaling frame has the following fields:

- Reduced block sequence number (RBSN): the sequence number of a signaling block.
- Radio transaction identifier (RTI) has identical value in those radio blocks that have a segment of one single upper layer signaling message.
- Final segment (FS) bit identifies the block which contains the last segment of a single upper layer signaling message.
- Power reduction (PR) tells if the mobile station shall adjust its transmission power for upcoming radio blocks.
- TFI is the identifier of the TBF to which the RLC block belongs. The TBF identifies the mobile station that will receive the frame.
- Reduced block sequence number extension (RBSNe) is the sequence number when extended RLC/MAC control message segmentation is used.
- Final segment extension (FSe) bit identifies the block that contains the last segment of one single upper layer signaling message when extended message segmentation is used.
- The payload of the RLC frame.

#### 5.2.4.3 LLC Protocol

**Logical Link Control (LLC)** protocol transports upper layer protocol messages over the logical link between the mobile station and SGSN. GPRS LLC protocol is specified in 3GPP TS 44.064 [69]. The LLC protocol provides the following services:

- Acknowledged and non-acknowledged modes like the RLC protocol. Acknowledged mode uses frame checksums and retransmissions for error control. In the non-acknowledged mode, LLC can be configured to either drop corrupted frames or pass them to the upper layer protocol, which would take care of correcting the errors.
- Flow control and message sequence control over the logical link.
- Encryption and integrity protection of transmitted data using the keys created during the authentication process.
- Point-to-multipoint messages from an SGSN to multiple mobile stations.

Temporary logical link identifier (TLLI) identifies a logical link between the GPRS mobile station and the SGSN. More precisely, the SGSN assigns a TLLI to the mobile station to identify it. As long as the mobile station stays in the cells within the routing area served by the SGSN, the link and its TLLI identifier remain the same. But when the mobile station moves to a cell under another SGSN, a new logical link is opened and the old link is closed. The MS gets a new TLLI from the new SGSN. The link is kept alive over any idle periods when no user data is transferred.

Multiple parallel data flows may be multiplexed to the logical link. Those data flows are identified with SAPI code of the LLC protocol. The following SAPI values are defined in GPRS:

- SAPI = 1: the flow is used to transport GMM messages
- SAPI = 2: tunneling of messages
- SAPI = 3: messages using QoS level 1
- SAPI = 5: messages using QoS level 2
- SAPI = 7: short messages over GPRS
- SAPI = 8: tunneling of messages
- SAPI = 9: messages using QoS level 3
- SAPI = 11: messages using QoS level 4

The QoS levels are used to assign priorities between different types of messages when the network is under high load. There are no fixed QoS parameter values or for any SAPI, but those are negotiated when taking SAPI into use. Data link connection identifier (DLCI) is the combination of TLLI and SAPI to identify a data flow over the logical link

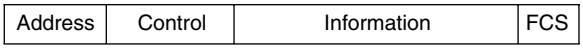


**Figure 5.28** Structure of the GPRS LLC frame.

The LLC frame structure shown in Figure 5.28 resembles HDLC protocol frames. The LLC frame has the following fields:

- Address field, consisting of the following subfields:
  - The protocol discriminator (PD) has value 0 for GPRS LLC.
  - The command/response (C/R) bit that tells if the LLC frame contains a command or response.
  - SAPI identifies the flow and defines the QoS level of the message. The specific upper layer protocol GMM, SMS, or SNDCP transported by the LLC frame can also be deduced from the SAPI.
- Control field, which describes the type of the frame:
  - Acknowledged or non-acknowledged mode
  - Supervisory function or control function
- Information field, which contains the upper layer protocol data payload.
- The frame check sequence (FCS), a checksum of 24 bits calculated over the frame.

The maximum size of an LLC frame in GPRS is 1600 octets.

#### 5.2.4.4 SNDCP Protocol

**GPRS subnetwork dependent convergence protocol (SNDCP)** is specified in 3GPP TS 44.065 [70]. The SNDCP protocol has the following tasks:

- Compress the headers and data of the transported packet data protocol before segmentation. Usage of compression is negotiated when opening the PDP context for the mobile station.
- Splitting the transported data to segments that can be carried as payload of LLC frames.
- Adapt different packet data protocols to the LLC protocol used over the link. Multiplex the packet data protocol messages with the same QoS level to one single SAPI flow of the LLC layer.
- Use either acknowledged or non-acknowledged LLC mode on the logical link for data transfer. Establish and release LLC connections for acknowledged mode.
- Reassemble and decompress data received from the LLC and forward it to the correct packet data protocol entity.

The SNDCP frame has the following fields shown in Figure 5.29:

- X-bit, always 0
- F-bit (first segment indicator) tells if the SNDPC frame contains the first segment of an upper layer protocol message
- T-bit protocol data unit ([PDU] type) tells if the frame uses acknowledged or non-acknowledged mode.
- M-bit (more) tells if the SNDPC frame contains the last segment of an upper layer protocol message.
- NSAPI identifier tells the type of the packet data protocol carried as the payload of SNDCP.
- DCOMP tells the type of compression applied to the upper layer data.
- PCOM tells the type of compression applied to the addresses of the carried packet data protocol.
- Segment number used for non-acknowledged SNDCP mode.

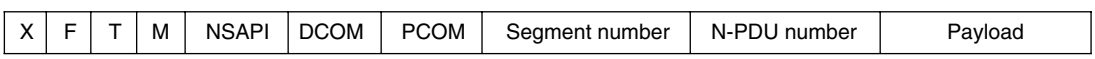


**Figure 5.29** Structure of GPRS SNDCP frame.

- N-PDU number is the sequence number of the upper layer protocol frame.
- Payload of the SNDCP frame for carrying upper layer data segments.

### 5.2.5 Protocols of GPRS Network

#### 5.2.5.1 NS Layer Protocols

**Network Service (NS)** layer provides a link layer connection between the PCU and SGSN. For the link implementation, 3GPP has defined two options:

- The original GPRS design relied on E1 links on top of which virtual connections were created with the frame relay protocol, described in Chapter 3, Section 3.2.1.
- The newer design was to use the internet protocol over Ethernet fiber links. This option has gradually replaced the frame relay in GPRS network deployments. Similar links are used also between the GGSN and SGSN.

With frame relay, a link of the NS layer is a virtual connection created over all the physical cable links and other pieces of network equipment between the PCU and SGSN. Every single piece of equipment along the virtual connection path shall support the FR protocol and have a static routing configured to forward FR frames between correct physical links. This kind of connection is called **permanent virtual circuit (PVC)**. The frame relay provides the following features:

- Permanent end-to-end virtual circuits that can be set up by the network management system
- Statistical multiplexing of data packets from different virtual circuits to physical links

The PCU has one PVC circuit to the SGSN while the SGSN has one PVC to every PCU connected to it. One virtual connection to a PCU carries all the GPRS data flows for mobile stations served by the PCU.

With IP over Ethernet, the frame relay switches have been replaced by IP routers. No virtual connections are used, but the Ethernet frames are terminated at the end of each link. The IP packets are then routed between the PCU and SGSN.

#### 5.2.5.2 BSSGP Protocol

**Base station subsystem GPRS protocol (BSSGP)** is used on top of the NS layer between the SGSN and PCU. The GPRS BSSGP protocol is specified in 3GPP TS 48.018 [71]. When using frame relay on the NS layer, BSSGP maps traffic from BSSGP virtual circuits (BVC) to the PVCs of the NS layer. The BSSGP protocol takes care of BVC packet flow control and buffering of data packets received from different sources before forwarding them to the links. BSSGP has three layers of data buffers on top of each other, as shown in Figure 5.30. The buffers are called as buckets, as they behave like ATM buckets described in *Online Appendix H.5.4*.

- The bucket for an individual packet flow context (PFC), which carries an individual data flow for mobile station. Usage of the PFC flow control and buckets is optional.
- The bucket for the complete aggregate packet data flow toward a mobile station.
- The bucket for the packet data flow passing through the BVC to the NS layer.

Buffering is used for statistical multiplexing, since the amount of data sent or received by mobile stations may temporarily exceed the capacity reserved for the BVC. The excess packets are buffered to queue for transmission. If a buffer would overflow, some of the packets are dropped and an LLC-DISCARDED PDU message is sent to the source of the dropped packets to inform it about the buffer overflow. The source could then reduce its data rate.

The BSSGP protocol uses FLOW-CONTROL PDU messages specific to each bucket to adjust the sizes of buffers in the end of the connection and the output data rate from the buffer. The user data packets (LLC PDUs) are carried as the payload of BSSGP UNITDATA PDU messages.

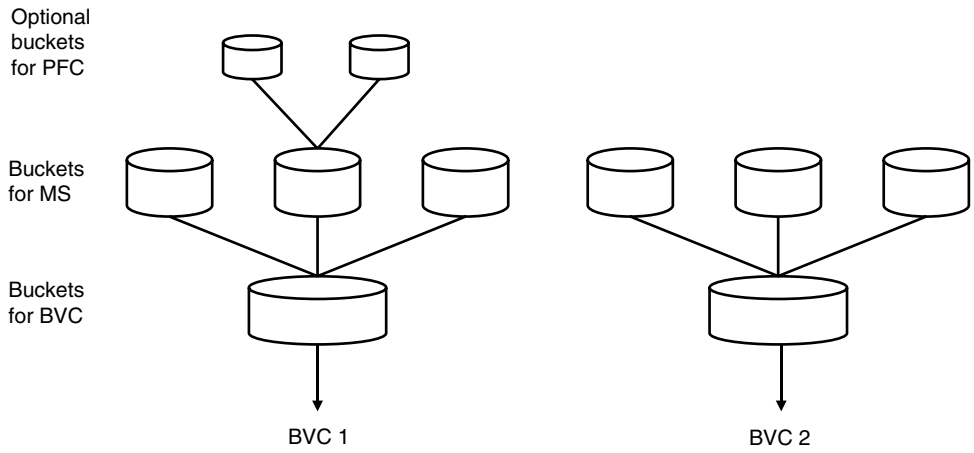


**Figure 5.30** Buffers of BSSGP protocol.

In addition to user data transport, the BSSGP protocol supports also various GPRS mobility management and PDP context management signaling procedures. An SGSN uses the BSSGP protocol to instruct the BSS subsystem to page a mobile station to activate the data connection when a data packet arrives to the mobile station. Also, the PS handover control messages are carried over BSSGP.

BSSGP protocol messages start with the PDU type field, the value of which determines the composition of other fields within the message.

#### 5.2.5.3 GTP Protocol

**GPRS Tunneling Protocol (GTP)** is used between the GGSN and SGSN to transport both user data and signaling messages. Basically, it would be possible to transport both types of data directly on top of the IP network used between the GGSN and the base station. The drawback is that any move of a mobile station between cells would cause the routing tables of the IP routers to reflect the new location of the IP address of the mobile station. Such a network-wide routing table update is both a slow and heavy operation. The GTP tunneling approach solves this problem by hiding the movements of the mobile station from the underlying IP network. Instead, only SGSNs track the locations of mobile stations. Other routers within the GPRS network see only IP addresses of tunnel endpoints, rather than IP addresses assigned to the mobile stations. The SGSNs inform GGSNs via which SGSN and related tunnel the mobile stations can be reached. The IP routing tables are then modified only at GGSN per MS but not in the rest of the IP network infrastructure between the GGSN and mobile station. At the GGSN, the endpoint of routing is the SGSN that servers the mobile station, rather than the mobile station itself.

GTP is divided to the GTP-U and GTP-C subprotocols, where U stands for user and C for control. User data flows between the GPRS mobile station and an external packet data network are carried within GTP-U tunnels created between the GGSN and SGSN. The GPRS signaling messages between the GGSN and SGSN and are sent with GTP-C protocol. PDP context management messages, tracking area update messages or GTP tunnel management messages are examples of GPRS signaling messages. The GPRS GTP protocol is specified in 3GPP TS 29.060 [72].

The Gn interface between GSN nodes uses the packet switched IP protocol stack. GTP protocol enables the GPRS network to transport multiple different user packet data protocols (such as X.25 and IP) so that the GGSN and SGSN nodes do not need to understand and interpret those protocols. The user data packets are encapsulated

into GTP-U packets, which form tunnels maintained with the GTP-C protocol. The GTP-U packets are carried over the network with underlying TCP/UDP/IP protocols.

User data packets from external networks are routed via GGSNs to GPRS mobile stations. In those packets, the destination is identified with the address that the GGSN has given for the mobile station when the PDP context was created. The GGSN routes those packets toward the mobile station and its SGSN over the GTP-U tunnel of the PDP context. The same tunnel is also used for uplink data packets from the mobile station to the external packet data network. The tunneling mechanism encapsulates the inner user data packet into an outer GTP-U packet of the tunnel. The source and destination addresses of the outer GTP-U packet are IP addresses of the GGSN and SGSN. In this way, GTP relies on IP routing mechanisms. The IP address that the mobile station has for its PDP context is used in the downlink packet routing process as follows:

- When a user data IP packet arrives from an external PDN network to the GGSN, its destination IP address is used to select the PDP context and GTP tunnel to transport the user data packet to the correct SGSN node.
- When the SGSN receives the user data packet, it checks the destination IP address of the packet to route it to the destination mobile station. The packet arrives to the mobile station via the base station under which the mobile station currently camps.

If GGSN receives packets from an external data network with destination addresses not mapped to any of its PDP contexts, those packets shall be processed in either of the following two ways:

- If the GGSN finds from its database that the address is fixedly reserved for a mobile station, the GGSN tries to find out which SGSN is currently serving the mobile station. If the mobile station has attached to GPRS service, the GGSN opens a PDP context to the mobile station and forwards the packets to it.
- If the GGSN does not find the destination address from its database, the packet is dropped.

The structure of GTP frame depends on the purpose to which the frame is used. There are always the following fields in the frame:

- Version of the GTP protocol
- Protocol type: GTP or GTP'. GTP' is a charging protocol based on GTP.
- E, S, and PN-bits, which tell if the frame contains extension headers, sequence number and/or N-PDU number of the upper layer protocol frame.
- Message type
- Payload length
- Tunnel endpoint identifier (TEID), which identifies the endpoint of the GTP tunnel. TEID is generated from the user's MCC, MNC, and MSIN numbers at the PDP context activation.

The frame may additionally have also the following fields, as shown in Figure 5.31:

- Sequence number of the frame
- N-PDU number of the upper layer protocol, such as LLC
- Other additional fields
- The payload of the GTP frame

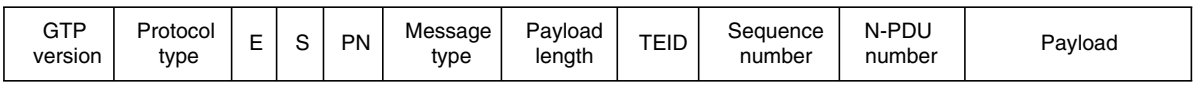


**Figure 5.31** Structure of the GPRS GTP data frame.

### 5.2.6 Radio Resource Management

#### 5.2.6.1 Opening and Releasing of Dedicated GPRS Radio Channels

The GPRS mobile station is in either of the two following modes, depending on whether it has a dedicated packet data channel or not:

1) **Packet idle mode:** No dedicated packet data channel has been granted for the mobile station in packet idle mode. The mobile station listens to the messages sent to it over the PCH and PPCH channels as well as the SYSTEM INFORMATION messages broadcasted on BCCH (and earlier PBCCH) channels. The mobile station may also send a random access request over the RACH channel. The network responds to such access requests on the AGCH channel, after which the mobile station moves to the dedicated mode. The mobility management state of the MS is either **idle** or **standby**.
2) **Dedicated mode:** The mobile station has an active packet data connection with the network in the dedicated mode. The network has granted the station with a PDTCH user data channel and a PACCH signaling channel. Additionally, the network has allocated the mobile station a PTCCH channel, which is used to adjust the timing advance of the mobile station. The mobility management state of the MS is **ready**.

When the mobile station moves from idle to dedicated mode, a TBF is created. The TBF is released when moving back to idle. In the dedicated mode, the mobile station has a packet data connection open at least up to the SGSN at GPRS attach, but up to the GGSN when the PDP context has been activated. The packet data connection is opened separately from the mobile station toward the network (uplink) and from the network to mobile station (downlink). The request to activate the connection may be initiated either by the mobile station or network.

The mobile station moves from the packet idle mode to the dedicated mode by performing an access procedure, because of one of the following reasons:

1) The mobile station has to send a signaling message or user data.
2) The mobile station should receive an incoming data packet. In this case, the mobile station requests access after the network has paged the station.
3) The mobile station sends an RLC/MAC control message.

There are three ways to perform the GPRS access procedure:

- One-phase access: After receiving the random access request, the network immediately grants the mobile station with a single PDCH. One-phase access can only be used if the mobile station responds to paging or wants to use the RLC acknowledged mode over one single PDCH.
- Two-phase access: After receiving the random access request, the network grants the mobile station with PDCH access to one or two radio blocks only. The mobile station uses the grant to send a packet resource request, based on which the network grants the mobile station with a packet data channel. Two-phase access must be used if the mobile station either requests multiple PDCHs for higher data rates or wants to use the non-acknowledged RLC mode.
- Single block access: After receiving the random access request, the network grants the mobile station with PDCH access to one radio block. The mobile station uses the grant to send an RLC/MAC control message or to initiate the two- phase access.

The complete GPRS access procedure is done as shown in Figure 5.32:

1) The mobile station requests a dedicated packet data channel by sending either an RRC CHANNEL REQUEST or RLC/MAC EGPRS PACKET CHANNEL REQUEST random access message to the BSC over the GSM RACH channel. With a CHANNEL REQUEST message, the mobile station may either request one-phase access or single block access. With an EGPRS PACKET CHANNEL REQUEST message, the mobile station

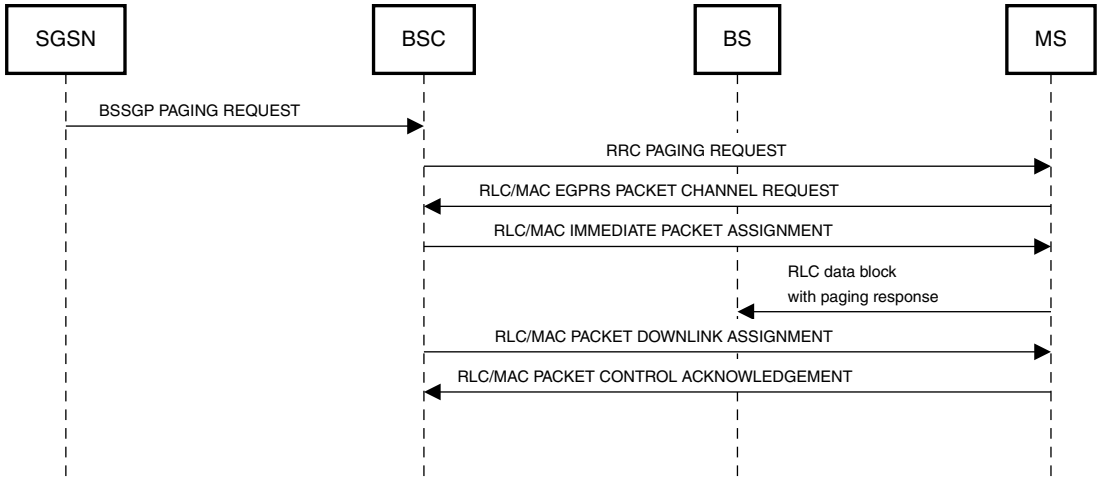


**Figure 5.32** GPRS downlink channel activation for MT data.

may request either a one- or two-phase access procedure and provide further information about the request type specific options.

2) The BSC responds to the mobile station over the GSM AGCH channel with either an RRC IMMEDIATE ASSIGNMENT or a MAC/RLC IMMEDIATE PACKET ASSIGNMENT message. If one-phase access is used, the message describes the PDCH channel, which is continuously allocated to the mobile station and provides the TFI and USF identifiers of the TBF. The message may also have an optional bit vector indicating the radio blocks allocated to the mobile station. The message completes the one-phase or single block access procedure. Instead of the one-phase PDCH grant, in its response the network may alternatively provide only single or multiple PDCH radio blocks for the following cases:
   - The mobile station requested single block access.
   - The mobile station requested two-phase access.
   - The mobile station requested one-phase access but the network decided to use the two-phase access.
3) In the two-phase access, the mobile station uses the granted radio block to send an RLC/MAC PACKET RESOURCE REQUEST message over the PACCH to the BSC. This message describes the details of the channel request, the radio access capabilities of the mobile station, the temporary logical link identity (TLLI) identifier of the logical link, and the TFI, if the request is related to an existing TBF. The packet channel can be reserved either for transporting a defined amount of data or until further notice.
4) The BSC responds by sending either an RLC/MAC PACKET UPLINK/DOWNLINK ASSIGNMENT or a MULTIPLE TBF UPLINK/DOWNLINK ASSIGNMENT message to describe the PDCH allocation. The former type of message is used for a single TBF and the latter for multiple TBFs and data flows. The message contains the following pieces of information related to the dedicated packet data channel:
   - The TFI identifier of the TBF, used to identify the downlink GPRS radio blocks allocated for the TBF and the TBF itself for any further requests
   - PDCH timeslots allocated for the TBF and the parameters to define the frequency hopping schemes on them
   - Array of USF identifiers, one per PDCH timeslot, used for identifying uplink PDCH radio blocks allocated dynamically for the mobile station
   - The coding scheme, MAC, and RLC modes to be used on the TBF
   - Timing advance and power control parameters

When the GPRS mobile station has a PDP context in the standby state, the SGSN activates the downlink data channel for a mobile terminated data packet as follows:

1) The SGSN sends a BSSGP PAGING REQUEST to the BSS, causing the BSC to send an RRC PAGING REQUEST to the mobile station. The MS is identified by the P-TMSI identifier of the subscriber. The MS responds with a random access message, which tells the reason of the request as one-phase access for a paging response. The BSC then sends an immediate assignment message to allocate a single signaling PDCH for the mobile station. The mobile station then sends its response to the paging request over the newly allocated signaling channel.
2) After completing paging, the BSC sends a packet downlink assignment message to the mobile station. This message describes the PDCH timeslot, power control, and timing parameters to be used for the packet data channel over which the MT data packet will arrive. After taking the downlink channel into use, the mobile station may at any moment reserve also an uplink data channel by sending a channel request within the packet data acknowledgment messages.

For further details about the messages used in this procedure, please refer to *Online Appendix I.3.1* (Figure 5.32).

The network may release the uplink connection when the mobile station decrements the countdown value counter of the MAC frame to zero to tell that all user data has been sent. The mobile station may start using the countdown mechanism either spontaneously or after the network has requested the connection release by sending an RLC/MAC PACKET PDCH RELESE message to the mobile station. To finally release the uplink connection, the BSC sends an RLC/MAC PACKET UPLINK ACK message with Final_Ack value 1.

The downlink connection is released so that the network sends an RLC frame with value 1 in its FBI field. The mobile station acknowledges the release by setting the Final_Ack value as 1 to the RLC/MAC PACKET DOWNLINK ACK response. If the connection uses unacknowledged RLC mode, the mobile station may send a separate RLC/MAC PACKET CONTROL ACK message. The mobile station may also request the network to release the connection by sending a message with its TBF_RELEASE bit set.

### 5.2.7 Mobility Management

#### 5.2.7.1 GPRS Attach

In the GPRS attach, the mobile station announces itself to an SGSN. The purpose of GPRS attach is to get a SGSN to start tracking the location of the mobile station so that the network could route mobile terminated packet data to the station. The mobile station attaches to one single SGSN node at any time. This SGSN serves the routing area within which the mobile station is located. At the GPRS attach, the SGSN authenticates the subscriber and checks which services the subscriber is entitled to use.

The GPRS mobile station may be in one of the three GPRS mobility management states:

- **Idle:** The mobile station is not attached to a GPRS network.
- **Ready:** The mobile station is attached to a GPRS network and has a PDP context. An MS enters ready state whenever signaling or user data is sent to/from it over GPRS. After the data transmission stops, the mobile station stays in ready state until expiration of timer T3314. In the ready state, the mobile station must report any cell reselection performed.
- **Standby:** The mobile station enters the standby state when it exits the ready state by the timer expiration. In the standby state, the mobile station reports cell reselections only when the routing area changes. The network can move the mobile station from the standby to the ready state by paging MS for incoming data.

The GPRS attach procedure is performed as shown in Figure 5.33:

1) The mobile station searches the GSM network and synchronizes itself to the FCCH and SCH channels of the cell. The mobile station starts reading system information messages. From the SYSTEM INFORMATION TYPE13 message, the mobile station acquires parameters needed for GPRS attach, such as routing area code, timer values, and supported optional GPRS features.

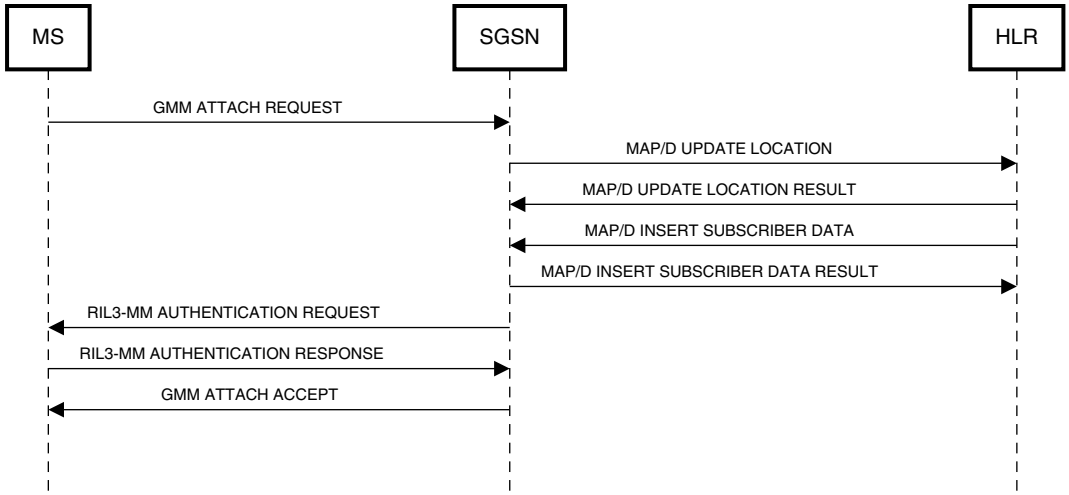


**Figure 5.33** GPRS attach procedure.

2) The mobile station opens a GPRS dedicated packet signaling channel as described in Section 5.2.6.1. The mobile station uses the channel to send a GMM ATTACH REQUEST to the SGSN, in order to register itself to the GPRS service. Additionally, the mobile station may request registration to the GSM service for SMS and voice calls. The mobile station identifies itself with its P-TMSI identifier allocated to the station and gives the RAI identifier of the routing area where that P-TMSI was most recently used.
3) The SGSN updates the new location of the subscriber to the HLR of the subscriber's home network. The HLR confirms if the subscriber is entitled to use the GPRS service of the attached network and sends the GPRS subscriber information back to the SGSN. Thereafter, the SGSN authenticates the subscriber and allocates a new P-TMSI identifier for the mobile station. The SGSN completes the sequence with an attach accept response to the mobile station, referring to the new P-TMSI.

For further details about the messages used in these procedures and protocols below GMM, please refer to *Online Appendix I.3.2*.

The mobile station may also perform a combined GSM/GPRS attach procedure in which the SGSN informs an MSC over the Gs interface about the location of the mobile station. Both the SGSN and MSC inform the HLR about the location of the MS within the packet switched and circuit switched domains, respectively. If the HLR knows any old SGSN and MSC, which have previously served the mobile station, the HLR sends cancel location messages to them (Figure 5.33).

The mobile station may disconnect from the GPRS service by sending the SGSN a GMM DETACH REQUEST. The SGSN acknowledges this message with a GMM DETACH ACCEPT response. Thereafter the SGSN will tear down any related active PDP contexts by sending a DELETE PDP CONTEXT REQUEST messages to all the GGSN nodes that had active PDP contexts for the disconnected mobile station.

#### 5.2.7.2 Cell Reselection

Like a GSM station, the GPRS mobile station selects the serving cell based on the signal quality measurements. The GPRS mobile station may perform cell reselection either autonomously or with the GPRS specific network-assisted cell change (NACC) procedure. These procedures work as follows:

- Autonomous cell selection works as in GSM. The mobile station learns frequencies used by the neighboring cells from the SYSTEM INFORMATION 2 message. After doing measurements, the MS may decide to change the serving cell. The MS synchronizes to the new cell and reads its system information messages.

- With NACC, the difference is that after making measurements and deciding to change the cell, the MS may send an RLC/MAC PACKET CELL CHANGE NOTIFICATION message to the serving base station. The base station responds with an RLC/MAC PACKET NEIGHBOR CELL DATA message with relevant parts of the system information of the new cell to speed up the MS to connect to the new cell.

#### 5.2.7.3 Routing Area Update

When moving from one cell to another in the standby state, the GPRS mobile station checks if the new cell belongs to a different routing area than the old cell. If that is the case, the mobile station shall acquire a dedicated channel and send a routing area update message to announce its new location to the network. Since the dedicated channel is used to send a single signaling message, the mobile station uses the one-phase access method to get a PACCH allocation for those radio blocks needed to send the update.

Routing area update messages are not used when the mobile station is using TBF. In that case, the network tracks the location of the mobile station in the accuracy of a cell as follows. The mobile station in the dedicated mode moves between two cells within a single routing area. The mobile station releases its TBF connection toward the old cell and opens a new TBF for the new cell. When any packets sent by the mobile station reach the SGSN over the new TBF, SGSN detects the location of the mobile station from the global cell identifier added by the PCU to the packets.

These are the following major scenarios for the GPRS routing area update procedure:

- The mobile station moves from a routing area to another. In this case, the mobile station sends a routing area update message.
- The mobile station moves simultaneously between two routing areas and GSM location areas. In this case, the mobile station updates both its routing area and location area with a combined update procedure.
- The mobile station sends a periodic routing area update even if it has not changed the cell.
- The mobile station sends a routing area update right after attaching to GPRS.

The GPRS routing area update procedure is performed as shown in Figure 5.34:

1) The mobile station sends a GMM ROUTING AREA UPDATE REQUEST message to the SGSN that serves new cell. The MS identifies itself with its P-TMSI identifier and the identifier of its old routing area in case the SGSN was changed. The new SGSN retrieves the mobility management and PDP contexts of the mobile station from the old SGSN. After providing the context data, the old SGSN establishes a GTP tunnel to the new SGSN and sends any data packets buffered for the mobile station via the tunnel. The new SGSN forwards those packets to the mobile station.
2) The new SGSN contacts all the GGSN nodes that have active PDP contexts for the mobile station. Those GGSN nodes establish new GTP tunnels to the new SGSN and tear down the old ones toward the old SGSN.
3) The new SGSN updates the location of the mobile station to the HLR, which now tells the old SGSN to purge any expired location and subscriber data records for the subscriber. The HLR thereafter sends the subscriber data records to the new SGSN, so that the new SGSN can authenticate the subscriber. Finally, the new SGSN acknowledges the routing area update procedure.

For further details about the messages used in these procedures, please refer to *Online Appendix I.3.3*.

### 5.2.8 Packet Data Connections

#### 5.2.8.1 PDP Context Management

To transport packet data over GPRS, the mobile station must open **PDPC** after attaching to the GPRS service. GPRS attach enabled the network to track the routing area of the mobile station, but a PDP context is needed for GPRS data transfer. The mobile station gets a packet data protocol address at the PDP context activation.

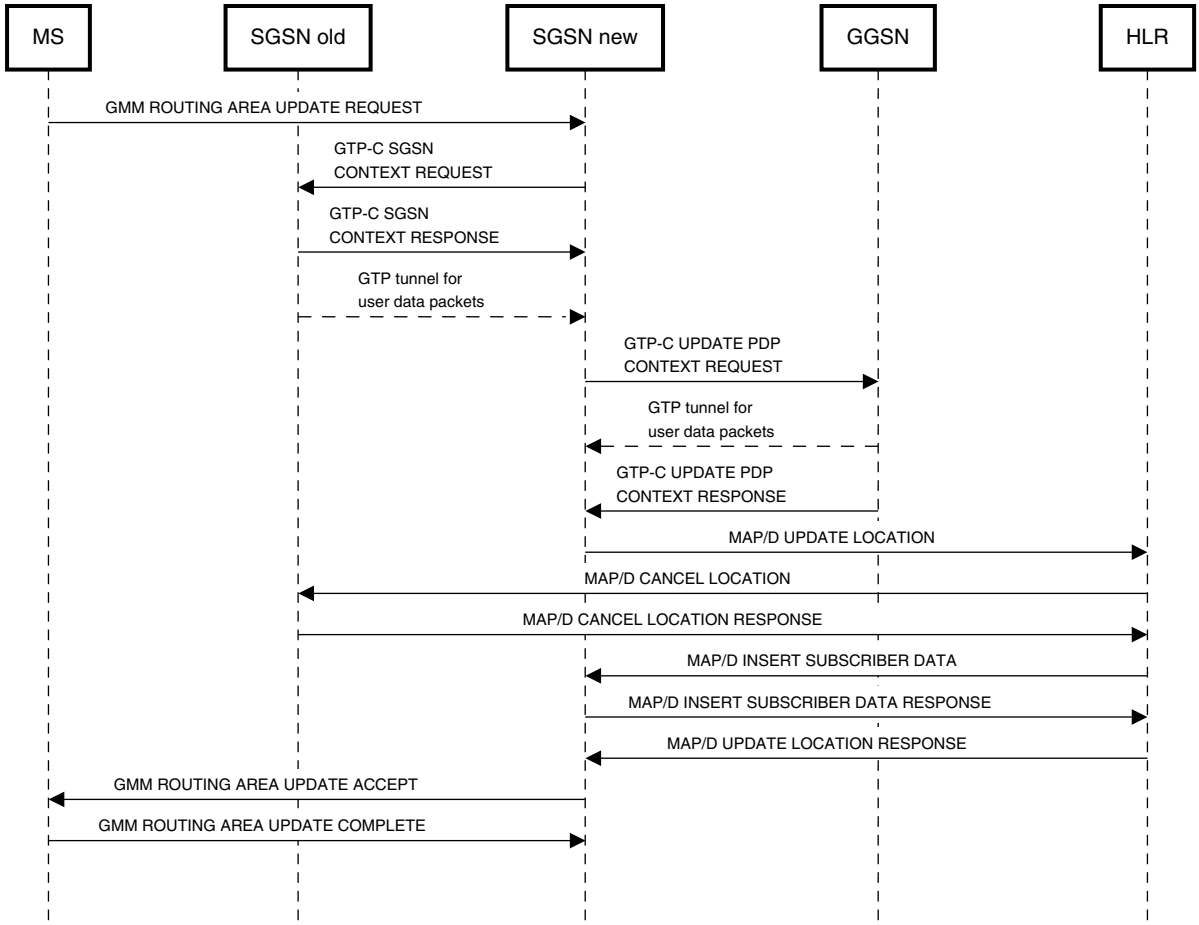


**Figure 5.34** Routing area update for GPRS.

This address is used as a source or destination address within the transported user data packets. The PDP context activation involves both the GGSN and SGSN for setting up GTP tunnels for the mobile station and updating their internal routing tables for the new packet data protocol address granted to the mobile station. The packet data protocol used by the mobile station is in practice IP protocol while GPRS also supports X.25 protocol. The X.25 protocol was still in use when the GPRS protocol was designed but has since become obsolete. If the mobile station supports simultaneous GPRS connectivity toward different external data networks, the mobile station may open multiple PDP contexts toward different GGSN nodes. In this case, the mobile station gets a new PDP address for each of the contexts opened.

An active PDP context provides the mobile station with a packet data connection toward a single **access point (AP)** of an external data network and its packet data service. Every packet data service, such as MMS multimedia messaging or generic Internet access, has its own access point. The access point is identified with its unique APN. When using the IP protocol, the APN is a domain name, which globally identifies both the GGSN node, the specific packet data service, and its provider. The format of the APN follows the convention of <service name>.mnc<MNC>.mcc<MCC>.gprs where any part limited with <> would be replaced with the corresponding name or numeric code of the entity. MNC and MCC are the mobile network and country codes of the operator which owns the GGSN. The mobile station uses the APN when requesting activation of a PDP context for the packet data service.

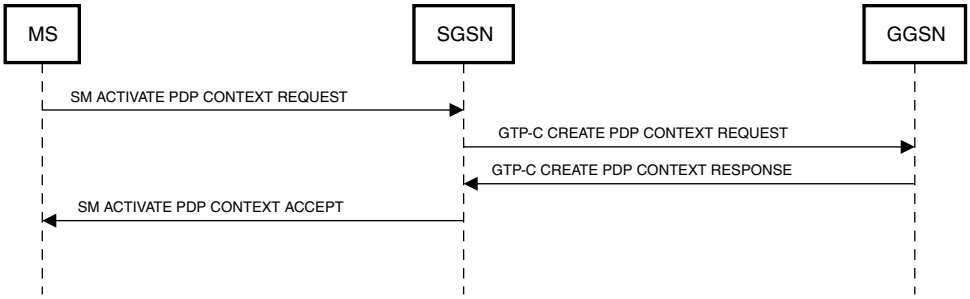


**Figure 5.35** GPRS PDP context activation by mobile station.

The PDP context is represented as a data structure stored to the mobile station, SGSN and GGSN nodes. This structure has the following key elements:

- The type of the packet data protocol used: IP or X.25
- The packet data protocol address reserved for the mobile station either permanently or for the lifetime of the PDP context
- The QoS service level requested for the PDP context by the mobile station
- Data compression support for the transported packet data
- The address of the GGSN, which is the anchor for the PDP context

Activation of a PDP context is done as shown in Figure 5.35:

1) The mobile station sends an SM ACTIVATE PDP CONTEXT REQUEST message to the SGSN. This message identifies the PDP type, APN name, QoS parameters, SNDCP protocol, NSAPI identifier, and the packet data protocol address requested by the mobile station.
2) The SGSN checks the subscriber data received from the HLR at GPRS attach. If the subscriber has the right to activate the requested type of PDP context, the SGSN selects the GGSN gateway that supports the requested PDP type and APN. For instance, when the mobile station wants to access the Internet, the SGSN may use a local DNS server to return the IP address of the GGSN whose domain name matches with the APN received from the mobile station.
3) The SGSN sends a GTP-C CREATE PDP CONTEXT REQUEST message to the selected GGSN, which allocates a PDP address for the mobile station. The GGSN may use an address permanently assigned for the station or use a dynamically allocated address retrieved from a local DHCP server.
4) The GGSN creates a GTP protocol tunnel toward the SGSN and gives a TEID for the tunnel. The GGSN stores the mapping between the TEID and the packet data address allocated to the MS, to be used for routing user data packets over the correct tunnel. The GGSN sends a GTP-C CREATE PDP CONTEXT RESPONSE message to inform the SGSN about the TEID of the GTP tunnel and the PDP address allocated for the mobile station.
5) SGSN finally sends an SM ACTIVATE PDP CONTEXT ACCEPT message to the mobile station. This message provides the mobile station with the allocated PDP address and other parameters of the PDP context (Figure 5.35).

If the mobile station has a permanently allocated PDP address, other packet data protocol endpoints may send data to it even when the station does not have an active PDP context. In such a case, the GGSN has to activate the PDP context. After receiving a data packet, the GGSN shall find out the routing area where the mobile station is located and thereafter create GTP tunnels to the SGSN serving the station. The PDP context is activated by the GGSN as follows:

1) The GGSN sends a MAP/D SEND ROUTING INFO FOR GPRS to the HLR, identifying the subscriber with the IMSI code mapped to the permanent destination PDP address. In its response, the HLR provides the address of the SGSN currently serving the mobile station.
2) The GGSN sends a GTP-C CREATE PDP CONTEXT REQUEST message to the SGSN, which sends a SM REQUEST PDP CONTEXT ACTIVATION message to the mobile station. This message triggers the mobile station to initiate the PDP context activation procedure for the given packet data protocol address and APN. The activation procedure is like that described earlier.

The mobile station may request deactivation of a PDP context by sending an SM DEACTIVATE PDP CONTEXT REQUEST message to the SGSN. Consequently, the SGSN sends a GTP-C DELETE PDP CONTEXT REQUEST message to the GGSN. The GTP tunnel is torn down, and after getting acknowledgment from the GGSN, the SGSN returns an SM DEACTIVATE PDP CONTEXT ACCEPT response to the mobile station.

#### 5.2.8.2 Transfer of Packet Data in GPRS System

The path of packet data in GPRS network can be divided into three segments, each relying on a specific protocol stack for relaying user data packets. These stacks were described in Section 5.2.2.3.

- The segment between the GPRS mobile station and the BSS subsystem
- The segment between the BSS and SGSN
- The segment between the SGSN and GGSN

When forwarding user data packets from the mobile station over these segments, the PCU, SGSN, and GGSN nodes behave as follows:

1) The mobile station sends user data within RLC/MAC frames over the allocated PDTCH channel. The TLLI identifier within the RLC frame identifies the LLC link of the PDP context. The RLC/MAC frames contain segments of LLC frames, which the PCU forwards over the trunk connection to the SGSN.
2) The SGSN checks the SAPI identifier of the received LLC frames to find out the upper layer protocol to which the payload of the LLC frame belongs. The LLC payload contains user data packets encapsulated into SNDCP packets. The NSAPI field of the SNDCP header tells the type of packet data protocol used. The SGSN terminates LLC and SNDCP protocols and unwraps the user data packet from the SNDCP packet. The SGSN then accesses the header of the user data packet to check the PDP destination address. The SGSN uses this address to route the user data packets over the correct GTP tunnel, which has been set up for the PDP context. The SGSN encapsulates the user data packets to GTP-U packets sent to the GGSN node in the end of the tunnel.
3) The GGSN unwarps the received GTP-U packets and forwards the user data packets to the external packet data network identified within the PDP context.

User data packets arriving from the external data network toward the mobile station are processed in the reverse manner.

## 5.3 EDGE

While GPRS provided a solution for delivering variable-rate packet switched data flows over the GSM air interface, the provided data rates were modest in comparison to fixed Internet access technologies, such as ADSL. To increase mobile data rates, 3GPP enhanced the GPRS solution with a few techniques, such as advanced modulation and coding scheme (MCS)s.

**Enhanced data rates for GSM evolution (EDGE)** means a set of techniques used to increase bitrates of circuit switched GSM and packet switched GPRS data connections. EDGE covers two separate solutions: Enhanced

Circuits Switched Data (ECSD) and Enhanced General Packet Radio Service (EGPRS). EGPRS can be considered as an essentially new air interface toward the GPRS system. Both ECSD and EGPRS rely on modulation methods specified in 3GPP TS 45.004 [31].

EDGE was introduced into 3GPP GSM and GPRS standards in GSM Phase 2+ release 98. After EDGE was launched, 3GPP introduced a new acronym, GERAN, to cover radio access networks of the GSM family: GERAN stands for GSM-EDGE Radio Access Network. 3GPP has continued to evolve GERAN specifications and introduce various enhancements for GERAN over successive 3GPP specification releases.

### 5.3.1 ECSD

**Enhanced circuit switched data (ECSD)** brings new modulation and line coding methods for GSM CSD bursts. The new methods support improved data rates up to 43.2 kbps per timeslot. The maximum transfer rate of an ECSD connection is 64 kbps with two GSM timeslots, each providing 32 kbps data rate. Compared to HSCSD, the maximum data rate of ECSD is the same, but it is achieved with a smaller number of timeslots. That saves GSM transmission resources for other connections.

### 5.3.2 EGPRS

**Enhanced general packet radio service (EGPRS)** is an improved version of GPRS to provide higher data transfer rates, theoretically up to 400 kbps. In practical network conditions, the maximum achievable bitrate is limited approximately to 100 kbps. The most important new EGPRS methods are as follows:

- New modulation and channel coding methods for the PDCH channel to increase the transmission rates up to 60 kbps per GSM timeslot.
- Merging of RLC and MAC protocols so that each radio block has one single RLC/MAC header area instead of separate RLC and MAC headers. This reduces the amount of RLC/MAC overhead. Note that the RLC/MAC messages referred to in Section 5.2.7 already followed this EDGE convention.
- Usage of two new complementary techniques to improve the retransmission process:
  - **Incremental redundancy (IR):** When an RLC/MAC frame is retransmitted, the punctured bits removed after the convolutional coding are selected differently for the retransmitted frame compared to the earlier transmissions of the frame. This allows the receiver to combine information from different radio blocks carrying copies of the frame and to reconstruct the original frame even if every copy would have its own bit errors.
  - **Link adaptation (LA):** When the signal quality of the channel is bad enough to cause many retransmissions, a more robust but slower coding scheme can be used to improve the probability of forward error correction to catch and fix the bit errors.

EGPRS supports nine different **MCS** options to be used for link adaptation. All of these methods share the following features:

- The RLC/MAC header is encoded separately from the payload data. Both the header and payload have their own checksums calculated before the convolutional coding. For headers, stronger protection is applied than for the payload by allocating a higher number of bits to the checksum per the number of header bits being protected.
- **Convolutional coding** with 1/3 rate (three output bits per one input bit) is used by all of the MCS schemes.
- **Puncturing** is used after convolutional coding to adjust the bitrate. Some of the bits in predefined positions are dropped before transmission to increase bitrate with the cost of making the forward error correction weaker. Each MCS scheme has a few optional puncturing schemes that can be used to achieve specific data rate.
- A new puncturing scheme (CPS) indicator field of the RLC/MAC header is used to communicate the chosen combination of MCS and puncturing to the remote end.

**Table 5.3** EGPRS modulation and coding schemes.

| Coding scheme | Modulation method | PDCH data rate (kbps) | Coding ratio (%) | User data bits per radio block | Encoded header bits | Encoded data bits |
|---|---|---|---|---|---|---|
| MCS-1 | GMSK | 8.8 | 53 | 176 | 68 DL / 80 UL | 372 |
| MCS-2 | GMSK | 11.2 | 66 | 224 | 68 DL / 80 UL | 372 |
| MCS-3 | GMSK | 14.8 | 85 | 296 | 68 DL / 80 UL | 372 |
| MCS-4 | GMSK | 17.6 | 100 | 352 | 68 DL / 80 UL | 372 |
| MCS-5 | 8PSK | 22.4 | 37 | 448 | 100 DL / 136 UL | 1248 |
| MCS-6 | 8PSK | 29.6 | 49 | 592 | 100 DL / 136 UL | 1248 |
| MCS-7 | 8PSK | 44.8 | 76 | 896 | 124 DL / 160 UL | 1224 |
| MCS-8 | 8PSK | 54.4 | 92 | 1088 | 124 DL / 160 UL | 1224 |
| MCS-9 | 8PSK | 59.2 | 100 | 1184 | 124 DL / 160 UL | 1224 |

- USF code is separately precoded to make sure that the uplink blocks are received by the correct mobile station. MCS schemes 1–4 encode USF with 12 bits while schemes 5–9 are with as many as 36 bits.

Properties of the EGPRS coding schemes [28] are summarized in Table 5.3.

MCS 1–4 use GMSK modulation, with which a burst carries 114 information bits and a radio block of four bursts totals 456 bits. The 8PSK modulation used in schemes 5–9 is able to represent 3 bits in one coding symbol; thus, the number of information bits per radio block is tripled to 1348 downlink and 1384 uplink. In the preceding table, the max data rates are given per timeslot or PDCH. Higher bitrates can be reached by granting the mobile station with multiple slots or PDCHs to be used in parallel. For MCS coding schemes 7–9, the RLC block size has been reduced to two bursts instead of four. This reduces the amount of data to be retransmitted if an RLC block is corrupted by sending one of its bursts over a badly disturbed RF channel.

A base station is able to serve multiple mobile stations with different GPRS and EGPRS coding schemes in different PDCH timeslots. The coding scheme applied to a PDCH can be selected individually for every radio block, based on the bit error rates (BER) measured for the earlier blocks. The base station itself measures BER of uplink traffic and relies on the reports received from mobile station about the downlink traffic. The new EGPRS-specific MCS schemes are used only on dedicated packet channels. The common and shared channels that are used for both GSM and GPRS still rely on the GSM coding schemes. Otherwise, mobile stations without EGPRS support could not use the cell.

### 5.3.3 EGPRS2

The final evolution step of EGPRS is EGPRS2, which brought the following enhancements to the spec:

- New types of modulation: Quadrature phase shift keying (QPSK), 16-QAM, and 32-QAM, in addition to 8PSK.
- New coding schemes, which are different for uplink and downlink.
- **Turbo coding** instead of the traditional GPRS convolutional coding. An overview to turbo coding is given in *Online Appendix A.6.4*.
- A new reduced transmission time interval (RTTI) in addition to the basic transmission timer interval (BTTI). BTTI means the traditional GPRS case where a radio block consists of a single PDCH timeslot of four consecutive TDMA frames. With RTTI, a radio block is transmitted with a pair of PDCH timeslots within two consecutive TDMA frames. The RTTI decreases the GPRS transmission latency from 20 to 10 ms.

**Table 5.4** EGPRS2 coding schemes.

| Coding schemes | Direction | Modulation method | PDCH data rate | Coding ratios (%) |
|---|---|---|---|---|
| DAS-5 . . . DAS-7 | Downlink | 8-PSK | 22.4–32.8 | 37–54 |
| DAS-8 . . . DAS-9 | Downlink | 16-QAM | 44.8–54.4 | 56–68 |
| DAS-10 . . . DAS-12 | Downlink | 32-QAM | 65.5–98.4 | 64–96 |
| DBS-5 . . . DBS-6 | Downlink | 8-PSK | 22.4–29.6 | 49–63 |
| DBS-7 . . . DBS-9 | Downlink | 16-QAM | 44.8–67.2 | 47–71 |
| DBS-10 . . . DBS-12 | Downlink | 32-QAM | 88.8–118.4 | 72–98 |
| UAS-7 . . . UAS-11 | Uplink | 16-QAM | 44.8–76.8 | 55–95 |
| UBS-5 . . . UBS-6 | Uplink | 8-PSK | 22.4–29.6 | 47–62 |
| UBS-7 . . . UBS-9 | Uplink | 16-QAM | 44.8–67.2 | 46–70 |
| UBS-10 . . . UBS-12 | Uplink | 32-QAM | 88.8–118.4 | 71–96 |

Table 5.4 gives an overall summary of EGPRS2 coding schemes.

EGPRS2 mobile stations are divided into two categories: EGPRS2-A and EGPRS2-B. Category A devices support only DAS and UAS schemes, while category B devices support all the EGPRS2 coding schemes.

## 5.4 Questions

**1** Please list the services provided by GSM for its users.

**2** Which are the types of elements and their roles in the GSM BSS subsystem?

**3** What is IMSI?

**4** What are the main advantages of GSM frequency hopping?

**5** What kind of goals does a good voice codec design meet?

**6** How does a GSM phone select the used GSM network?

**7** In which ways is GPRS better for packet switched data compared to GSM?

**8** What are the three types of GPRS network elements added on top of the GSM architecture?

**9** What is a temporary block flow and how is it created?

**10** What does “modulation and coding scheme” mean?

**11** Why does GPRS use tunneling?

**12** What does GERAN mean?

## References


1 Mouly, M. and Pautet, M.-B. (1992). *The GSM System for Mobile Communications*. Palaiseau: Cell & Sys.
2 Sauter, M. (2021). *From GSM to LTE-Advanced Pro and 5G : an introduction to mobile networks and mobile broadband*. West Sussex: Wiley.
3 ITU-T Recommendation T.30 Procedures for document facsimile transmission in the general switched telephone network.
4 3GPP TS 23.081 Line Identification Supplementary Services; Stage 2.
5 3GPP TS 23.091 Explicit Call Transfer (ECT) Supplementary Service; Stage 2.
6 3GPP TS 23.082 Call Forwarding (CF) Supplementary Services; Stage 2.
7 3GPP TS 23.083 Call Waiting (CW) and Call Hold (HOLD) Supplementary Services; Stage 2.
8 3GPP TS 23.088 Call Barring (CB) Supplementary Services; Stage 2.
9 3GPP TS 23.086 Advice of Charge (AoC) Supplementary Services; Stage 2.
10 3GPP TS 23.084 Multi Party (MPTY) Supplementary Services; Stage 2.
11 3GPP TS 23.085 Closed User Group (CUG) Supplementary Services; Stage 2.
12 3GPP TS 23.089 Unstructured Supplementary Service Data (USSD).
13 3GPP TS 02.03 Teleservices Supported by a GSM Public Land Mobile Network (PLMN).
14 3GPP TS 03.20 Security-Related Network Functions.
15 3GPP TS 23.002 Network Architecture.
16 3GPP TS 42.017 Subscriber Identity Module (SIM); Functional Characteristics.
17 3GPP TS 48.052 Base Station Controller - Base Transceiver Station (BSC - BTS) Interface; Interface Principles.
18 3GPP TS 48.002 Base Station System - Mobile-services Switching Centre (BSS - MSC) interface; Interface principles.
19 Anttalainen, T. and Jääskeläinen, V. (2015). *Introduction to Communications Networks*. Norwood: Artech House.
20 3GPP TS 23.060 General Packet Radio Service (GPRS); Service description; Stage 2.
21 3GPP TS 23.003 Numbering, Addressing And Identification.
22 3GPP TS 29.010 Information Element Mapping Between Mobile Station - Base Station System (MS - BSS) and Base Station System - Mobile-Services Switching Centre (BSS - MSC); Signalling Procedures and the Mobile Application Part (MAP).
23 3GPP TS 44.001 Mobile Station - Base Station System (MS - BSS) interface; General Aspects And Principles.
24 3GPP TS 48.006 Signalling Transport Mechanism Specification for the Base Station System - Mobile Services Switching Centre (BSS - MSC) interface.
25 3GPP TS 48.058 Base Station Controller - Base Transceiver Station (BSC - BTS) Interface; Layer 3 specification.
26 3GPP TS 43.051 GSM/EDGE Overall description; Stage 2.
27 3GPP TS 48.008 Mobile Switching Centre - Base Station System (MSC-BSS) Interface; Layer 3 specification.
28 3GPP TS 45.001 GSM/EDGE Physical Layer on the Radio Path; General Description.
29 3GPP TS 45.002 GSM/EDGE Multiplexing and Multiple Access on the Radio Path.
30 3GPP TS 45.003 GSM/EDGE Channel Coding.
31 3GPP TS 45.004 GSM/EDGE Modulation.
32 3GPP TS 45.005 GSM/EDGE Radio Transmission and Reception.
33 3GPP TS 45.008 GSM/EDGE Radio Subsystem Link Control.
34 3GPP TS 45.009 GSM/EDGE Link Adaptation.
35 3GPP TS 05.02 Multiplexing and Multiple Access on the Radio Path.
36 3GPP TS 44.003 Mobile Station - Base Station System (MS - BSS) Interface Channel Structures and Access Capabilities.
37 3GPP TS 44.004 GSM/EDGE Layer 1; General Requirements.

**38** 3GPP TS 43.013 Discontinuous Reception (DRX) in the GSM system.
**39** 3GPP TS 44.005 GSM/EDGE Data Link (DL) Layer; General aspects.
**40** 3GPP TS 44.006 Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification.
**41** 3GPP TS 24.008 Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Stage 3.
**42** 3GPP TS 44.018 Mobile Radio Interface Layer 3 Specification; GSM/EDGE Radio Resource Control (RRC) protocol.
**43** 3GPP TS 48.004 Base Station System - Mobile-services Switching Centre (BSS - MSC) interface; Layer 1 specification.
**44** 3GPP TS 48.054 Base Station Controller - Base Transceiver Station (BSC - BTS) interface; Layer 1 Structure of Physical Circuits.
**45** 3GPP TS 48.056 Base Station Controller - Base Transceiver Station (BSC - BTS) interface; Layer 2 Specification.
**46** 3GPP TS 29.002 Mobile Application Part (MAP) Specification.
**47** 3GPP TS 23.096 Name Identification Supplementary Services; Stage 2.
**48** 3GPP TS 24.010 Mobile Radio Interface Layer 3; Supplementary Services Specification; General Aspects.
**49** 3GPP TS 06.10 Full Rate Speech Transcoding.
**50** 3GPP TS 46.010 Full Rate speech; Transcoding.
**51** 3GPP TS 06.20 Half Rate Speech Transcoding.
**52** 3GPP TS 46.020 Half Rate Speech; Half Rate Speech Transcoding.
**53** 3GPP TS 46.001 Full Rate Speech; Processing Functions.
**54** 3GPP TS 46.002 Half Rate Speech; Half Rate Speech Processing Functions.
**55** 3GPP TS 23.040 Technical Realization of the Short Message Service (SMS).
**56** 3GPP TS 24.011 Point-to-Point (PP) Short Message Service (SMS) Support on Mobile Radio Interface.
**57** 3GPP TS 22.034 High Speed Circuit Switched Data (HSCSD); Stage 1.
**58** 3GPP TS 23.034 High Speed Circuit Switched Data (HSCSD); Stage 2.
**59** 3GPP TS 24.022 Radio Link Protocol (RLP) for Circuit Switched Bearer and Teleservices.
**60** ITU-T Recommendation V.110 Support by an ISDN of data terminal equipments with V-series type interfaces.
**61** 3GPP TS 23.008 Organization of Subscriber Data.
**62** 3GPP TS 23.009 Handover Procedures.
**63** Bates, R. (2002). *GPRS General Packet Radio Service*. New York: McGraw-Hill.
**64** 3GPP TS 22.060 General Packet Radio Service (GPRS); Service Description; Stage 1.
**65** 3GPP TS 03.02 Network Architecture.
**66** 3GPP TS 43.064 General Packet Radio Service (GPRS); Overall Description of the GPRS Radio Interface; Stage 2.
**67** 3GPP TS 44.060 General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) Interface; Radio Link Control / Medium Access Control (RLC/MAC) protocol.
**68** 3GPP TS 44.160 General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) Interface; Radio Link Control / Medium Access Control (RLC/MAC) Protocol Iu Mode.
**69** 3GPP TS 44.064 Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) Layer Specification.
**70** 3GPP TS 44.065 Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP).
**71** 3GPP TS 48.018 General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP).
**72** 3GPP TS 29.060 General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface.