FROM GSM TO LTE-ADVANCED PRO AND 5G

AN INTRODUCTION TO MOBILE NETWORKS AND MOBILE BROADBAND

FOURTH EDITION

MARTIN SAUTER

WILEY

From GSM to LTE-Advanced Pro and 5G

From GSM to LTE-Advanced Pro and 5G

An Introduction to Mobile Networks and Mobile Broadband

Fourth Edition

Martin Sauter

WirelessMoves
Cologne
Germany

WILEY

This fourth edition first published 2021

Edition History
John Wiley and Sons Ltd (1e 2011); John Wiley and Sons Ltd (2e 2014); John Wiley and Sons Ltd (3e 2017)

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office
The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data

Names: Sauter, Martin, author. | John Wiley & Sons, Ltd., publisher.
Title: From GSM to LTE-Advanced Pro and 5G : an introduction to mobile networks and mobile broadband / Martin Sauter.
Other titles: From GSM to LTE
Description: Fourth edition. | Hoboken, NJ : Wiley, 2021. | Includes bibliographical references and index.
Identifiers: LCCN 2020031695 (print) | LCCN 2020031696 (ebook) | ISBN 9781119714675 (cloth) | ISBN 9781119714705 (adobe pdf) | ISBN 9781119714699 (epub)
Subjects: LCSH: Mobile communication systems. | Global system for mobile communications. | Long-Term Evolution (Telecommunications). | 5G mobile communication systems.
Classification: LCC TK5103.2 .S28 2021 (print) | LCC TK5103.2 (ebook) | DDC 621.3845/6–dc23
LC record available at https://lccn.loc.gov/2020031695
LC ebook record available at https://lccn.loc.gov/2020031696

Cover Design: Wiley
Cover Images: Abstract background with purple and brown polygons © Hamster3d/Getty Images, binary code © ABIDAL/Getty Images, Illuminated Fernsehturm And Cityscape Against Sky At Night © Philip Gaube/EyeEm/Getty Images

Set in 9.5/12.5pt STIXTwoText by SPi Global, Pondicherry, India

10 9 8 7 6 5 4 3 2 1

Contents

Preface to Fourth Edition

Wireless technologies like GSM, UMTS, LTE, VoLTE, 5G NR, Wireless LAN, and Bluetooth have revolutionized the way we communicate by making services like telephony and Internet access available anytime and from almost anywhere. Currently, a great variety of technical publications offer background information about these technologies but they all fall short in one way or another. Books covering these technologies usually describe only one of the systems in detail and are generally too complex as a first introduction. The Internet is also a good source, but the articles one finds are usually too short and superficial or only deal with a specific mechanism of one of the systems. For this reason, it was difficult for me to recommend a single publication to students in my telecommunication classes, which I have been teaching in addition to my work in the wireless telecommunication industry. This book aims to change this.

Each of the eight chapters in this book gives a detailed introduction to and overview of one of the wireless systems mentioned above, and how it has been deployed in practice. Special emphasis has also been put on explaining the thoughts and reasoning behind the development of each system. For readers who want to test their understanding of a system, each chapter concludes with a list of questions. For further investigation, all chapters contain references to the relevant standards and documents. These provide ideal additional sources to find out more about a specific system or topic. In addition, a companion website with further background information and the latest news is available at http://www.wirelessmoves.com.

Since the previous edition of the book was published in 2017, mobile networks have again evolved significantly. As this book focuses on being a guide to how current network technology is being used in the field, this new edition has been significantly updated.

From a user's point of view, few things have changed in 2G and 3G networks, and some network operators have even switched-off one of the two technologies. In most parts of the world, however, 2G remains an important technology, especially for machine communication and nationwide network coverage for voice telephony. This is why even 2G and 3G networks continue to evolve on the network side. The first three chapters of the book where thus updated to reflect the completed effort to evolve these systems towards IP transport links and virtual circuit switching.

Most innovations in recent years have focused on the development and initial deployment of 5G New Radio (5G NR) and the 5G Core Network (5GC). A new chapter was therefore added to this edition that explains the need for 5G. This new chapter then gives a

thorough overview of the parts of the new system that have been deployed in practice thus far, and how mobile networks are likely to evolve in the future.

The 4G LTE system has also evolved significantly in recent years to address the increasing bandwidth demand. Consequently, the chapter on LTE was extended and now includes additional material on topics such as how downlink and uplink carrier aggregation is used today, multi-antenna transmissions (MIMO), handover mechanisms between 3G and 4G networks, and a discussion on the typical number of users and throughput of a cell site today.

In the chapter on Wireless LAN (Wi-Fi), additional sections have been added on the new 802.11ax (Wi-Fi 6) standard, the new WPA3 authentication scheme, the use of Protected Management Frames, and inter-Access Point roaming functionality.

While working on the book, I have gained tremendous benefit from wireless technologies that are currently available. Whether at home or while traveling, Wireless LAN, LTE, and 5G have provided reliable connectivity for my research and have allowed me to communicate with friends and loved ones at any time, from anywhere. In a way, the book is a child of the technologies it describes.

Many people have been involved in revising the different chapters and have given invaluable suggestions on content, style, and grammar. I would therefore like to thank Prashant John, Timothy Longman, Tim Smith, Peter van den Broek, Prem Jayaraj, Kevin Wriston, Greg Beyer, Ed Illidge, Debby Maxwell, and John Edwards for their kind help and good advice.

Furthermore, my sincere thanks go to Berenike, who has stood by me during this project with her love, friendship, and good advice.

Cologne, June 2020 *Martin Sauter*

1

Global System for Mobile Communications (GSM)

At the beginning of the 1990s, the Global System for Mobile Communications (GSM), triggered an unprecedented change in the way people communicated with each other. While earlier analog wireless telephony systems were country specific and used only by a few, GSM was adopted around the globe and was used by billions of people during its peak years. This was mostly achieved by steady improvements in all areas of telecommunication technology and the resulting steady price reductions for both infrastructure equipment and mobile devices. This chapter discusses the architecture of this system, which also forms the basis for the packet-switched extension called General Packet Radio Service (GPRS), discussed in the chapter on GPRS and EDGE, and for the Universal Mobile Telecommunications System (UMTS), which we describe in the chapter on UTMS and HSPA.

Although the first standardization activities for GSM date back to the middle of the 1980s, GSM is still widely used today. In recent years however, 4G LTE networks have become tremendously popular and a new service was standardized to support voice calls over the LTE radio network. This service is referred to as Voice over LTE (VoLTE) and is discussed in a separate chapter. Although efforts to roll out VoLTE are significant, many mobile voice calls are still handled by GSM and UMTS networks, to which devices without VoLTE support fall back for this service. In addition, even if a device and a network support VoLTE, a transfer to GSM or UMTS is still required when the user leaves the LTE coverage area. Also, GSM and UMTS networks are still predominantly used for voice telephony when a subscriber roams internationally, as at the time of publication only a few network operators had extended their VoLTE service for roaming. Consequently, knowledge of GSM is still required for a thorough understanding of how mobile networks are deployed and used in practice today.

Over the years, the way GSM was deployed in practice changed significantly. To understand today's system architecture, this chapter first introduces how GSM was initially designed and then describes with how the system has evolved over the next decades.

From GSM to LTE-Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband, Fourth Edition. Martin Sauter.

1.1 Circuit-Switched Data Transmission

Initially, GSM was designed as a circuit-switched system that established a direct and exclusive connection between two users on every interface between all network nodes of the system. Section 1.1.1 gives a first overview of this traditional architecture. Over time, this physical circuit switching has been virtualized and network nodes are now connected over IP-based broadband connections. The reasons for this and further details on virtual circuit switching can be found in Section 1.1.2.

1.1.1 Classic Circuit Switching

The GSM mobile telecommunication network has been designed as a circuit-switched network in a similar way to fixed-line phone networks of the time. At the beginning of a call, the network established a direct connection between two parties, which was then used exclusively for that conversation. As shown in Figure 1.1, the switching center used a switching matrix to connect any originating party to any destination party. Once the connection was established, the conversation was then transparently transmitted via the switching matrix between the two parties. The switching center only became active again to clear the connection in the switching matrix if one of the parties wanted to end the call. This approach was identical in both mobile and fixed-line networks. Early fixed-line telecommunication networks were designed only for voice communication, for which an analog connection between the parties was established. In the mid-1980s, analog technology was superseded by digital technology in the switching center. This meant that calls were no longer sent over an analog line from the originator to the terminator. Instead, the switching center digitized the analog signal that it received from the subscribers, which were directly attached to it, and forwarded the digitized signal to the terminating switching center. There, the digital signal was again converted back to an analog signal, which was then sent over the copper cable to the terminating party. In some countries, ISDN (Integrated Services Digital Network) lines were quite popular. With this system, the transmission became fully digital and the conversion back to an analog audio signal was done directly in the phone.

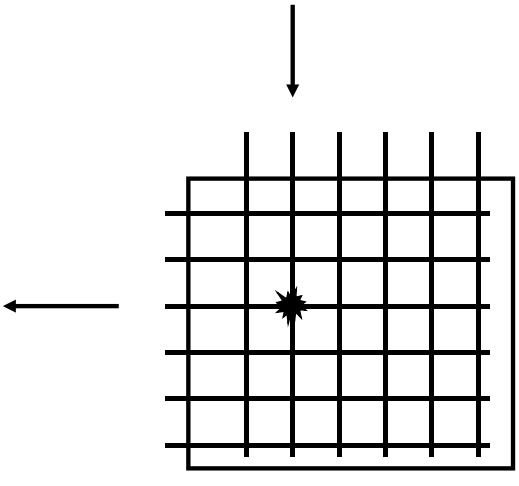

Figure 1.1 Switching matrix in a switching center.

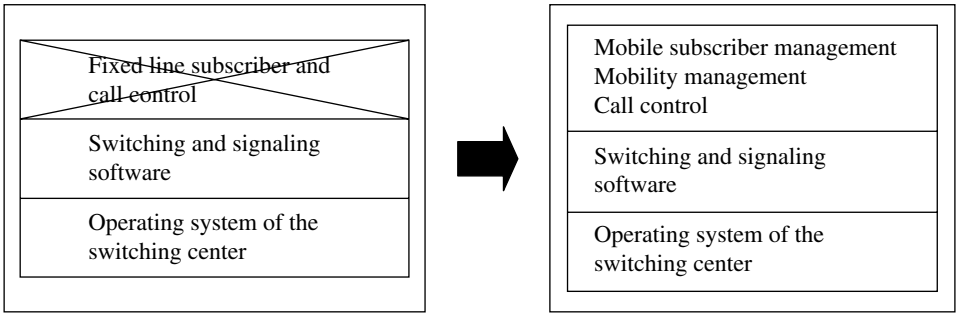

Figure 1.2 Necessary software changed to adapt a fixed-line switching center for a wireless network.

GSM reused much of the fixed-line technology that was available at the time the standards were created. Thus, existing technologies such as switching centers and long-distance communication equipment were used. The main development for GSM, as shown in Figure 1.2, was the means to wirelessly connect the subscribers to the network. In fixed-line networks, subscriber connectivity is very simple as only two dedicated wires are necessary per user. In a GSM network, however, the subscribers are mobile and can change their location at any time. Thus, it was not possible to use the same input and output in the switching matrix for a user for each call as was the case in fixed-line networks.

As a mobile network consists of many switching centers, with each covering a certain geographical area, it was not even possible to predict in advance which switching center a call should be forwarded to for a certain subscriber. This meant that the software for subscriber management and routing of calls of fixed-line networks could not be used for GSM. Instead of a static call-routing mechanism, a flexible mobility management architecture in the core network became necessary, which needed to be aware of the current location of the subscriber to route calls to them at any time.

It was also necessary to be able to flexibly change the routing of an ongoing call, as a subscriber can roam freely and thus might leave the coverage area of the radio transmitter of the network over which the call was established. While there was a big difference between the software of a fixed switching center and a Mobile Switching Center (MSC), the hardware as well as the lower layers of the software, which were responsible, for example, for the handling of the switching matrix, were mostly identical. Therefore, most telecommunication equipment vendors at the time like Ericsson, Nokia, and Alcatel-Lucent offered their switching center hardware for both fixed-line and mobile networks. Only the software in the switching center determined whether the hardware was used in a fixed or mobile network (see Figure 1.2).

1.1.2 Virtual Circuit Switching over IP

While voice calls in the 1990s were the dominating form of communication, this has significantly changed today. While voice calls remain important, other forms of communication via the Internet play an even larger role. All these services share the Internet Protocol (IP) as a transport protocol to connect people globally.

While circuit switching establishes an exclusive channel between two parties, the Internet is based on transferring individual data packets. A link with a high bandwidth is used to transfer the packets of many users. By using the destination address contained in each packet, each network node that the packet traverses decides over which outgoing link to forward the packet. Further details can be found in the chapter on GPRS.

Owing to the rise of the Internet and IP-based applications, network operators thus had to maintain two separate networks: a circuit-switched network for voice calls and a packet-switched network for Internet-based services.

As the simultaneous operation of two different networks is very inefficient and costly, network operators have replaced the switching matrix in the MSC with a device referred to as a media gateway. This allowed them to virtualize circuit switching and to transfer voice calls over IP packets. The physical presence of a circuit-switched infrastructure is thus no longer necessary and the network operator can concentrate on maintaining and expanding a single IP-based network. This approach has been standardized under the name 'Bearer-Independent Core Network' (BICN).

The basic operation of GSM is not changed by this virtualization. The main differences can be found in the lower protocol layers for call signaling and voice call transmission. The move toward IP-based communication also took place in the GSM radio network, especially once radio base station sites started to support several radio technologies such as GSM, UMTS, LTE, and 5G NR simultaneously. Typically, connectivity is provided over a single IP-based link today.

The GSM air interface between the mobile devices and the network was not affected by the transition from circuit to packet switching. For mobile devices, the transition from circuit switching to IP-based interfaces was completely transparent.

1.2 Standards

As many network infrastructure manufacturers compete globally for orders from telecommunication network operators, standardization of interfaces and procedures is necessary. Without standards, which are defined by the International Telecommunication Union (ITU), it would not be possible to make phone calls internationally, and network operators would be bound to the supplier they initially select for the delivery of their network components. One of the most important ITU standards, discussed in Section 1.4, is the Signaling System Number 7 (SS-7), which is used for call routing. Many ITU standards, however, only represented the lowest common denominator as most countries had specified their own national extensions. In practice, this incurred a high cost for software development for each country, as a different set of extensions needs to be implemented in order for a vendor to be able to sell its equipment. Furthermore, the interconnection of networks of different countries was complicated by this.

GSM, for the first time, set a common standard for Europe for wireless networks. Due to its success, it was later adopted around the globe. This is the main reason why subscribers can roam in GSM networks across the world that have roaming agreements with each other. The common standard also substantially reduced research and development costs as hardware and software could now be sold worldwide with only minor adaptations for

the local market. The European Telecommunication Standards Institute (ETSI), which is also responsible for a number of other standards, was the main body responsible for the creation of the GSM standard. The ETSI GSM standards are composed of a substantial number of standards documents, which are called a technical specification (TS), and describe a particular part of the system. In the following chapters, many of these specifications are referenced and can thus be used for further information about a specific topic. Due to the global success of GSM, the 3rd Generation Partnership Project (3GPP) was later founded as a global organization and ETSI became one of the regional standardization bodies of the project. Today, 3GPP is responsible for maintaining and further developing the GSM, UMTS, LTE, and 5G standards. All documents are freely available on the Internet at http://www.etsi.org [1] or at http://www.3gpp.org [2].

1.3 Transmission Speeds

The smallest transmission speed unit in a classic circuit-switched telecommunication network was the digital signal level 0 (DS0) channel. It had a fixed transmission speed of 64 kbit/s. Such a channel could be used to transfer voice or data, and thus it was usually not called a speech channel but simply referred to as a user data channel.

The main reference unit of a telecommunication network was an E-1 connection in Europe and a T-1 connection in the United States, which used either a twisted pair or coaxial copper cable. The gross datarate was 2.048 Mbit/s for an E-1 connection and 1.544 Mbit/s for a T-1. An E-1 was divided into 32 timeslots of 64 kbit/s each, as shown in Figure 1.3, while a T-1 was divided into 24 timeslots of 64 kbit/s each. One of the timeslots was used for synchronization, which meant that 31 timeslots for an E-1 or 23 timeslots for a T-1, respectively, were used to transfer data. In practice, only 29 or 30 timeslots were used for user data transmission while the rest (usually one or two) were used for SS-7 signaling data (see Figure 1.3). More about SS-7 can be found in Section 1.4.

A single E-1 connection with 31 DS0s was typically not enough to connect two switching centers with each other. An alternative was an E-3 connection over twisted pair or coaxial cables. An E-3 connection was defined at a speed of 34.368 Mbit/s, which corresponded to 512 DS0s.

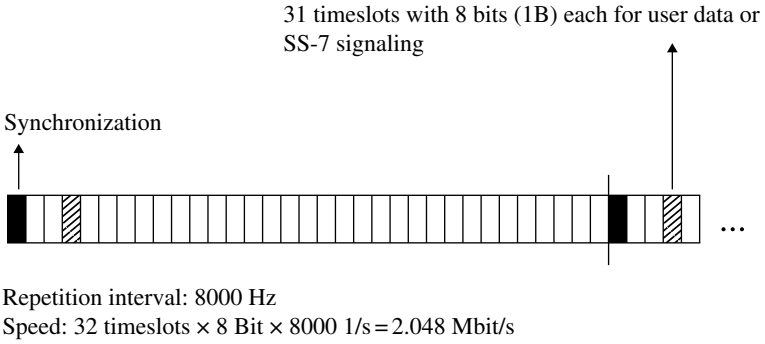

Figure 1.3 Timeslot architecture of an E-1 connection.

Table 1.1 STM transmission speeds and number of DS0s.

STM level	Speed (Mbit/s)	Approximate number of DS0 connections
STM-1	155.52	2300
STM-4	622.08	9500
STM-16	2488.32	37,000
STM-64	9953.28	148,279

For higher transmission speeds and for long distances, optical systems based on the synchronous transfer mode (STM) standard were used. Table 1.1 shows some datarates and the number of 64 kbit/s DS0 channels that were transmitted per pair of fibers.

For virtual circuit switching over IP, optical Ethernet links are typically used between network nodes. Transmission speeds of one Gbit/s or more are used on these links. Unlike the circuit-switched technology described above, Ethernet is the de facto standard for IP-based communication over fiber and copper cables and is widely used. As a consequence, network equipment can be built much more inexpensively.

1.4 The Signaling System Number 7

For establishing, maintaining, and clearing a connection, signaling information needs to be exchanged between the end user and network devices. In traditional fixed-line networks, analog phones signaled their connection request when the receiver was lifted off the hook and a dialed phone number was sent to the network either via pulses (pulse dialing) or via tone dialing, which was called dual tone multifrequency (DTMF) dialing. With fixed-line ISDN phones and GSM mobile phones, the signaling is done via a separate dedicated signaling channel, and information such as the destination phone number is sent as messages.

If several components in the network are involved in the call establishment, for example, if originating and terminating parties are not connected to the same switching center, it is also necessary that the different nodes in the network exchange information with each other. This signaling is transparent for the user, and a protocol called the Signaling System Number 7 (SS-7) is used for this purpose. SS-7 is also used in GSM networks and the standard was enhanced by ETSI to fulfill the special requirements of mobile networks, for example, subscriber mobility management.

The SS-7 standard defines three basic types of network nodes:

- Service Switching Points (SSPs) are switching centers that are more generally referred to as network elements and are able to establish, transport, or forward voice and data connections.
- Service Control Points (SCPs) are databases and application software that can influence the establishment of a connection. In a GSM network, SCPs can be used, for example, for storing the current location of a subscriber. During call establishment to a mobile subscriber, the switching centers query the database for the current location of the

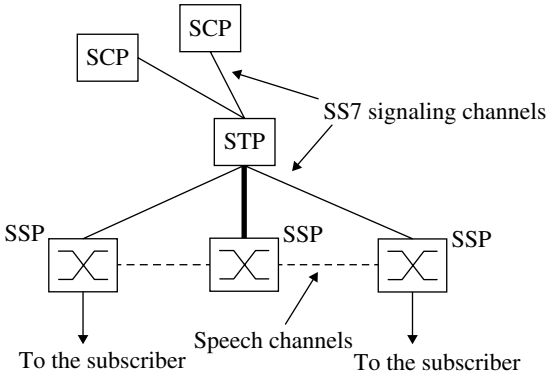

Figure 1.4 An SS-7 network with an STP, two SCP databases, and three switching centers.

subscriber to be able to forward the call. More about this procedure can be found in Section 1.6.3 about the Home Location Register (HLR).

- Signaling Transfer Points (STPs) are responsible for the forwarding of signaling messages between SSPs and SCPs as not all network nodes have a dedicated link to all other nodes of the network. The principal functionality of an STP can be compared to an IP router in the Internet, which also forwards packets to different branches of the network. Unlike IP routers, however, STPs only forward signaling messages that are necessary for establishing, maintaining, and clearing a call. The calls themselves are directly carried on dedicated links between the SSPs.

Figure 1.4 shows the general structure of an SS-7 circuit-switched telecommunication network and the way the nodes, as described above, are interconnected with each other.

The SS-7 protocol stack is also used in virtual circuit-switched networks for communication between the network nodes. Instead of dedicated signaling timeslots on an E-1 link, signaling messages are transported in IP packets. Section 1.4.1 describes the classic SS-7 protocol stack and follows with the way SS-7 messages are transported over IP networks.

1.4.1 The Classic SS-7 Protocol Stack

SS-7 comprises a number of protocols and layers. A well-known model for describing telecommunication protocols and different layers is the Open System Interconnection (OSI) 7-layer model, which is used in Figure 1.5 to show the layers on which the different SS-7 protocols reside.

The Message Transfer Part 1 (MTP-1) protocol describes the physical properties of the transmission medium on layer 1 of the OSI model. Thus, this layer is also called the physical layer. Properties that are standardized in MTP-1 are, for example, the definition of the different kinds of cables that can be used to carry the signal, signal levels, and transmission speeds.

On layer 2, the data link layer, messages are framed into packets and a start and stop identification at the beginning and end of each packet are inserted into the data stream, so that the receiver is able to detect where one message ends and where a new message begins.

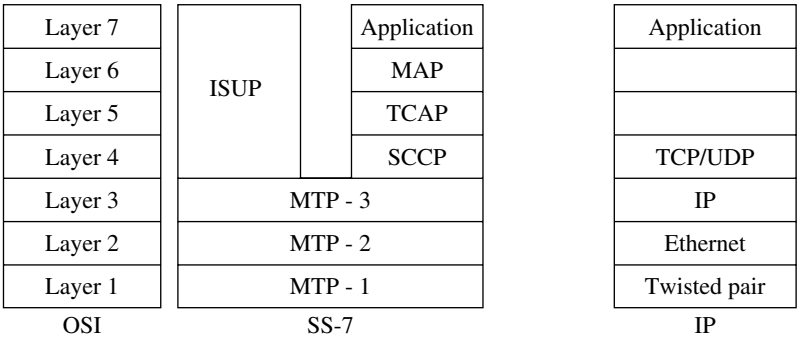

Figure 1.5 Comparison of the SS-7, OSI, and TCP/IP protocol stacks.

Layer 3 of the OSI model, which is called the network layer, is responsible for packet routing. To enable network nodes to forward incoming packets to other nodes, each packet gets a source and destination address on this layer. This is done by the MTP-3 protocol of the SS-7 stack. For readers who are already familiar with the TCP/IP protocol stack, it may be noted at this point that the MTP-3 protocol fulfills the same tasks as the IP protocol. Instead of IP addresses, however, the MTP-3 protocol uses so-called 'point codes' to identify the source and the destination of a message.

A number of different protocols are used on layers 4–7, depending on the application. If a message needs to be sent to establish or clear a call, the Integrated Services Digital Network User Part (ISUP) protocol is used. Figure 1.6 shows how a call is established between two parties by using ISUP messages. In the example, party A is a mobile subscriber while party B is a fixed-line subscriber. Thus, A is connected to the network via an MSC, while B is connected via a fixed-line switching center.

To call B, the phone number of B is sent by A to the MSC. The MSC then analyzes the National Destination Code (NDC) of the phone number, which usually comprises the first two to four digits of the number, and detects that the number belongs to a subscriber in the fixed-line network. In the example shown in Figure 1.6, the MSC and the fixed-line switching center are directly connected with each other. Therefore, the call can be directly forwarded to the terminating switching center. This is quite a realistic scenario, as direct connections are often used if, for example, a mobile subscriber calls a fixed-line phone in the same city.

As B is a fixed-line subscriber, the next step for the MSC is to establish a voice channel to the fixed-line switching center. This is done by sending an ISUP Initial Address Message (IAM). The message contains, among other data, the phone number of B and informs the fixed-line switching center of the channel that the MSC would like to use for the voice path. In the example, the IAM message is not sent directly to the fixed-line switching center. Instead, an STP is used to forward the message.

At the other end, the fixed-line switching center receives the message, analyzes the phone number, and establishes a connection via its switching matrix to subscriber B. Once the connection is established via the switching matrix, the switch applies a periodic current to the line of the fixed-line subscriber so that the fixed-line phone can generate an alerting tone. To indicate to the originating subscriber that the phone number is complete and the

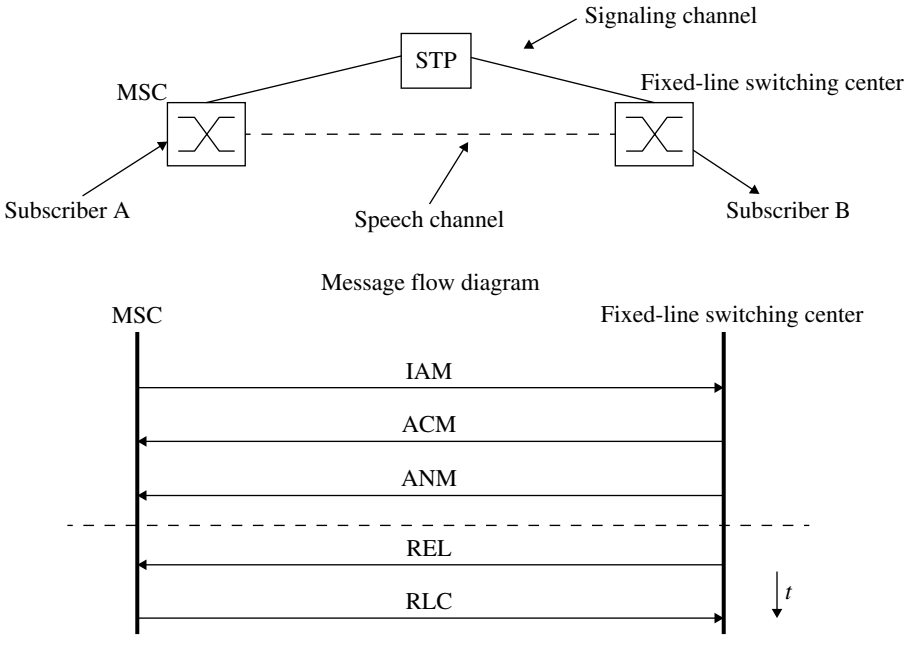

Figure 1.6 Establishment of a voice call between two switching centers.

destination party has been found, the fixed-line switch sends back an Address Complete Message (ACM). The MSC then knows that the number is complete and that the terminating party is being alerted about the incoming call.

If B answers the call, the fixed-line switching center sends an Answer Message (ANM) to the MSC and conversation can start.

When B ends the call, the fixed-line switching center resets the connection in the switching matrix and sends a Release (REL) message to the MSC. The MSC confirms the termination of the connection by sending back a Release Complete (RLC) message. If A had terminated the call, the messages would have been identical, with only the direction of the REL and RLC reversed.

For communication between the switching centers (SSPs) and the databases (SCPs), the Signaling Connection and Control Part (SCCP) is used on layer 4. SCCP is very similar to TCP and User Datagram Protocol (UDP) in the IP world. Protocols on layer 4 of the protocol stack enable the distinguishing of different applications on a single system. TCP and UDP use ports to do this. If a personal computer, for example, is used as both a web server and a File Transfer Protocol (FTP) server at the same time, both applications would be accessed over the network via the same IP address. However, while the web server can be reached via port 80, the FTP server waits for incoming data on port 21. Therefore, it is quite easy for the network protocol stack to select the application to which incoming data packets should be forwarded. In the SS-7 world, the task of forwarding incoming messages to the correct application is done by SCCP. Instead of port numbers, SCCP uses Subsystem Numbers (SSNs).

For database access, the Transaction Capability Application Part (TCAP) protocol has been designed as part of the SS-7 family of protocols. TCAP defines a number of different modules and messages that can be used to query all kinds of different databases in a uniform way.

1.4.2 SS-7 Protocols for GSM

Apart from the fixed-line-network SS-7 protocols, the following additional protocols were defined to address the special needs of a GSM network.

- **The Mobile Application Part (MAP).** This protocol has been standardized in 3GPP TS 29.002 [3] and is used for the communication between an MSC and the HLR, which maintains subscriber information. The HLR is queried, for example, if the MSC wants to establish a connection to a mobile subscriber. In this case, the HLR returns information about the current location of the subscriber. The MSC is then able to forward the call to the mobile subscriber's switching center, establishing a voice channel between itself and the next hop by using the ISUP message flow that has been shown in Figure 1.6. MAP is also used between two MSCs if the subscriber moves into the coverage area of a different MSC while a call is ongoing. As shown in Figure 1.7, the MAP protocol uses the TCAP, SCCP, and MTP protocols on lower layers.
- **The Base Station Subsystem Mobile Application Part (BSSMAP).** This protocol is used for communication between the MSC and the radio network. Here, the additional protocol is necessary, for example, to establish a dedicated radio channel for a new connection to a mobile subscriber. As BSSMAP is not a database query language like the MAP protocol, it is based directly on SCCP instead of TCAP being used in between.
- **The Direct Transfer Application Part (DTAP).** This protocol is used between the user's mobile device, which is also called mobile station (MS), and the MSC, to communicate transparently. To establish a voice call, the MS sends a 'Setup' message to the MSC. As in the example in Section 1.4.1, this message contains the phone number of the called subscriber, among other things. As it is only the MSC's task to forward calls, all

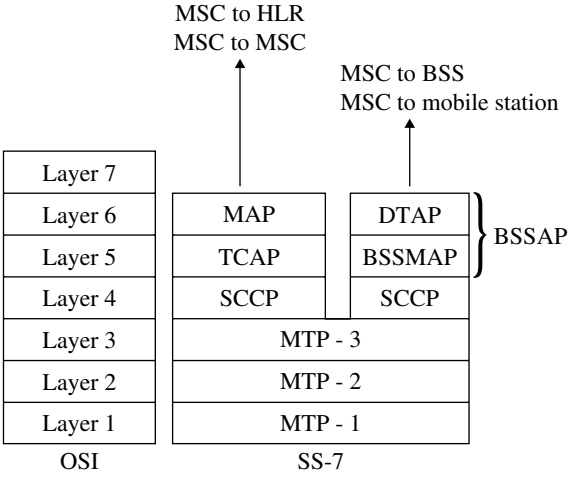

Figure 1.7 Enhancement of the SS-7 protocol stack for GSM.

network nodes between the MS and the MSC forward the message transparently and thus need not understand the DTAP protocol.

1.4.3 IP-Based SS-7 Protocol Stack

Today, an IP network is used for the transmission of SS-7 signaling messages and the MTP-1 and MTP-2 protocols were replaced by the IP and the transport-medium-dependent lower-layer protocols (e.g. Ethernet). Figure 1.8 shows the difference between the IP stack and the classic stack presented in the previous section.

In the IP stack, layer-4 protocols are either UDP or TCP for most services. For the transmission of SS-7 messages, however, a new protocol has been specified, which is referred to as Stream Control Transmission Protocol (SCTP). When compared to TCP and UDP, it offers advantages when many signaling connections between two network nodes are active at the same time.

On the next protocol layer, SCTP is followed by the M3UA (MTP-3 User Adaptation Layer) protocol. As the name implies, the protocol is used to transfer information that is contained in the classic MTP-3 protocol. For higher protocol layers such as SCCP, M3UA simulates all functionalities of MTP-3. Therefore, the use of an IP protocol stack is transparent to all higher-layer SS-7 protocols.

In the industry, the IP-based SS-7 protocol stack or the IP-based transmission of SS-7 messages is often referred to as SIGTRAN (signaling transmission). The abbreviation originated from the name of the IETF (Internet Engineering Task Force) working group that was created for the definition of these protocols.

As described in Section 1.1.1, the ISUP protocol was used for the establishment of voice calls between switching centers and the assignment of a 64 kbit/s timeslot. In an IP-based network, voice calls are transmitted in IP packets, and consequently, the ISUP protocol had to be adapted as well. The resulting protocol is referred to as the Bearer-Independent Call Control (BICC) protocol, which largely resembles ISUP.

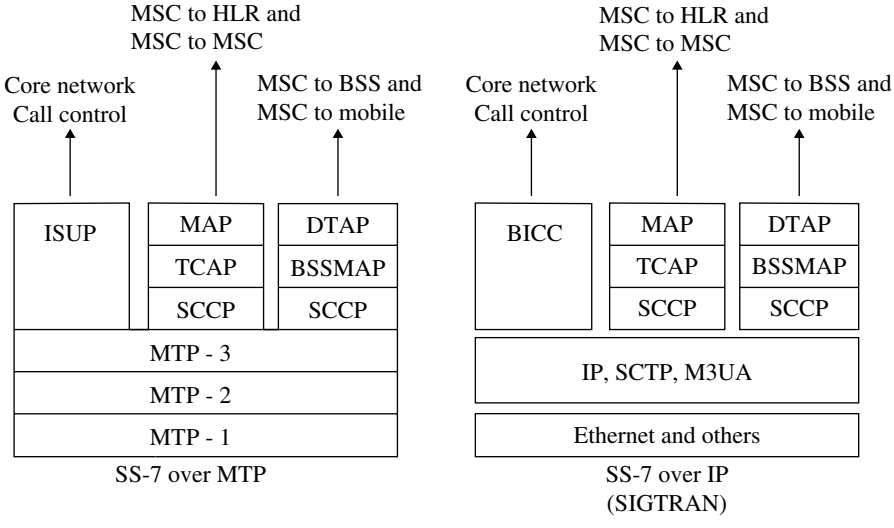

Figure 1.8 Comparison of the classic and IP-based SS-7 protocol stacks.

1.5 The GSM Subsystems

A GSM network is split into three subsystems, which are described in more detail below:

- **The Base Station Subsystem (BSS)**, which is also called 'radio network,' contains all nodes and functionalities that are necessary to connect mobile subscribers wirelessly over the radio interface to the network. The radio interface is usually also referred to as the 'air interface.'
- **The Network Subsystem (NSS)**, which is also called 'core network,' contains all nodes and functionalities that are necessary for switching of calls, for subscriber management and mobility management.
- **The Intelligent Network Subsystem (IN)** comprises SCP databases that add optional functionality to the network. One of the most important optional IN functionalities of a mobile network is the prepaid service, which allows subscribers to first fund an account with a certain amount of money which can then be used for network services like phone calls, Short Messaging Service (SMS) messages, and of course, Internet access. When a prepaid subscriber uses a service of the network, the responsible IN node is contacted and the amount the network operator charges for a service is deducted from the account in real-time.

1.6 The Network Subsystem

The most important responsibilities of the NSS are call establishment, call control, and routing of calls between different fixed and mobile switching centers and other networks. Furthermore, the NSS is responsible for subscriber management. The nodes necessary for these tasks in a classic network architecture are shown in Figure 1.9. Figure 1.10 shows the nodes required in IP-based core networks. Both designs are further described in the following sections.

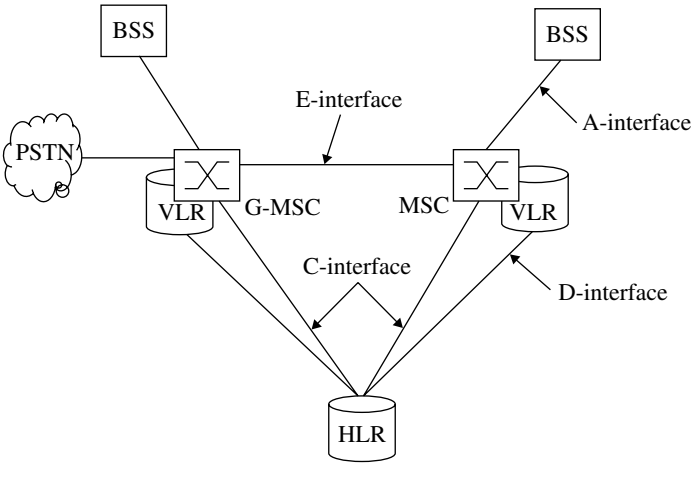

Figure 1.9 Interfaces and nodes in a classic NSS architecture.