GSM Networks: Protocols, Terminology, and Implementation

GSM Networks: Protocols, Terminology, and Implementation

Gunnar Heine



Artech House
Boston • London

Samsung Ex. 1032, Page 2 of 417

Library of Congress Cataloging-in-Publication Data
Heine, Gunnar.
[GSM—Signalisierung verstehen und praktisch anwenden. English]
GSM networks : protocols, terminology, and implementation / Gunnar Heine
p. cm. — (Artech House mobile communications library)
Translation of: GSM—Signalisierung verstehen und praktisch anwenden.
Includes bibliographical references and index.
ISBN 0-89006-471-7 (alk. paper)
1. Global system for mobile communications. I. Title.
TK5103.483.H4513 1998
621.3845'6—dc21 98-51784
CIP

British Library Cataloguing in Publication Data
Heine, Gunnar
GSM networks : protocols, terminology, and implementation—
(Artech House mobile communications library)
1. Global system for mobile communications
I. Title
621.3'8456

ISBN 0-89006-471-7

Cover design by Lynda Fishbourne

© 1998 Franzis' Verlag GmbH
Translated from GSM - Signalisierung verstehen und praktisch anwenden (Franzis' Verlag 1998)
English translation version:

© 1999 ARTECH HOUSE, INC.
685 Canton Street
Norwood, MA 02062

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

International Standard Book Number: 0-89006-471-7
Library of Congress Catalog Card Number: 98-51784

10 9 8 7 6 5 4 3 2 1

Contents

1	**Introduction**	**1**
1.1	About This Book	1
1.2	Global System for Mobile Communication (GSM)	2
1.2.1	The System Architecture of GSM: A Network of Cells	3
1.2.2	An Overview on the GSM Subsystems	4
1.3	The Focus of This Book	7
1.4	Signaling	8
1.4.1	What is Signaling?	8
1.4.2	How is Signaling Performed?	8
1.4.3	What is Signaling Used For?	10
1.5	Representation of Messages	10
2	**The Mobile Station and the Subscriber Identity Module**	**13**
2.1	Subscriber Identity Module	13
2.1.1	The SIM as a Database	15
2.1.2	Advantage for the Subscriber	15
2.2	Mobile Station	17
2.2.1	Types of Mobile Stations	17

Samsung Ex. 1032, Page 4 of 417

2.2.2 Functionality 17
2.2.3 Mobile Stations as Test Equipment 18

3 The Base Station Subsystem 19

3.1 Base Transceiver Station 19
3.1.1 Architecture and Functionality of a Base Transceiver Station 20
3.1.2 Base Transceiver Station Configurations 22
3.2 Base Station Controller 25
3.2.1 Architecture and Tasks of the Base Station Controller 26
3.3 Transcoding Rate and Adaptation Unit 28
3.3.1 Function of the Transcoding Rate and Adaptation Unit 28
3.3.2 Site Selection for Transcoding Rate and Adaptation Unit 28
3.3.3 Relationship Between the Transcoding Rate, Adaptation Unit, and Base Station Subsystem 29

4 The Network Switching Subsystem 31

4.1 Home Location Register and Authentication Center 32
4.2 Visitor Location Register 33
4.3 The Mobile-Services Switching Center 34
4.3.1 Gateway MSC 36
4.3.2 The Relationship Between MSC and VLR 36
4.4 Equipment Identity Register 37

5 The OSI Reference Model 39

5.1 Reasons for Standardization 39
5.2 Layering in the OSI Reference Model 40
5.3 Data Types of the OSI Reference Model 41
5.4 Information Processing in the OSI Reference Model 42

5.5	Advantages of the OSI Reference Model	42
5.6	The Seven Layers of the OSI Reference Model	43
5.6.1	Layer 1: The Physical Layer	43
5.6.2	Layer 2: The Data Link Layer	43
5.6.3	Layer 3: The Network Layer	44
5.6.4	Layer 4: The Transport Layer	44
5.6.5	Layer 5: The Session Layer	45
5.6.6	Layer 6: The Presentation Layer	45
5.6.7	Layer 7: The Application Layer	46
5.7	Comprehension Issues	46
5.7.1	An Analogy: The Move to Europe	47
6	**The Abis-Interface**	**51**
6.1	Channel Configurations	51
6.2	Alternatives for Connecting the BTS to the BSC	52
6.2.1	BTS Connection in a Serial Configuration	54
6.2.2	Connection of BTSs in Star Configuration	55
6.3	Signaling on the Abis-Interface	55
6.3.1	OSI Protocol Stack on the Abis-Interface	55
6.3.2	Layer 2	56
6.3.3	Layer 3	71
6.4	Bringing an Abis-Interface Into Service	87
6.4.1	Layer 1	87
6.4.2	Layer 2	87
7	**The Air-Interface of GSM**	**89**
7.1	The Structure of the Air-Interface in GSM	89
7.1.1	The FDMA/TDMA Scheme	89
7.1.2	Frame Hierarchy and Frame Numbers	90
7.1.3	Synchronization Between Uplink and Downlink	93
7.2	Physical Versus Logical Channels	94
7.3	Logical-Channel Configuration	94

7.3.1 Mapping of Logical Channels Onto Physical Channels 95
7.3.2 Possible Combinations 97
7.4 Interleaving 100
7.5 Signaling on the Air Interface 101
7.5.1 Layer 2 $LAPD_m$ Signaling 101
7.5.2 Layer 3 107

8 Signaling System Number 7 125

8.1 The SS7 Network 125
8.2 Message Transfer Part 126
8.3 Message Types in SS7 127
8.3.1 Fill-In Signal Unit 127
8.3.2 Link Status Signal Unit 128
8.3.3 Message Signal Unit 128
8.4 Addressing and Routing of Messages 130
8.4.1 Example: Determination of DPC, OPC, and SLS in a Hexadecimal Trace 131
8.4.2 Example: Commissioning of an SS7 Connection 132
8.5 Error Detection and Error Correction 133
8.5.1 Send Sequence Numbers and Receive Sequence Numbers (FSN, BSN, BIB, FIB) 135
8.5.2 BSN/BIB and FSN/FIB for Message Transfer 135
8.6 SS7 Network Management and Network Test 138
8.6.1 SS7 Network Test 139
8.6.2 Possible Error Cases 140
8.6.3 Format of SS7 Management Messages and Test Messages 142
8.6.4 Messages in SS7 Network Management and Network Test 142

9 Signaling Connection Control Part 153

9.1 Tasks of the SCCP 153

9.1.1	Services of the SCCP: Connection-Oriented Versus Connectionless	154
9.1.2	Connection-Oriented Versus Connectionless Service	154
9.2	The SCCP Message Format	156
9.3	The SCCP Messages	158
9.3.1	Tasks of the SCCP Messages	158
9.3.2	Parameters of SCCP Messages	159
9.3.3	Decoding a SCCP Message	167
9.4	The Principle of a SCCP Connection	167
10	**The A-Interface**	**171**
10.1	Dimensioning	171
10.2	Signaling Over the A-Interface	173
10.2.1	The Base Station Subsystem Application Part	173
10.2.2	The Message Structure of the BSSAP.	174
10.2.3	Message Types of the Base Station Subsystem Management Application Part	176
10.2.4	Decoding of a BSSMAP Message	183
11	**Transaction Capabilities and Mobile Application Part**	**185**
11.1	Transaction Capabilities Application Part	185
11.1.1	Addressing in TCAP	186
11.1.2	The Internal Structure of TCAP	187
11.1.3	Coding of Parameters and Data in TCAP	189
11.1.4	TCAP Messages Used in GSM	198
11.2	Mobile Application Part	208
11.2.1	Communication Between MAP and its Users	209
11.2.2	MAP Services	211
11.2.3	Local Operation Codes of the Mobile Application Part	214

11.2.4 Communication Between Application, MAP, and TCAP 220

12 Scenarios 225

12.1 Location Update 227
12.1.1 Location Update in the BSS 227
12.1.2 Location Update in the NSS 227
12.2 Equipment Check 227
12.3 Mobile Originating Call 233
12.3.1 Mobile Originating Call in the BSS 233
12.3.2 Mobile Originating Call in the NSS 233
12.4 Mobile Terminating Call 244
12.4.1 Mobile Terminating Call in the BSS 244
12.4.2 Mobile Terminating Call in the NSS 244
12.5 Handover 251
12.5.1 Measurement Results of BTS and MS 251
12.5.2 Analysis of a MEAS_RES/MEAS_REP 255
12.5.3 Handover Scenarios 256

13 Quality of Service 275

13.1 Tools for Protocol Measurements 275
13.1.1 OMC Versus Protocol Analyzers 276
13.1.2 Protocol Analyzer 278
13.2 Signaling Analysis in GSM 280
13.2.1 Automatic Analysis of Protocol Traces 280
13.2.2 Manual Analysis of Protocol Traces 284
13.3 Tips and Tricks 285
13.3.1 Identification of a Single Connection 285
13.4 Where in the Trace File to Find What Parameter? 287
13.5 Detailed Analysis of Errors on Abis Interface and A-Interface 287
13.5.1 Most Important Error Messages 291

13.5.2 Error Analysis in the BSS 296

Glossary 303

About the Author 405

Index 407

1

Introduction

1.1 About This Book

Someone who wants to get to know the customs of a country frequently receives the advice to learn the language of that country. Why? Because the differences that distinguish the people of one country from those of another are reflected in the language. For example, the people of the islands of the Pacific do not have a term for *war* in their language. Similarly, some native tribes in the rain forests of the Amazon use up to 100 different terms for the color *green.*

The reflection of a culture in its language also applies to the area of computers. A closer look reveals that a modern telecommunications system, like the Global System for Mobile Communication (GSM), is nothing more than a network of computers. Depending on the application, a language has to be developed for such a communications network. That language is the signaling system, which allows intersystem communication by defining a fixed protocol. The study of the signaling system provides insight into the internal workings of a communication system.

The main purpose of this book, after briefly describing the GSM subsystems, is to lay the focus on the communications method—the signaling between these subsystems— and to answer questions such as which message is sent when, by whom, and why.

Because it is not always possible to answer all questions in a brief description or by analyzing signaling, details are covered in greater depth in the glossary. Furthermore, most of the items in the glossary contain references to GSM and International Telecommunication Union (ITU) Recommendations, which in turn allow for further research.

Samsung Ex. 1032, Page 11 of 417

For the engineer who deals with GSM or its related systems on a daily basis, this book has advantages over other GSM texts in that it quickly gets to the point and can be used as a reference source. I hope the readers of this book find it helpful in filling in some of the gray areas on the GSM map.

1.2 Global System for Mobile Communication (GSM)

When the acronym GSM was used for the first time in 1982, it stood for *Groupe Spéciale Mobile*, a committee under the umbrella of *Conférence Européenne des Postes et Télécommunications* (CEPT), the European standardization organization.

The task of GSM was to define a new standard for mobile communications in the 900 MHz range. It was decided to use digital technology. In the course of time, CEPT evolved into a new organization, the European Telecommunications Standard Institute (ETSI). That, however, did not change the task of GSM. The goal of GSM was to replace the purely national, already overloaded, and thus expensive technologies of the member countries with an international standard.

In 1991, the first GSM systems were ready to be brought into so-called friendly-user operation. The meaning of the acronym GSM was changed that same year to stand for Global System for Mobile Communications. The year 1991 also saw the definition of the first derivative of GSM, the Digital Cellular System 1800 (DCS 1800), which more or less translates the GSM system into the 1800 MHz frequency range.

In the United States, DCS 1800 was adapted to the 1900 MHz band (Personal Communication System 1900, or PCS 1900). The next phase, GSM Phase 2, will provide even more end-user features than phase 1 of GSM did. In 1991, only "insiders" believed such a success would be possible because mobile communications could not be considered a mass market in most parts of Europe.

By 1992, many European countries had operational networks, and GSM started to attract interest worldwide. Time has brought substantial technological progress to the GSM hardware. GSM has proved to be a major commercial success for system manufacturers as well as for network operators.

How was such success possible? Particularly today, where Code Division Multiple Access (CDMA), Personal Handy Phone System (PHS), Digital Enhanced Cordless Telecommunications (DECT), and other systems try to mimic the success of GSM, that question comes to mind and is also discussed within the European standardization organizations.

The following factors were major contributors to the success of GSM:

- The liberalization of the monopoly of telecommunications in Europe during the 1990s and the resulting competition, which consequently lead to lower prices and more "market";
- The knowledge-base and professional approach within the Groupe Spéciale Mobile, together with the active cooperation of the industry;
- The lack of competition: For example, in the United States and Japan, competitive standards for mobile services started being defined only after GSM was already well established.

The future will show which system will prevail as the next generation of mobile communications. ETSI and the Special Mobile Group (SMG), renamed GSM, are currently standardizing the Universal Mobile Telecommunication System (UMTS). Japan is currently improving PHS.

The various satellite communications systems that now push into the market are another, possibly decisive, factor in providing mobile communications on a global basis.

1.2.1 The System Architecture of GSM: A Network of Cells

Like all modern mobile networks, GSM utilizes a cellular structure as illustrated in Figure 1.1.

The basic idea of a cellular network is to partition the available frequency range, to assign only parts of that frequency spectrum to any base transceiver station, and to reduce the range of a base station in order to reuse the scarce frequencies as often as possible. One of the major goals of network planning is to reduce interference between different base stations.

Anyone who starts thinking about possible alternatives should be reminded that current mobile networks operate in frequency ranges where attenuation is substantial. In particular, for mobile stations with low power emission, only small distances (less than 5 km) to a base station are feasible.

Besides the advantage of reusing frequencies, a cellular network also comes with the following disadvantages:

- An increasing number of base stations increases the cost of infrastructure and access lines.
- All cellular networks require that, as the mobile station moves, an active call is handed over from one cell to another, a process known as handover.

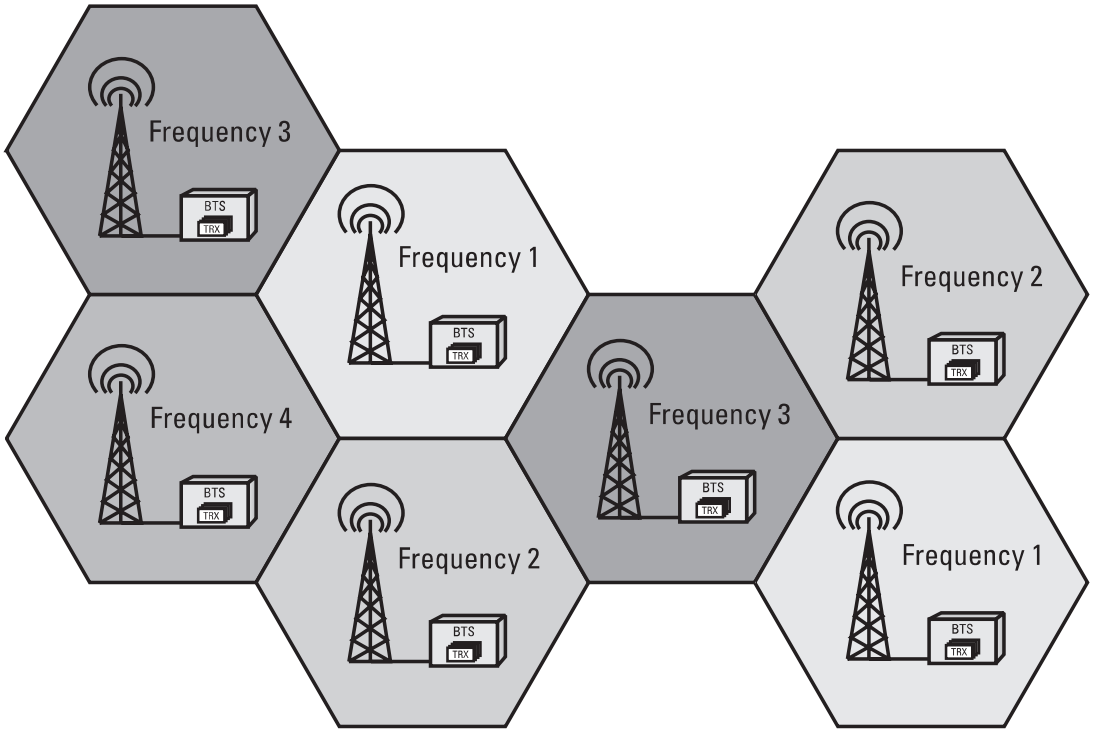


Figure 1.1 The radio coverage of an area by single cells.

- The network has to be kept informed of the approximate location of the mobile station, even without a call in progress, to be able to deliver an incoming call to that mobile station.
- The second and third items require extensive communication between the mobile station and the network, as well as between the various network elements. That communication is referred to as signaling and goes far beyond the extent of signaling that fixed networks use. The extension of communications requires a cellular network to be of modular or hierarchical structure. A single central computer could not process the amount of information involved.

1.2.2 An Overview on the GSM Subsystems

A GSM network comprises several elements: the mobile station (MS), the subscriber identity module (SIM), the base transceiver station (BTS), the base station controller (BSC), the transcoding rate and adaptation unit (TRAU), the mobile services switching center (MSC), the home location register (HLR), the visitor location register (VLR), and the equipment identity register (EIR). Together, they form a public land mobile network (PLMN). Figure 1.2 provides an overview of the GSM subsystems.

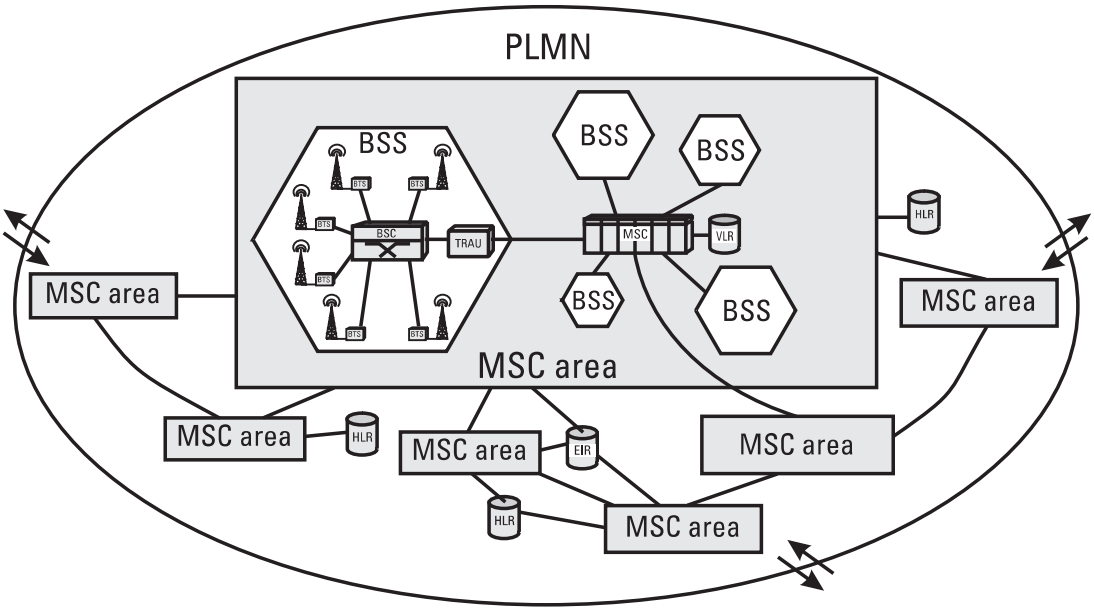


Figure 1.2 The architecture of a PLMN.

1.2.2.1 Mobile Station



GSM-PLMN contains as many MSs as possible, available in various styles and power classes. In particular, the handheld and portable stations need to be distinguished.

1.2.2.2 Subscriber Identity Module



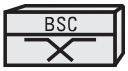
GSM distinguishes between the identity of the subscriber and that of the mobile equipment. The SIM determines the directory number and the calls billed to a subscriber. The SIM is a database on the user side. Physically, it consists of a chip, which the user must insert into the GSM telephone before it can be used. To make its handling easier, the SIM has the format of a credit card or is inserted as a plug-in SIM. The SIM communicates directly with the VLR and indirectly with the HLR.

1.2.2.3 Base Transceiver Station



A large number of BTSs take care of the radio-related tasks and provide the connectivity between the network and the mobile station via the Air-interface.

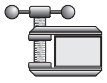
1.2.2.4 Base Station Controller



The BTSs of an area (e.g., the size of a medium-size town) are connected to the BSC via an interface called the Abis-interface. The

BSC takes care of all the central functions and the control of the subsystem, referred to as the base station subsystem (BSS). The BSS comprises the BSC itself and the connected BTSs.

1.2.2.5 Transcoding Rate and Adaptation Unit



One of the most important aspects of a mobile network is the effectiveness with which it uses the available frequency resources. Effectiveness addresses how many calls can be made by using a certain bandwidth, which in turn translates into the necessity to compress data, at least over the Air-interface. In a GSM system, data compression is performed in both the MS and the TRAU. From the architecture perspective, the TRAU is part of the BSS. An appropriate graphical representation of the TRAU is a black box or, more symbolically, a clamp.

1.2.2.6 Mobile Services Switching Center



A large number of BSCs are connected to the MSC via the A-interface. The MSC is very similar to a regular digital telephone exchange and is accessed by external networks exactly the same way. The major tasks of an MSC are the routing of incoming and outgoing calls and the assignment of user channels on the A-interface.

1.2.2.7 Home Location Register



The MSC is only one subcenter of a GSM network. Another subcenter is the HLR, a repository that stores the data of a large number of subscribers. An HLR can be regarded as a large database that administers the data of literally hundreds of thousands of subscribers. Every PLMN requires at least one HLR.

1.2.2.8 Visitor Location Register



The VLR was devised so that the HLR would not be overloaded with inquiries on data about its subscribers. Like the HLR, a VLR contains subscriber data, but only part of the data in the HLR and only while the particular subscriber roams in the area for which the VLR is responsible. When the subscriber moves out of the VLR area, the HLR requests removal of the data related to a subscriber from the VLR. The geographic area of the VLR consists of the total area covered by those BTSs that are related to the MSCs for which the VLR provides its services.

1.2.2.9 Equipment Identity Register



The theft of GSM mobile telephones seems attractive, since the identities of subscribers and their mobile equipment are separate. Stolen equipment can be reused simply by using any valid SIM. Barring of a subscriber by the operator does not bar the mobile equipment. To prevent that kind of misuse, every GSM terminal equipment contains a unique identifier, the international mobile equipment identity (IMEI). It lies within the realm of responsibilities of a network operator to equip the PLNM with an additional database, the EIR, in which stolen equipment is registered and so can be used to bar fraudulent calls and even, theoretically, to track down a thief (by analyzing the related SIM data).

1.3 The Focus of This Book

This book describes briefly the GSM subsystems, their structure, and their tasks. However, the focus of this book lies not on the GSM network elements themselves but on the interfaces between them.

Among others, the following issues will be addressed:

- What signaling standards and what protocols are used to serve connection requests by mobile subscribers?
- How are the various interfaces utilized?
- What happens in case of errors?
- Although GSM uses available signaling standards, where are the GSM specific adaptations?

One has to remember that most of the signaling is necessary to support the mobility of a subscriber. All messages of the area mobility management (MM) and radio resource management (RR), in particular, serve only that purpose. Only a fraction of the exchanged messages are used for the connection setup as such, and those are all the messages that are related to call control (CC).

A presentation of the Open System Interconnection (OSI) Reference Model is mandatory in a book in which the focus is on signaling.

Another focus of the text is on the application of the various protocols for error analysis. Which error indication is sent by the system and when? How is such an indication interpreted? What are the potential sources of errors?

A word on coding of parameters and messages should be added here: Coding of message types and other essential parameters are always included. However, because this book has no intention of being a copy of the GSM Recommendations, it deliberately refrains from providing a complete list of all parameters of all interfaces.

The value of protocol test equipment for error analysis and routine testing is indisputably high, but what help do programs for automatic analysis provide? Those questions will be answered as well.

A large part of this book is taken up by a glossary, which provides descriptions of all abbreviations, terms, and processes that a reader may confront during work on GSM.

1.4 Signaling

The main focus of this book is on the signaling between the various network elements of GSM. The questions arise of what signaling actually constitutes and what it is used for. Although we do not want to go back to the basics of telecommunications to answer those questions, a number of basic explanations do seem necessary.

1.4.1 What is Signaling?

Signaling is the language of telecommunications that machines and computers use to communicate with each other. In particular, the signals that a user enters need to be converted to a format that is appropriate for machines and then transmitted to a remote entity. The signals (e.g., the identity of a called party) are not part of the communication as such, that is, they are not a payload or a revenue-earning entity.

Signaling is comparable to the pilots and the flight attendants on an airplane. The crew members are no "payload," but they are necessary to carry the payload. Another, perhaps more appropriate, illustration is to consider the now almost extinct telephone operator, whose function it was to carry out the signaling function and switching of a telecommunications system by connecting cables between the appropriate incoming and outgoing lines.

1.4.2 How is Signaling Performed?

When calls were set up manually, signaling consisted mostly of direct current impulses, which allowed a central office to determine the dialed digits. Some

readers may still remember the rotary telephone sets, in which the impulses were created mechanically by the spin of the rotor. The situation changed completely with the entry of computer technology into telecommunications. The microchip utilized by telecommunications opens today, at the end of the twentieth century, a multitude of new signaling functionality, which were unthinkable even 20 years ago. Computers are the backbone of modern telecommunications systems.

This new technology makes mobile communications possible in the first place. The signaling requirements of modern mobile systems are so vast that the former technology would not have been able to manage them. Computerization, however, did not change much of the principle. As in the old days, electrical or optical signals are sent, over an appropriate medium (typically serially) and interpreted by the receiver. What did change is the speed of the transmission. The progress in this area has been exponential.

The smallest unit of a signal is called a *bit* and can, for example, be represented by an electric voltage, which a receiver can measure during a specified period of time. If the receiver measures the voltage as "low" over the specified time period, it interprets the value as a 0. If the voltage is "high," the receiver interprets the value as a 1. It does not matter which level represents which value, so long as both the sender and the receiver agree on which is which.

A sequence of bits allows the coding and sending of complex messages, which, in turn, allows a process to be controlled or information to be conveyed. The result is a bit stream, as shown in Figure 1.3.

Pulse code modulation (PCM) is the worldwide process for transmission of digital signals. PCM is used to transmit both signaling data and payload. PCM is categorized into hierarchies, depending on the transmission rate. The PCM link of 2 megabits per second (Mbps) (one that is referred to frequently in this book) is only one variant of many. By utilizing a time-division

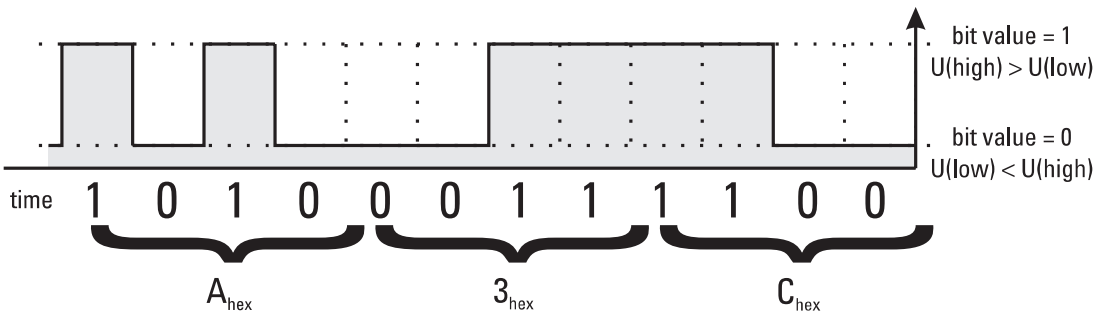


Figure 1.3 Decoding of a bit stream.

multiplexing technique, such a 2-Mbps PCM link can, among others, be partitioned into 32 independent channels, each capable of carrying 64 kilobits per second (Kbps).

Another aspect of the change that the digital technology has enabled reveals its advantage only after a second look. Almost all signaling standards, like Signaling System Number 7 (SS7) and Link Access Protocol for the D-channel (LAPD) separate the traffic channel from the signaling or control channel. This is referred to as outband signaling, in contrast to inband signaling. In the case of inband signaling, all the control information is carried within the traffic channel. Although outband signaling requires the reservation of a traffic channel, it makes a more efficient use of resources overall. The reason for that lies in the reduced occupation time of the traffic channel, which is not needed during call setup. Both call setup and call release can be carried out for many connections via one control channel, since signaling data use the resources more economically. One 64-Kbps time slot out of a 2-Mbps PCM link typically is used for signaling data; a call setup consumes about 1 to 2 Kbps.

1.4.3 What is Signaling Used For?

The main task of signaling is still to set up and to clear a connection between end users or machines. Today, constantly new applications are added. Among them are automated database accesses, in which telecommunications systems call each other and which are fairly transparent to a caller, or the wide area of supplementary services, of which only call forwarding is mentioned here as an example. The glossary provides a list of all GSM supplementary services.

1.5 Representation of Messages

When working with protocol test equipment and in practical work, message names usually are abbreviated. Most GSM and ITU Telecommunication Standardization Sector (ITU-T) Recommendations list the well-defined abbreviations and acronyms, which this book also uses to a large extent. The complete message names and explanations can be found in the respective chapters.

Since a picture often expresses more than a thousand words, this book contains a large number of figures and protocol listings. The various messages illustrated in the figures show parameters, which are formatted per interface and are presented as shown in Figures 1.4(a) through 1.4(e).

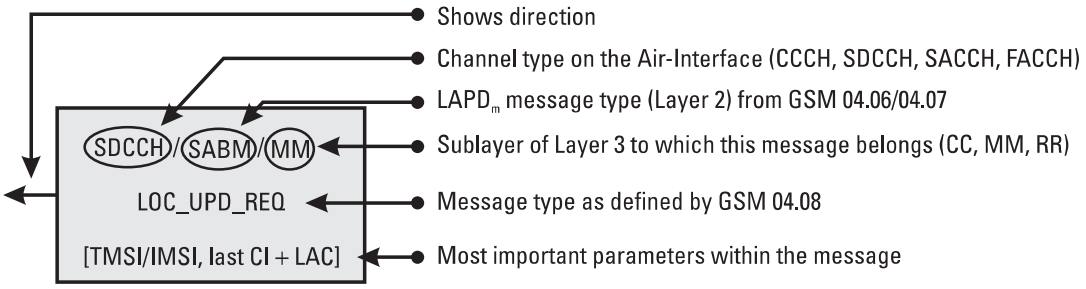


Figure 1.4(a) Format for messages over the Air-interface ($LAPD_m$, GSM 04.08).

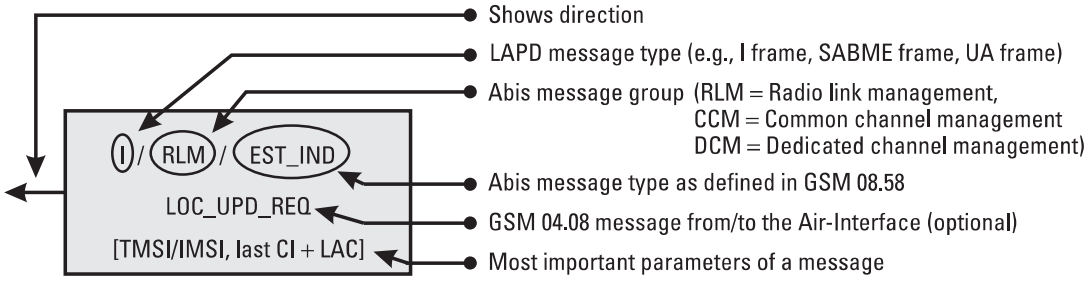


Figure 1.4(b) Format for messages over the Abis-interface (LAPD, GSM 08.58).

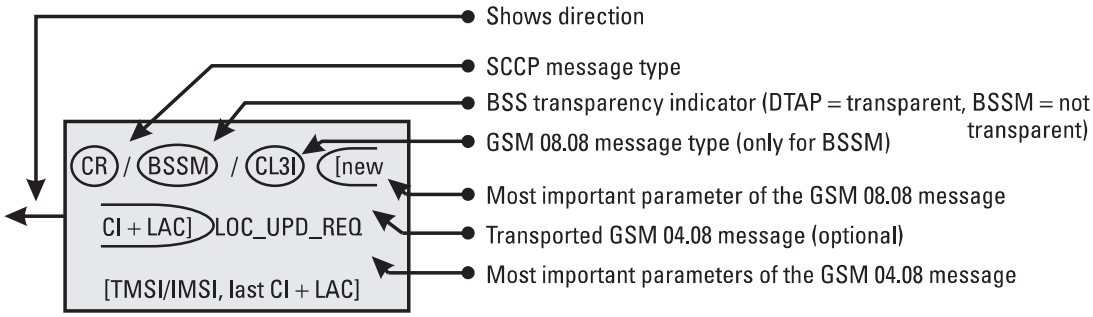


Figure 1.4(c) Format for messages over the A-interface [SS7, signaling connection control part (SCCP), GSM 08.06, GSM 08.08].

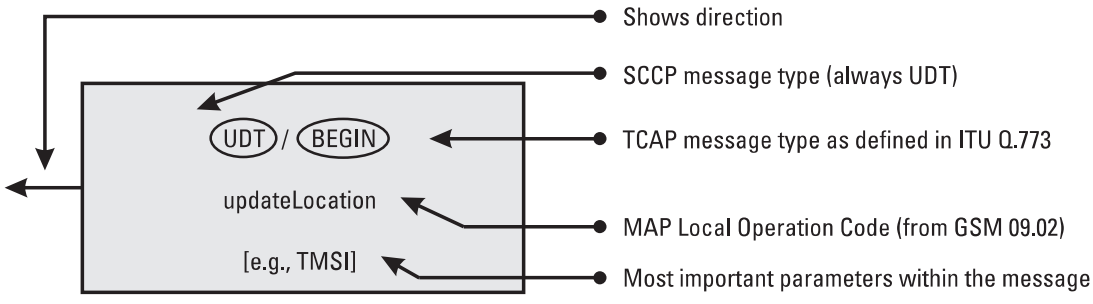


Figure 1.4(d) Format for mobile application part (MAP) messages over all network switching subsystem (NSS) interfaces [SS7, SCCP, transaction capabilities application part (TCAP), MAP].

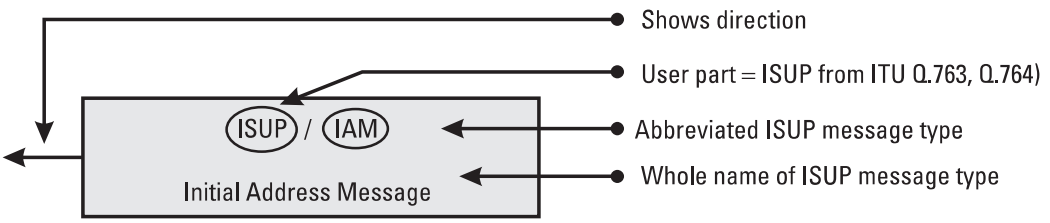


Figure 1.4(e) Format for ISUP messages between MSCs and toward the Integrated Services Digital Network (ISDN) [SS7 and the ISDN user part (ISUP)].

2

The Mobile Station and the Subscriber Identity Module

The GSM telephone set and the SIM are the only system elements with which most users of GSM have direct contact. The GSM telephone set and the SIM form an almost complete GSM system within themselves with all the functionality, from ciphering to the HLR. Figure 2.1 shows a block diagram of a mobile station with a SIM slot.

2.1 Subscriber Identity Module

The SIM is a microchip that is planted on either a check card (ID-1 SIM) or a plastic piece about 1 cm square (plug-in SIM). Figure 2.2 shows both variants. Except for emergency calls, a GSM mobile phone cannot be used without the SIM. The GSM terminology distinguishes between a mobile station and mobile equipment. The mobile equipment becomes a mobile station when the SIM is inserted. There is no difference in functionality between the ID-1 SIM and the plug-in SIM, except for size, which is an advantage for the plug-in SIM when used in a small handheld telephone. Today, many network operators offer (at an additional cost) identical pairs of ID-1 SIM/plug-in SIM, so the same SIM can be used in a car phone and in a handheld telephone.

Samsung Ex. 1032, Page 23 of 417

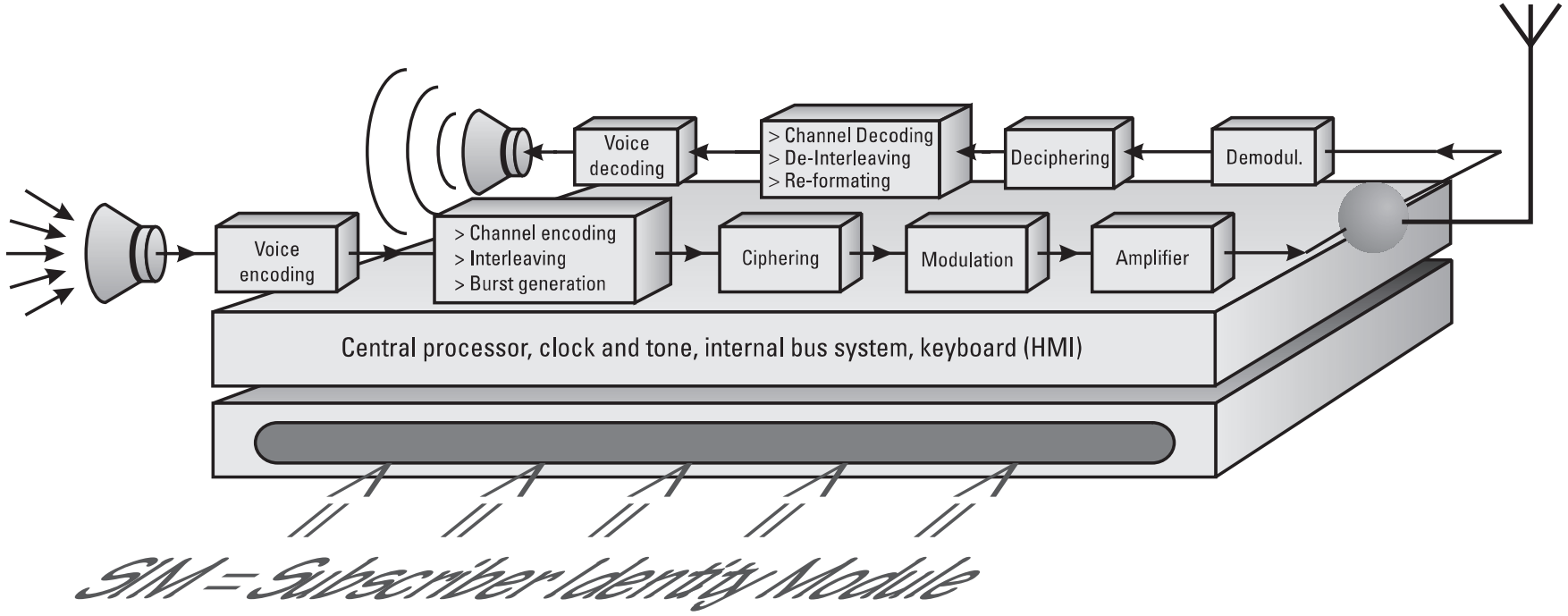


Figure 2.1 Block diagram of a GSM MS.

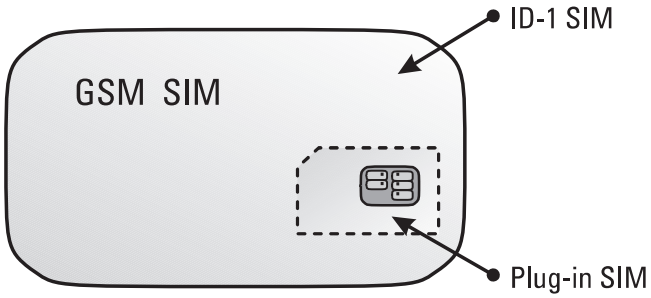


Figure 2.2 Plug-in SIM and ID-1 SIM.

2.1.1 The SIM as a Database

The major task of a SIM is to store data. That does not mean that the data is only subscriber data. One has to differentiate between data types for various tasks. The most important parameters that a SIM holds are presented in Table 2.1. It should be noted that the list is not complete and that the SIM can also be used to store, for example, telephone numbers.

2.1.2 Advantage for the Subscriber

The SIM is one of the most interesting features for a user of GSM, because it permits separation of GSM telephone equipment and the related database. In other words, the subscriber to a GSM system is not determined by the identity of the mobile equipment but by the SIM, which always has to be inserted into the equipment before it can be used. This is the basis for personal mobility.

Table 2.1
Data Stored on a SIM

Parameter	Remarks
Administrative data	
PIN/PIN2 (m/v)	Personal identification number; requested at every powerup (PIN or PIN2)
PUK/PUK2 (m/f)	PIN unblocking key; required to unlock a SIM
SIM service table (m/f)	List of the optional functionality of the SIM
Last dialed number) (o/v)	Redial
Charging meter (o/v)	Charges and time increments can be set
Language (m/v)	Determines the language for prompts by the mobile station

Table 2.1 (continued)

Parameter	Remarks
Security related data	
Algorithm A3 and A8 (m/f)	Required for authentication and to determine Kc
Key Ki (m/f)	Individual value; known only on SIM and the HLR
Key Kc (m/v)	Result of A8, Ki, and random number (RAND)
CKSN (m/v)	Ciphering key sequence number
Subscriber data	
IMSI (m/f)	International mobile subscriber identity
MSISDN (o/f)	Mobile subscriber ISDN; directory number of a subscriber
Access control class(es) (m/f)	For control of network access
Roaming data	
TMSI (m/v)	Temporary mobile subscriber identity
Value of T3212 (m/v)	For location updating
Location updating status	Is a location update required?
LAI (m/v)	Location area information
Network color codes (NCCs) of restricted PLMNs (m/v)	Maximum of 4 PLMNs can be entered on a SIM after unsuccessful location update; cause "PLMN not allowed." Oldest entry deleted when more than 4 restricted PLMNs are found.
NCCs of preferred PLMNs (o/v)	What PLMN should the MS select, if there is more than one to choose from and the home PLMN is not available?
PLMN data	
NCC, mobile country code (MCC), and mobile network code (MNC) of the home PLMN (m/f)	Network identifier
Absolute radio frequency channel numbers (ARFCNs) of home PLMN (m/f)	Frequencies for which the home PLMN is licensed.

Legend: m = mandatory; o = optional; f = fixed, unchangeable value; v = changeable

Because of the SIM, a GSM customer can use different telephones (e.g., a car phone and a handheld phone) and still be reachable under the same directory number. Even in case of a defect in the user's GSM telephone, any other GSM telephone can be used instead, simply by changing the SIM.

2.2 Mobile Station

A GSM terminal is, even for experts, a technical marvel. Consider the rate at which prices have fallen, the complexity of the devices, and the large number of different types of equipment available. All the functionality known from the BTS transmitter/receiver (TRX), like Gaussian minimum shift keying (GMSK) modulation/demodulation up to channel coding/decoding, also needs to be implemented in an MS.

Other MS-specific functionalities need to be mentioned, like dual-tone multifrequency (DTMF) generation and the most important issue, the economical use of battery power.

From the perspective of the protocol, the MS is not only a peer of the BTS but communicates directly with the MSC and the VLR, via the mobility management (MM) and call control (CC). Furthermore, the MS has to be able to provide a transparent interface (terminal adaptation function, or TAF) for data and fax connections to external devices.

2.2.1 Types of Mobile Stations

The most common way to distinguish among GSM mobile equipment is by the power class ratings, in which the value specifies the maximum transmission power of an MS.

When GSM was introduced, five power classes were defined for GSM 900, of which the most powerful class allowed for a 20W output. That class is no longer supported; currently, the most powerful rating is 8W. The power emission of DCS 1800 and PCS 1900 mobiles is generally lower. The Glossary lists the power classes for all three standards.

2.2.2 Functionality

GSM Recommendation 02.07 describes in detail what functionality mobile equipment has to support and what features are optional. The most important and mandatory features are:

- DTMF capability;
- Short-message service (SMS) capability;
- Availability of the ciphering algorithms A5/1 and A5/2;
- Display capability for short messages, dialed numbers, and available PLMN;
- Support of emergency calls, even without the SIM inserted;
- "Burned-in" IMEI.

2.2.3 Mobile Stations as Test Equipment

An MS is a useful test tool for the laboratory testing of a new network function. Several manufacturers offer, for that purpose, a semistationary MS, which allows manipulation of specific system parameters, to test the behavior of new software or hardware.

Besides those complex and expensive pieces of equipment used mainly in laboratories, a number of standard mobile telephones exist, which can easily be modified with additional packages to act as mobile test equipment. Such equipment is connected to a personal computer and uses standard functionality to monitor signaling between the network and the MS. Usually, it is also able to represent the test results in tabular or graphical form.

Despite those advantages, the test mobile stations seldom are used for protocol and error analysis, because the results are not representative from a statistical point of view and can be gathered only with substantial effort and time.

Nonetheless, special test mobiles are necessary tools for network operators, to monitor coverage and evaluate the behavior of handover as a customer would experience it.

3

The Base Station Subsystem

Via the Air-interface, the BSS provides a connection between the MSs of a limited area and the network switching subsystem (NSS). The BSS consists of the following elements:

- One or more BTSs (base tranceiver station);
- One BSC (base station controller);
- One TRAU (transcoding rate and adaptation unit).

The tasks and the structure of those elements or modules are described in this chapter.

3.1 Base Transceiver Station

The BTS provides the physical connection of an MS to the network in form of the Air-interface. On the other side, toward the NSS, the BTS is connected to the BSC via the Abis-interface.

The manufacturers of BTS equipment have been able to reduce its size substantially. The typical size in 1991 was that of an armoire; today the size is comparable to that of a mailbox. The basic structure of the BTS, however, has not changed. The block diagram and the signal flow of a BTS with one TRX are shown in Figure 3.1. The GSM Recommendations allow for one BTS to host up to 16 TRXs. In the field, the majority of the BTSs host between one and four TRXs.

Samsung Ex. 1032, Page 29 of 417

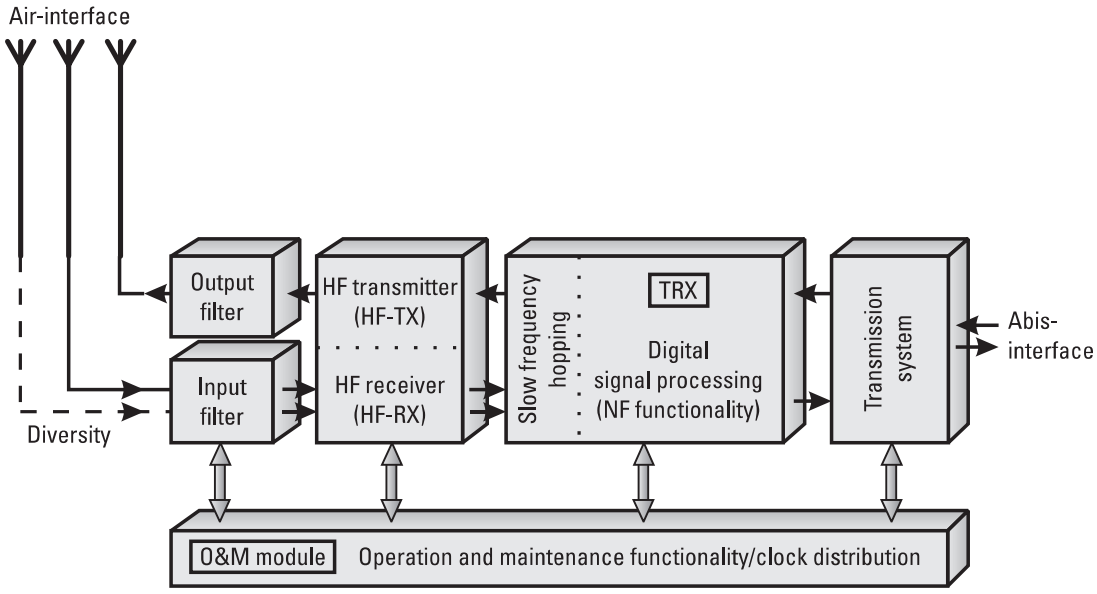


Figure 3.1 Block diagram of a BTS with one TRX.

3.1.1 Architecture and Functionality of a Base Transceiver Station

3.1.1.1 Transmitter/Receiver Module

The TRX module is, from the perspective of signal processing, the most important part of a BTS. The TRX consists of a low-frequency part for digital signal processing and a high-frequency part for GMSK modulation and demodulation. Both parts are connected via a separate or an integrated frequency hopping unit. All other parts of the BTS are more or less associated with the TRXs and perform auxiliary or administrative tasks.

A TRX with integrated frequency hopping serves the tasks listed in Table 3.1.

3.1.1.2 Operations and Maintenance Module

The operations and maintenance (O&M) module consists of at least one central unit, which administers all other parts of the BTS. For those purposes, it is connected directly to the BSC by means of a specifically assigned O&M channel. That allows the O&M module to process the commands from the BSC or the MSC directly into the BTS and to report the results. Typically, the central unit also contains the system and operations software of the TRXs. That allows it to be reloaded when necessary, without the need to "consult" the BSC. Furthermore, the O&M module provides a human-machine interface (HMI), which allows for local control of the BTS.

Table 3.1
Tasks of a TRX With Integrated Frequency Hopping

Function	LF	HF
Channel coding and decoding	●	
Interleaving and ordering again	●	
Encryption and decryption (ciphering)	●	
Slow frequency hopping	●	
Burst formatting	●	
TRAU frame formatting and conversion in direction to/from the BSC, setup of the LAPD connection to the BSC	●	
GMSK modulation of all downlink data	●	●
GMSK demodulation of all received MS signals	●	●
Creation and transmission of the broadcast common control channel (BCCH) on channel 0 of the BCCH-TRX	●	●
Measurement of signal strength and quality for active connections	●	●
Provision of the results to the BSC (MEAS_RES message)		
Interference measurements (idle channel measurements) on free channels and forwarding of the results to the BSC in a RF_RES_IND message	●	●

LF = low frequency part of the TRX; HF = high frequency part of the TRX.

3.1.1.3 Clock Module

The modules for clock generation and distribution also are part of the O&M area. Although the trend is to derive the reference clock from the PCM signal on the Abis-interface, a BTS internal clock generation is mandatory. It is especially needed when a BTS has to be tested in a standalone environment, that is, without a connection to a BSC or when the PCM clock is not available due to link failure.

Still, there is a cost savings benefit in the approach of deriving the clock from the PCM signal. By doing so, much cheaper internal clock generators can be applied, because they do not require the same long-term stability as an independent clock generator. Besides, there is no need for frequent maintenance checks on the clock modules, since they synchronize themselves with the clock coming from the PCM link.

When analyzing errors in call handling, particularly in the area of handover, even minor deviations from the clock have to be considered as possible

causes for errors. GSM requires that all the TRXs of a BTS use the same clock signal. The accuracy of the signal has to have a precision of at least 0.05 parts per million (ppm). For example, a clock generator that derives the clock from a 10 MHz signal has to be able to provide a clock with a frequency accuracy of 10 MHz ±0.5 Hz ($10 \cdot 10^6$ Hz $\cdot$ 0.05 $\cdot$ $10^{-6} = 0.5$ Hz).

3.1.1.4 Input and Output Filters

Both input and output filters are used to limit the bandwidth of the received and the transmitted signals. The input filter typically is a nonadjustable wideband filter that lets pass all GSM 900, all DCS 1800, or all PCS 1900 frequencies in the uplink direction. In contrast, remote-controllable filters or wideband filters are used for the downlink direction that limits the bandwidth of the output signal to 200 kHz. When necessary, the O&M center (OMC) controls the settings of the filters, as in the case of a change in frequency.

3.1.2 Base Transceiver Station Configurations

Different BTS configurations, depending on load, subscriber behavior, and morph structure, have to be considered to provide optimum radio coverage of an area. The most important BTS configurations of a BTS are presented next.

3.1.2.1 Standard Configuration

All BTSs are assigned different cell identities (CIs). A number of BTSs (in some cases, a single BTS) form a location area. Figure 3.2 shows three location areas with one, three, and five BTSs. The systems are usually not fine-synchronized (see *synchronized handover* in the Glossary), which prevents synchronized handover between them. That method of implementing BTSs is the one most frequently used. For urban areas with growing traffic density, that may change soon. For this situation, the configurations described in Sections 3.1.2.2 and 3.1.2.3 are more appropriate.

3.1.2.2 Umbrella Cell Configuration

The umbrella cell configuration consists of one BTS with high transmission power and an antenna installed high above the ground that serves as an "umbrella" for a number of BTSs with low transmission power and small diameters (Figure 3.3).

Such a configuration appears to make no sense at first, because the frequency of the umbrella cell can not be reused in all the cells of that area due to interference. Interference even over a large distance was one of the reasons why the high radio and television towers were abandoned as sites for antennas shortly after they were brought into service at the initial network startup.

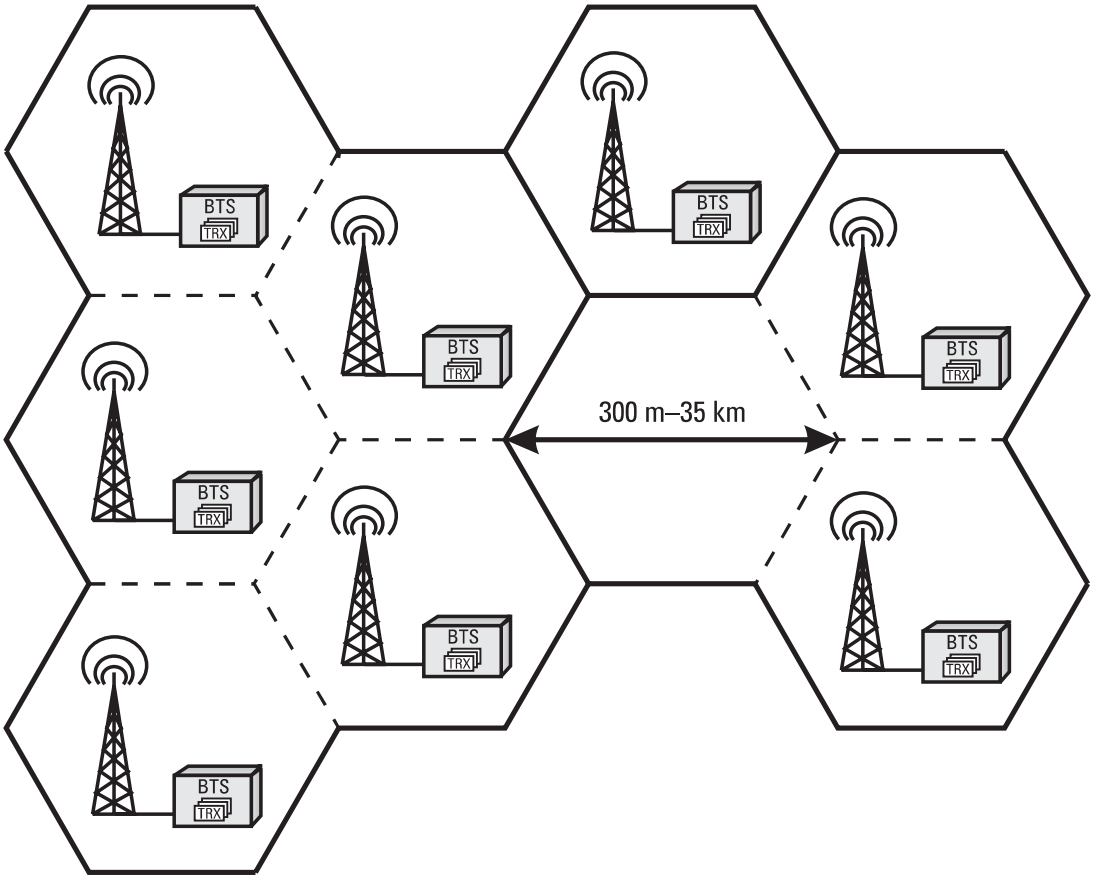


Figure 3.2 BTSs in standard configuration.

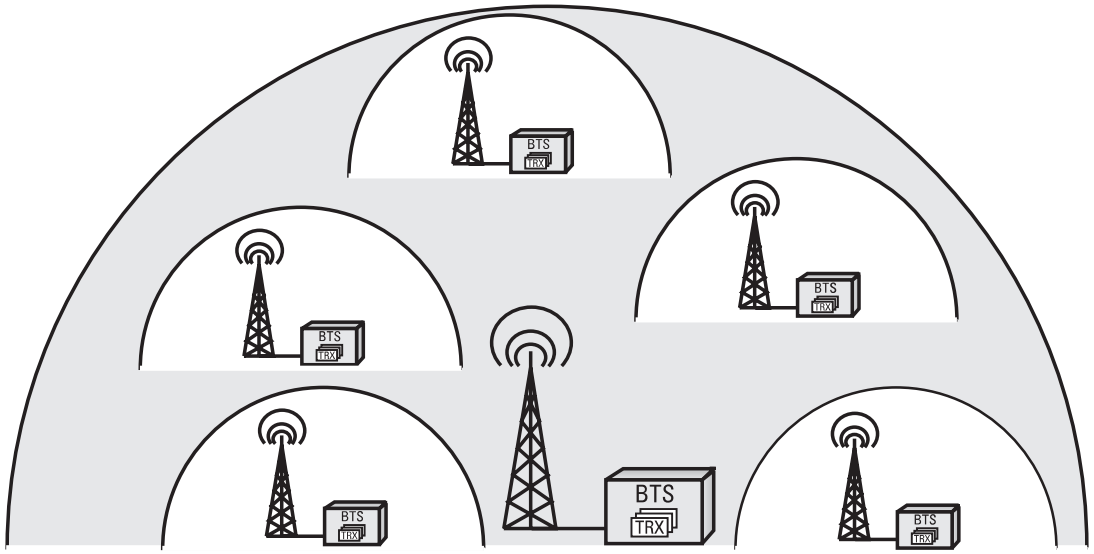


Figure 3.3 Umbrella cell with five smaller cells.

The umbrella cell configuration still has its merits in certain situations and therefore may result in relief from load and an improvement of the network. For example, when cars are moving at rather high speeds through a network of small cells, almost consecutive handovers from one cell to the next are necessary to maintain an active call. This situation is applicable in every urban environment that features city highways. Consequently, the handovers result in a substantial increase of the signaling load for the network as well as in an unbearable signal quality degradation for the end user. On the other hand, small cells are required to cope with the coverage demand in an urban environment.

The way out of this dilemma is to use both large and small cells at the same time, that is, the umbrella cell configuration. The umbrella cell can be protected from overload when traffic from only fast-moving users is assigned to it. This, on the other hand, reduces the signaling load of the small cells and improves the signal quality for the fast-moving traffic. The speed of a user can be determined to sufficient accuracy by the change of the timing advance (TA) parameter. Its value is updated in the BSC every 480 milliseconds (ms) by means of the data provided in the MEAS_RES message. The BSC decides whether to use the umbrella cell or one of the small cells. GSM has not specified the umbrella cell configuration, which requires additional functionality in the BSC, a manufacturer's proprietary function.

3.1.2.3 Sectorized (Collocated) Base Transceiver Stations

The term sectorized, or collocated, BTSs refers to a configuration in which several BTSs are collocated at one site but their antennas cover only an area of 120 or 180 degrees. Figure 3.4 illustrates the concept. Typically, it is implemented with BTSs with few TRXs and low transmission power. Like the umbrella cell configuration, this configuration is used mostly in highly populated areas. A peculiarity is that it is fairly easy to fine-synchronize the cells with each other, which allows for synchronized handover between them. Even though in a collocated configuration, one channel per BTS has to be used for the generation of the BCCH, such a configuration has the following advantages:

- Sectorized, or collocated, BTSs are well suited for a serial connection of the Abis-interface (discussed in detail in Chapter 6). This configuration has the potential to save costs for access lines to the BSC. Otherwise, multiple sites require multiple (leased) lines.
- From the radio perspective, the advantage of using cells with a 120-degree angle is that it allows reuse of frequencies in one sector

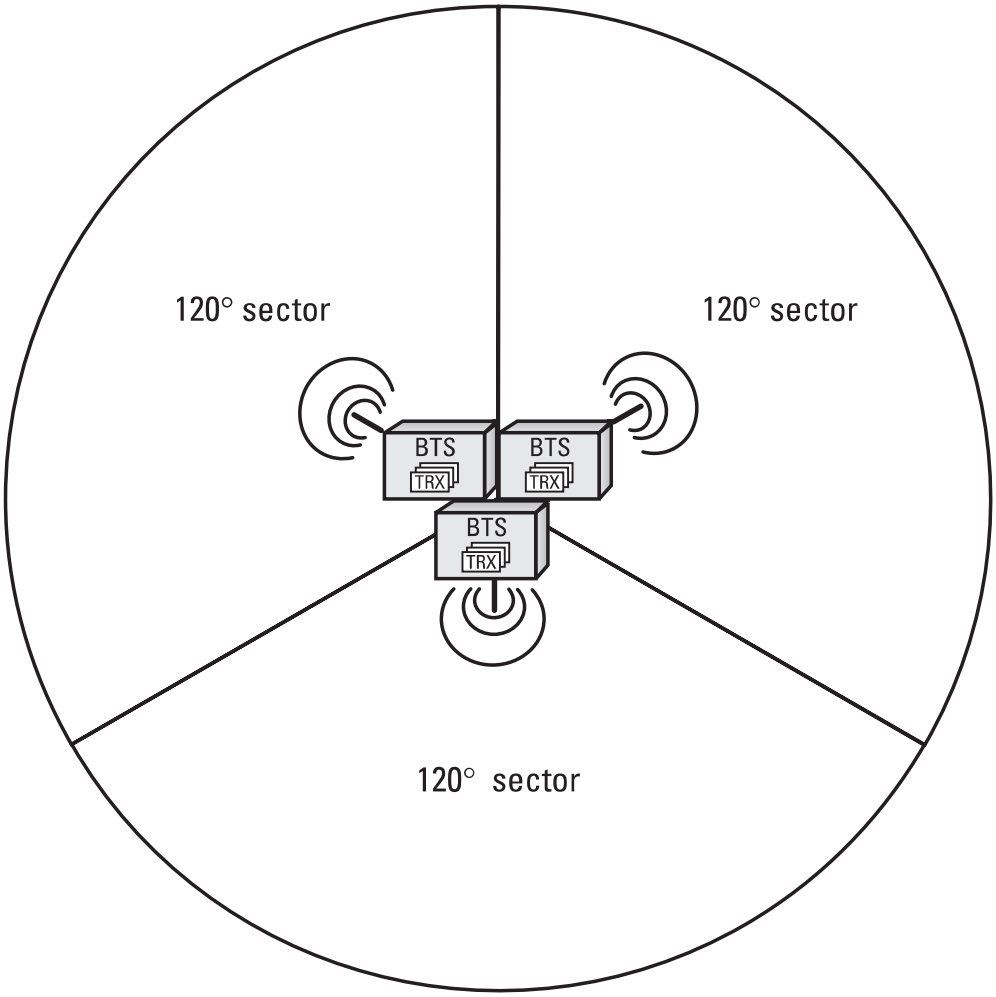


Figure 3.4 Coverage of an area with three sectorized BTSs. Each BTS covers a segment of 120 degrees.

(one direction), which otherwise would cause interference with neighbor cells if an omnidirectional cell were used.

- Sectorization eases the demand for frequencies, particularly in an urban environment.

3.2 Base Station Controller

The BSC forms the center of the BSS. A BSC can, depending on the manufacturer, connect to many BTSs over the Abis-interface. The BSC is, from a technical perspective, a small digital exchange with some mobile-specific extensions. The BSC was defined with the intention of removing most of the radio-related load from the MSC. The BSC's architecture and its tasks are a

consequence of that goal. For simplicity, Figure 3.5 uses the same hardware for both the Abis-interface and the A-interface, which is not a requirement.

3.2.1 Architecture and Tasks of the Base Station Controller

3.2.1.1 Switch Matrix

Because the BSC has the functionality of a small digital exchange, its function is to switch the incoming traffic channels (A-interface from the MSC) to the correct Abis-interface channels. The BSC, therefore, comes with a switch matrix that (1) takes care of the relay functionality and (2) can be used as the internal control bus.

3.2.1.2 Terminal Control Elements of the Abis-Interface

The connection to the BTSs is established via the Abis-terminal control elements (TCEs), which, more or less independently from the BSC's central unit, provide the control function for a TRX or a BTS. The number of Abis TCEs that a BSC may contain depends largely on the number of BTSs and on the system manufacturer.

Major tasks of the Abis-TCEs are to set up LAPD connections toward the BTS peers, the transfer of signaling data, and last—but not least—the transparent transfer of payload.

Depending on the manufacturer, the Abis TCEs also may be responsible for the administration of BTS radio resources. That entails the assignment and

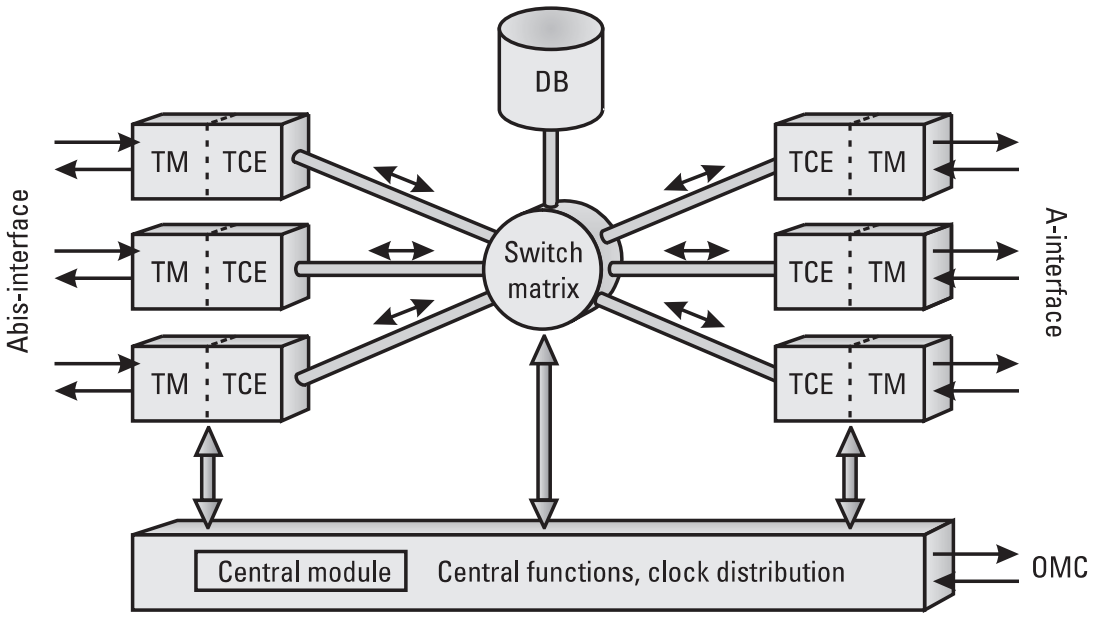


Figure 3.5 Block diagram of a BSC.

release of signaling and traffic channels over the Abis-interface and the Air-interface and for the evaluation of measurement results from the BTS concerning busy and idle channels, which are relevant for power control and used in making decisions about handovers. The final control functionality always remains with the BSC, although GSM explicitly allows the BTS to preprocess the measurement results. Depending on the manufacturer, those functions also can be assumed or controlled by a central unit.

Connections from the Abis TCEs to the A-TCEs are realized by the switch matrix. On the other side, the PCM connections are achieved by associated transmission elements.

3.2.1.3 A-Interface Terminal Control Elements

The connection of a BSC to the MSC is established via the A-TCEs. Although every BSC is connected to only one MSC, a large number of A-TCEs is needed to support the A-interface, since all the payload and the major part of the signaling data of the entire BSS have to be conveyed over this interface.

Among the tasks of some, but usually not all A-TCEs is setting up and operating the SS7/SCCP connection toward the MSC. The number of necessary signaling channels depends largely on the predicted traffic load (see also Chapter 10).

3.2.1.4 Database

The BSC is the control center of the BSS. In that capacity, the BSC must maintain a relatively large database in which the maintenance status of the whole BSS, the quality of the radio resources and terrestrial resources, and so on are dynamically administrated. Furthermore, the BSC database contains the complete BTS operations software for all attached BTSs and all BSS specific information, such as assigned frequencies.

3.2.1.5 Central Module

One of the major tasks of the BSC is to decide when a handover should take place. The BSC may decide on intra-BTS handover and intra-BSC handover without needing the MSC. In contrast, for all BSC external handovers, the BSC needs to involve the MSC. Handover decision and power control are main tasks of the central module.

3.2.1.6 Connection to the OMC

Another functionality that many manufacturers have decided the central module should perform is the connection to the OMC. Every BSS is supervised and managed by an OMC via the BSC.

3.3 Transcoding Rate and Adaptation Unit

3.3.1 Function of the Transcoding Rate and Adaptation Unit

One of the most interesting functions in GSM involves the TRAU, which typically is located between the BSC and the MSC. The task of the TRAU is to compress or decompress speech between the MS and the TRAU. The used method is called regular pulse excitation–long term prediction (RPE-LTP). It is able to compress speech from 64 Kbps to 16 Kbps, in the case of a fullrate channel (net bit rate with fullrate is 13 Kbps) and to 8 Kbps in the case of a halfrate channel (net bit rate with halfrate is 6.5 Kbps).

Note that the TRAU is not used for data connections.

3.3.2 Site Selection for Transcoding Rate and Adaptation Unit

Although speech compression is intended mainly to save resources over the Air-interface, it also is suitable to save line costs when applied on terrestrial links, as illustrated schematically in Figure 3.6. When the TRAU is installed at the MSC site (see top portion of Figure 3.6), a fullrate speech channel uses only 16 Kbps over the link from the BSC to the MSC.

The specifications allow for the installation of the TRAU between the BTS and the BSC. That requires, however, the use of 64-Kbps channels between the BSC and the MSC and hence the use of more links (see bottom portion of Figure 3.6).

This variant is, therefore, used only infrequently. In fact, most of the time, the TRAU is installed at the site of the MSC to get the most benefit from the compression.

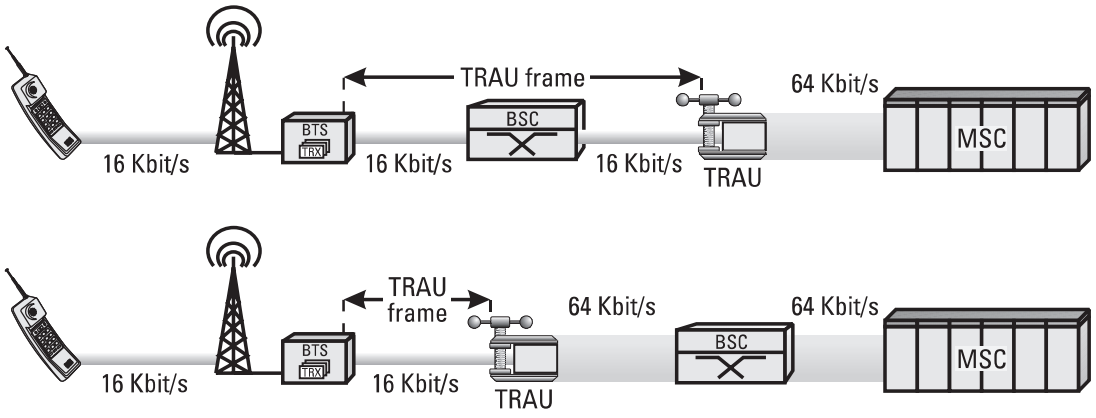


Figure 3.6 Possible sites for the TRAU in the signal chain.

3.3.3 Relationship Between the Transcoding Rate and Adaptation Unit, and Base Station Subsystem

The TRAU is functionally assigned to the BSS, independently of where it actually is located. The reason for that is the following.

Both the BTS and the TRAU have an interface for payload that is transparent for the BSC. The payload is formatted in TRAU frames, then transparently sent over PCM links between the TRAU and the BTS in cycles of 20 ms. That applies to both directions. The data contained in the TRAU frames form the input and output values for channel coding.

For data connections, the compression functionality has to be switched off. The type of connection (data/speech) is communicated to the TRAU during the assignment of the traffic channel. As illustrated in Figure 3.7, the BTS starts to transmit TRAU frames in the uplink, immediately after receiving the CHAN_ACT message. Those TRAU frames carry inband signaling, which is exchanged between the BTS-TRX (or more precisely the coding unit) and the TRAU, to consolidate the characteristics of a connection. Part of the control information is, in particular, synchronization data, discontinuous transmission (DTX) on/off, and the connection type (halfrate/fullrate).

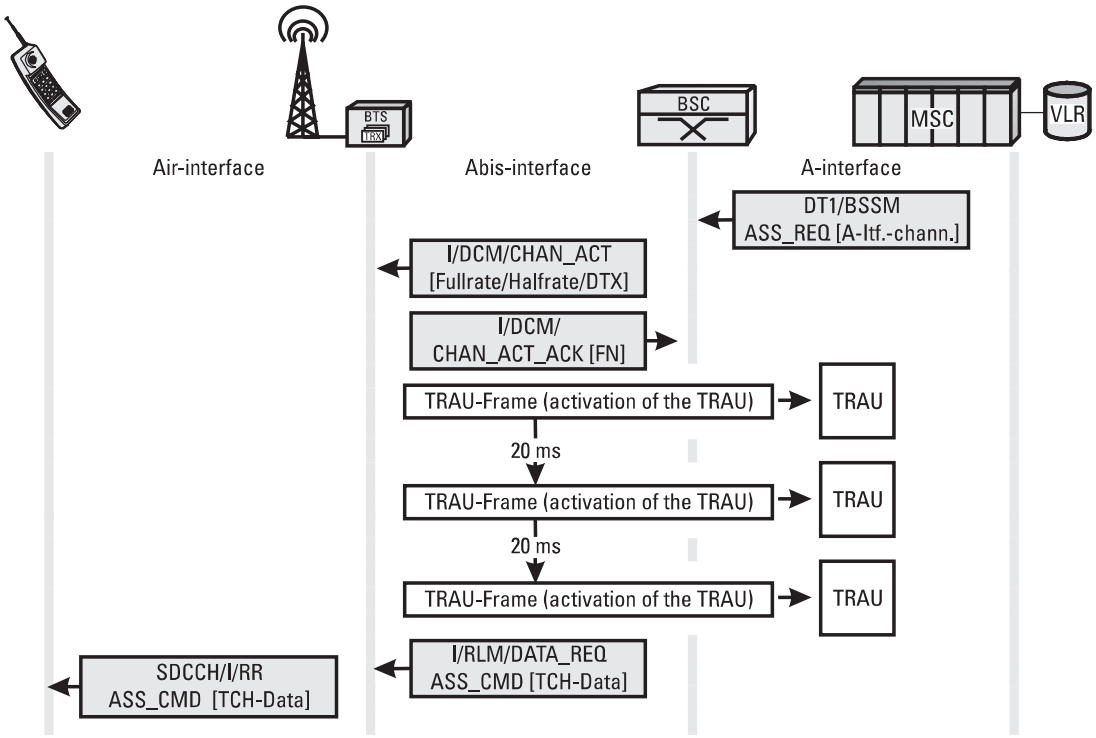


Figure 3.7 Activation of the TRAU during assignment of a traffic channel.

Note that TRAU frames are sent over traffic channels and not over the associated control channels and hence are transparent to protocol analysis. The TRAU frames are, nevertheless, very important for error analysis on data connections.

4

The Network Switching Subsystem

The NSS plays the central part in every mobile network. While the BSS provides the radio access for the MS, the various network elements within the NSS assume responsibility for the complete set of control and database functions required to set up call connections using one or more of these features: encryption, authentication, and roaming. To satisfy those tasks, the NSS consists of the following:

- MSC (mobile switching center);
- HLR (home location register)/authentication center (AuC);
- VLR (visitor location register);
- EIR (equipment identity register).

The subsystems are interconnected directly or indirectly via the worldwide SS7 network. The network topology of the NSS is more flexible than the hierarchical structure of the BSS. Several MSCs may, for example, use one common VLR; the use of an EIR is optional, and the required number of subscribers determines the required number of HLRs.

Figure 4.1 provides an overview of the interfaces between the different network elements in the NSS. Note that most interfaces are virtual, that is, they are defined as reference points for signaling between the network elements.

Samsung Ex. 1032, Page 41 of 417

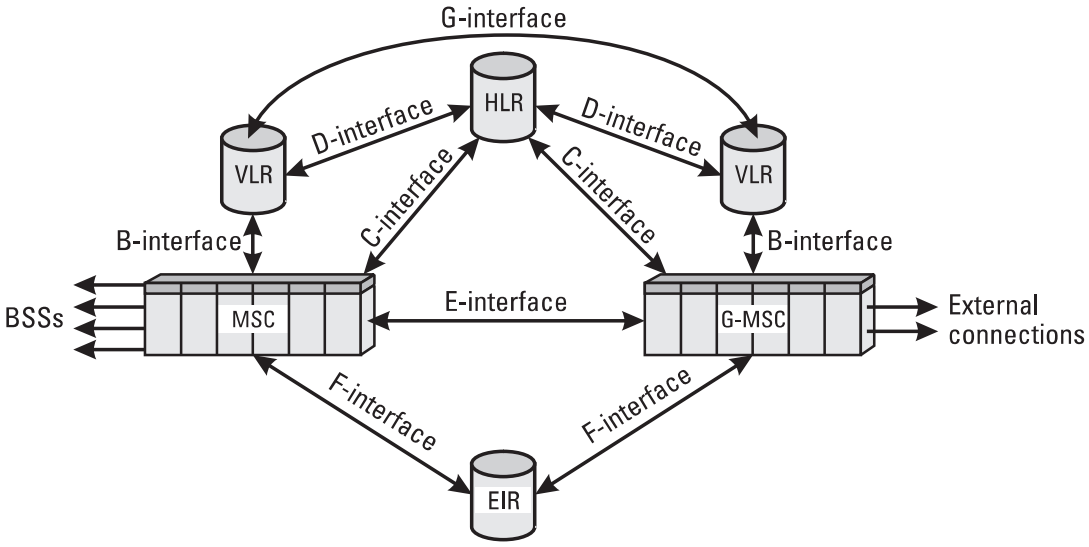


Figure 4.1 The NSS.

4.1 Home Location Register and Authentication Center

Every PLMN requires access to at least one HLR as a permanent store of data. The concept is illustrated in Figure 4.2. The HLR can best be regarded as a large database with access times that must be kept as short as possible. The faster the response from the database, the faster the call can be connected. Such a database is capable of managing data for literally hundreds of thousands subscribers.

Within the HLR, subscriber-specific parameters are maintained, such as the parameter K_i, which is part of security handling. It is never transmitted on any interface and is known only to the HLR and the SIM, as shown in Figure 4.2.

Each subscriber is assigned to one specific HLR, which acts as a fixed reference point and where information on the current location of the user is stored. To reduce the load on the HLR, the VLR was introduced to support the HLR by handling many of the subscriber-related queries (e.g., localization and approval of features).

Because of the central function of the HLR and the sensitivity of the stored data, it is essential that every effort is taken to prevent outages of the HLR or the loss of subscriber data.

The AuC is always implemented as an integral part of the HLR. The reason for this is that although GSM mentions the interface between the AuC and the HLR and has even assigned it a name, the H-interface, it was never specified in sufficient detail to be a standalone entity. The only major function assigned to the AuC is to calculate and provide the authentication-triplets, that

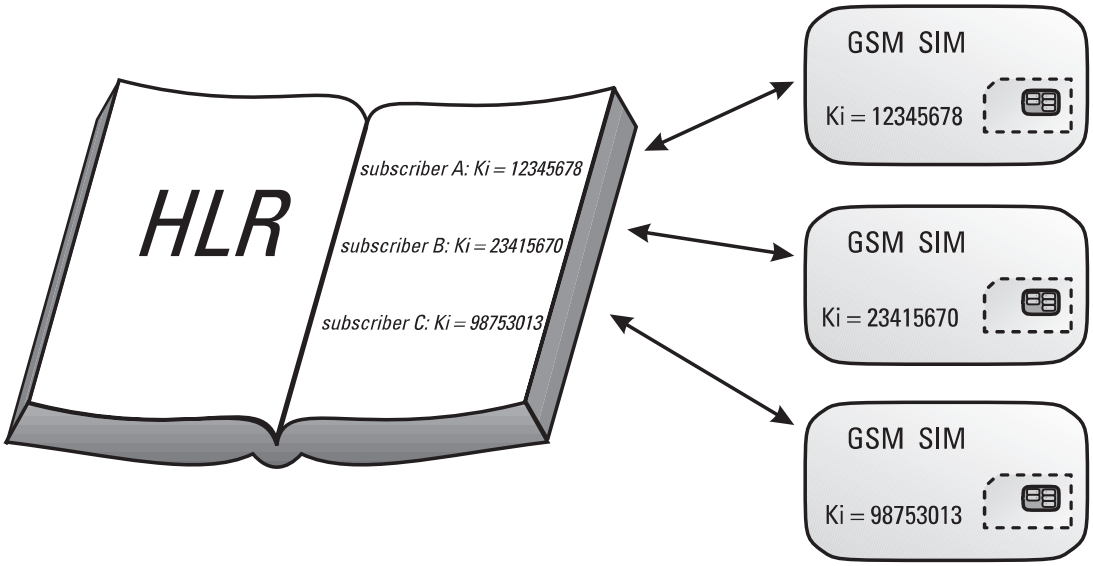


Figure 4.2 Only the SIM and the HLR know the value of K_i.

is, the signed response (SRES), the random number (RAND), and K_c. For each subscriber, up to five such triplets can be calculated at a time and sent to the HLR. The HLR, in turn, forwards the triplets to the VLR, which uses them as input parameters for authentication and ciphering.

The Glossary provides a detailed description of the authentication procedure.

4.2 Visitor Location Register

The VLR, like the HLR, is a database, but its function differs from that of the HLR While the HLR is responsible for more static functions, the VLR provides dynamic subscriber data management. Consider the example of a roaming subscriber. As the subscriber moves from one location to another, data are passed between the VLR of the location the subscriber is leaving ("old" VLR) to the VLR of the location being entered ("new" VLR). In this scenario, the old VLR hands over the related data to the new VLR. There are times when the new VLR has to request the subscriber's HLR for additional data.

This question then arises: Does the HLR in GSM assume responsibility for the management of those subscribers currently in its geographic area? The answer is no. Even if the subscriber happens to be in the home area, the VLR of that area handles the dynamic data. This illustrates another difference between the HLR and the VLR. The VLR is assigned a limited geographical area, while the HLR deals with tasks that are independent of a subscriber's location. The

term *HLR area* has no significance in GSM, unless it refers to the whole PLMN. Typically, but not necessarily, a VLR is linked with a single MSC. The GSM standard allows, as Figure 4.3 illustrates, the association of one VLR with several MSCs.

The initial intentions were to specify the MSC and the VLR as independent network elements. However, when the first GSM systems were put into service in 1991, numerous deficiencies in the protocol between the MSC and the VLR forced the manufacturers to implement proprietary solutions. That is the reason the interface between the MSC and the VLR, the B-interface, is not mentioned in the specifications of GSM Phase 2. GSM Recommendation 09.02 now provides only some basic guidelines on how to use that interface.

Table 4.1 lists the most important data contained in the HLR and the VLR.

4.3 The Mobile-Services Switching Center

From a technical perspective, the MSC is just an ordinary Integrated Services Digital Network (ISDN) exchange with some modifications specifically required to handle the mobile application. That allows suppliers of GSM systems to offer their switches, familiar in many public telephone networks, as MSCs. SIEMENS with its EWSD technology and ALCATEL with the S12 and the E10 are well-known examples that benefit from such synergy.

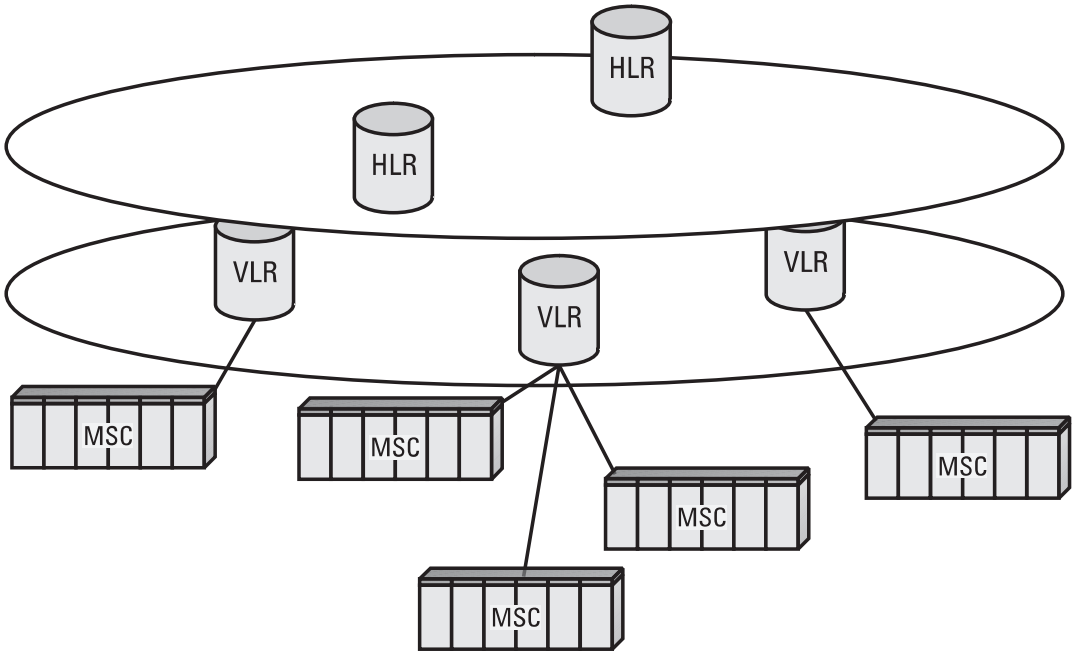


Figure 4.3 The NSS hierarchy.

Table 4.1
The Most Important Data in the HLR and the VLR

Parameter	HLR/AuC	VLR
Subscriber specific:		
IMSI	●	●
K_i	●	
TMSI		●
Service restrictions	●	
Supplementary services	●	●
MSISDN (basic)	●	●
MSISDN (other)	●	
Authentication and ciphering:		
A3	●	
A5/X (in BSS)		
A8	●	
RAND up to five triplets	●	●
SRES up to five triplets	●	●
K_c up to five triplets	●	●
CKSN		●
Subscriber location/call forwarding:		
HLR number		●
VLR number	●	
MSC number	●	●
LAI		●
IMSI detach		●
MSRN		●
LMSI	●	●
Handover number		●

The modifications of exchanges required for the provision of mobile service affect, in particular, the assignment of user channels toward the BSS, for which the MSC is responsible, and the functionality to perform and control

inter-MSC handover. That defines two of the main tasks of the MSC. We have to add the interworking function (IWF), which is needed for speech and non-speech connections to external networks. The IWF is responsible for protocol conversion between CC and the ISDN user part (ISUP), as well as for rate adaptation for data services.

4.3.1 Gateway MSC

An MSC with an interface to other networks is called a gateway MSC. Figure 4.4 shows a PLMN with gateway MSCs interfacing other networks. Network operators may opt to equip all of their MSCs with gateway functionality or only a few. Any MSC that does not possess gateway functionality has to route calls to external networks via a gateway MSC.

The gateway MSC has some additional tasks during the establishment of a mobile terminating call from an external network. The call has to enter the PLMN via a gateway MSC, which queries the HLR and then forwards the call to the MSC where the called party is currently located.

4.3.2 The Relationship Between MSC and VLR

The sum of the MSC areas determines the geographic area of a PLMN. Looking at it another way, the PLMN can be considered as the total area covered by the BSSs connected to the MSCs. Since each MSC has its "own" VLR, a

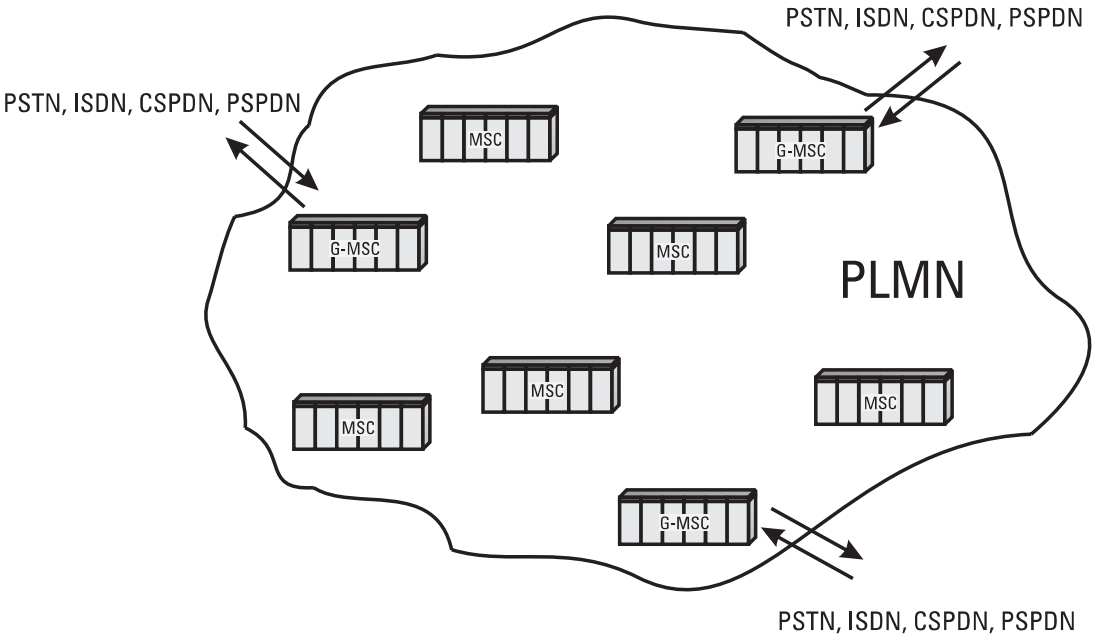


Figure 4.4 The functionality of the gateway MSC.

PLMN also could be described as the sum of all VLR areas. Note that a VLR may serve several MSCs, but one MSC always uses only one VLR. Figure 4.5 illustrates this situation.

That relationship, particularly the geographic interdependency, allows for the integration of the VLR into the MSC. All manufacturers of GSM systems selected that option, since the specification of the B-interface was not entirely available on time. In GSM Phase 2, the B-interface is no longer an open interface (as outlined above). It is expected that this trend will continue.

A network operator still has the freedom to operate additional MSCs with a remote VLR, but that is somewhat restrictive in that all the MSCs must be supplied by the same manufacturer.

4.4 Equipment Identity Register

The separation of the subscriber identity from the identifier of the MS (described in Chapter 2) also bears a potential pitfall for GSM subscribers. Because it is possible to operate any GSM MS with any valid GSM SIM, an opportunity exists for a black market in stolen equipment. To combat that, the EIR was introduced to identify, track, and bar such equipment from being used in the network.

Each GSM phone has a unique identifier, its IMEI, which cannot be altered without destroying the phone. The IMEI contains a serial number and a

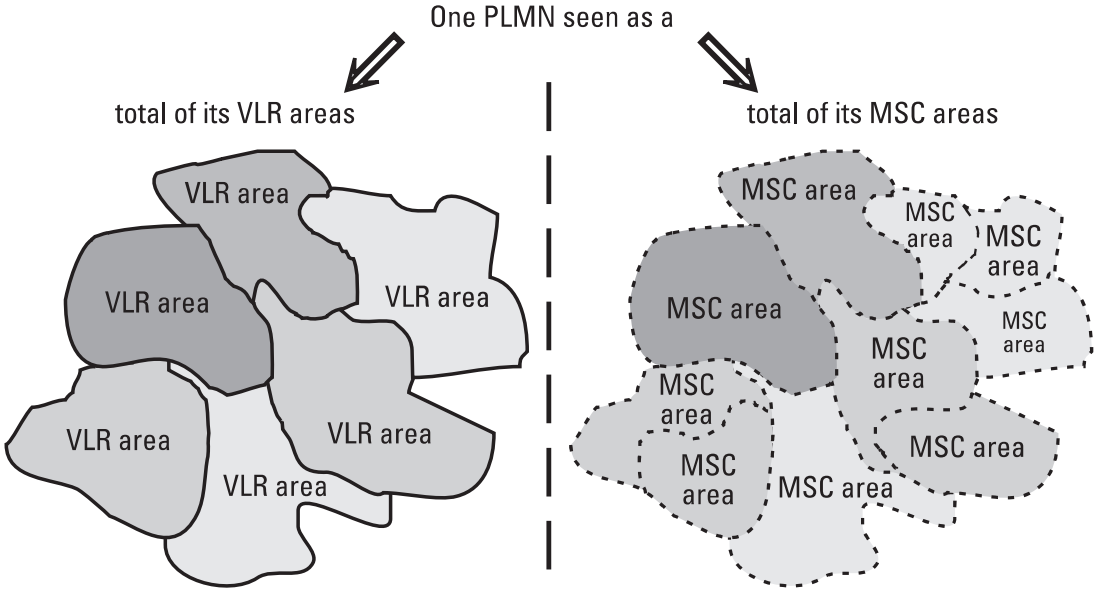


Figure 4.5 Geographic relationship between the MSC and the VLR.

type identifier. More detailed description of the structure of the IMEI is given in the Glossary.

Like the HLR or the VLR, the EIR basically consists of a database, which maintains three lists: (1) the "white list" contains all the approved types of mobile stations; (2) the "black list" contains those IMEIs known to be stolen or to be barred for technical reasons; and (3) the "gray list" allows tracing of the related mobile stations.

The prices for mobile equipment have fallen dramatically due to the great success of GSM; consequently, the theft rate is low. Several GSM operators have decided not to install the EIR or, at least, to postpone such installation for a while.

If the EIR is installed, there is no specification on when the EIR should be interrogated. The EIR may be queried at any time during call setup or location update. Chapter 12 describes this in detail.

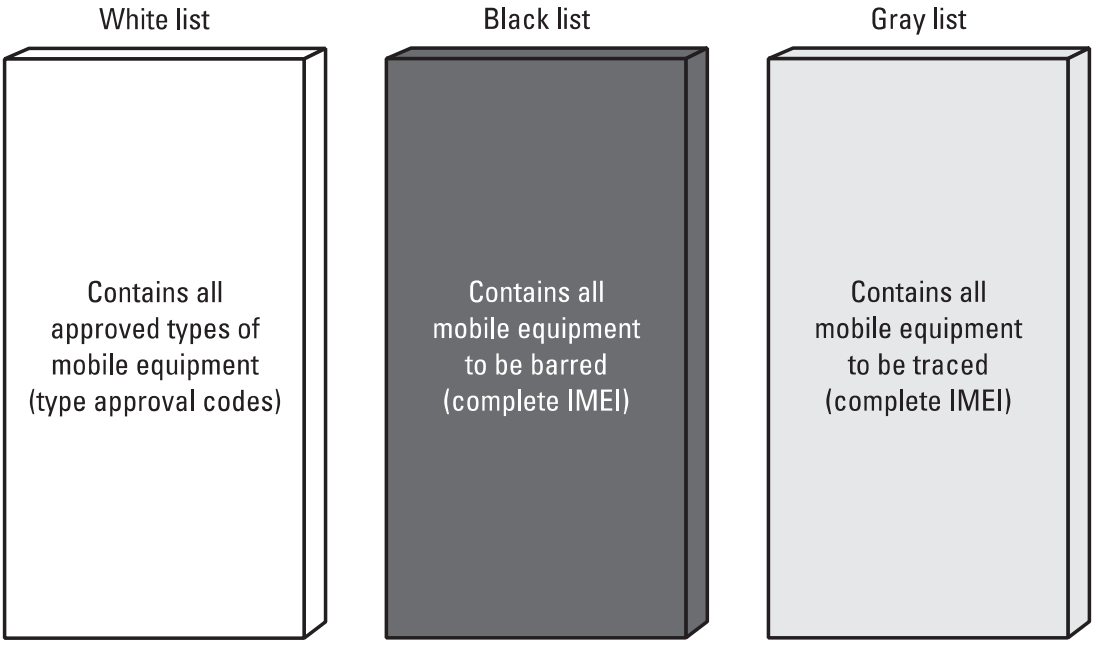


Figure 4.6 Contents of the EIR.

5

The OSI Reference Model

5.1 Reasons for Standardization

The Open System Interconnection (OSI) Reference Model was specified by ITU, in cooperation with ISO and IEC, and is documented in Recommendation X.200. Although the OSI model is applicable in many areas, it is used mostly in the area of communication between computers. Its purpose is to organize and formalize the communication method.

The basic idea of the OSI Reference Model is to separate the various parts that, in their totality, form a communications process. Separation of concerns is achieved by layering and modularization of transactions and tasks. This approach results from the following reasoning:

- The use of microprocessors in telecommunications not only allowed for the creation of new services, but at the same time increased the requirements on communications of exchanges and computers.
- When humans communicate by means of telephone or letters, they do not want to be concerned with the details of the physical transfer of the information. They just want to communicate. The same applies to the layers of the OSI Reference Model, in which each layer has a fixed role in the process of communications.
- A computer is a modular structure, which starts with the transistor on the lowest level and, with modularity built on top of modularity, ends up as a super-computer. To use such a system becomes easier when the tasks themselves can be modularized.

Samsung Ex. 1032, Page 49 of 417

- Telephone systems are used for many applications. These applications became possible only because the application itself had become more independent of the process of pure data transmission. Modems and fax machines, for instance, rely on the functionality of the services of a lower layer and adapt their own functionality accordingly. The telephone network, on the other hand, is not concerned with the content or the representation of the transmitted data.
- The OSI Reference Model enables two products from different manufacturers to communicate. Many interworking problems cannot be solved simply by the interface specification shown in Figure 5.1. Each telephone set and every exchange can be regarded as network element A, B, or C. If, for example, the manufacturer of one network element implements all the functionality of a particular application and the second manufacturer implements only those functions that are necessary for a particular task, then, generally speaking, the two devices cannot be interconnected.

5.2 Layering in the OSI Reference Model

The OSI Reference Model breaks down or separates the communication process into seven independent layers. The following are the general "rules" of the OSI model:

- Two layers that lie above each other work independently. Each layer receives a service from the layer immediately below and provides a service to the layer immediately above. The lower layer does not care

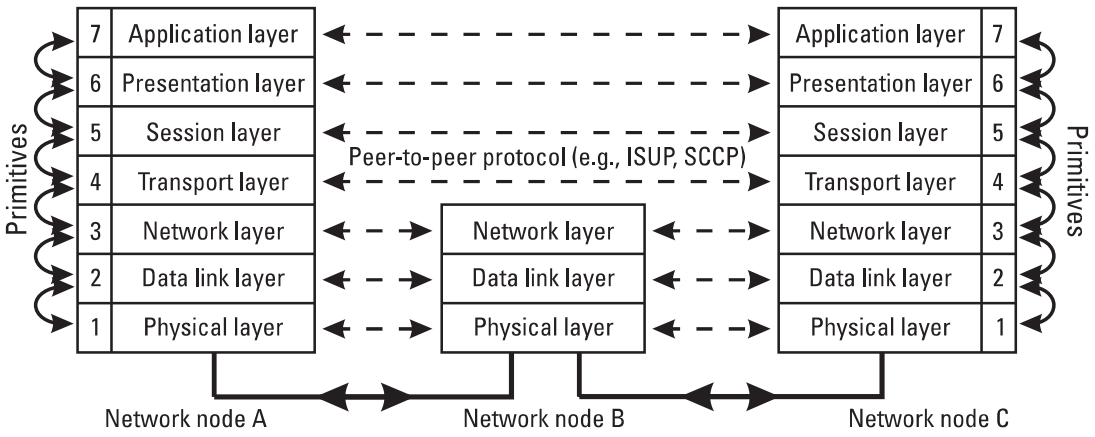


Figure 5.1 The layers and message types of the OSI Reference Model.

about the content of the received information. Consider the analogy of sending mail. The post office is not concerned about the content of a letter, which it has received to deliver. Its only concern is the address on the envelope, which it follows in order to make the delivery. This constitutes a service, which is independent of the contents of the letter.

- Each layer communicates directly only with the layers immediately below and above itself and indirectly with its peer layer at the remote end. Let us again refer to the post office analogy. Neither the sender nor the addressee is concerned about the details of the service, that is, about how the letter is routed, and neither the sender nor the addressee needs to communicate with the letter carrier. They only need to have access to a mailbox. The two parties communicate with each other by writing or reading the letter.
- If a communications process involves more than two network nodes, the intermediate network node or nodes need only provide the functionality of Layers 1 through 3. As Figure 5.1 shows, network node B is equipped only with Layers 1, 2, and 3. Layers 4 through 7 are required at the end points of a connection only. Going back to the letter delivery example, in this "communications process" all post offices and postal workers are involved only in transport and error-free delivery of the letter. All other parts of the communication process are available only at the sender and receiver sides.
- The protocols used for Layers 1 through 3 on the interface between A and B are not necessarily the same as those used on the interface between B and C. For example, Layer 2, between the BTS and the BSC in GSM, uses the LAPD protocol, while the SS7 protocol is used between the BSC and the MSC. In that case, network node B would represent the BSC.

5.3 Data Types of the OSI Reference Model

All messages exchanged between Layer N and Layer $(N-1)$ are called primitives. In practical work, except for measurements within a network element, there usually is no need to become involved in the inner workings of the primitives, it suffices to know that they exist and to have an idea of their function.

All message exchange on the same level (or layer) between two network elements, A and B, is determined by what is known as peer-to-peer protocol. Consequently, all messages that can be seen on any GSM interface between two nodes belong to the group of peer-to-peer protocols.

5.4 Information Processing in the OSI Reference Model

The tasks of the Layers 7 down to 2 mainly are to add processing information. When, for example, Layer 6 receives a primitive from Layer 7, it adds header information, which allows the "partner" layer on the other end to process the received data according to the appropriate peer-to-peer protocol. The partner layer is responsible for removing the header information. Figure 5.2 illustrates the relationship. The obvious result is the increase in the data that needs to be transmitted.

5.5 Advantages of the OSI Reference Model

The major advantage of the OSI Reference Model lies in the fact that the various layers are independent of each other. What does independence in this context mean? It means that Layer *N* shares a common protocol with its peer Layer *N* and with the layers immediately above and below it but not with any other layers. The OSI Reference Model defines only the interface between them and not the way a certain layer is implemented. Therefore, it is, for example, irrelevant to a large degree how the physical signal transmission is achieved. The transmission medium used for the data transfer may be cable, direct radio, satellite, or any other appropriate means.

That permits the design and use of modules on a general level, a statement that has to be tempered by the actual application. It certainly matters,

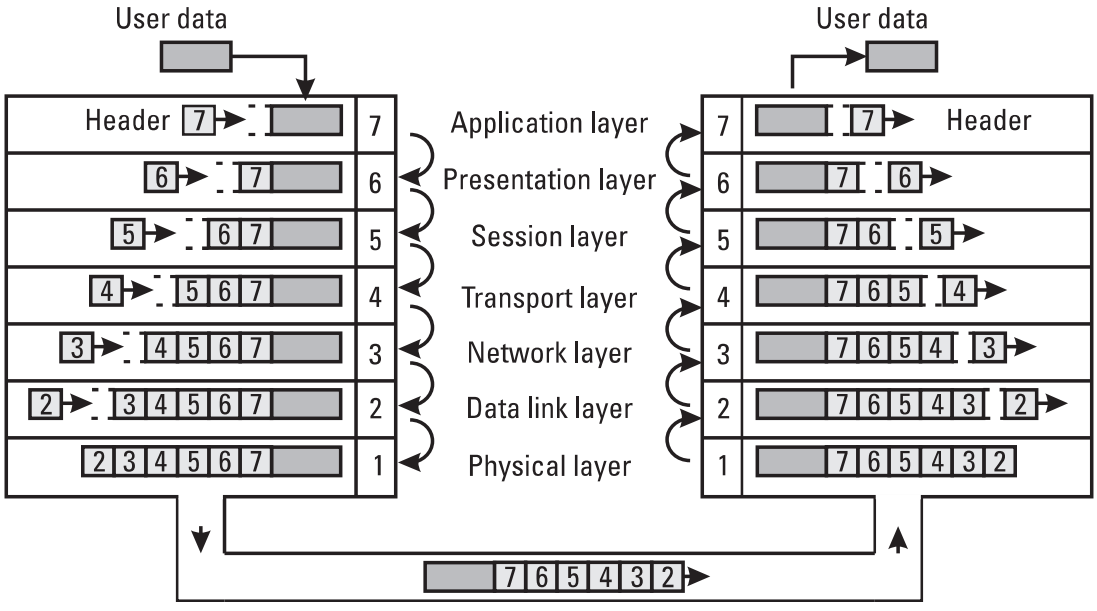


Figure 5.2 Data flow in the OSI Reference Model.

with respect to the propagation delay, whether transmission is via cable or satellite, where the propagation delays may be substantial.

5.6 The Seven Layers of the OSI Reference Model

5.6.1 Layer 1: The Physical Layer

The Physical Layer is responsible for the actual transmission of the data and the provision of the necessary facilities. The facilities can be, for example, a copper wire, a satellite connection, direct radio, or an optical fiber. The Physical Layer may include some synchronization features that do not have any significance for the higher layers, since those features are purely hardware related. Examples of such features are the clear-to-send (CTS) signal and the ready-to-send (RTS) signal of the serial interface on a computer (COM-Port).

Layer 1 does not know data types or data formats and is not able to distinguish between control data and user data. That characteristic, in particular, distinguishes Layer 1 from the other layers. The data packets received from Layer 2 are transmitted without additional verification. Each data packet consists of either a single bit or a number of bits.

With regard to the Air-interface of a GSM system, the GMSK modulation and the HF equipment in the MS and the BTS are part of Layer 1. Over the terrestrial interfaces, the PCM, including signal levels and propagation delays, is part of Layer 1.

Naturally, the implementation of the Physical Layer depends greatly on the type of interface and might change frequently. For example, between the BTS and the BSC, Layer 1 might be implemented as microwave transmission on the first section, as optical fiber on a second section, and as plain cable on a third section.

5.6.2 Layer 2: The Data Link Layer

The Data Link Layer is responsible for the packaging of the data to be transmitted. The data are combined into packets or frames and then handed to the Physical Layer for synchronous or asynchronous transmission. A widespread method for such framing is the high-level data link control (HDLC) protocol, which provides a general structure for data frames and forms, which is the basis for the SS7 protocol as well as for the LAPD protocol. The Glossary provides a description of the HDLC frame format.

The main purpose of all the tasks of Layer 2 is that of error detection and correction. Data frames are formed by introducing start/stop marks and by

calculation of checksums (frame check sequence, or FCS), which can be checked for consistency by Layer 2 at the receiving side. When the receiver detects an error, it tries to correct the error or requests retransmission.

The Data Link Layer plays a vital part in protocol testing, because all data packets from Layer 3 have to be carried in a Layer 2 frame. Note that Layer 2 information is relevant only between two adjacent network nodes and that the Layer 2 protocol might change from interface to interface. For example, the Layer 2 protocol in GSM changes as the data pass on their way from the MS first at the BTS where $LAPD_m$ converts to LAPD and then again in the BSC where LAPD converts to MTP 2/SS7.

On the GSM Air-interface, Layer 2 is formed by the $LAPD_m$, together with channel coding and burst formatting. On the Abis-interface, it is LAPD, and the remaining interfaces use the MTP 2 of the SS7 protocol. Note that in $LAPD_m$, no frame check sequence is required because channel coding takes care of error detection and correction.

5.6.3 Layer 3: The Network Layer

The Network Layer prescribes the path a message has to take and who the recipient of that message is. All the information necessary to route a data packet is the responsibility of Layer 3. Layer 3 has significance only on a per-section base, as already known from Layers 1 and 2. Every network node has to analyze and possibly modify the Layer 3 information. The RR protocol between the MS, the BTS, the BSC, and the MSC belongs to Layer 3, as well as all the address information needed to route a call in an SS7 system.

The best analogy for Layer 3 information is the address information on the envelope of a letter, which has to be evaluated by every network node (post office) in its delivery path.

The equal treatment of MM, CC, and RR on the Air-interface by GSM is misleading, since MM and CC information does not belong to Layer 3. Rather, RR provides the necessary transport capability to transparently carry MM and CC information between the MS and the NSS.

5.6.4 Layer 4: The Transport Layer

Layer 4 provides the methods that guarantee the proper end-to-end ordering of message packets, before the data are handed to the higher layers (sequencing). Such handling becomes necessary when a message is partitioned into data packets. The term segmentation is used to describe the process of breaking down the information into packets. Furthermore, in contrast to the lower layers, the Transport Layer performs end-to-end data control. The Transport Layer

checks the consistency of a message, when a message is composed of several pieces. The task of the Transport Layer in the OSI Reference Model is similar to that of the Data Link Layer and the Network Layer. At the time when OSI was defined, it was essential to rely on a powerful Layer 4, since Layers 2 and 3 could not handle this task alone.

The difference between Layers 2 and 3 on one side and Layer 4 on the other lies in the end-to-end application of Layer 4. While Layers 2 and 3 are relevant only on a per-interface basis, Layer 4 procedures are applied between the two end points of a connection.

A good example of a Layer 4 task is the numbering of boxes during a house move or counting them at the destination, as well as arranging them in the right order, that is, setting up the cupboard before unpacking the dishes. It is obvious that this task is not directly related to the transport or any security issue; nevertheless, the task is important for a smooth sequence of events.

5.6.5 Layer 5: The Session Layer

The Session Layer was assigned for global synchronization purposes. Both parties use the Layer 5 to coordinate the communication process between themselves. It is used in GSM between the MSC and the MS to distinguish between a mobile terminating call (MTC), a location update (LU), and a mobile originating call (MOC). Part of the synchronization is the ability to determine which information needs to be sent, when, and by whom. Another example for Layer 5 is the dialog part of the component sublayer of the transaction capabilities application part (TCAP). Two TCAP users can coordinate the type of a process, by means of the dialog part of a message and so, for example, distinguish between an LU and the activation of a supplementary service.

To come back to the example used for Layer 4: The decision about the order of packages with dishes or cupboard parts has to be made by Layer 5. Layer 4 only carries out the request.

5.6.6 Layer 6: The Presentation Layer

Generally speaking, the Presentation Layer is a means of data definition and preparation before the data are passed to the Application Layer. The Presentation Layer is able to distinguish different data types and to perform data compression and decompression. A typical example for a Layer 6 implementation is ASN.1, the Abstract Syntax Notation number 1, as defined by ITU in Recommendations X.208 and X.209.

Referring again to the analogy of the relocation, different types of boxes are necessary depending on the “data type” (i.e., cups, plates, clothing,

furniture), and they need different treatment during transmission and on the receiving side (wash the dishes, set up the cupboard, etc.).

5.6.7 Layer 7: The Application Layer

The Application Layer is the interface of a specific application to the transmission medium or, in other words, to the Layers 1 through 6. Note that Layer 7 does not actually contain the application but provides an interface between the application and the communication process. Just as much as the implementation of Layer 1 depends on the physical transmission medium, so also the implementation of Layer 7 depends on the specific user.

An example best illustrates this concept, since the preceding definition is somewhat theoretical.

The president of a company does not organize a dinner party himself. That task is delegated to a third party, typically a secretary, who makes all the arrangements, including the tracking of confirmations and cancellations. The president who is not concerned with the preparation of the dinner is, in this example, the application. The third party, perhaps the president's secretary, on the other hand, does not need to be present at the dinner and does not need to know the reasons for any of the dinner speeches or to understand the reasons for inviting a certain person. The secretary has some freedom and acts independently within that area of freedom to ensure that the dinner party is well prepared and presented.

Another, more technical example is the Layer 6 of the TCAP that was specified by ITU as a general interface for all kinds of users. It is the responsibility of the users to provide Layer 6 a suitable interface, that is, a buffer. That interface or buffer is realized by Layer 7 in the according applications.

5.7 Comprehension Issues

Because of the somewhat fuzzy borders between the various layers, it is sometimes difficult to apply the OSI Reference Model to an actual problem. That is particularly true for someone who is new to the subject, and misunderstandings frequently occur.

The reason for such problems lies in the theoretical approach of the definition of the model or in the overlapping tasks of the layers. GSM adds even more complexity by switching between layers for the data transfer on the different interfaces (A, Abis, Air).

For example, when the BTS receives a Layer 2 SABM frame from the MS, it forwards that information as an EST_IND message toward the BSC,

wrapped into an I-frame. The EST_IND message, clearly Layer 3 information, can be regarded as a translation of the SABM frame (Figure 5.3). This "leap" can be explained by the fact that Layers 1 through 3 are valid only on a link-by-link basis.

The remainder of this book frequently refers to the OSI Reference Model. For that reason, it is important to understand the model, its function, and the difference between the layers. The following analogy is presented to try to help give a better understanding of the "theory."

5.7.1 An Analogy: The Move to Europe

Since we all have different experiences in life and see things from different perspectives, the relationship to the OSI model is immediately emphasized during the course of this analogy, "The move to Europe."

5.7.1.1 The Moving Family as the User or Application

A family that has to move wants to have to do as little work as possible, particularly tasks like disassembly, packing, unpacking, reassembly, setting up furniture, washing dishes, cleaning rooms, and so on.

The moving family is comparable to the user or the application in the OSI model, which is outside the model. The user communicates with the moving company and defines the schedule as to when to make the move, where to move, and when the move should be finished.

5.7.1.2 The Moving Company as OSI Layers 7, 6, and 5

Let us assume, for the purpose of this analogy, that the moving company has local branches all over the world that are governed by the same business rules. The moving company has many employees: some work in the office to

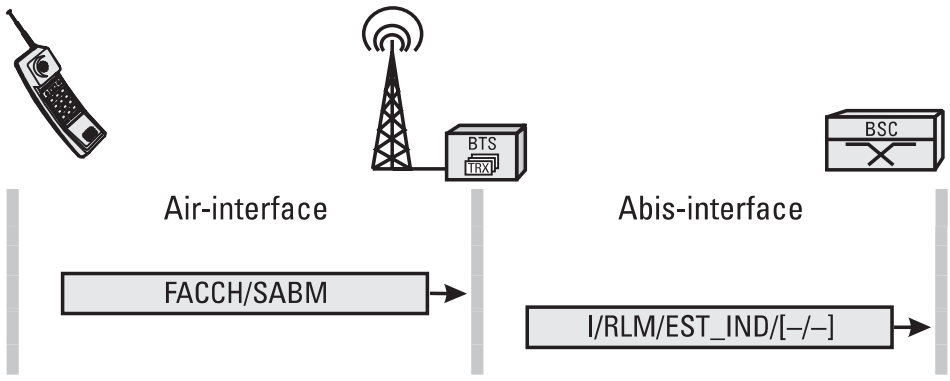


Figure 5.3 "Leap" in the layers between the air interface and the Abis interface.

coordinate the whole process, while others work onsite to do all the packing and unpacking.

The moving company has a selection of different packaging materials specifically designed for the purpose of moving household items (see *ASN.1* in the Glossary). The moving company can be likened to Layers 5, 6, and 7 of the OSI model. The employees in the office, who control the whole process, can be likened to Layer 7. The onsite employees whose function it is to separate the various household items, such as the clothes, dishes, furniture, and so on, and to pack them appropriately can be likened to part of Layer 6.

This task is similar to the processing of parameters and data in the Presentation Layer (Layer 6). The onsite employees label the boxes, according to their contents (e.g., books, clothes, dishes), which makes it easier for their counterparts in Europe to do the opposite task of unpacking. The packing and labeling procedure in Layer 5 ensures that the moving company at the destination side sets up the bookcases before unpacking the books or sets up the bureaus before unpacking the clothes. Otherwise, the books and the dishes would be unpacked before there are places to put them.

The different boxes for the various goods and the labels on the boxes are, technically speaking, peer-to-peer protocols in OSI Layers 5 and 6, which add some overhead to the process of moving household goods.

Neither the employees in the office nor those onsite deal with the actual transportation process. For that, the moving company uses the services of a transportation company.

5.7.1.3 The Transportation Company as OSI Layer 4

The transportation company is responsible for the end-to-end transportation, which is comparable to a Layer 4 task. The people who work for the transportation company count and number the boxes (error detection and segmentation) and write the destination address, based on the information they have received from the moving company (Layer 7) on the boxes. The numbering of the boxes is as requested by the moving company, that is, the employees onsite (Layer 5), who inform the transportation company as to what order (or sequence) the individual boxes have to be shipped to the destination.

Note that the numbering of the boxes creates a new peer-to-peer protocol. The transportation company does not know what the labels "bookcase," "dishes," and so on, mean in particular because they have no knowledge of the specific requirements. It is for that reason that Layer 4 translates the Layer 5 specific information into its own protocol, in this case, the numbering scheme.

When everything is done, the transportation company hands over all the boxes to the selected shipping company (Layer 3), which selects the method of physical transportation according to price and availability.

5.7.1.4 The Shipping Company as OSI Layer 3

The shipping company or its employees are equivalent to Layer 3. They are not concerned about the contents of the shipment, the numbers on the boxes, or the labels that characterize the contents. They take the boxes, process the address (routing information), and arrange for the packaging of the boxes into containers for transportation.

The long distance between the origination in America and the final destination in Europe is taken in a number of smaller steps (truck, railroad, plane, ship) and requires the reloading of the boxes into different containers. That also requires that, for each leg of the journey, addresses for the temporary, intermediate destinations have to be assigned

5.7.1.5 Truck, Railroad, Boat, and Airplane as OSI Layer 2

The various containers that have to be used, the types of which are determined mainly by the means of transport, correspond to Layer 2.

Starting at the home, a truck is used to transport the boxes to the railway station. A railroad wagon is used to transport them to the airport, harbor, and so on. The larger units correspond to the various Layer 2 protocols that are used over the link between any two nodes of a telecommunications network.

In the telecommunications environment (cargo shipping), it is Layer 2 (the means of transport) that serves the purpose of providing a secure physical transport medium for the actual data (household goods).

The checksum in a telecommunications environment corresponds to the truck driver's checklist. This illustrates the difference between what Layer 4 does for data security compared with Layer 2. While Layer 4 numbers and accounts for the boxes of one user (moving family), Layer 2 performs that task for one container that, in general, is shared by many users. That is, Layer 2 sees the process from the viewpoint of the shipping company, and Layer 4 sees it from the perspective of the user.

5.7.1.6 The Infrastructure as Layer 1

What remains is indicating the constituent parts of Layer 1. These are the roads, railroad tracks, engines, and people— everything and everyone that contributes to the physical transportation process. Just as in a move to Europe, the Physical Layer in telecommunications changes between intermediate nodes.

6

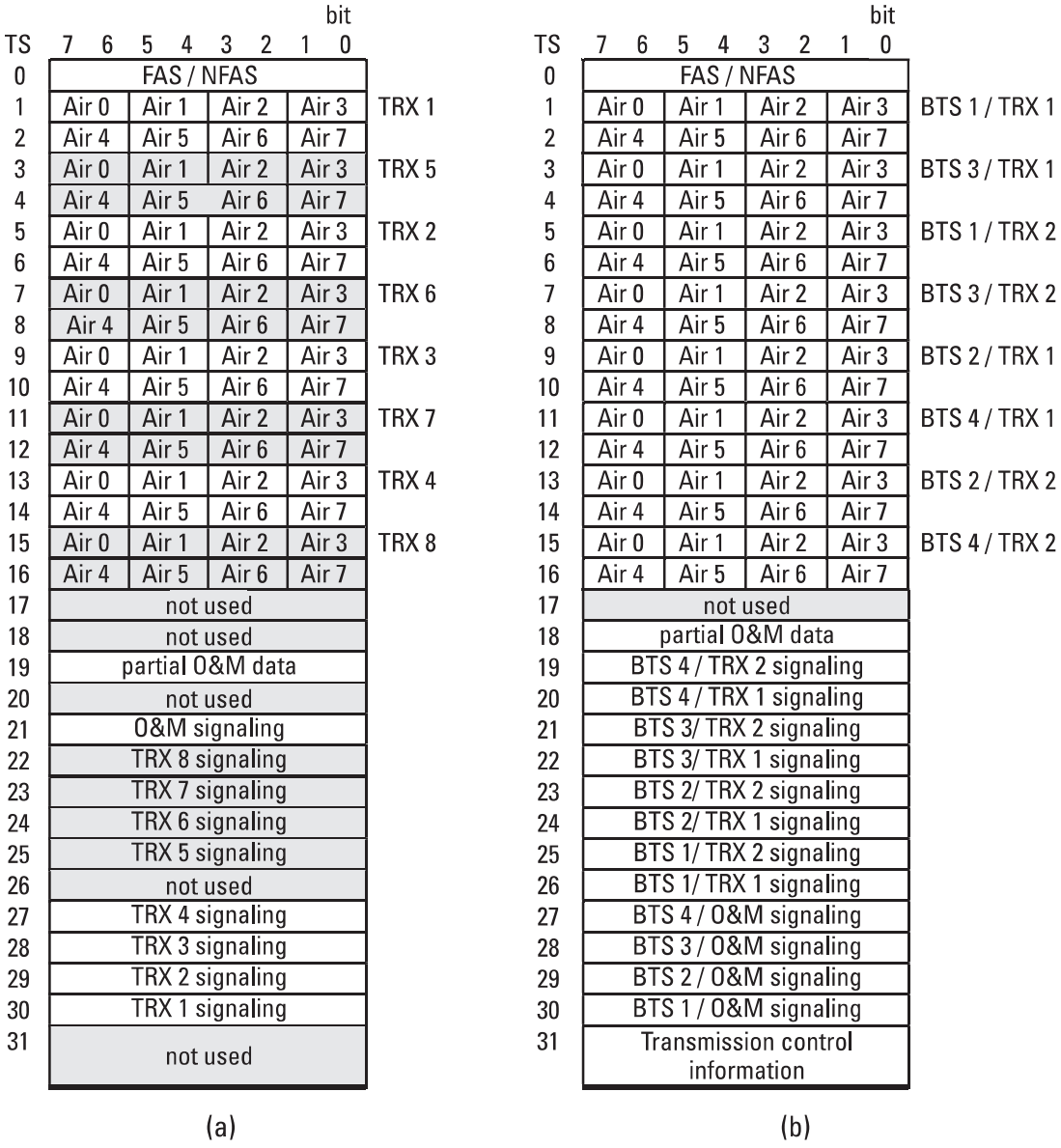
The Abis-Interface

The Abis-interface is the interface between the BTS and the BSC. It is a PCM 30 interface, like all the other terrestrial interfaces in GSM. It is specified by ITU in the G-series of recommendations. The transmission rate is 2.048 Mbps, which is partitioned into 32 channels of 64 Kbps each. The compression techniques that GSM utilizes packs up to 8 GSM traffic channels into a single 64-Kbps channel. GSM never specified the Abis-interface in every detail, as was also the case with the B-interface (the interface between the MSC and the VLR). The Abis-interface is regarded as proprietary, which leads to variations in the Layer 2 protocol between manufacturers, as well as to different channel configurations. The consequence is that, normally, a BTS from manufacturer A cannot be used with a BSC from manufacturer B.

6.1 Channel Configurations

Figure 6.1 presents two possible channel configurations of the Abis-interface. Note the fixed mapping of the air-interface traffic channels (Air0, Air1, …) onto a time slot of the Abis-interface. This fixed mapping has the advantage that it is possible to determine which Abis time slot will be used when a particular air-interface channel is assigned.

Samsung Ex. 1032, Page 60 of 417



TS	bit 7	6	5	4	3	2	1	0	
0	FAS / NFAS								
1	Air 0		Air 1		Air 2		Air 3		TRX 1
2	Air 4		Air 5		Air 6		Air 7		
3	Air 0		Air 1		Air 2		Air 3		TRX 5
4	Air 4		Air 5		Air 6		Air 7		
5	Air 0		Air 1		Air 2		Air 3		TRX 2
6	Air 4		Air 5		Air 6		Air 7		
7	Air 0		Air 1		Air 2		Air 3		TRX 6
8	Air 4		Air 5		Air 6		Air 7		
9	Air 0		Air 1		Air 2		Air 3		TRX 3
10	Air 4		Air 5		Air 6		Air 7		
11	Air 0		Air 1		Air 2		Air 3		TRX 7
12	Air 4		Air 5		Air 6		Air 7		
13	Air 0		Air 1		Air 2		Air 3		TRX 4
14	Air 4		Air 5		Air 6		Air 7		
15	Air 0		Air 1		Air 2		Air 3		TRX 8
16	Air 4		Air 5		Air 6		Air 7		
17	not used								
18	not used								
19	partial O&M data								
20	not used								
21	O&M signaling								
22	TRX 8 signaling								
23	TRX 7 signaling								
24	TRX 6 signaling								
25	TRX 5 signaling								
26	not used								
27	TRX 4 signaling								
28	TRX 3 signaling								
29	TRX 2 signaling								
30	TRX 1 signaling								
31	not used								

(a)

TS	bit 7	6	5	4	3	2	1	0	
0	FAS / NFAS								
1	Air 0		Air 1		Air 2		Air 3		BTS 1 / TRX 1
2	Air 4		Air 5		Air 6		Air 7		
3	Air 0		Air 1		Air 2		Air 3		BTS 3 / TRX 1
4	Air 4		Air 5		Air 6		Air 7		
5	Air 0		Air 1		Air 2		Air 3		BTS 1 / TRX 2
6	Air 4		Air 5		Air 6		Air 7		
7	Air 0		Air 1		Air 2		Air 3		BTS 3 / TRX 2
8	Air 4		Air 5		Air 6		Air 7		
9	Air 0		Air 1		Air 2		Air 3		BTS 2 / TRX 1
10	Air 4		Air 5		Air 6		Air 7		
11	Air 0		Air 1		Air 2		Air 3		BTS 4 / TRX 1
12	Air 4		Air 5		Air 6		Air 7		
13	Air 0		Air 1		Air 2		Air 3		BTS 2 / TRX 2
14	Air 4		Air 5		Air 6		Air 7		
15	Air 0		Air 1		Air 2		Air 3		BTS 4 / TRX 2
16	Air 4		Air 5		Air 6		Air 7		
17	not used								
18	partial O&M data								
19	BTS 4 / TRX 2 signaling								
20	BTS 4 / TRX 1 signaling								
21	BTS 3/ TRX 2 signaling								
22	BTS 3/ TRX 1 signaling								
23	BTS 2/ TRX 2 signaling								
24	BTS 2/ TRX 1 signaling								
25	BTS 1/ TRX 2 signaling								
26	BTS 1/ TRX 1 signaling								
27	BTS 4 / O&M signaling								
28	BTS 3 / O&M signaling								
29	BTS 2 / O&M signaling								
30	BTS 1 / O&M signaling								
31	Transmission control information								

(b)

Figure 6.1 (a) Star configuration (fullrate) and (b) serial connection (four BTSs with two TRX each).

6.2 Alternatives for Connecting the BTS to the BSC

The line resources on the Abis-interface usually are not used efficiently. The reason is that a BTS, typically, has only a few TRXs, which implies small traffic volume capability. Consequently, the line between the BTS and the BSC is used only to a fraction of its capacity. Figure 6.1(a), the star configuration, shows the case of a BTS with four TRXs, in which only 47% of the 2 Mbps

actually is needed. The shaded areas mark the unused channels. When the BTS has only one TRX, that value goes down to 16%. Such waste of resources has a historical background, and it would not change much if halfrate channels were used.

When GSM specified the BTS, it defined that a BTS may have up to 16 TRXs. Two 2-Mbps interfaces are required to connect such a BTS to the BSC, because a single 2-Mbps interface is able to support only up to 10 TRXs, including O&M signaling.

Proportionally fewer resources are required on the Abis-interface when a BTS with a smaller number of TRXs is installed. The remainder cannot easily be used.

Experience has shown that the optimum for a BTS is in the range of one to four TRXs. This compromise reflects several parameters:

- Capacity. How many traffic and signaling channels does a BTS need to provide, on average and during busy hours, to avoid an overload condition?
- Available frequency range. What is the minimum distance between BTSs beyond which a given TRX frequency may be reused?

Network operators worldwide have had bad experiences, particularly with the latter point.

When digital radio was introduced, the assumption was that the impact of the disturbances, same-channel interference or neighbor channel interference, would be relatively minor. Soon after the introduction of commercial service, that assumption was found to be wrong, when more and more interference problems between BTSs appeared and degraded the quality of service. Problems with large, powerful cells were experienced, particularly in urban areas and city centers, where more and more minicells and microcells are being used.

The conclusion was to move in the direction of using more cells with fewer TRXs and smaller output power (<1W) rather than in the direction of fewer cells with more TRXs and high output power. That configuration requires a larger number of BTSs than the alternative to cover any given area. Connecting the larger number of BTSs to the BSCs, in turn, requires a larger number of links (Abis-interfaces).

Because of that trend, together with the high costs for links between the BTS and the BSC and the low efficiency when using such links, another configuration was introduced, the serial connection of BTSs.

6.2.1 BTS Connection in a Serial Configuration

In a serial configuration, the BTSs are connected in a line or a ring topology. Only one BTS, for the line topology, or two BTSs, for the ring topology, are physically connected to the BSC. Figures 6.2 and 6.3 illustrate those topologies. For the network operator, the advantage of the serial approach over the star configuration is that it saves line costs. Furthermore, the serial connection allows for more efficient use of resources, as illustrated in Figure 6.1(b). This advantage becomes particularly obvious, when colocated or sectored BTSs are used (see Section 3.1.2.3). The disadvantage, however, is that a single link failure causes the loss of the connection to a large number of BTSs

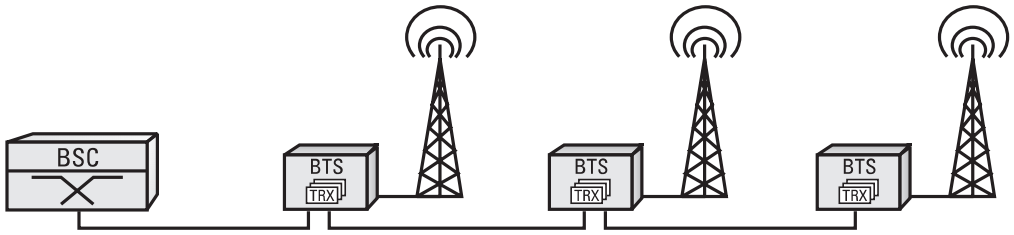


Figure 6.2 Serial connection of BTSs in a line topology. The disadvantage is that a single link failure results in total loss of connection to a number of BTSs.

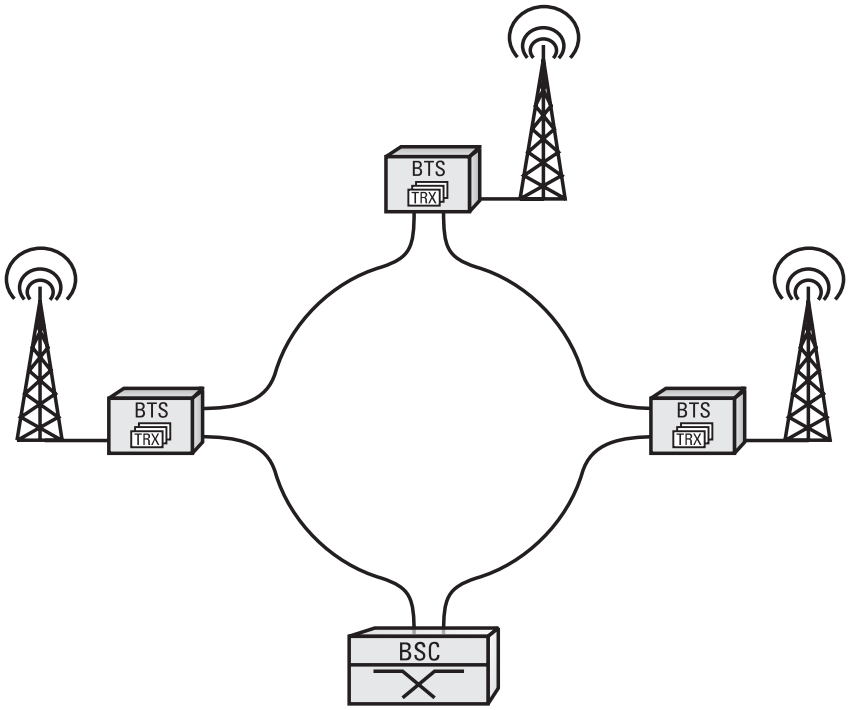


Figure 6.3 Serial connection of BTSs in a ring topology. The advantage is that a single link failure never results in total loss of connection to any BTS.

(for serial configuration). For that reason, the use of a ring configuration provides some redundancy in which the signal can always go in one of two directions, so that in the event of a link failure, it is still possible to provide an alternative connection.

6.2.2 Connection of BTSs in Star Configuration

The star configuration was the most popular when the first systems were deployed in 1991–1992. In a star configuration, every BTS has it own connection, an Abis-interface to the BSC. Figure 6.4 illustrates a star configuration with three BTSs.

6.3 Signaling on the Abis-Interface

6.3.1 OSI Protocol Stack on the Abis-Interface

The Abis-interface utilizes Layers 1 through 3 of the OSI protocol stack (Figure 6.5). Layer 1 forms the D-channel. The LAPD is in Layer 2, and Layer 3 is divided into the TRX management (TRXM), the common channel management (CCM), the radio link management (RLM), and the dedicated channel management (DCM).

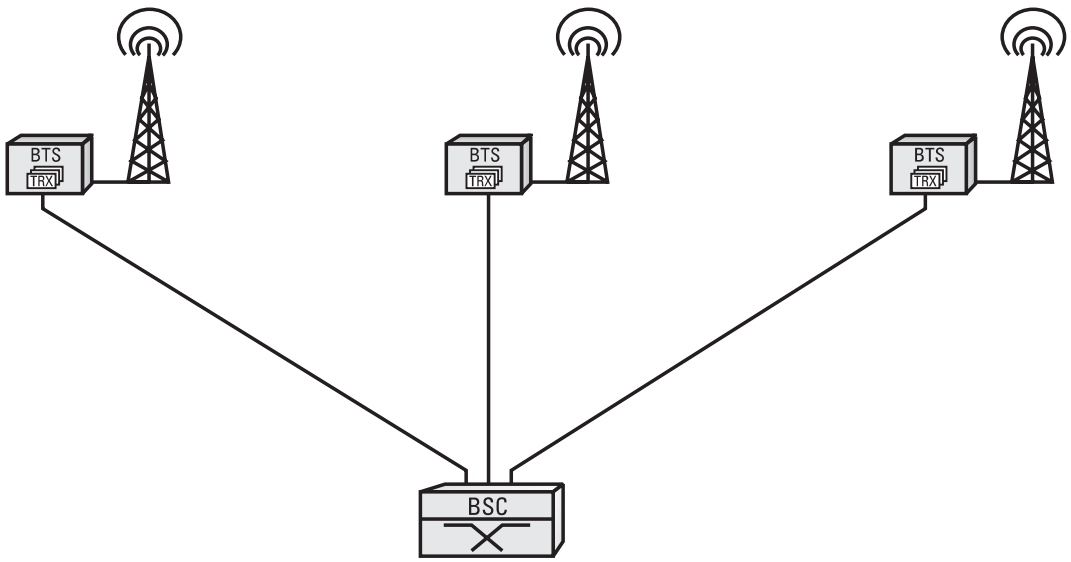


Figure 6.4 Connection of BTSs in a star configuration. The disadvantages are the high costs for links and that a single link failure always causes loss of a BTS.

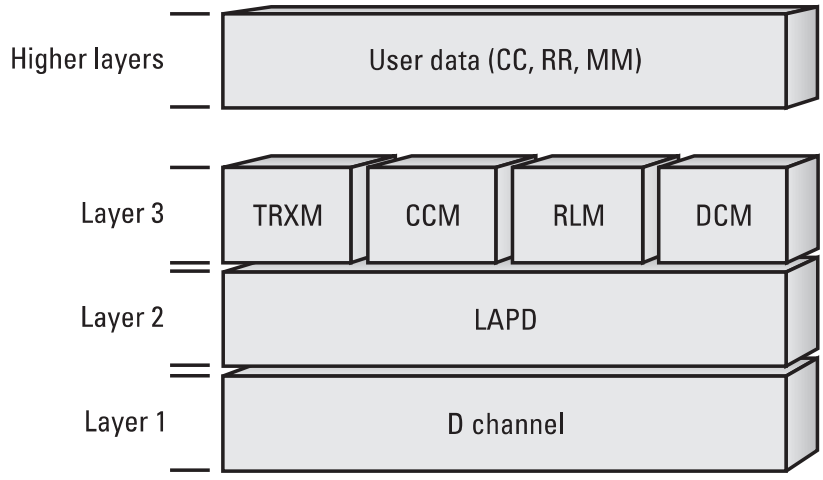


Figure 6.5 The OSI protocol stack on the Abis interface.

6.3.2 Layer 2

6.3.2.1 Link Access Protocol for D-channel

The ISDN D-channel protocol, which GSM largely has adopted, provides the basics of signaling on the Abis-interface. This link access protocol is also referred to as LAPD. The format of LAPD, as defined by ITU in Recommendations Q.920 and Q.921, is presented first before we discuss the GSM specifics. Note that GSM does not use all the functionality that ITU Q.920 and Q.921 describe. The XID frame, for example, is currently not used.

6.3.2.2 LAPD Frame

The underlying concept of the LAPD frame is the more general HDLC format, which partitions a message into an address field, a control field, a checksum, and a flag field at both ends of the message. LAPD messages in the OSI Reference Model belong to Layer 2 and are separated into three groups, according to their particular use:

- The information-frame (I-frame) group consists of only the I frame. (The unnumbered information, or UI frame, belongs to the unnumbered frame group.)
- The supervisory frame group consists of the receive-ready (RR) frame, the receive-not-ready (RNR) frame, and the reject (REJ) frame.
- The unnumbered frame group. This group comprises the set-asynchronous-balance-mode-extended (SABME) frame, the disconnected-mode (DM) frame, the UI frame, the disconnect (DISC)

frame, the unnumbered-acknowledgment (UA) frame, the frame-reject (FRMR) frame, and the exchange-identification (XID) frame.

Figures 6.6 and 6.7 illustrate the format of LAPD modulo 128 and LAPD modulo 8. The control field (defined later in the text) of the unnumbered frames is only 1 octet long (that is the case for both modulo 8 and modulo 128). The shaded area of the control field defines the message group, which is defined as follows:

- Information frame: 1st byte, bit 0 = 0
- Supervisory frames: 1st byte, bit 0 = 1, bit 1 = 0
- Unnumbered frames: 1st byte, bit 0 = 1, bit 1 = 1

Figure 6.6 and Figure 6.7 show the coding of the message type of the control field. While the group of I frames does not require any further definition, bits 2 and 3 of the first byte of a supervisory frame identify the frame type. The same task is performed by bits 2, 3, 5, 6, and 7 for the larger number of unnumbered frames.

6.3.2.3 Differences Between LAPD Modulo 128 and LAPD Modulo 8

Manufacturers have implemented LAPD differently. Some have chosen to implement LAPD modulo 8 (as shown in Figure 6.7), in which the control field consists of 8 bits, while others have chosen to implement LAPD modulo 128, which uses a 16-bit control field (as shown in Figure 6.6). Analyzing an LAPD trace file, there is no explicit possibility to distinguish between the two.

One has to rely on a consistency check, which can be performed, for example, by comparing the lengths of frames. Supervisory frames in the 8-bit version (modulo 8) are three octets long, while the ones with 16-bit-long control field (modulo 128) are four octets long. This method fails, however, for the variable-length I frames and the unnumbered frames.

On the practical side, there is only one difference between LAPD modulo 128 and LAPD modulo 8. That is the definition of the range of values for the send sequence number, N(S), and the receive sequence number, N(R). In an 8-bit-wide control field, the range for N(S) and N(R) is always between 0 and 7, while the 16-bit control field allows for values of N(S) and N(R) between 0 and 127. Hence, the two methods are referred to as LAPD modulo 8 and LAPD modulo 128, respectively.

The consequence of that is, for modulo 8, no more than eight messages may be transmitted without an acknowledgment. The difference is of little importance in GSM, since the requirement on unacknowledged frames

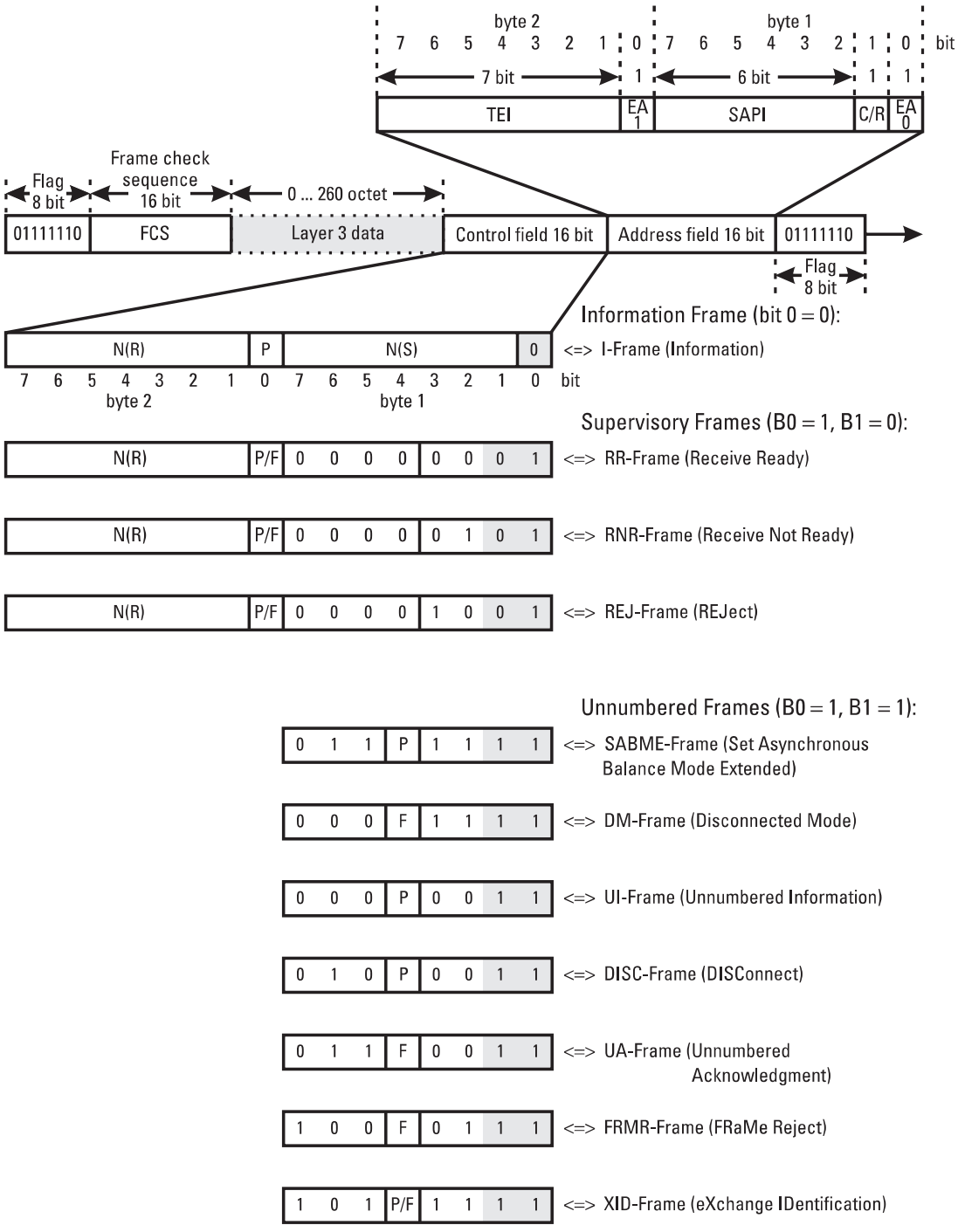


Figure 6.6 The format of an LAPD frame modulo 128.

is restricted even further by other influences. The number of unacknowledged frames for the service access point identifier (SAPI) = 0 is two, and the number of unacknowledged frames for SAPI = 62 and for SAPI = 63 is one.

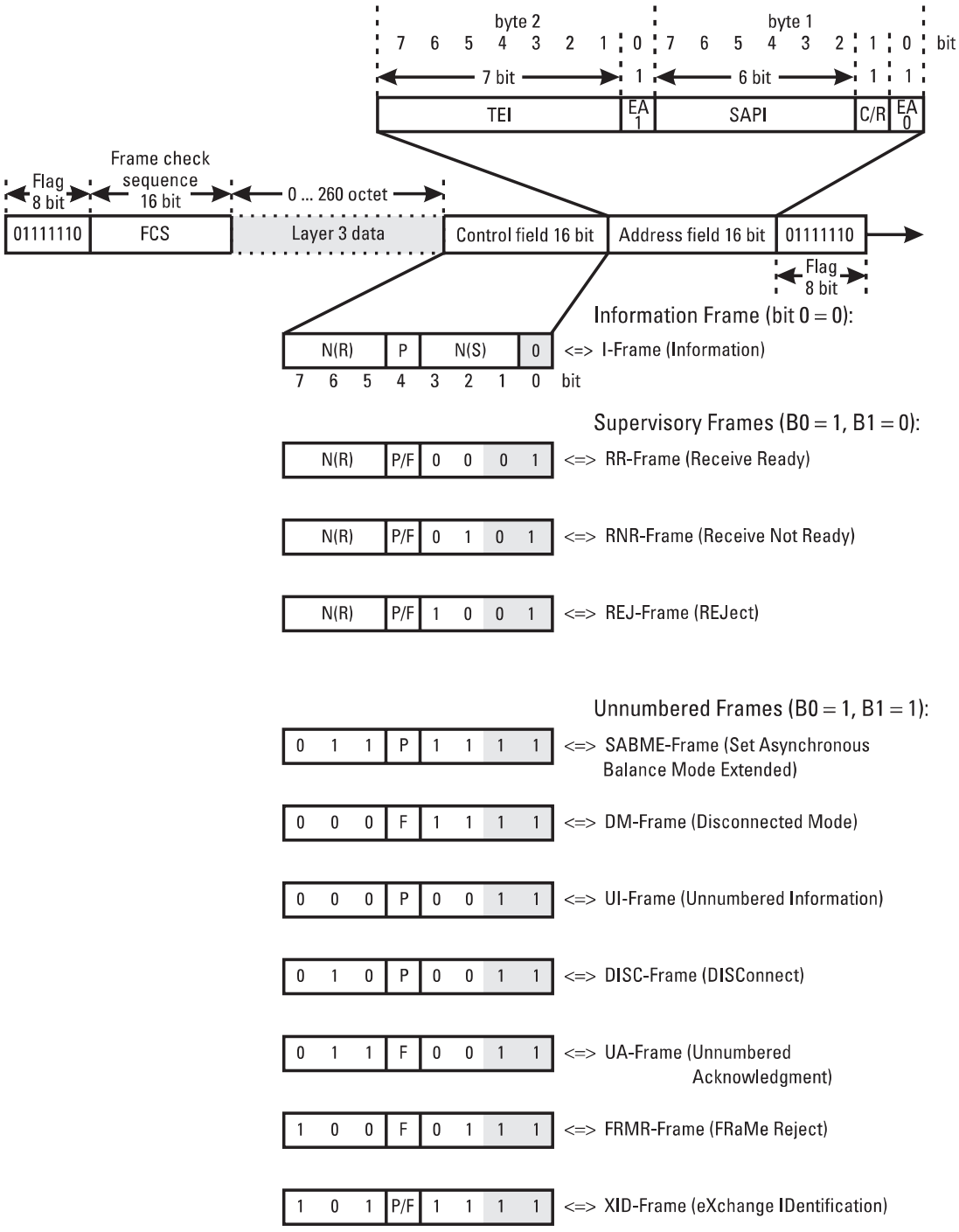


Figure 6.7 The Format of an LAPD frame modulo 8.

Nonetheless, because the modulo 128 variant is more widely used in GSM, that method is described in more detail. Furthermore, all tables and examples refer to the 16-bit variant.

6.3.2.4 Parameters of an LAPD Message

Flag

Every LAPD frame starts and ends with a flag. The flag consists of a 0-bit followed by six consecutive 1-bits and ends with a 0-bit, that is, $01111110_{bin} = 7E_{hex}$. That sequence is used as an indicator of the beginning and end of a frame. To prevent confusion, when this particular bit sequence occurs within the body of a message, some precautions need to be taken. If this pattern is part of a message, the sender has to change the sequence by inserting a 0-bit between the fifth and sixth bit. The receiver then has to remove the extra 0-bit.

Frame Check Sequence

The 16-bit long frame check sequence (FCS) is used for error detection (Figure 6.8). A checksum is calculated, using the data between the start flag and the FCS. The result is sent in the FCS field. The same operation is performed at the receiver's end, and the values of the respective FCSs are compared. The receiver will request a retransmission in the event that the calculated FCS does not match the one received.

Address Field

The parameters of the address field of a LAPD modulo 128 frame and a LAPD modulo 8 frame are described in the following paragraphs.

Service Access Point Identifier

The SAPI is a 6-bit field and defines the type of user to which a message is addressed. The functionality of the SAPI in the LAPD is similar to the function of the subsystem number (SSN) within the SCCP. SAPI is used, for instance, to determine whether a message is for O&M or if it is part of the call setup. GSM uses three different values for SAPI on the Abis-interface. Their uses are listed in Table 6.1. Note that these SAPI values are independent of those defined for the similar $LAPD_m$ standard that is used on the Air-interface. SAPI also indicates the transfer priority of a message. SAPI 62 and SAPI 63 have a

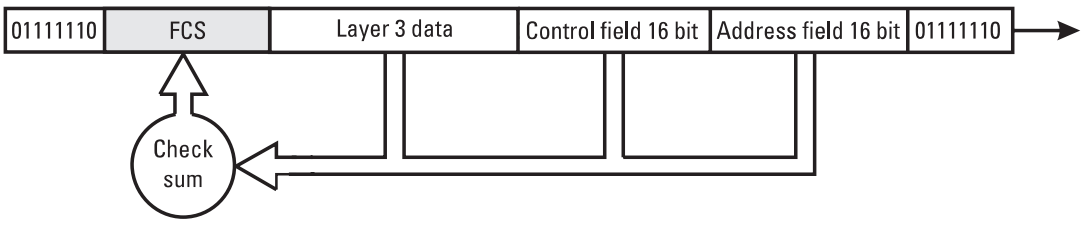


Figure 6.8 The frame check sequence.

Table 6.1
Possible Values of SAPI on the Abis-Interface

SAPI (decimal)	Priority	Meaning
0	2	Radio signaling (radio signaling link, or RSL)
62	1	O&M messages (O&M link, or OML)
63	1	Layer 2 management

higher priority for message transfer than SAPI 0. The consequence is that it is still possible, in the event of an overload situation or other problems, to exchange O&M information between the BTS and the BSC, while other information is delayed or even lost.

Terminal Endpoint Identifier

The TEI is a 7-bit field. In contrast to the SAPI, the TEI allows for distinction among several functionally identical entities. GSM uses the TEI, for example, to distinguish among the various TRXs. One TEI is assigned to each TRX. That provides the ability to distinguish between TRXs during analysis of a trace file.

Command/Response Bit

The command/response (C/R) bit determines whether a message contains a command, an answer, or an acknowledgment of a command, as illustrated in Figure 6.9 and Table 6.2. Note that the values of the C/R in a command frame are the same as the acknowledgment in the reverse direction.

As required by the ITU definition, an LAPD connection always contains a network side and a user side. When the network side sends a command, then C = 1. The user's side responds with an answer where the value of R equals 1. If a command from the user's side contains a zero value for C then the response from the network will be R = 0. There are some messages that can only be commands and others that can only be responses. In the GSM system, the BSC is defined as the network and the BTS as the user.

Extension Address Field-Bits

The address field contains one EA-bit per octet. The EA-bit of the first octet is set permanently to 0, as shown in Figures 6.6 and 6.7, which indicates that the following octet is also part of the address field. The EA-bit of the second octet is set to 1, which indicates that it is the last octet of the address field.

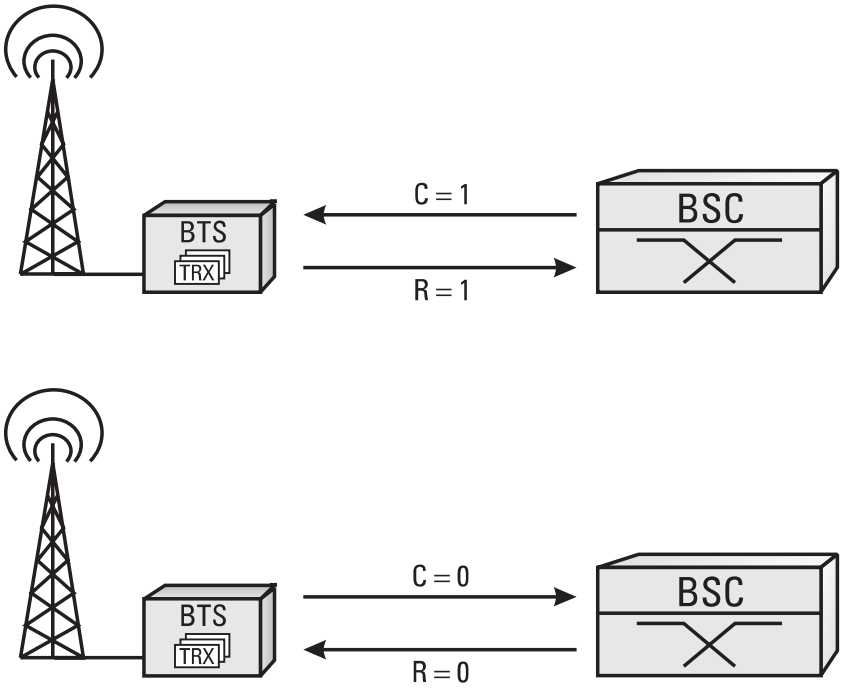


Figure 6.9 Possible values of the C/R-bit.

Table 6.2
The C/R-Bit in Command Frames and Response Frames

Frame Type	Direction	C/R?
Command frames	BSC → BTS	1
	BTS → BSC	0
Response frames	BSC → BTS	0
	BTS → BSC	1

Control Field

The length of the control field depends on the frame type and is either 8 or 16 bits long. It contains the following information.

Polling Bit (P-Bit), Final Bit (F-bit), and P/F-Bit For frame types that can be used only as commands, the corresponding bit is the P-bit. In frames that can be used only as responses, the corresponding bit is the F-bit. In frame types that can be used as both commands and responses, all variants are possible. The P-bit informs the receiver of a command message that the sender expects an

answer, even if the message type normally would not require an acknowledgment. Real polling on the Abis-interface is used only when BSC and BTS are in an idle state and need to test the connection periodically (i.e., the exchange of RR frames).

When a command frame is received where the P-bit is set to 1, the answer frame needs to be returned with the F-bit set to 1. LAPD allows for the acknowledgment of an I frame, where the P-bit is set to 0, with either an I frame or a supervisory frame. I frames, however, where the P-bit is set to 1, have to be acknowledged immediately with a supervisory frame. The P-bit of UI frames is always set to 0. That is why a UI frame, although a command per definition, does not require an acknowledgment. Example 6.3 describes polling for an RSL.

Send Sequence Number and Receive Sequence Number The N(S) and the N(R) serve the purpose of acknowledging the transfer and the receipt of I frames. The method of counting can be modulo 8 or modulo 128. In the case of modulo 8, three bits are used for the counter, allowing for values of frame numbers between 0 and 7. Seven bits are used for the counter in the case of modulo 128, allowing for values between 0 and 127. On the Air-interface ($LAPD_m$), only modulo 8 is used, whereas both variants are used on the Abis-interface. The functionality as such is independent of the value range of the counters. When one side (BSC or BTS) sends an I frame, the counter N(S) on the sender side is incremented by 1. Note that the value of N(S) in the just sent I frame still has the old value, that is, the increment occurs only after the frame is sent.

When an I frame reaches the receiver, it is checked to see if the received values of N(S) and N(R) match those the receiver has stored. The value for N(S) for the received I frame has to match the actual value of N(R) on the receiver side. If the frame also is without errors (FCS), the receiver increments the value for N(R) and sends that new value in an RR frame back to the sender. The sender expects acknowledgment within a specified time frame. If that time period expires without the acknowledgment, the I frame is sent again. Note that according to Specifications Q.920 and Q.921, an acknowledgment does not have to be given by a supervisory frame but also can be given by an I frame. Consequently, the sending of an RR frame is not necessary if the receiver has to send an I frame, too. However, GSM does not make use of that option. Every I frame gets acknowledged with an RR frame. Until the acknowledgment is received, the sender has to buffer an I frame. The following example illustrates this strategy.

Function of N(S) and N(R) The BTS sends an I frame and increments its counter N(S). The BSC receives the I frame, increments counter N(R),

and sends an RR frame with a new value of N(R) back to the BTS. The BTS does not need to continue to buffer the I frame after it receives the acknowledgment from the BSC.

Next the BSC sends an I frame to the BTS and increments its counter N(S) to 1. Again, note that the values of N(S) and N(R) in the transmitted I frames correspond inversely to the ones stored internally in the BTS. The BTS then checks for consistency of the information and increments, if everything is right, its counter N(R) and responds to the BSC with an RR frame with the new value of N(R). This procedure is illustrated in Figure 6.10.

RR frames need to be exchanged between BTS and BSC within certain time intervals during the so-called idle case, when no data are being transported. The values of N(S) and N(R) are not changed during that process, which is called polling. However, they have to correspond inversely to each other.

This applies to both LAPD modulo 8 and to LAPD modulo 128.

Frame Type The control field identifies, among other things, the frame type. Table 6.3 lists which values (in hexadecimal) the control field of an LAPD frame modulo 128 can assume in a trace file. Digits marked with an X indicate a "don't care" condition, that is, the value of the digit is irrelevant in identifying the frame type.

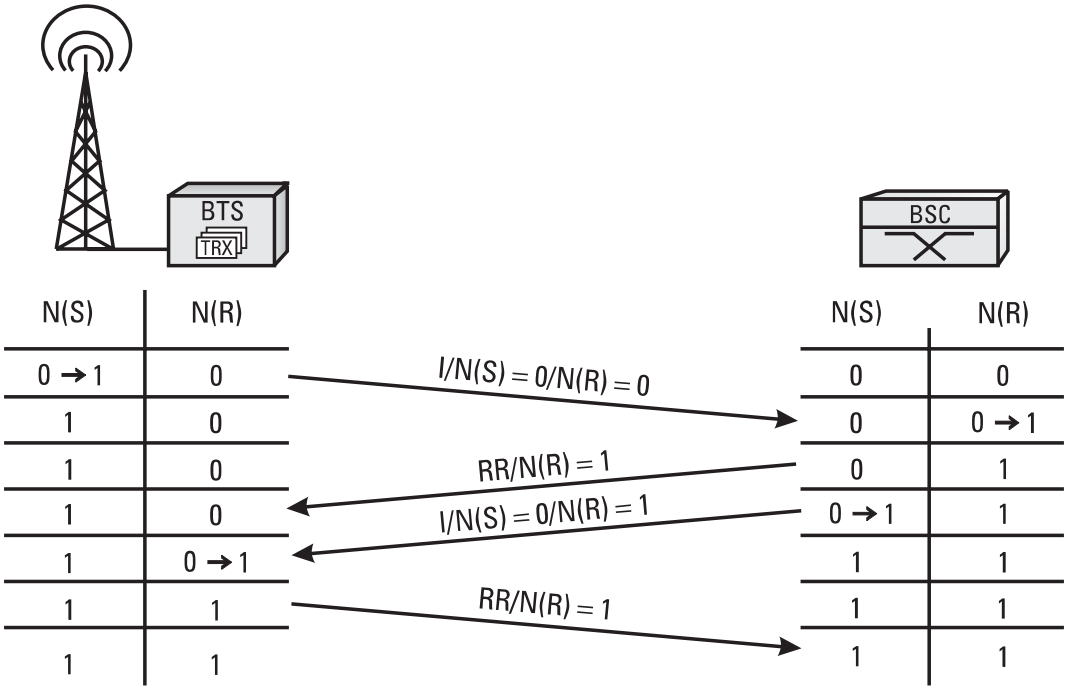


Figure 6.10 Function of the counters N(S) and N(R).

Table 6.3
Frame Types of the Abis-Interface

Name	Command-Frame?	Response-Frame?	Possible Values of the Control Field (in Hex)
I-frame group			
I	Yes	No	(X0 XX), (X2 XX), (X4 XX), (X6 XX), (X8 XX) if 1st byte is even it is an I-Frame
Supervisory frame group			
RR	Yes	Yes	(01 XX)
RNR	Yes	Yes	(05 XX)
REJ	Yes	Yes	(09 XX)
Unnumbered frame group			
FRMR	No	Yes	(87), (97)
DISC	Yes	No	(53) because P-bit is always 1
UI	Yes	No	(03) because P-bit is always 0
DM	No	Yes	(0F), (1F)
SABME	Yes	No	(7F) because P-bit is always 1
UA	No	Yes	(73) because P-bit is always 1
XID	Yes	Yes	(AF), (BF) (not used in GSM)

Detection of Frame Type of LAPD Frames The LAPD messages in Figure 6.11 have been recorded on the Abis-interface by means of a low-level protocol analyzer. For our imaginary analysis, complete decoding is not required; only the message types are identified.

It is known that the first three octets in line number 0010 of the UBFD (user buffer = trace file specific) always contain the address and the control field of the respective LAPD message.

Note how difficult it would be without this knowledge to identify the relevant information in a given trace file. If one encounters such a situation, the best way to proceed is to look for supposedly included fields like the address and control fields within an LAPD message by using a regular editor (see Figure 6.10).

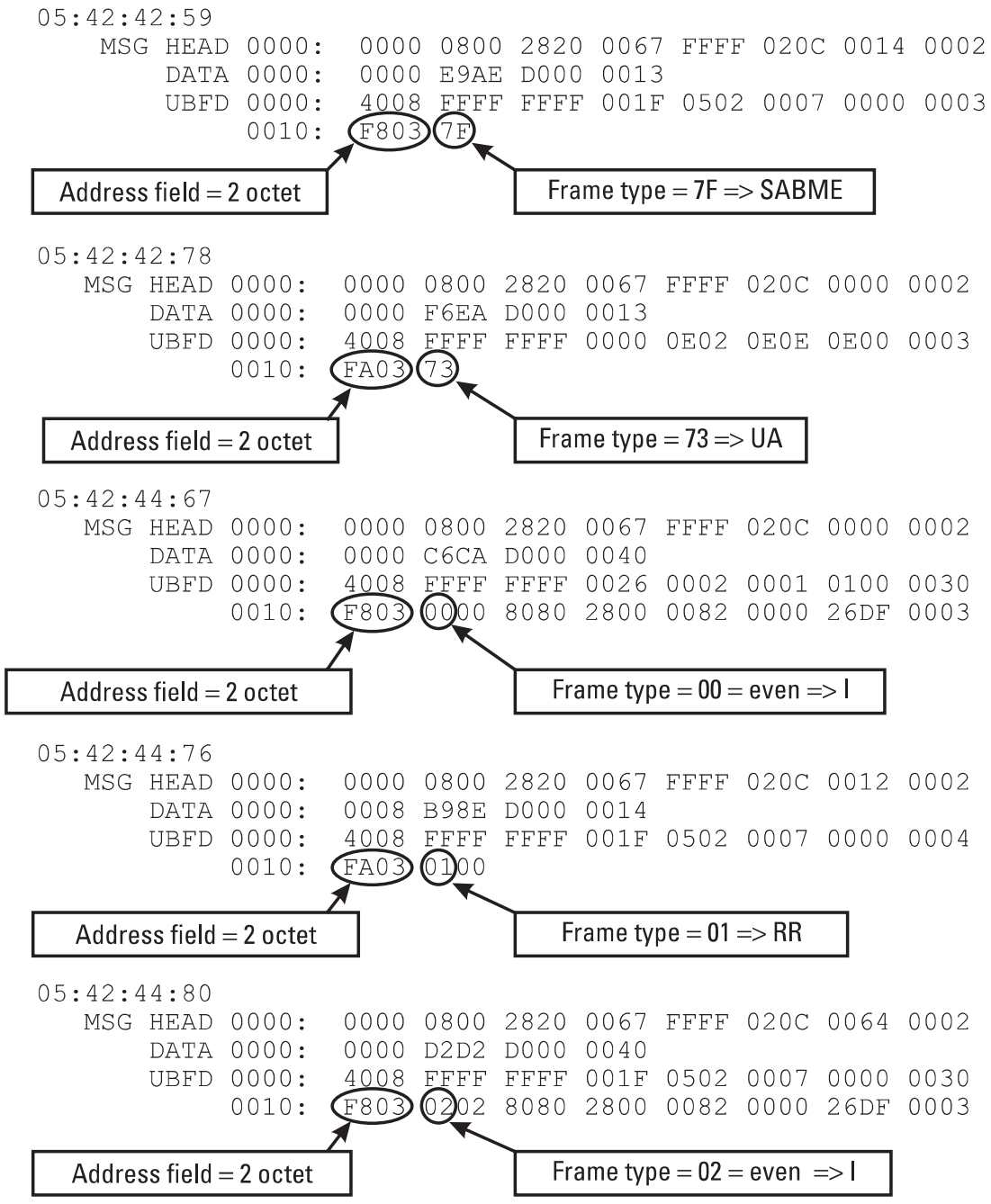


Figure 6.11 Hexadecimal LAPD trace file.

Tasks of Various Frame Types

I Frame The I frame (Figure 6.12) is used to transfer Layer 3 information. It is always a command, irrespective of its direction. The error-free reception of this frame has to be acknowledged by the recipient with an RR frame.

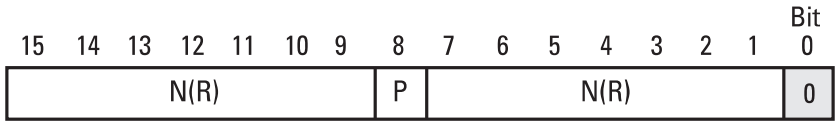


Figure 6.12 Control field of an I frame (modulo 128).

Otherwise, an RNR frame or an REJ frame is sent, because the frame could not be processed due to some error or overload condition and thereby requests retransmission of the I frame. I frames contain both an N(S) and an N(R).

RR Frame An RR frame (Figure 6.13) acknowledges that an I frame has been received. It also is used for the polling between the BTS and the BSC.

During idle phases (no I-frame transmission), RR frames are exchanged between the BSC and the BTS with a periodicity based on the value of timer T203 (the default value of T203 is 10 seconds). It may be assumed that Layer 2 of a connection is working fine when polling of RR frames can be seen on the Abis-interface. No conclusion, however, can be drawn as to the state of the Layer 3 connection.

RNR Frame The RNR frame (Figure 6.14) is used to signal that no more I frames can be accepted. This situation may arise when too many unprocessed I frames are stored in the input buffer, so that no space is available for more I frames. In this situation, an RNR frame is sent to the remote end.

The RNR frame requests a halt to the transmission of I frames and requires the transmitter to wait for an RR frame before transmission can be resumed.

This frequently results in an overload situation on the sender side because data for transmission quickly backs up, which, in turn, results in the sender also

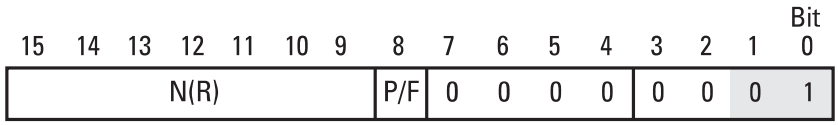


Figure 6.13 Control field of an RR frame (modulo 128).

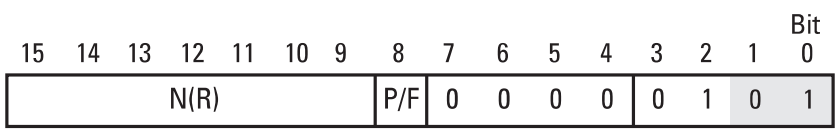


Figure 6.14 Control field of an RNR frame (modulo 128).

sending an RNR frame. The value of N(R) in the RNR message is that it indicates which I frame was last received correctly.

REJ Frame In contrast to the RNR frame, which is used to signal an overload situation and hence to request the temporary halt to transmission, the REJ frame (Figure 6.15) is used to indicate a transmission error condition that has been detected by analysis of the FCS. The REJ frame contains a value for N(R), which indicates the first I frame that has to be repeated.

An REJ frame is also used to indicate that I frames with a wrong value for N(S) or N(R) were received. That requests the retransmission of all I frames with a value of N(R) and higher.

SABME Frame SABME frames (Figure 6.16) are sent when no Layer 2 connection has been established.

DM Frame The transmitting side uses a DM frame (Figure 6.17) to indicate that it can no longer maintain the Layer 2 connection.

A DM frame indicates that the sender will immediately tear down the Layer 2 connection without waiting for an acknowledgment from the receiver. The DM frame is used to take a connection out of service, as is the case with the DISC frame, but without waiting for or expecting an acknowledgment.

UI Frame Unlike an I frame, a UI frame (Figure 6.18) contains neither a send sequence number nor a receive sequence number. Another difference is that the

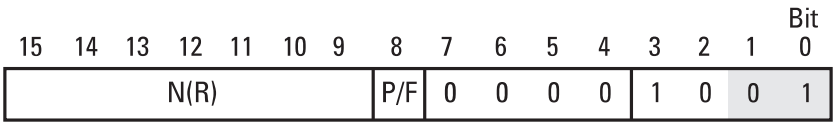


Figure 6.15 Control field of an REJ frame (modulo 128).

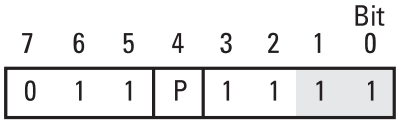


Figure 6.16 Control field of a SABME frame.

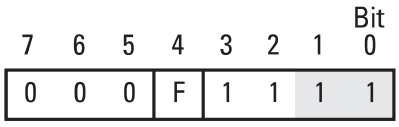


Figure 6.17 Control field of a DM frame.

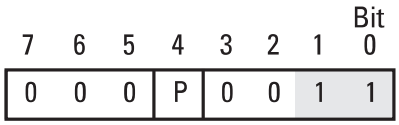


Figure 6.18 Control field of a UI frame.

content of a UI frame does not require an acknowledgment (P-bit = 0). UI frames are used on the Abis-interface to convey MEAS_RES messages.

DISC Frame The DISC frame (Figure 6.19) is used to take a Layer 2 connection out of service. The transmitter informs its peer that it intends to tear down the Layer 2 connection. In contrast to the DM frame, the DISC frame is used for regular maintenance tasks, and an acknowledgment (UA) is expected.

UA Frame The UA frame (Figure 6.20) is used to answer a SABME frame or a DISC frame. It acknowledges a Layer 2 connection being brought into service as well as one taken out of service.

FRMR Frame The FRMR frame (Figure 6.21) indicates that a received message was garbled, wrong, or unexpected (protocol error). That is different from the REJ frame, which indicates to the peer entity that I frames have to be repeated starting at N(R).

This kind of error cannot be corrected by retransmission of a frame. The problem usually occurs when there are errors with the transmission between

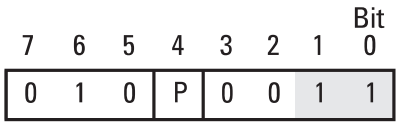


Figure 6.19 Control field of a DISC frame.

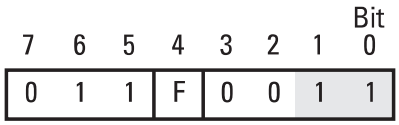


Figure 6.20 Control field of a UA frame.

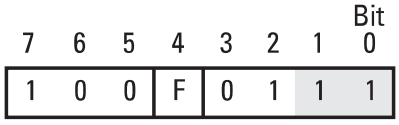


Figure 6.21 Control field of an FRMR frame.

the BTS and the BSC. The FRMR frame may be sent as an answer to any frame, and its use is not restricted to being a response to faulty I frames.

To allow for proper identification of the faulty frame, the header and as much content of the faulty frame as possible are sent back to the peer entity within the FRMR frame.

Problems in the transmission area or at the opposite end of the connection can be assumed when FRMR frames are detected.

XID Frame Although the XID frame is not part of the Abis-interface, according to GSM 08.56, it will be described here.

The XID frame (Figure 6.22) is used to synchronize the various transmission parameters between the user and the network. It coordinates the various timers when the Layer 2 connection is brought into service. It also determines the number of unacknowledged I frames that have to be stored.

Example: Decoding and Analysis of Layer 2 Messages To decode and analyze Layer 2 messages when observing a protocol analyzer, one needs to be able to interpret the displayed measurement results. This example describes such decoding work by analyzing the following trace file. Note that the channels are mostly in idle state because no data have to be transferred between the TRX and the BSC. RR frames are exchanged periodically between the TRX and the BSC according to the value of the timer T203. Sometimes ghost CHAN_REQ messages are decoded by the BTS receiver, created by the unavoidable electromagnetic noise in the environment. Unfortunately, that false CHAN_REQ decoding may put an additional signaling load on the system. Figure 6.23 presents a short section of a trace file that was captured with the SIEMENS K1103 protocol analyzer.

- Note the following details, which can be retrieved from a rather uninteresting trace file without any error messages.
- Timer T203, in this case, is set to 3.4 seconds. The time can be derived from the time difference between two consecutive RR frames from the same TRX.

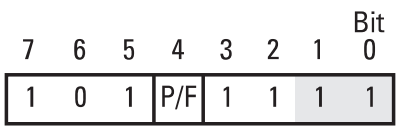


Figure 6.22 Control field of an XID frame.

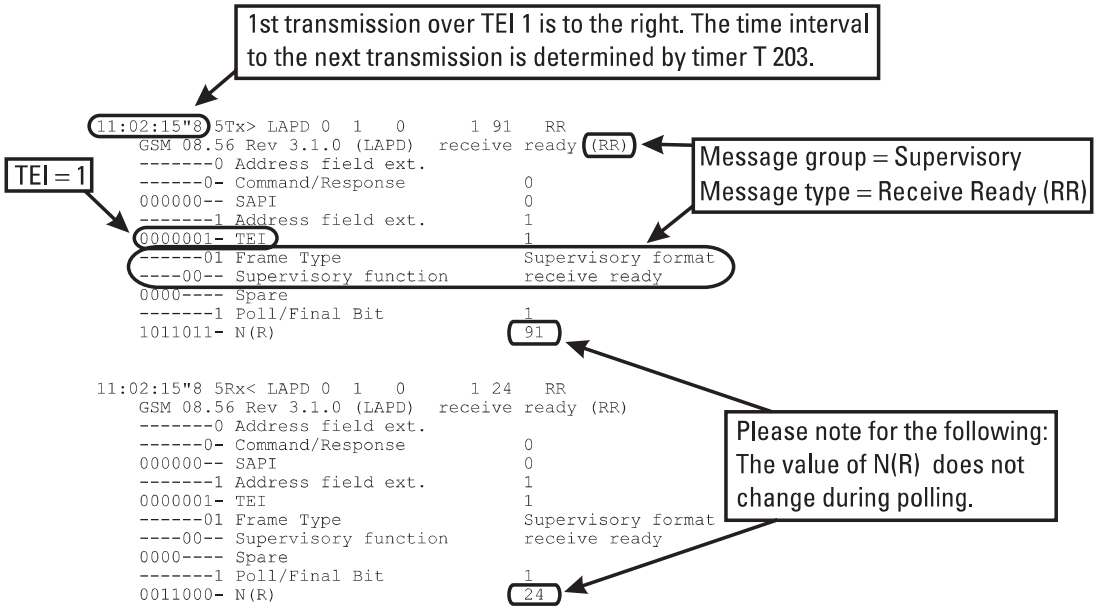


Figure 6.23(a) Tracefile as taken from a K1103.

- The messages from left to right are sent by the TRX, while the messages from right to left are sent by the BSC. That can be deduced from the CHAN_RQD at the end of the trace file, a message that can come only from the BTS and in this case is sent from left to right.
- The P/F-bit is set to 1 during polling to request the distant end to answer. For "normal" data exchange, the P/F-bit is set to 0.

In this example, the TRX polls the BSC.

6.3.3 Layer 3

Layer 3 information within I frames and UI frames follows the Layer 2 header. Because of differences in format, it is particularly important during protocol testing to distinguish between Layer 3 information for administrative tasks (SAPI 62 and 63) and Layer 3 information for connection setup and release (SAPI 0).

SAPI 0 is allocated to the RSL and carries user signaling, that is, all messages for connection setup and release. On the Abis-interface, messages for SMS and supplementary services (SS) also are dedicated to SAPI 0, which differs from the handling on the Air-interface.

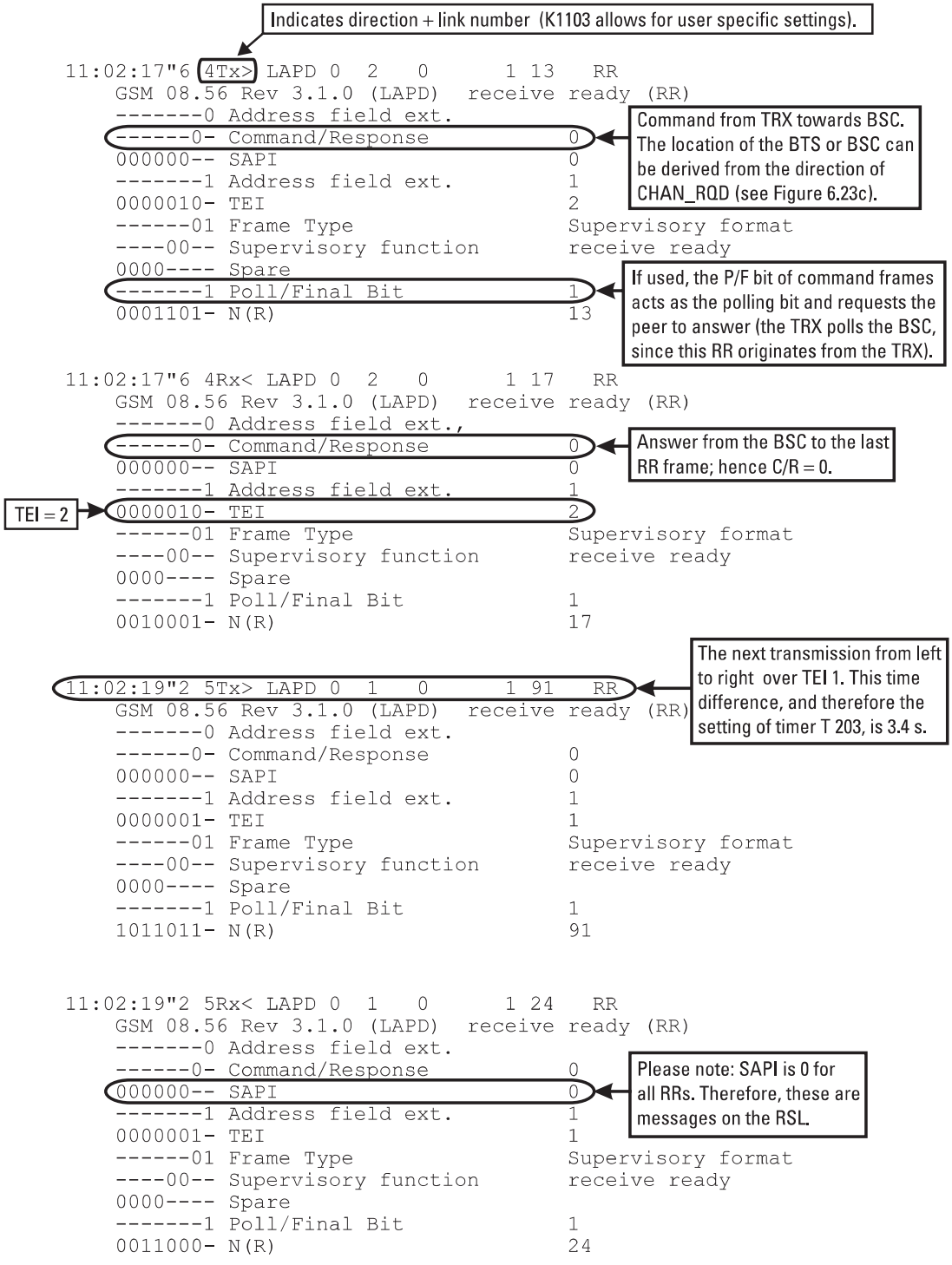


Figure 6.23(b) Tracefile as taken from a K1103.

Administrative data, on the other hand, are assigned to SAPI 62 and 63. Administrative tasks are control commands from the BSC (OMC) to the BTS,

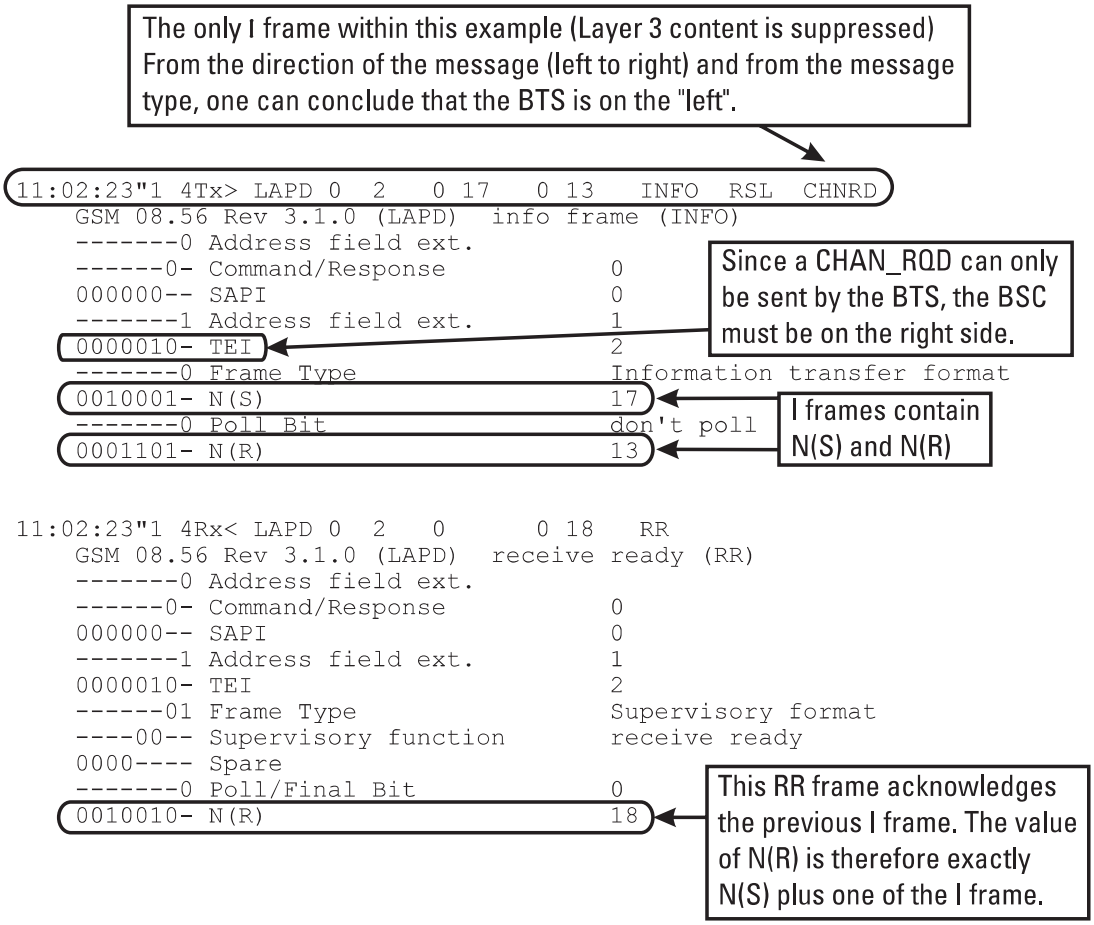


Figure 6.23(c) Tracefile as taken from a K1103.

as well as complete software packages and files, which the BSC (OMC) sends to the BTS.

6.3.3.1 Layer 3 on RSL (SAPI 0)

Figure 6.24 illustrates the format of Layer 3 on the RSL. The parameters are described in more detail. Note at this point how Layer 3 is embedded in Layer 2.

Message Discriminator and the T-Bit

The message discriminator classifies all the messages defined in Layer 3 of the Abis-interface into groups or classes (see Figure 6.5). Together, the groups form Layer 3 on the Abis-interface. The purpose of the T-bit indicates whether the BTS should process an incoming message (e.g., MEAS_RES) or if the message should be transparent to the BTS (T = 1). The distinction applies to both the uplink and the downlink.

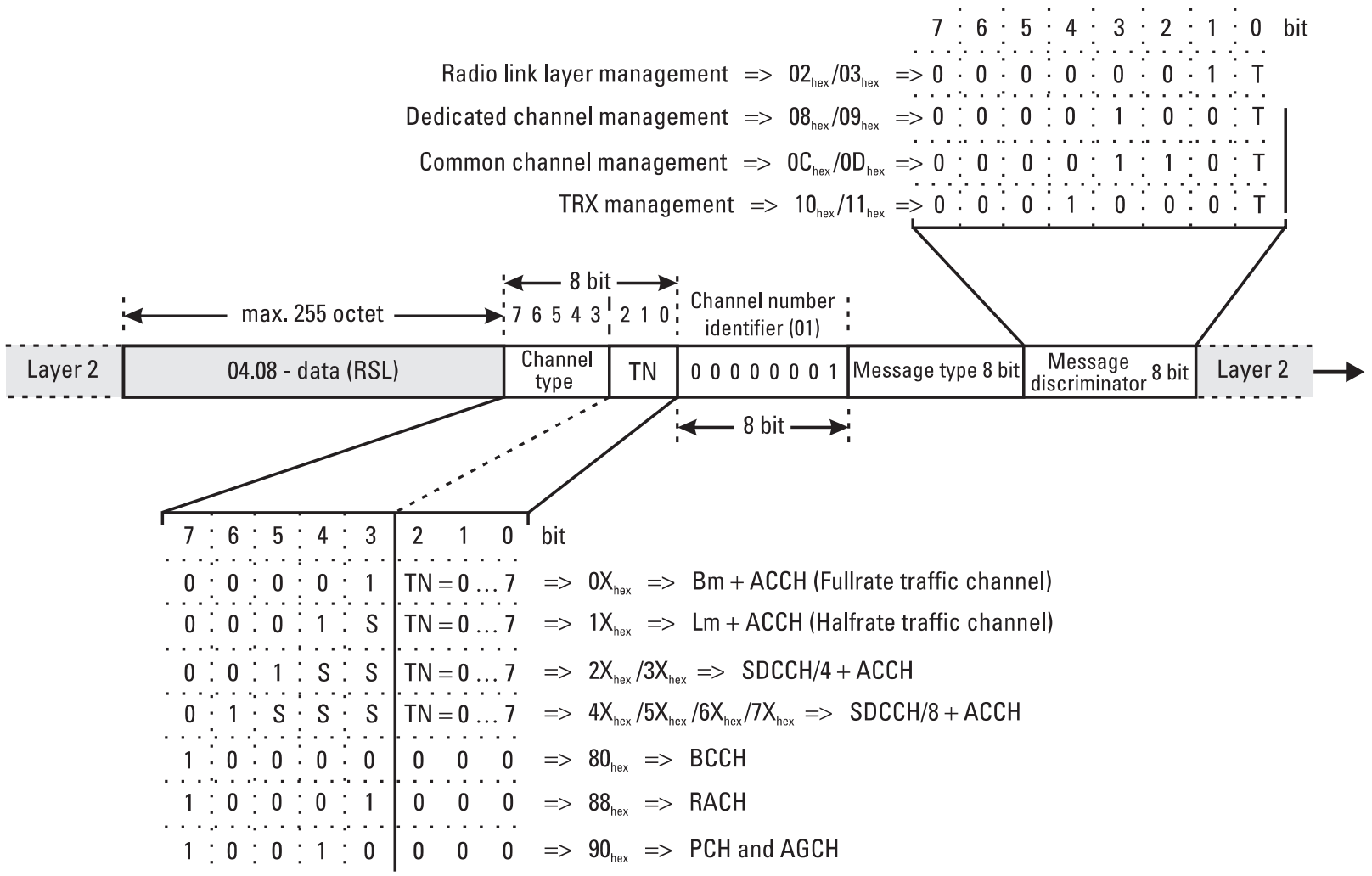


Figure 6.24 Formatting of Layer 3 signaling on the RSL.

Figure 6.24 shows the hexadecimal values the message discriminator can take, depending on the T-bit and how those values translate into the different message classes.

The classes organize messages according to their use:

- RLM. This group contains all the messages necessary for the control of a Layer 2 connection between the MS and the BTS. That includes connection setup and release, as well as the reporting of Layer 2 problems on the Air-interface to the BSC. The DATA_REQ and the DATA_IND messages, which are used for the transparent signaling data transport between MSC and MS, also belong to this group.
- CCM and TRXM. All messages that carry common control channel (CCCH) signaling data to and from the Air-interface are assigned to the CCM. That includes the transfer of cell broadcast information to the BTS. Messages used for TRXM also belong to this group.
- DCM. All messages that are used to control Layer 1 of the Air-interface belong to DCM.

Message Types

Tables 6.4, 6.5, and 6.6 list all the messages that are defined on the Abis-interface. The letters in message names that appear in uppercase form the message mnemonics used in the context and the protocol presentations.

Channel Number

The channel number is a parameter that identifies the channel type, the time slot, and the subchannel that are used for a connection on the Air-interface. Note that the channel number only indirectly corresponds to the terrestrial channel used on the Abis-interface. This parameter consists of an element identifier, which is hard coded to 01_{hex} plus the actual information, which is formatted as shown in Figure 6.24 and in Table 6.7.

- The S-bits specify the subchannel (if required) and can take a value in the range from 0 to 7.
- The X-bits identify the time slot (not the frequency) on the Air-interface and can take a value in the range from 0 to 7.
- Table 6.7 shows that it is easy to derive the channel type from the hexadecimal representation. For example, channels 08, 09, 0A, …, are all fullrate traffic channels, because the first digit is set to 0, which applies only to the fullrate traffic channel.

Table 6.4
Messages for RLM

ID (Hex)	Name	Direction	Explanation
01	DATA REQest	BSC → BTS	Transport container for the transparent transfer of BSSAP data from the NSS to the mobile station.
02	DATA INDication	BTS → BSC	Transport container for the transparent transfer of BSSAP data from the MS to the NSS.
03	ERROR INDication	BTS → BSC	Informs the BSC of a problem in Layer 2 of the air interface (e.g., acknowledgments are missing, MS sends $LAPD_m$ frames with a wrong address or control field, radio link failure/Layer 2). Note that not every ERR_IND message in a protocol trace means a dropped call.
04	ESTablish REQest	BSC → BTS	Request for the BTS to establish a Layer 2 connection on the Air-interface. The BTS subsequently sends an $LAPD_m$ SABM frame to the mobile station.
05	ESTablish CONFirm	BTS → BSC	Answer to EST_REQ. Message sent to the BSC after the BTS receives an $LAPD_m$ UA frame from the mobile station.
06	ESTablish INDication	BTS → BSC	Response from the BTS on receiving an $LAPD_m$ SABM frame from the mobile station. *Note:* A SABM on the Air-interface may contain Layer 3 data (Example: LOC_UPD_REQ). In that case, EST_IND contains Layer 3 data.
07	RELease REQest	BSC → BTS	Request to a BTS to release an existing Layer 2 connection on the air interface. After the BTS receives this, it sends an $LAPD_m$ DISC frame to the mobile station.
08	RELease CONFirm	BTS → BSC	Answer to REL_REQ. Message sent to the BSC after the BTS has received an $LAPD_m$ UA answer frame (for an LAPDm DISC frame) from the mobile station.
09	RELease INDication	BTS → BSC	Response from the BTS when receiving an $LAPD_m$ DISC frame from the mobile station. In this case, the BTS releases the Layer 2 connection without waiting for a response from the BSC.
0A	UNIT DATA REQest	BSC → BTS	Transport frame for messages sent in $LAPD_m$ UI frames over the Air-interface (downlink).
0B	UNIT DATA INDication	BTS → BSC	Transport frame for messages received by the BTS as $LAPD_m$ UI frames (uplink).

Table 6.5
Messages for CCM and TRXM

ID (Hex)	Name	Direction	Explanation
11	BCCH INFOrmation	BSC → BTS	Transport frame for SYS_INFO messages where the BTS permanently transmits SYS_INFO 1–4 in the BCCH time slot 0.
12	CCCH LOAD INDication	BTS → BSC	Informs the BSC about the traffic load on the common control channels of the Air-Interface. The frequency of transmission of CCCH_LOAD_IND may be adjusted by the OMC.
13	CHANnel ReQuireD	BTS → BSC	Message sent by the BTS after a CHAN_REQ message is received from the mobile station. The CHAN_RQD message actually contains more information than CHAN_REQ, in particular the TA parameter, which is determined by the BTS.
14	DELETE INDication	BTS → BSC	Infrequent message caused by an overload situation on the Air-interface when a common control channel could not be sent.
15	PAGing CoMmanD	BSC → BTS	Response of the BSC on receiving a PAGING command from the MSC. Contains IMSI and/or TMSI and the paging group of the called mobile station.
16	IMMediate ASSign CoMmanD	BSC → BTS	Contains all information for assignment of a SDCCH on the Air-Interface. Used by the BSC as a response on receiving a correct CHAN_RQD.
17	SMS BroadCast REQest	BSC → BTS	Transfers cell broadcast service (CBS) messages to the BTS, which the cell broadcast center (CBC) sends to all mobile stations within a given area. The SMS_BC_REQ message can transfer only 22 octets of data (plus one octet header), as opposed to the SMS_BC_CMD message. As a result, it requires four SMS_BC_REQ messages to transport one complete CBS message with a length of 88 octets.
19	RF RESource INDication	BTS → BSC	The BTS uses this message to periodically inform the BSC about quality and quantity of the available resources on the air interface. The information on quality is derived from the idle-channel measurements of the TRX receivers. It enables the BSC to refrain from assigning channels with lower quality.
1A	SACCH FILLing	BSC → BTS	Message sent to the BTS, together with the BCCH-INFO, when a TRX is put into service. The SACCH_FILL message informs the TRXs as to which data of an active connection should be transmitted in the SYS_INFO 5- 6.

Table 6.5 (continued)

ID (Hex)	Name	Direction	Explanation
1B	OVERLOAD	BTS → BSC	Message to prevent an overload on the Air-Interface or the TRX. After receiving this message, the BSC reduces the rate of transmission of new messages. The rate is further reduced when more OVERLOAD messages are received from the BTS. If no more OVERLOAD messages are received within the time frame, defined by timer T2, the transfer rate is increased gradually.
1C	ERROR REPORT	BTS → BSC	The ERROR_REPORT message is used when a protocol error has been detected by the TRX and no other response message exists. The ERROR_REPORT message contains, among others, the message that could not be processed. Reason for such errors could be (1) an undefined message type or message discriminator (e.g., caused by bit errors or protocol errors on the Abis-interface) or (2) that the TRX is unable to activate ciphering requested by the BSC.
1D	SMS BroadCast CoMmanD	BTS → BSC	The SMS_BC_CMD message is a new GSM Phase 2 message that is used for transfer of CB/SMSCB messages. Its task corresponds to the SMS_BC_REQ message but with the proviso that the SMS_BC_CMD message is capable of carrying all 88 octets of a CBS message at one time.

Table 6.6
Messages for DCM

ID (Hex)	Name	Direction	Explanation
21	CHANnel ACTivation	BSC → BTS	Message to reserve and activate channels on the Air-interface. It is sent before seizure and contains an accurate description of the requested channel (halfrate/fullrate, DTX on/off, channel type, etc.). The BTS needs this information to activate the transcoders (TRAU). An example for this process can be found in Chapter 3.
22	CHANnel ACTivation ACKnowledge	BTS → BSC	The BTS acknowledges with this message the reception of a CHAN_ACT message and activation of the requested channel. *Note:* A reception of a CHAN_ACT_ACK message does not necessarily indicate that a channel activation was performed without error.

Table 6.6 (continued)

ID (Hex)	Name	Direction	Explanation
23	CHANnel ACTivation Negative ACKnowledge	BTS → BSC	Negative answer to the CHAN_ACT message. The BTS could not provide the channel requested by the BSC. Possible reasons include overload and function not available.
24	CONNection FAILure	BTS → BSC	An important message for error analysis on the Abis-interface. CONN_FAIL is sent by the BTS in case of Layer 1 problems on the air interface (e.g., radio link failure/Layer 1).
25	DEACTivate SACCH	BSC → BTS	Request sent to the BTS to stop transmission over the slow associated control channel (SACCH). The DEACT_SACCH message is part of the release procedure.
26	ENCRyption CoMmanD	BSC → BTS	Activation of ciphering on the Air-interface. The ENCR_CMD message informs the BTS of which algorithm A5/X is to use and contains the complete CIPH_MOD_CMD message destined for the mobile station.
27	HANDover DETect	BTS → BSC	HND_DET is used during handover (not for intra-BTS and intra-BSC). After the target cell has received the HND_ACC message, it calculates the distance to the MS (TA) and sends the result in the HND_DET message to the BSC. In addition, the purpose of HND_DET is to inform the MSC about a successful handover as early as possible, to allow for a faster switching of the user channel on the A-interface, even before the HND_COM message is received (reduction of dead time during handover).
28	MEASurement RESult	BTS → BSC	Contains the mutual measurement results of the BTS and the MS. The MEAS_REP, which comes from the MS, is incorporated into a MEAS_RES message.
29	MODE MODify REQuest	BSC → BTS	GSM allows the channel mode on the air interface to be changed even during an active connection. If certain characteristics need to be adjusted, a MODE_MOD_REQ message is sent to the BTS that tells the BTS the new settings (e.g., switching between data and speech, DTX on or off).
2A	MODE MODify ACKnowledge	BTS → BSC	Confirmation for MODE_MOD_REQ. The BTS has received and processed the message, that is, the new transmission parameters have been adopted.
2B	MODE MODify Negative ACKnowledge	BTS → BSC	Negative response for a MODE_MOD_REQ message. The BTS is unable to provide the requested channel characteristics.

Table 6.6 (continued)

ID (Hex)	Name	Direction	Explanation
2C	PHYsical CONTEXT REQuest	BSC → BTS	Is used by the BSC to query the BTS about the latest values for the distance between the MS and the BTS, the power level, or channel type.
2D	PHYsical CONTEXT CONFirm	BTS → BSC	Answer to PHY_CONTEXT_REQ. The BTS provides the requested information to the BSC.
2E	RF CHANnel RELease	BSC → BTS	The RF_CHAN_REL message is sent to the BTS after the release of the Layer 2 connection on the air interface, to release the physical channel (Layer 1).
2F	MS POWER CONTROL	BSC → BTS	The MS_POWER_CON message is used by the BSC to adjust the output power of an MS according to the current radio conditions. The value range depends on the standard (GSM, DCS 1800, PCS 1900) and on the power class of the MS and ranges from 20 to 30 dB. Adjustments can be done in steps of 2 dB.
30	BS POWER CONTROL	BSC → BTS	The BS_POWER_CON message is used by the BSC to adjust the output power of the BTS. The value range is 30 dB and is independent of the type of standard (GSM, DCS 1800, PCS 1900). Adjustments can be done in steps of 2 dB.
31	PREPROCess CONFIGure	BSC → BTS	The PREPROC_CONF message is used only when the BTS is in charge to preprocess its own measurements and those received from the MS. In that case, not all measurement results are forwarded to the BSC, but the BTS preprocesses all data and periodically sends only a PREPRO_MEAS_REAS message to the BSC. The details of the preprocessing are manufacturer-dependent and may be configured by the network operator. The PREPROC_CONF message is necessary to coordinate the details of preprocessing between BSC and BTS.
32	PREPROcessed MEASurement RESult	BTS → BSC	See PREPROC_CONF.
33	RF CHannel RELease ACKnowledge	BTS → BSC	The RF_CH_REL_ACK message acknowledges that an RF_CHAN_REL message was received and processed. The BTS has released a previously occupied physical channel.
34	SACCH INFO MODIFY	BSC → BTS	The SACCH_INFO_MODIFY message is used to modify the SYS_INFOS 5 and 6, which are sent during an active connection. The BTS receives the original information about their content in the SACCH_FILL message.

Table 6.7
Coding of the Channel Number

7	6	5	4	3	2	1	0	Possible Values (in Hex)	Channel Type
0	0	0	0	1	X	X	X	0X	TCH (fullrate)
0	0	0	1	S	X	X	X	1X	TCH (halfrate)
0	0	1	S	S	X	X	X	2X, 3X	SDCCH/4
0	1	S	S	S	X	X	X	4X, 5X, 6X, 7X	SDCCH/8
1	0	0	0	0	0	0	0	80	BCCH
1	0	0	0	1	0	0	0	88	Uplink CCCH (RACH)
1	0	0	1	0	0	0	0	90	Downlink CCCH (PCH, AGCH)

Figure 6.25 shows an example of an RF_CHAN_REL message.

Decoding of Abis-Interface Messages (Layers 2 and 3)

Consider the following sequence of hexadecimal numbers taken from a trace on the Abis-interface. As usual, there was no protocol analyzer to decode from hexadecimal to mnemonics. Therefore, the analysis needs to be done "manually."

```
00 03 E2 D3 0C 13 01 88 13 E6 9D AB 11 00
```

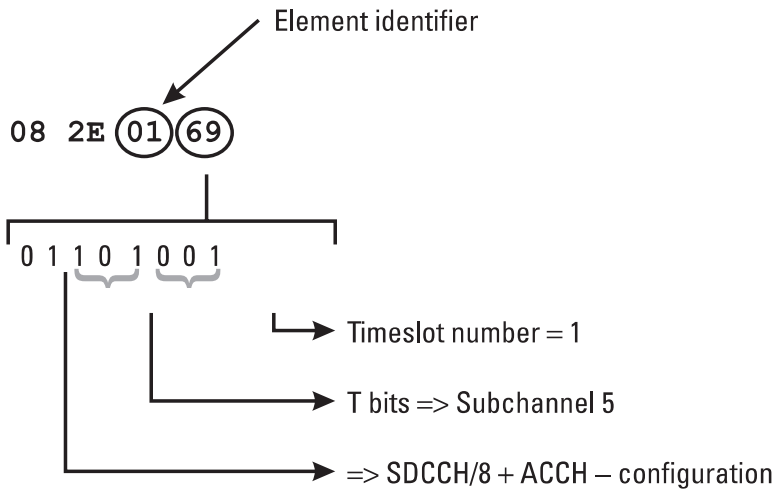


Figure 6.25 The RF_CHAN_REL message in hexadecimal format.

Decoding of Layer 2 Figures 6.6 and 6.7 are necessary to decode the Layer 2 data, illustrated in Figure 6.26. Note carefully that flags and the FCS are not contained in the preceding sequence. That is valid for most messages you will have to decode in your daily work.

Note the shaded bit in the first octet of the control field. That bit identifies the whole frame as an I frame (modulo 128).

The following information can be derived from the address and control fields:

- SAPI = 0 indicates that this is an RSL message.
- C/R = 0 and frame type = I frame indicate that this is a command from the BTS to the BSC.
- P = 1 indicates that the sender of the message expects an acknowledgment (RR frame).
- As indicated in Table 6.3, the frame is readily identified as an I frame by noticing that the first byte of the control field is E2, that is, an even number. That frequently is sufficient to make an identification of the frame type. Other examples are 01 for an RR frame or 03 for a UI frame.

Decoding of Layer 3 Decoding of Layer 3 data (Figure 6.27) on the Abis-interface is performed with the aid of GSM Recommendations 04.08 and 08.58 and with reference to Figure 6.24.

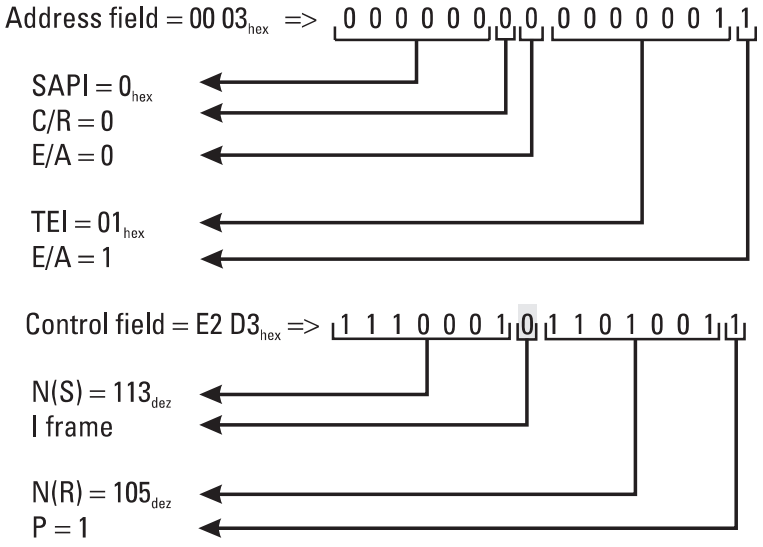


Figure 6.26 The decoding of Layer 2.

00 03 E2 D3	0C 13 01 88 13 E6 9D AB 11 00
Layer 2	Layer 3

Figure 6.27 Layer 2 and Layer 3 of the message.

Layer 3 information follows the address and the control fields, as illustrated in Figures 6.6, 6.7, and 6.24.

Figure 6.24 shows the format of Layer 3 data on the Abis-interface. It begins with one octet for the message discriminator (indicating the message group), one octet for the message type, then two bytes to specify the channel number. The message type determines the interpretation of the remainder of the message. Figure 6.27 would be interpreted as is shown in Figure 6.28 (all data are in hexadecimal).

Therefore, the remaining octets, 13 E6 9D AB 11 00, belong to the connection request of an MS. The decoding is illustrated in Figure 6.29 (taken from GSM 08.58).

6.3.3.2 Layer 3 on the Operation and Maintenance Link (SAPI 62)

Before describing the data format of SAPI 62, it should be mentioned that the differences between the various manufacturers become particularly obvious here. It is possible that in certain cases, the presented formats differ from your actual recordings.

Different data formats have to be used on the OML, the connection between BSC and the O&M unit in the BTS, from those used for connection setup and release. Transfer of operations software to the BTS and forwarding of maintenance commands fall into that category. In particular, for software transfer, a greater amount of data has to be transferred from the BSC to the BTS, which requires the segmentation and sequencing of the messages (refer to OSI Layer 4).

Message discriminator =	'0C'	Common control channel management message
Message type =	'13'	CHAN_RQD
Channel number =	'01 88'	Uplink CCCH (RACH)

Figure 6.28 Identification of the Layer 3 header.

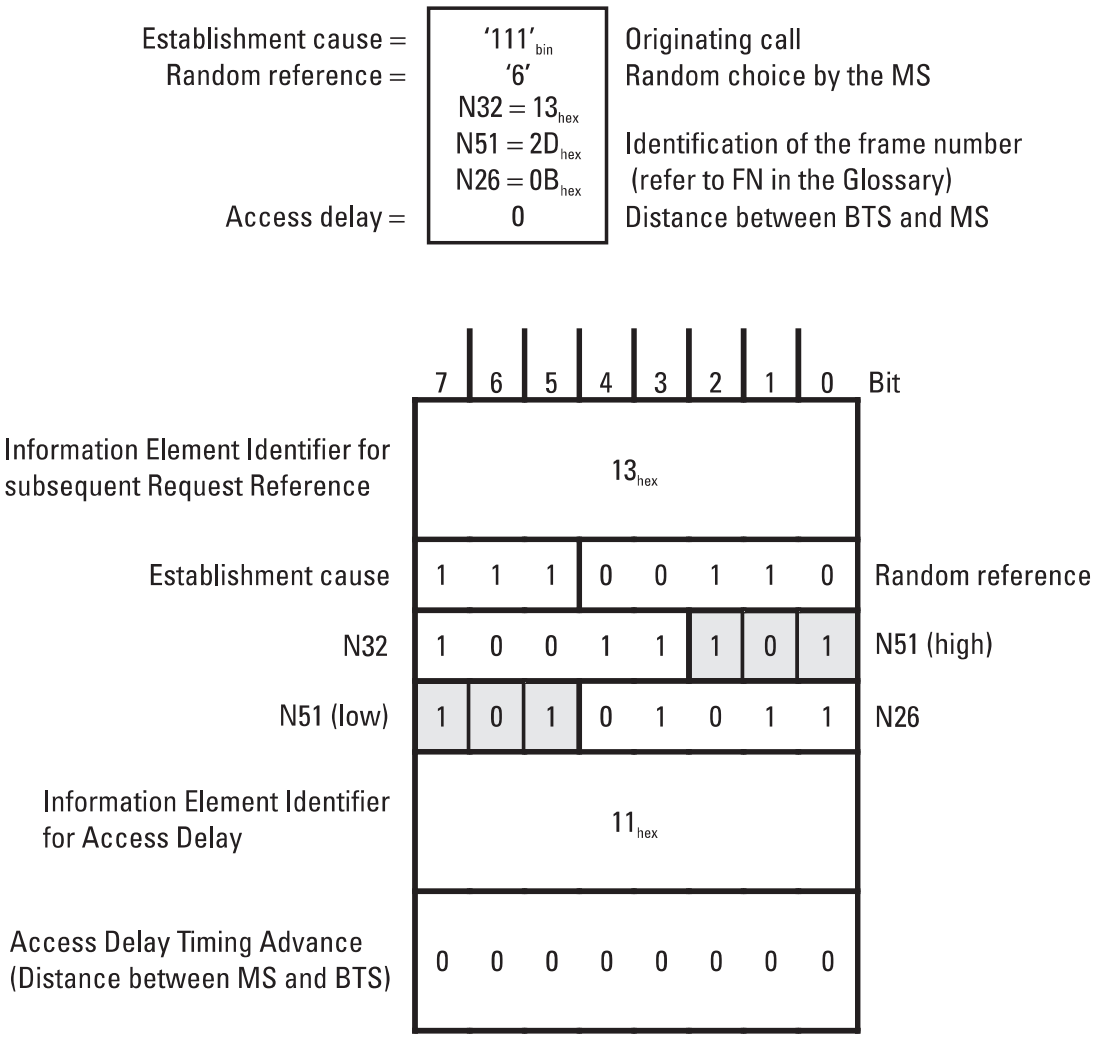


Figure 6.29 Format of a CHAN_RQD message (taken from GSM 08.58).

Although the format depends on the manufacturer, GSM still provides some guidelines in Recommendations GSM 08.59 and GSM 12.21. But because GSM 12.21 only recently has become available, many manufacturers still use their own proprietary protocols. Within those protocols, the manufacturers also implement the higher layers of the OSI model, which are missing on SAPI 0 (RSL).

Figure 6.30 shows the general format for data transfer on the OML.

Frame Structure

The Layer 2 differences for the data destined for SAPI 0, 62, or 63 were demonstrated in the discussion of Layer 2 and are not shown in Figure 6.30 (see Figures 6.6 and 6.7). The first octet of the O&M Layer 3 is an identifier, which

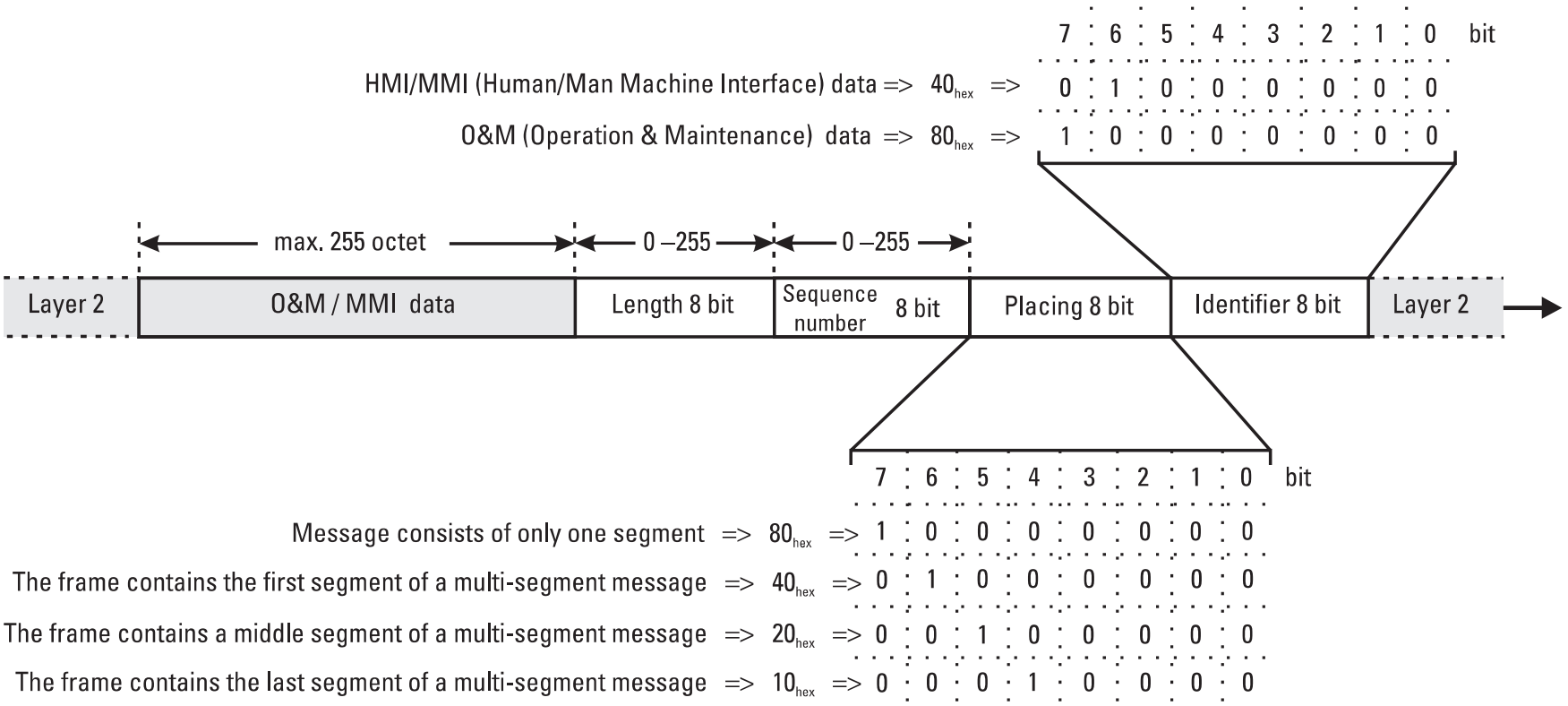


Figure 6.30 Format of Layer 3 on OML (SAPI 62).

Samsung Ex. 1032, Page 94 of 417

distinguishes between HMI data and O&M information. That detail must be noted to ensure the distinction between maintenance communication and data transmission.

The next octet is a placing octet, which indicates to the recipient whether a message is segmented, that is, whether it is made up of a number of submessages. The next parameter is the sequence number, which numbers the segmented messages.

The last octet of the header is a length indicator, which indicates how many octets of O&M data follow.

The O&M communication of the BTS with the BSC is illustrated in Figure 6.31 with the example of a file transfer. All messages shown are I frames. To reduce the clutter of the graphic, the acknowledging RR frames are not shown; normally, they would be present.

HMI Data

The OML also is required to transfer maintenance information to the BTS. The related commands have origins in either the OMC or the BSC.

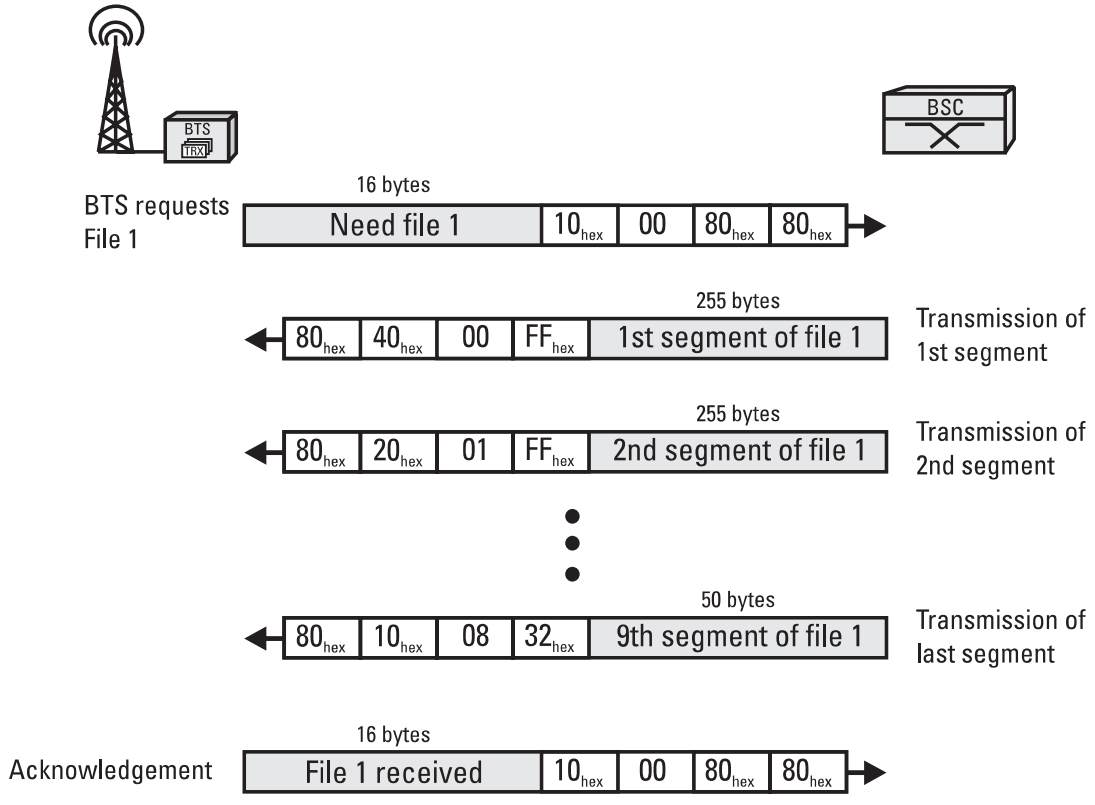


Figure 6.31 File transfer from the BSC to the BTS.

6.4 Bringing an Abis-Interface Into Service

6.4.1 Layer 1

To bring a link between the BTS and the BSC into service, a physical connection first has to be established.

Having a reliable physical link between the BSC and the BTS is the precondition to loading software into the BTS and bringing it up into service. Layer 1 can be tested with any tool capable of measuring bit errors. Another possibility, of course, is to retrieve the link state from the OMC.

6.4.2 Layer 2

When the Layer 1 connection has been established and the hardware on both sides, the BTS and the BSC, is operable, SABME frames can be detected in the time slots for signaling data at both ends, as illustrated in Figure 6.32. Note that these SABMEs are sent by the BSC side. The link establishment procedure then follows.

Data can be transported on the Abis-interface as soon as Layer 2 is operable.

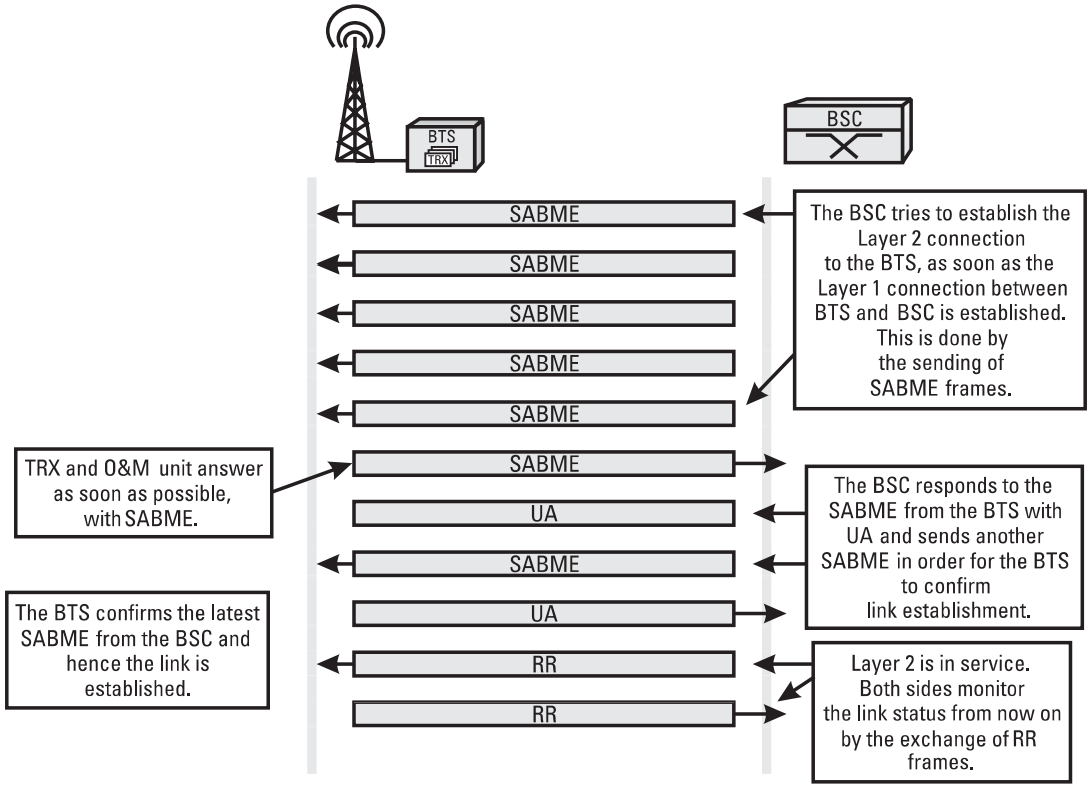


Figure 6.32 An Abis link is brought into service.

7

The Air-Interface of GSM

The Air-interface is the central interface of every mobile system and typically the only one to which a customer is exposed.

The physical characteristics of the Air-interface are particularly important for the quality and success of a new mobile standard. For some mobile systems, only the Air-interface was specified in the beginning, like IS-95, the standard for CDMA. Although different for GSM, the Air-interface still has received special attention. Considering the small niches of available frequency spectrum for new services, the efficiency of frequency usage plays a crucial part. Such efficiency can be expressed as the quotient of transmission rate (kilobits per second) over bandwidth (kilohertz). In other words, how much traffic data can be squeezed into a given frequency spectrum at what cost?

The answer to that question eventually will decide the winner of the recently erupted battle among the various mobile standards.

7.1 The Structure of the Air-Interface in GSM

7.1.1 The FDMA/TDMA Scheme

GSM utilizes a combination of frequency division multiple access (FDMA) and time division multiple access (TDMA) on the Air-interface. That results in a two-dimensional channel structure, which is presented in Figure 7.1. Older standards of mobile systems use only FDMA (an example for such a network is the C-Netz in Germany in the 450 MHz range). In such a pure FDMA system, one specific frequency is allocated for every user during a call. That quickly leads to overload situations in cases of high demand. GSM took into account

Samsung Ex. 1032, Page 97 of 417

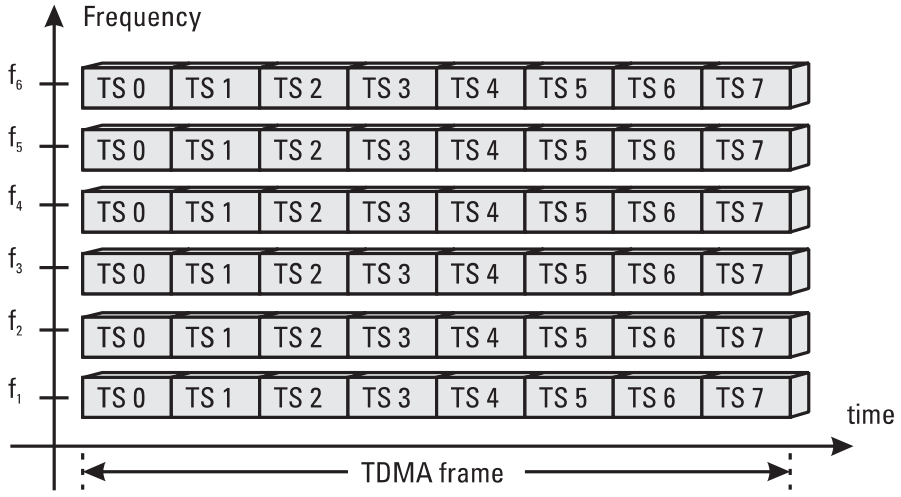


Figure 7.1 The FDMA/TDMA structure of GSM.

the overload problem, which caused most mobile communications systems to fail sooner or later, by defining a two-dimensional access scheme. In fullrate configuration, eight time slots (TSs) are mapped on every frequency; in a halfrate configuration there are 16 TSs per frequency.

In other words, in a TDMA system, each user sends an impulselike signal only periodically, while a user in a FDMA system sends the signal permanently. The difference between the two is illustrated in Figure 7.2. Frequency 1 (f1) in the figure represents a GSM frequency with one active TS, that is, where a signal is sent once per TDMA frame. That allows TDMA to simultaneously serve seven other channels on the same frequency (with fullrate configuration) and manifests the major advantage of TDMA over FDMA (f2).

The spectral implications that result from the emission of impulses are not discussed here. It needs to be mentioned that two TSs are required to support duplex service, that is, to allow for simultaneous transmission and reception. Considering that Figures 7.1 and 7.2 describe the downlink, one can imagine the uplink as a similar picture on another frequency.

GSM uses the modulation technique of Gaussian minimum shift keying (GMSK). GMSK comes with a narrow frequency spectrum and theoretically no amplitude modulation (AM) part. The Glossary provides more details on GMSK.

7.1.2 Frame Hierarchy and Frame Numbers

In GSM, every impulse on frequency 1, as shown in Figure 7.2, is called a burst. Therefore, every burst shown in Figure 7.2 corresponds to a TS. Eight bursts or TSs, numbered from 0 through 7, form a TDMA frame.

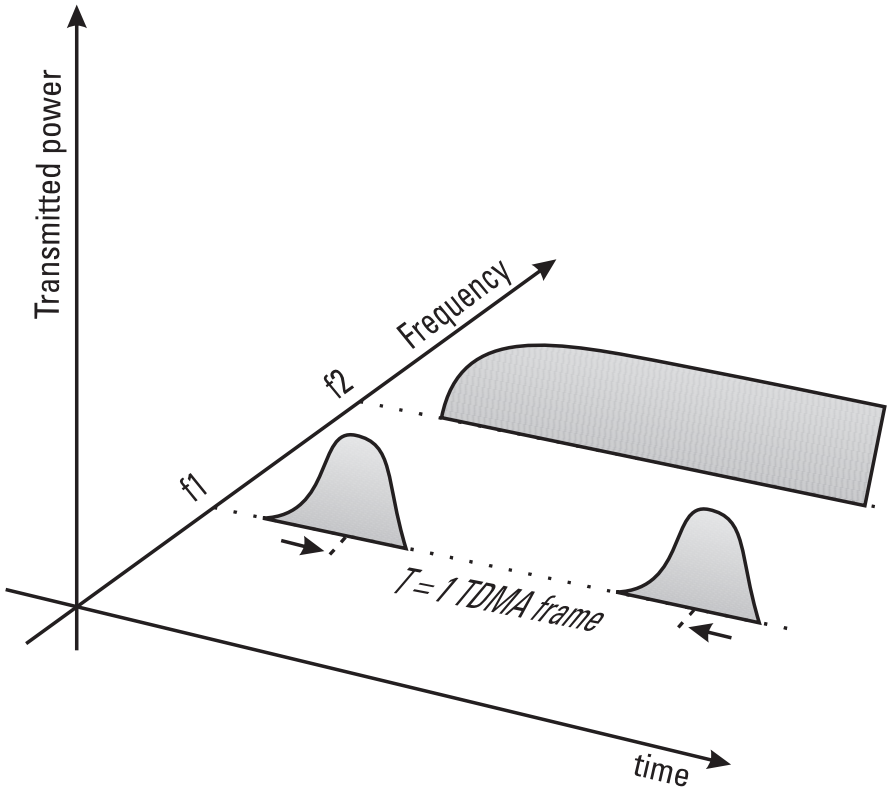


Figure 7.2 Spectral analysis of TDMA versus FDMA.

In a GSM system, every TDMA frame is assigned a fixed number, which repeats itself in a time period of 3 hours, 28 minutes, 53 seconds, and 760 milliseconds. This time period is referred to as hyperframe. Multiframe and superframe are layers of hierarchy that lie between the basic TDMA frame and the hyperframe. Figure 7.3 presents the various frame types, their periods, and other details, down to the level of a single burst as the smallest unit.

Two variants of multiframes, with different lengths, need to be distinguished. There is the 26-multiframe, which contains 26 TDMA frames with a duration of 120 ms and which carries only traffic channels and the associated control channels. The other variant is the 51-multiframe, which contains 51 TDMA frames with a duration of 235.8 ms and which carries signaling data exclusively. Each superframe consists of twenty-six 51-multiframes or fifty-one 26-multiframes. This definition is purely arbitrary and does not reflect any physical constraint. The frame hierarchy is used for synchronization between BTS and MS, channel mapping, and ciphering.

Every BTS permanently broadcasts the current frame number over the synchronization channel (SCH) and thereby forms an internal clock of the BTS. There is no coordination between BTSs; all have an independent clock, except for synchronized BTSs (see *synchronized handover* in the Glossary). An

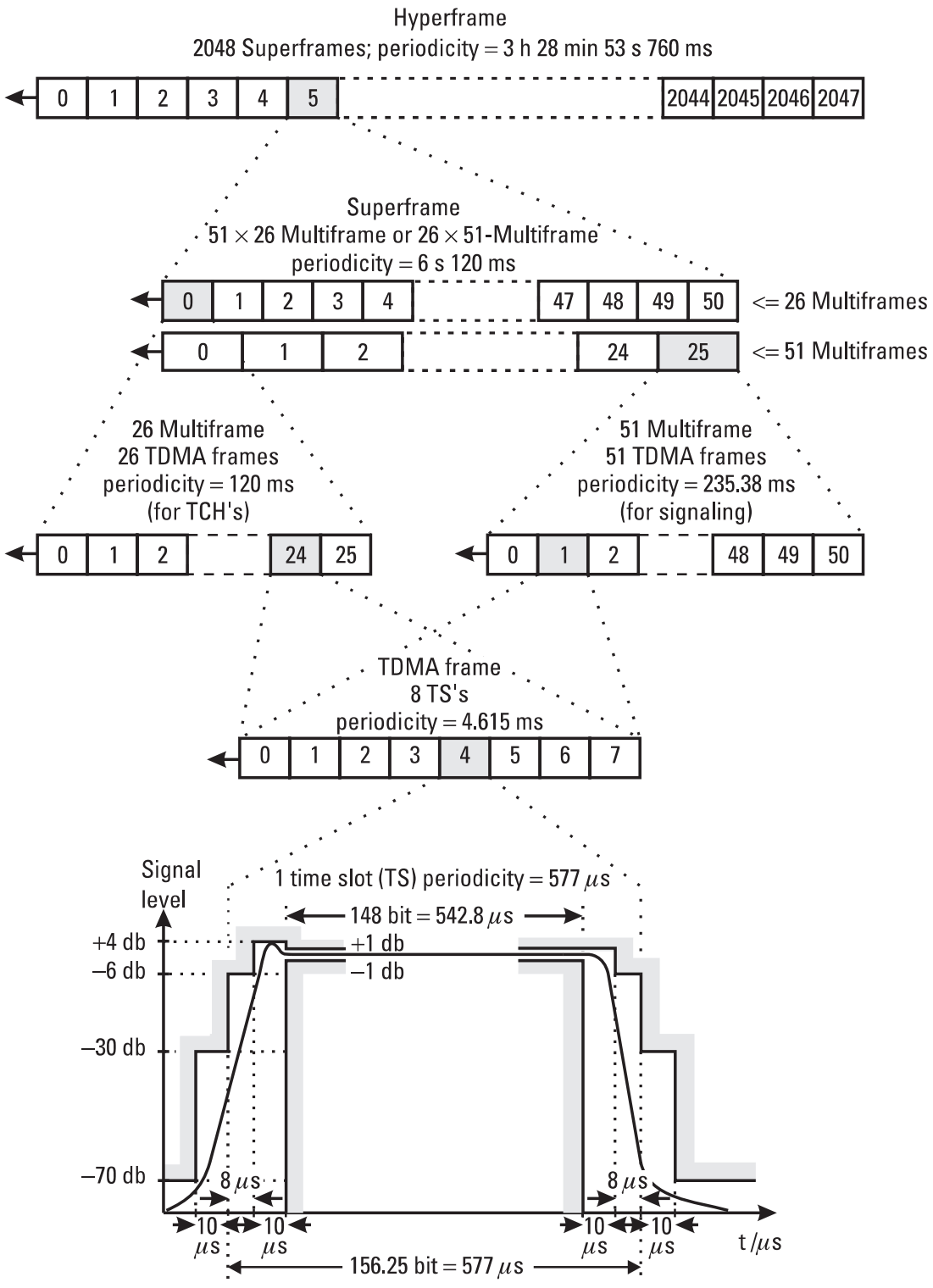


Figure 7.3 Hierarchy of frames in GSM.

MS can communicate with a BTS only after the MS has read the SCH data, which informs the MS about the frame number, which in turn indicates the

chronologic sequence of the various control channels. That information is very important, particularly during the initial access to a BTS or during handover.

Consider this example: an MS sends a channel request to the BTS at a specific moment in time, let's say frame number Y ($t = FN\ Y$). The channel request is answered with a channel assignment, after being processed by the BTS and the BSC. The MS finds its own channel assignment among all the other ones, because the channel assignment refers back to frame number Y.

The MS and the BTS also need the frame number information for the ciphering process. The hyperframe with its long duration was only defined to support ciphering, since by means of the hyperframe, a frame number is repeated only about every three hours. That makes it more difficult for hackers to intercept a call.

7.1.3 Synchronization Between Uplink and Downlink

For technical reasons, it is necessary that the MS and the BTS do not transmit simultaneously. Therefore, the MS is transmitting three timeslots after the BTS. The time between sending and receiving data is used by the MS to perform various measurements on the signal quality of the receivable neighbor cells.

As shown in Figure 7.4, the MS actually does not send exactly three timeslots after receiving data from the BTS. Depending on the distance between the two, a considerable propagation delay needs to be taken into account. That propagation delay, known as timing advance (TA), requires the MS to transmit its data a little earlier as determined by the "three timeslots delay rule."

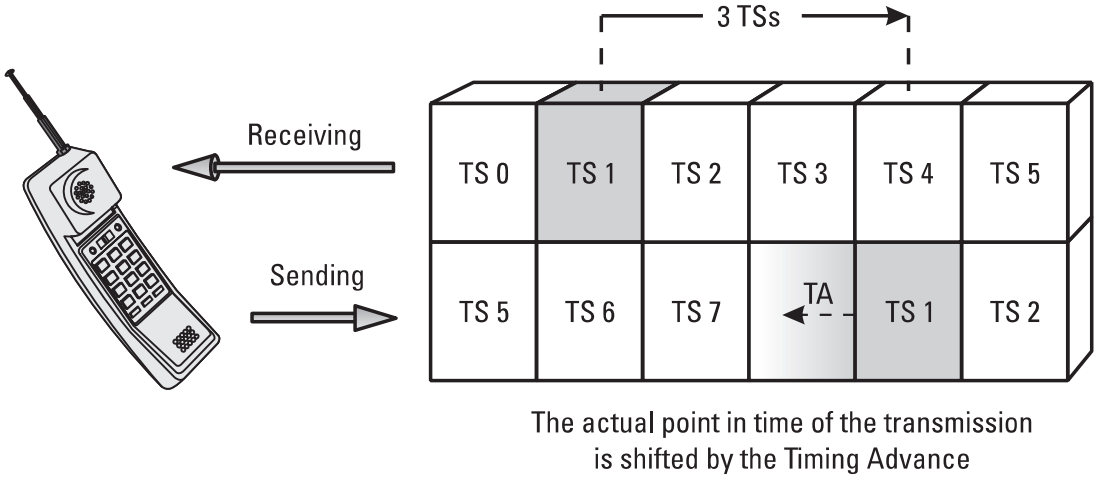


Figure 7.4 Receiving and sending from the perspective of the MS.

The larger the distance between the MS and the BTS is, the larger the TA is. More details are provided in the Glossary under *TA*.

7.2 Physical Versus Logical Channels

Because this text frequently uses the terms *physical channel* and *logical channel*, the reader should be aware of the differences between them.

- Physical channels are all the available TSs of a BTS, whereas every TS corresponds to a physical channel. Two types of channels need to be distinguished, the halfrate channel and the fullrate channel. For example, a BTS with 6 carriers, as shown in Figure 7.1, has 48 (8 times 6) physical channels (in fullrate configuration).
- Logical channels are piggybacked on the physical channels. Logical channels are, so to speak, laid over the grid of physical channels. Each logical channel performs a specific task.

Another aspect is important for the understanding of logical channels: during a call, the MS sends its signal periodically, always in a TDMA frame at the same burst position and on the same TS to the BTS (e.g., always in TS number 3). The same applies for the BTS in the reverse direction.

It is important to understand the mapping of logical channels onto available TSs (physical TSs)—which will be discussed later—because the channel mapping always applies to the same TS number of consecutive TDMA frames. (The figures do not show the other seven TSs.)

7.3 Logical-Channel Configuration

Firstly, the distinction should be made between traffic channels (TCHs) and control channels (CCHs). Distinguishing among the different TCHs is rather simple, since it only involves the various bearer services. Distinguishing among the various CCHs necessary to meet the numerous signaling needs in different situations, however, is more complex. Table 7.1 summarizes the CCH types, and the Glossary provides a detailed description of each channel and its tasks. Note that, with three exceptions, the channels are defined for either downlink or uplink only.

Table 7.1
Signaling Channels of the Air-Interface

Name	Abbreviation	Task
Frequency correction channel (DL)	FCCH	The "lighthouse" of a BTS
Synchronization channel (DL)	SCH	PLMN/base station identifier of a BTS plus synchronization information (frame number)
Broadcast common control channel (DL)	BCCH	To transmit system information 1–4, 7-8 (differs in GSM, DCS1800, and PCS1900)
Access grant channel (DL)	AGCH	SDCCH channel assignment (the AGCH carries IMM_ASS_CMD)
Paging channel (DL)	PCH	Carries the PAG_REQ message
Cell broadcast channel (DL)	CBCH	Transmits cell broadcast messages (see Glossary entry *CB*)
Standalone dedicated control channel	SDCCH	Exchange of signaling information between MS and BTS when no TCH is active
Slow associated control channel	SACCH	Transmission of signaling data during a connection (one SACCH TS every 120 ms)
Fast associated control channel	FACCH	Transmission of signaling data during a connection (used only if necessary)
Random access channel (UL)	RACH	Communication request from MS to BTS

Note: DL = downlink direction only; UL = uplink direction only.

7.3.1 Mapping of Logical Channels Onto Physical Channels

In particular, the downlink direction of TS 0 of the BCCH-TRX is used by various channels. The following channel structure can be found on TS 0 of a BCCH-TRX, depending on the actual configuration:

- FCCH;
- SCH;
- BCCH information 1–4;
- Four SDCCH subchannels (optional);
- CBCH (optional).

This multiple use is possible because the logical channels can time-share TS 0 by using different TDMA frames. A remarkable consequence of the approach is that, for example, the FCCH or the SCH of a BTS is not broadcast permanently but is there only from time to time. Time sharing of the same TS is not limited to FCCH and SCH but is widely used. Such an approach naturally results in a lower transmission capacity, which is still sufficient to convey all necessary signaling data. Furthermore, it is possible to combine up to four physical channels in consecutive TDMA frames to a block, so that it is possible for the same SDCCH to use the same physical channel in four consecutive TDMA frames, as illustrated in Figure 7.5. On the other hand, an SDCCH subchannel has to wait for a complete 51-multiframe before it can be used again.

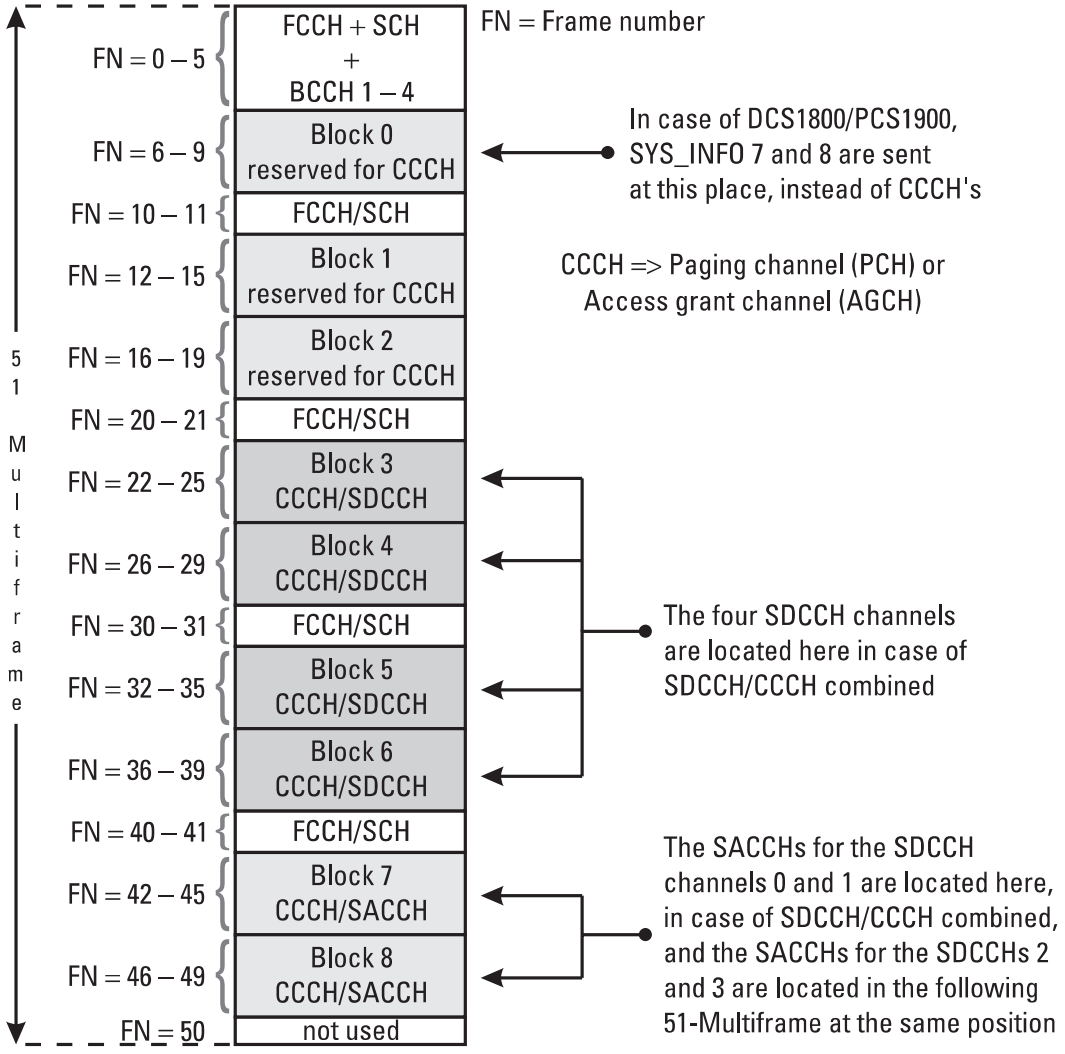


Figure 7.5 Example of the mapping of logical channels.

That clarifies another reason for the frame hierarchy of GSM. The structure of the 51-multiframe defines at which moment in time a particular control channel (logical channel) can use a physical channel (it applies similarly to the 26-multiframe).

Detailed examples are provided in Figure 7.6, for the downlink, and in Figure 7.7, for the uplink. The figures show a possible channel configuration for all eight TSs of a TRX. Both show a 51-multiframe in TSs 0 and 1, with a cycle time of 235.8 ms. Each of the remaining TSs, 2 through 7, carries two 26-multiframes, with a cycle time of $2 \cdot 120$ ms = 240 ms. That explains the difference in length between TS 0 and TS 1 on one hand and TS 2 through TS 7 on the other.

Figures 7.6 and 7.7 show that a GSM 900 system can send the BCCH SYS-INFO 1–4 only once per 51-multiframe. That BCCH information tells the registered MSs all the necessary details about the channel configuration of a BTS. That includes at which frame number a PAG_REQ is sent on the PCH and which frame numbers are available for the RACH in the uplink direction. The Glossary provides more details on the content of BCCH SYS-INFO 1–4.

The configuration presented in Figures 7.6 and 7.7 contains 11 SDCCH subchannels: 3 on TS 0 and another 8 on TS 1. SDCCH 0, 1, … refers to the SDCCH subchannel 0, 1, … on TS 0 or TS 1. The channel configuration presented in the figures also contains a CBCH on TS 0. Note that the CBCH will always be exactly at this position of TS 0 or TS 1 and occupies the frame numbers 8–11. The CBCH reduces, in both cases, the number of available SDCCH subchannels (that is why SDCCH/2 is missing in the example).

The configuration, as presented here, is best suited for a situation in which a high signaling load is expected while only a relatively small amount of payload is executed. Only the TSs 2 through 7 are configured for regular full-rate traffic.

The shaded areas indicate the so-called idle frame numbers, that is, where no information transfer occurs.

7.3.2 Possible Combinations

The freedom to define a channel configuration is restricted by a number of constraints. When configuring a cell, a network operator has to consider the peculiarities of a service area and the frequency situation, to optimize the configuration. Experience with the average and maximum loads that are expected for a BTS and how the load is shared between signaling and payload is an important factor for such consideration.

GSM 05.02 provides the following guidelines, which need to be taken into account when setting up control channels.

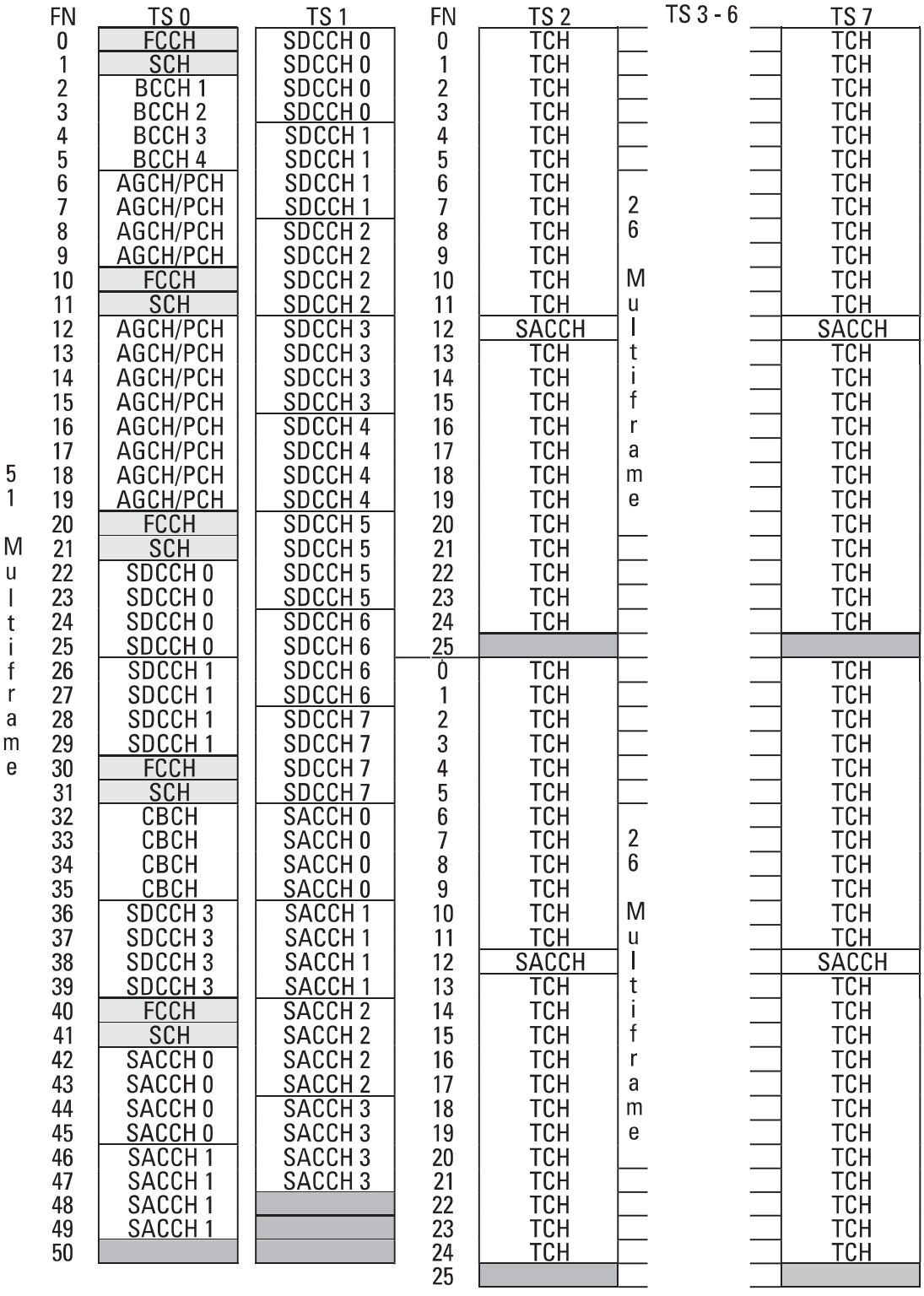


Figure 7.6 Example of the downlink part of a fullrate channel configuration of FCCH/SCH + CCCH + SDCCH/4 + CBCH on TS 0, SDCCH/8 on TS 1, and TCHs on TSs 2–7. The missing SACCHs on TS 0 and TS 1 can be found in the next multiframe, which is not shown here. There is no SDCCH/2 on TS 0, because of the CBCH.

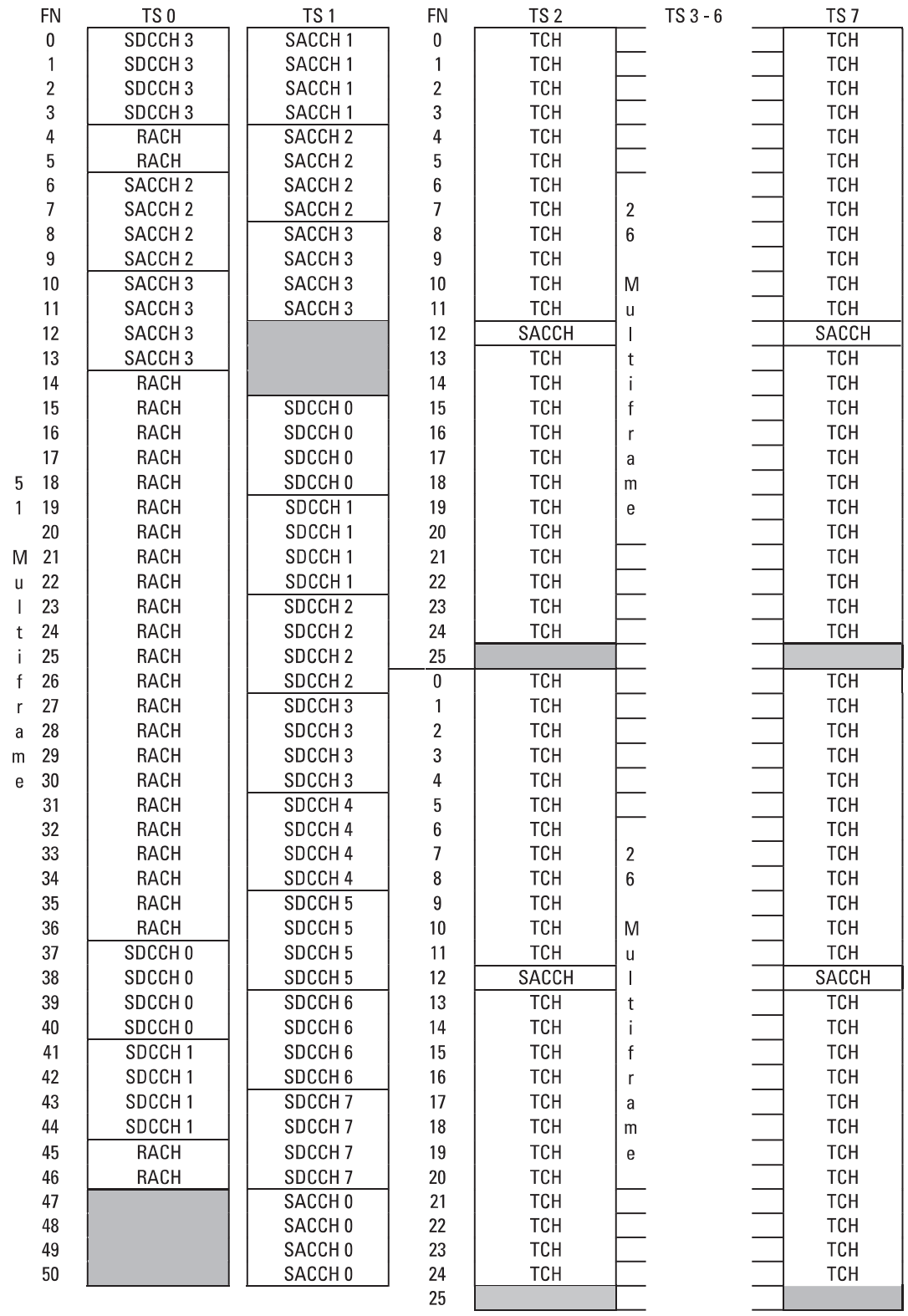


Figure 7.7 Example of the uplink part of a fullrate channel configuration. RACHs can be found only on TS 0 of the designated frame numbers. The missing SACCHs on TS 0 and TS 1 can be found in the next multiframe, which is not shown here.

- The FCCH and the SCH are always sent in TS 0 of the BCCH carrier at specific frame numbers (see Figure 7.5).
- The BCCH, RACH, PCH, and AGCH also must be assigned only to the BCCH carrier. These channels, however, allow for assignment to all even-numbered TSs, e.g., 0, 2, 4, and 6, as well as to various frame numbers.

In practice, two configurations are mainly used, which can be combined if necessary (compare Figure 7.6 and Figure 7.7):

- FCCH + SCH + BCCH + CCCH // SDCCH/8 addresses a channel configuration in which no SDCCH subchannels are available on TS 0. Eight such SDCCH subchannels are defined on TS 1. In that case, TS 1 obviously is not available as a traffic channel.
- FCCH + SCH + BCCH + CCCH + SDCCH/4 addresses a channel configuration in which all control channels are assigned to TS 0, in particular, to have TS 1 available to carry payload traffic. Because TS 0 needs to be used by the other control channels, too, it is possible to establish only four SDCCH subchannels, that is, only half the number compared to the preceding configuration.

A channel configuration is always related to a single TS and not to a complete TRX. It is not possible to combine traffic channels and SDCCHs. If necessary, a TS can be "sacrificed" to allow for additional SDCCHs.

7.4 Interleaving

The preceding descriptions were made under an assumption that is not valid for the Air-interface of GSM. That assumption is that data are transmitted in the order they were generated or received, that is, the first bit of the first (spoken) word is sent first. That is not the case for the Air-interface of GSM. Figure 7.8 illustrates the process of interleaving smaller packages of 456 bits over a larger time period, that is, distributing them in separate TSs. How the packets are spread depends on the type of application the bits represent. Signaling traffic and packets of data traffic are spread more than voice traffic. The whole process is referred to as interleaving.

The goal of interleaving is to minimize the impact of the peculiarities of the Air-interface that account for rapid, short-term changes of the quality of the

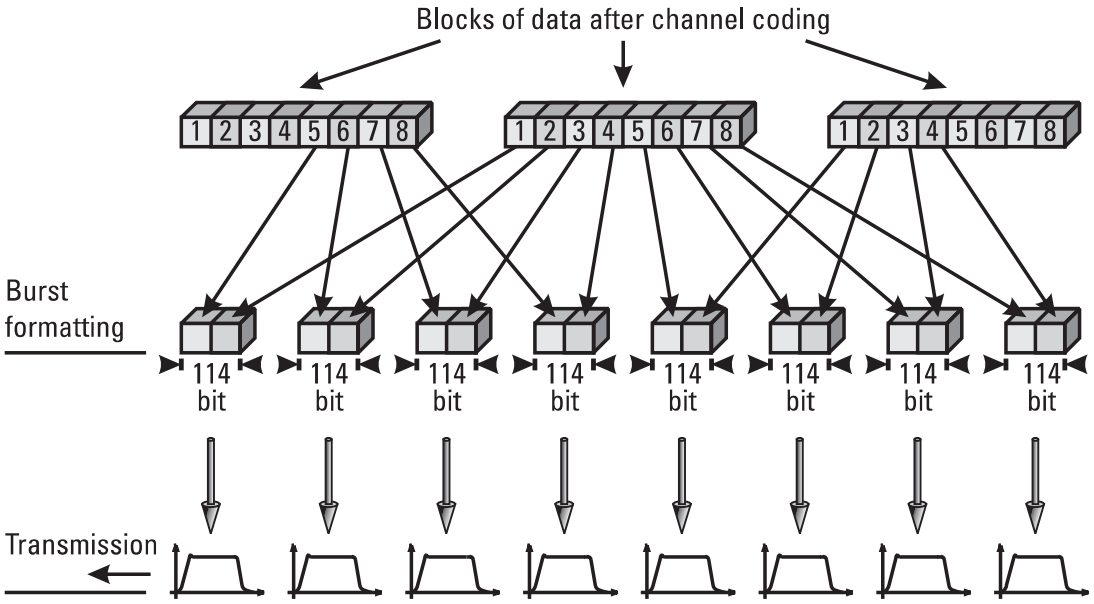


Figure 7.8 Interleaving of speech traffic.

transmission channel. It is possible that a particular channel is corrupted for a very short period of time and all the data sent during that time are lost. That could lead to loss of complete data packets of *n* times 114 bits. Interleaving does not prevent loss of bits, and if there is a loss, the same number of bits are lost. However, because of interleaving, the lost bits are part of several different packets, and each packet loses only a few bits out of a larger number of bits. The idea is that those few bits can be recovered by error-correction mechanisms.

7.5 Signaling on the Air-Interface

7.5.1 Layer 2 LAPD$_m$ Signaling

The only GSM-specific signaling of OSI Layers 1 and 2 can be found on the Air-interface, where LAPD$_m$ signaling is used. The other interfaces of GSM use already defined protocols, like LAPD and SS7.

The abbreviation LAPD$_m$ suggests that it refers to a protocol closely related to LAPD, which is correct. The "m" stands for "modified" and the frame structure already shows the closeness to LAPD. The modified version of LAPD is an optimized version for the GSM Air-interface and was particularly tailored to deal with the limited resources and the peculiarities of the radio link. All dispensable parts of the LAPD frame were removed to save resources. The

$LAPD_m$ frame, in particular, lacks the TEI, the FCS, and the flags at both ends. The $LAPD_m$ frame does not need those parts, since their task is performed by other GSM processes. The task of the FCS, for instance, to a large extent, is performed by channel coding/decoding.

7.5.1.1 The Three Formats of the $LAPD_m$ Frame

Figure 7.9 is an overview of the frame structure of $LAPD_m$. Three different formats of identical length (23 bytes) are defined; their respective uses depend on the type of information to be transferred.

- A-format. A frame in the A-format generally can be sent on any DCCH in both directions, uplink and downlink. The A-format frame is sent as a fill frame when no payload is available on an active connection, for example, in the short time period immediately after the traffic channel is connected.
- B-format. The B-format is used on the Air-interface to transport the actual signaling data; hence, every DCCH and every ACCH use this format. The maximum length of the Layer 3 information to be carried is restricted, depending on the channel type (SDCCH, FACCH, SACCH). This value is defined per channel type by the constant N201. If the information to be transmitted requires less space, this space has to be filled with fill-in octets.
- Bbis-format. For transmission of BCCH, PCH, and AGCH. There is no header in the Bbis-format that would allow for addressing or frame identification. Addressing is not necessary, since BCCH, PCH, and AGCH are CCCHs, in which addressing is not required. In contrast to the DCCH, the CCCH transports only point-to-multipoint messages.

Both frame types, the A-format and the B-format, are used in both directions, uplink and downlink. The Bbis format is required for the downlink only.

Also noteworthy is the relationship for signaling information between the maximum frame length of an $LAPD_m$ frame (= 23 byte ≡ 184 bit) and the number of input bits for channel coding (= 184 bit).

7.5.1.2 The Header of an $LAPD_m$ Frame

The Address Field

The address field starts with the bits EA and C/R, which perform the same tasks as the parameters with the same names in an LAPD frame. The same applies for SAPI, which takes on different values over the Air-interface than on

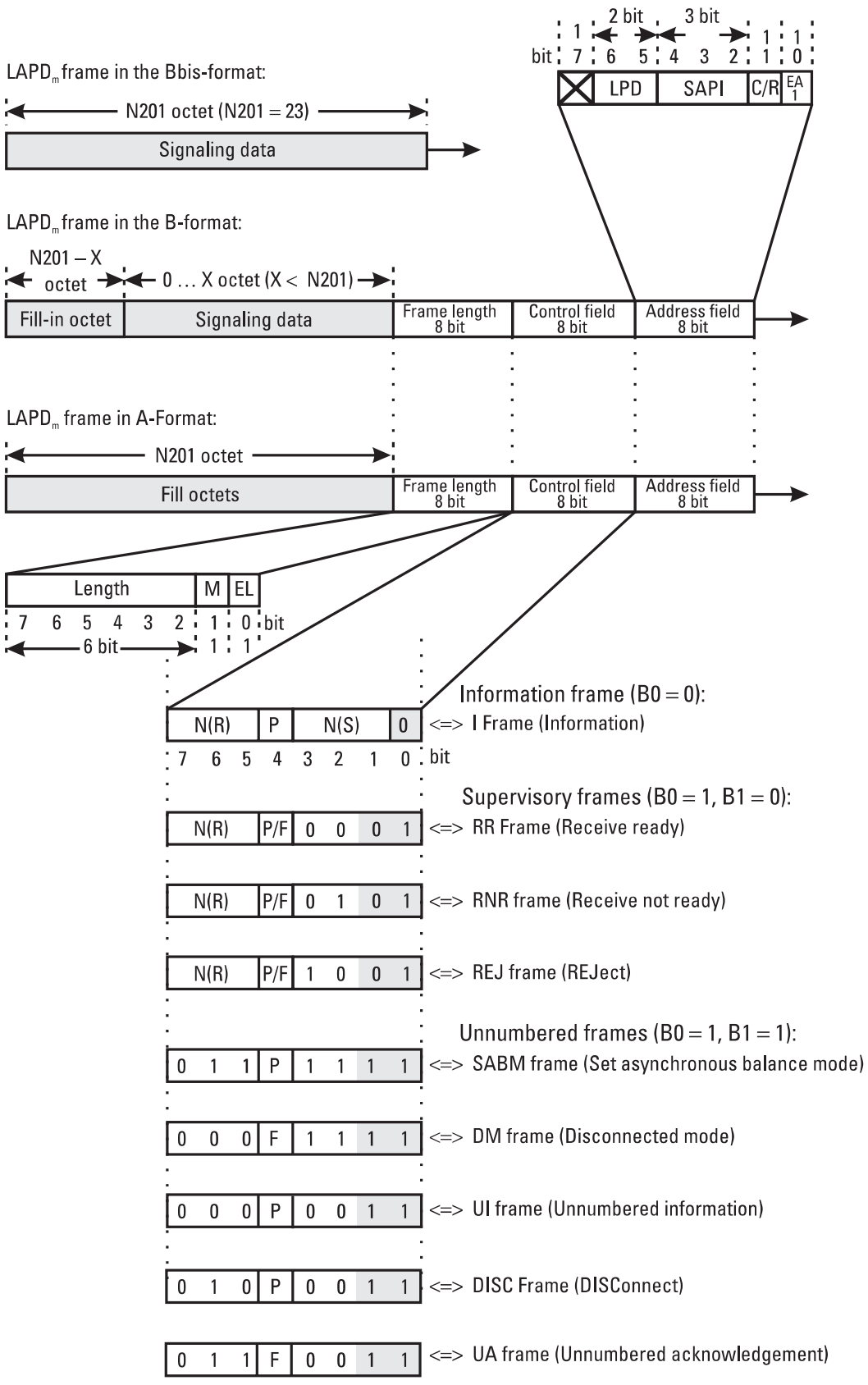


Figure 7.9 Frame format and frame type of $LAPD_m$.

the Abis-interface. Table 7.2 lists the possible values for SAPIs on the Air-interface and their uses. SAPI = 0 is used for all messages that deal with CC, MM, and RR, while SAPI = 3 is used for messages related to supplementary services and the SMS.

Furthermore, the address field of an $LAPD_m$ frame contains the 2-bit-long link protocol discriminator (LPD), which in GSM is, with one exception, always coded with 00_{bin}. The exception is the cell broadcast service (CBS), where LPD = 01_{bin}.

Control Field

The control field of an $LAPD_m$ frame is identical to that of an LAPD frame modulo 8. It defines the frame type and contains, in the case of I frames, the counters for N(S) and N(R); in the case of supervisory frames, it contains only N(R).

The *frame length indicator field* consists of three parts:

- Bit 0, the EL-bit. The EL-bit indicates if the current octet is the last one of the frame length indicator field. When this bit is set to 1, then another length indication octet follows, if set to 0, this octet is the last one. GSM does not allow the frame length indicator field to exceed one octet, and hence, the value of the EL-bit is always zero. GSM may change this restriction, if future applications require a different length.
- Bit 1, the M-bit. If entire messages are longer than the data field of the $LAPD_m$ frames allows, the information has to be partitioned and transmitted in consecutive frames. The M-bit is used in such a situation to indicate that the message was segmented and that further frames belonging to the same messages have to be expected. The M-bit of the last segment is set to zero, as illustrated in Figure 7.10.
- Bits 2–7, the length indicator. This field indicates the actual length of the information field. The value range is from zero to N201.

Table 7.2
Possible Values of SAPI on the Air-Interface

SAPI (Decimal)	Meaning
0	RR, MM, CC
3	SMS, SS

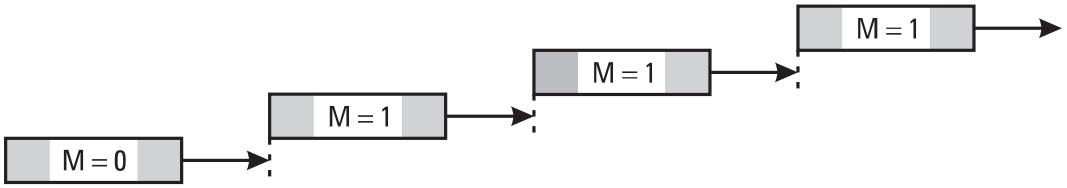


Figure 7.10 Segmentation in $LAPD_m$.

Information Field

For all three frame formats, the information field that carries signaling data consists of N201 octets, where N201 represents a value that is different for the various channel types (see *N201* in the Glossary). How many of the octets—in the case of a B-format—are actually part of Layer 3 depends on the data to be transported. It is important to note that all unused octets in case of the B-format and all octets of the A-format are so-called fill-in octets, which are coded in a precisely defined pattern. This bit pattern is different for uplink and downlink. If, for example, an SDCCH frame contains only 18 bytes of data, the remaining two bytes are occupied with fill-in octets (note that N201 for the SDCCH has a value of 20).

7.5.1.3 Differences Between LAPD and $LAPD_m$

The differences between LAPD and $LAPD_m$ are as follows:

- $LAPD_m$ frames exist in modulo 8 format only. Their control field, therefore, is always 1 octet long. The N(S) and the N(R) are in the range 0 to 7. That theoretically restricts the maximum number of unacknowledged I frames to seven.
- The address field of $LAPD_m$ is only 1 octet long and does not contain a TEI. The reason is that when a channel is already assigned, the connection on the Air-interface is always a point-to-point connection. Several simultaneous users, for example, on a terrestrial point-to-multipoint connection, do not exist, which makes the TEI superfluous.
- $LAPD_m$ frames do not contain an FCS, because channel coding and interleaving of Layer 1 already provide data security.
- $LAPD_m$ frames do not have a flag to indicate the start and end of a frame. That functionality is provided on the Air-interface by Layer 1, in particular by the burst segmentation.
- Unlike in LAPD, SABM frames and UA frames of $LAPD_m$ may even carry Layer 3 data. That saves time during connection setup.

- The maximum lengths of LAPD and $LAPD_m$ frames are very different. While LAPD frames can transport up to 260 octets of signaling data, $LAPD_m$ allows for only 23 octets. If a larger amount of data needs to be transported, segmentation has to be applied.
- $LAPD_m$ frames do not contain a length indicator (Layer 2).
- In LAPD, no fill-in octets are used when the data area is not completely occupied with signaling data.

7.5.1.4 Frame Types of $LAPD_m$

Fewer frame types are defined for the $LAPD_m$ protocol than for LAPD. The XID frame and the FRMR frame are missing in $LAPD_m$. Both frames are used for specific tasks and are not necessary in $LAPD_m$. Table 7.3 lists the frame types of $LAPD_m$ and their specific uses. As for LAPD, it is distinguished whether a frame is used to carry a command, a response, or both. $LAPD_m$ follows the definition of LAPD, that is, the P/F bit and the C/R bits are used the same way for both protocols.

Table 7.3
Frame Types of the Air-Interface

Name	Command Frame?	Answer Frame?	Possible Values of Control Field (Hex)
I-frame group:			
I	Yes	No	(0X), (2X), (4X), (6X), (8X) if even, then I frame
Supervisory-frame group			
RR	Yes	Yes	(1X)
RNR	Yes	Yes	(5X)
REJ	Yes	Yes	(9X)
Unnumbered-frame group			
DISC	Yes	No	(53) because P bit is always 1
UI	Yes	No	(03) because P bit always 0
DM	No	Yes	(0F), (1F)
SABME	Yes	No	(7F) because P bit always 1
UA	No	Yes	(73) because F bit always 1

7.5.2 Layer 3

Figure 7.11 illustrates the Layer 3 format on the Air-interface.

7.5.2.1 Protocol Discriminator

The 4-bit-long protocol discriminator (PD) is used on the Air-interface to classify all messages into groups and allows, within Layer 3, the addressing of various users, just as the message discriminator does on the Abis-interface. Every message is nonambiguously assigned to a PD or service class. A distinction between transparent and nontransparent services is possible at the same time. Supplementary services and the SMS are special, because they do not belong to CC but are still sent with the same PD. Table 7.4 lists all PDs and their service classes.

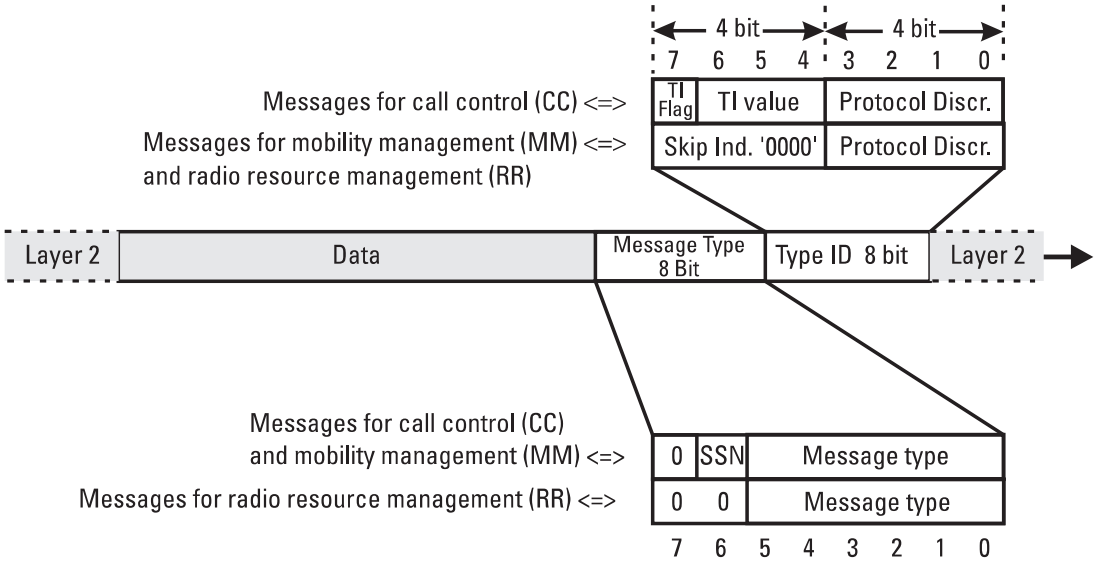


Figure 7.11 The Layer 3 format on the Air-interface.

Table 7.4
Protocol Discriminators on the Air-Interface

PD	Service Class
06	RR (radio resource management)
05	MM (mobility management)
03	CC (call control) SS (supplementary services) SMS (short-message services)

7.5.2.2 Radio Resource Management

Messages in the area of RR are necessary to manage the logical as well as the physical channels on the Air-interface. Depending on the message type, processing of RR messages is performed by the MS, in the BSS, or even in the MSC. Involvement of the BSS distinguishes RR from MM and CC.

7.5.2.3 Mobility Management

MM uses the channels that RR provides, to transparently exchange data between the MS and the NSS. From a hierarchical perspective, the MM lies above the RR, because MM data already are user data. The BSS does not, with a few exceptions, process MM messages. A typical application of MM is location update.

7.5.2.4 Call Control

Like MM, CC uses the connection that RR provides for information exchange. In contrast to MM, which is used only to maintain the mobility of a subscriber, CC is a real application that at the same time provides an interface to ISDN. (The relation between CC and ISDN is discussed in Chapter 10.)

7.5.2.5 Transaction Identifier and Skip Indicator

In CC, the PD is followed by the transaction identifier (TI); in MM and RR, the PD is followed by the skip indicator. The skip indicator in RR and MM messages is a 4-bit-long, fixed coded dummy value with 0000_{bin}. No specific task is assigned to the skip indicator. Messages in which the skip indicator is not 0000_{bin} are ignored by the receiver and indicate a transmission error.

The 4-bit-long TI, on the other hand, can distinguish among several simultaneous transactions of one MS. The format of the TI, shown in Figure 7.11, is separated into the TI flag and the TI value.

The TI flag (bit 7) is used to distinguish between the initiating side and the responding side of a transaction. For the initiating side, the TI flag is set to 0; for the responding side, it has a value of 1. Hence, in a MOC, the TI flags of all CC messages sent from the MS are set to 0. Correspondingly, the TI flags of all CC messages sent from the NSS have a value of 1. In a MTC, the reciprocal applies.

The initiating side also assigns the TI value, which can be in the range of 0 through 6. One TI value is assigned for every transaction, where it is allowed

that the MS and the NSS assign the same TI value to different transactions. The TI flag is used in that case to avoid ambiguity. Several simultaneous transactions are allowed only in the CC protocol, so neither MM nor RR require a TI.

Figure 7.12 illustrates this relation. When the MS is involved in an active call, it places the call on hold and sets up the second call.

7.5.2.6 The Message Type

The value of the protocol discriminator also determines the format of this octet (see Figure 7.11). The first six bits (bits 0 to 5) indicate the message type itself. Section 7.5.2.7 explains all the message types of the Air-interface in more detail. The format of its parameters is shown in Figure 7.13. A distinction is made between mandatory and optional parameters with fixed or variable length, which requires an information element identifier and/or a length indicator.

A special task takes bit number six of the message type. While bits 6 and 7 of the RR are fix-coded with 00_{bin}, bit 6 of MM and CC is held by the send sequence number. No special task is assigned to the send sequence number of MM and CC messages in the downlink direction and is, hence, fix-coded with 0. In the uplink direction, however, the send sequence number of MM and CC messages toggles between a value of 0 and 1. Figure 7.14 provides an example. Note that the send sequence number toggles simultaneously for both CC and MM. The change of the value of the send sequence number is significant for

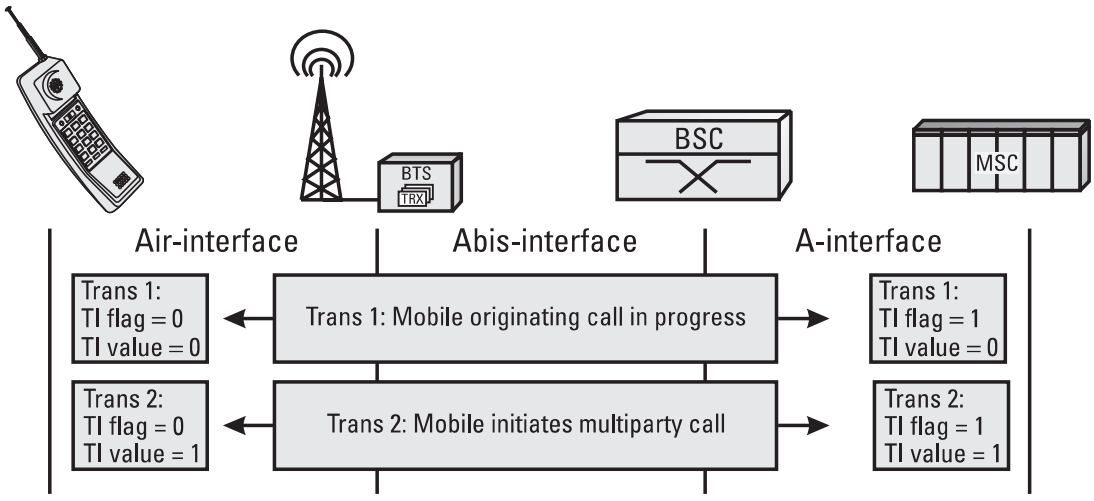


Figure 7.12 Task of the TI in case of several simultaneous CC transactions.

protocol testing, because of two possible values in the uplink direction of MM and CC messages.

7.5.2.7 The Message Type, Bits 0 Through 5

Tables 7.5, 7.6, 7.7, and 7.8 list all the messages that are defined on the Air-interface, together with brief descriptions of their tasks. The messages are ordered according to protocol groups into RR, MM, CC, and supplementary services. Note that two different hexadecimal values for the message type are possible, because of the send sequence number in bit 6 of the message type of MM and CC messages.

The characters in uppercase indicate the abbreviations used in the description.

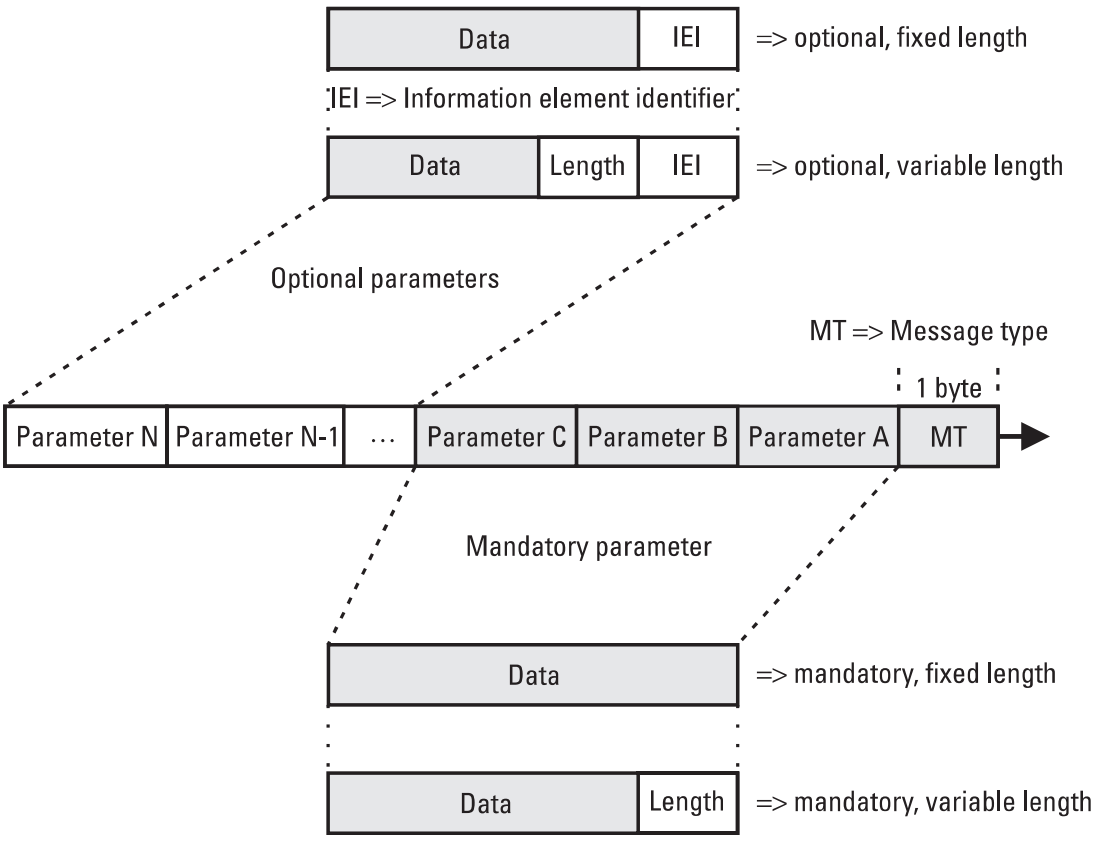


Figure 7.13 Parameter format and Air-interface signaling.

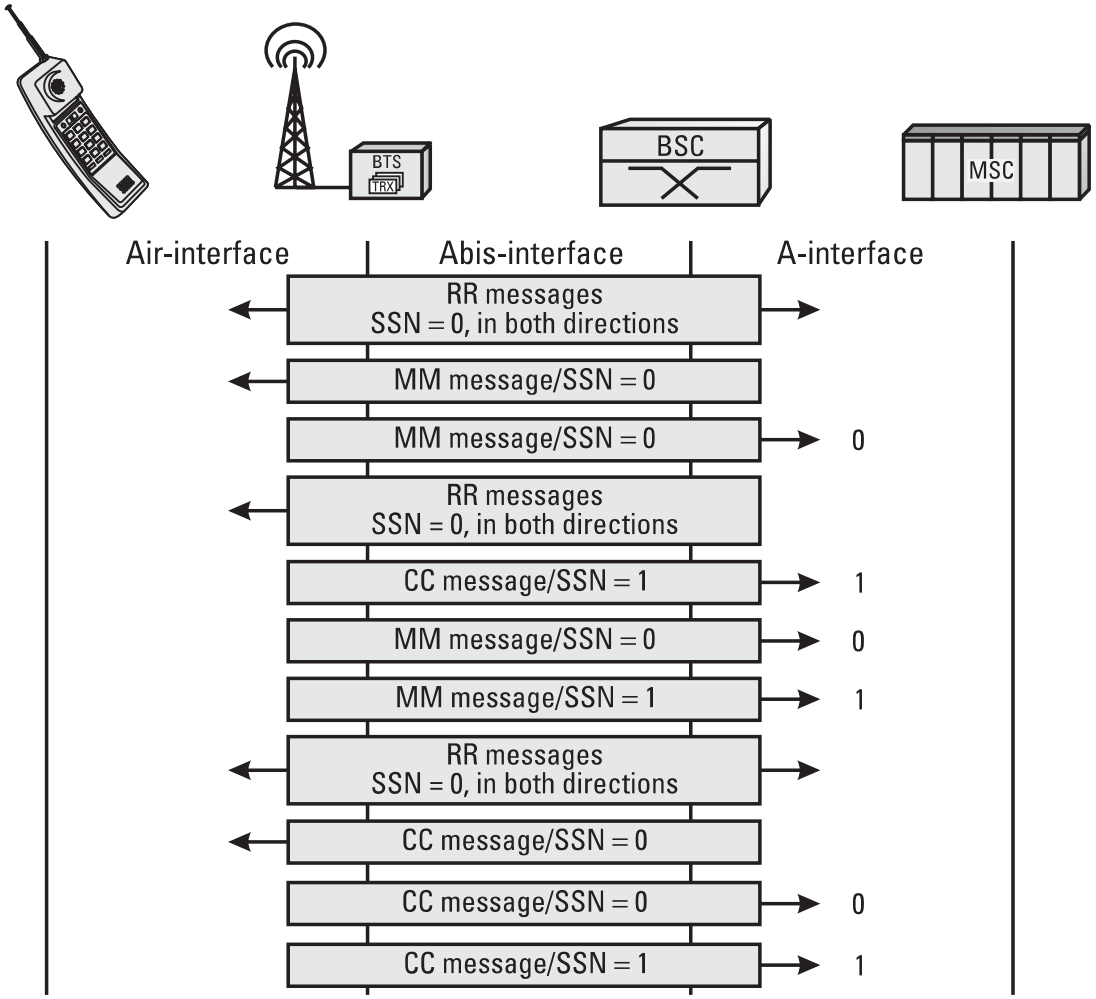


Figure 7.14 Use of the send sequence number.

Table 7.5
Radio Resource Management (Skip Indicator/Protocol Discriminator = 06)

ID (Hex)	Name	Direction	Description
-/-	CHANnel REQuest	MS → BTS	CHAN_REQ is a request of an MS for a channel when in the idle state. Although only 1 byte long this message already contains the reason for the connection request (answer to PAGING, Emergency Call, etc.) and an identifier for the channel type that the MS prefers. The CHAN_REQ has no hexadecimal message type, because the message does not conform to the regular format and is sent via an access burst.

Table 7.5 (continued)

ID (Hex)	Name	Direction	Description
-/-	HaNDover ACCess	MS → BTS	The MS sends consecutive HND_ACC messages on a new traffic channel for every handover (synchronized and nonsynchronized). The only exception is the intra-BTS handover via ASS_CMD. Like the CHAN_REQ, the HND_ACC does not follow the standard format and is sent in an access burst to the BTS. The handover reference is the only information that HND_ACC contains and is assigned with the HND_CMD message to allow for identification of the "correct" MS during BTS access.
02	SYStem INFOrmation 2bis	BTS → MS	The data area of the SYS_INFO 2 is not large enough to allow for distinction of the larger number of channels of DCS 1800, PCS 1900, and also GSM900 with extended band. Hence, SYS_INFO 2bis and 2ter were defined to broadcast, in particular, the frequencies of the neighbor cells, which do not fit into SYS_INFO 2
03	SYStem INFOrmation 2ter	BTS → MS	See SYS_INFO 2bis
05	SYStem INFOrmation 5bis	BTS → MS	The same restrictions for SYS_INFO 2 also apply to SYS_INFO 5, which had to be extended by SYS_INFO 5bis and 5ter to accommodate the greater number of channels of DCS 1800, PCS 1900, and GSM900 with extended band. Hence, SYS_INFO 5bis and 5ter mainly transport the BCCH frequencies of the neighboring cells, which do not fit into SYS_INFO 5. The messages are sent to the MS over the SACCH when an active connection exists.
06	SYStem INFOrmation 5ter	BTS → MS	See SYS_INFO 5bis
0A	PARTial RELease	BTS → MS	When an MS has activated two radio channels at the same time, and CC wants to release one channel, a PART_REL message is sent. For the time being, this is defined only for two halfrate channels.
0D	CHANnel RELease	BTS → MS	The CHAN_REL message is used when a connection is disconnected, to release the radio resources on the air interface. Cause 0 is used for normal clearing; for abnormal clearing, for instance, cause 1 is used.
0F	PARTial RELease COMplete	MS → BTS	With this message, the MS confirms receipt and processing of a PART_REL message.

Table 7.5 (continued)

ID (Hex)	Name	Direction	Description
10	CHANnel MODe MODify	BTS → MS	CHAN_MOD_MOD is sent by the network to the MS, to modify the transmission parameters of Layer 1 (change the transmission rate).
12	RR STATUS	MS ↔ BTS	A RR_STATUS message with an appropriate error cause is sent when one side receives an RR that has an error in Layer 3. These kind of protocol errors happen, for example, in case of bit errors on the air interface.
13	CLASSmark ENQuiry	BTS → MS	The network requests the technical identification (power class, available encryption algorithms A5/X, SMS capability, etc.) from the MS. The network expects a CLASS_CHANGE message as a response.
14	FREQuency REDEFinition	BTS → MS	The FREQ_REDEF message allows the network to change the configuration of an existing connection, e.g., the hopping sequence in frequency hopping.
15	MEASurement REPort	MS → BTS	MEAS_REP transfers the current measurement results of the MS to the BTS (uplink measurements). These measurements contain the sending levels of the serving cell and of the neighboring cells. In the case of an active connection, a MEAS_REP is sent to the BTS every 480 ms via the SACCH. The BTS forwards the MEAS_REP to the BSC, embedded in its own measurement results (MEAS_RES).
16	CLASSmark CHANGE	MS → BTS	The MS sends this message when the classmark changes (e.g., when a handheld phone is connected to a booster in a car) or when a request is made by the network (CLASS_ENQ). It contains the current technical capabilities of the MS.
17	CHANnel MODe MODify ACKnowledge	MS → BTS	The MS confirms with CHAN_MOD_MOD_ACK the change to another transmission mode that was requested with CHAN_MOD_MOD.
18	SYStem INFOrmation 8	BTS → MS	See SYS_INFO 7.
19	SYStem INFOrmation 1	BTS → MS	Contains the access rights and frequencies of a BTS. The Glossary provides an example for a BCCH/SYS_INFO 1.
1A	SYStem INFOrmation 2	BTS → MS	Transmission of neighbor cell frequencies, access rights (e.g., access control class), and network color code (NCC). The Glossary provides an example of BCCH/SYS_INFO 2.

Table 7.5 (continued)

ID (Hex)	Name	Direction	Description
1B	SYStem INFOrmation 3	BTS → MS	Identification of the BTS (cell identity) and the location area and further information about organization of the CCCHs within the BTS. The Glossary provides an example of a BCCH/SYS_INFO 3.
1C	SYStem INFOrmation 4	BTS → MS	SYS_INFO 4 only repeats information of data already sent in the SYS_INFOs 1 - 3.
1D	SYStem INFOrmation 5	BTS → MS	The BTS uses SYS_INFO 5 (via SACCH) to inform the MS, during an active connection, about the BCCH frequencies of the available neighbor cells. This is particularly important after a handover when the MS cannot read the SYS_INFOs 1–4 of the new BTS.
1E	SYStem INFOrmation 6	BTS → MS	During an active connection, the current BTS (serving cell) provides the MS with all the necessary data of the serving cell by means of the SYS_INFO 6 (via SACCH).
1F	SYStem INFOrmation 7	BTS → MS	SYS_INFO 7 and 8 are used only for DCS1800 and PCS1900 to provide the registered MSs with additional information to access the serving cell (cell selection parameters).
21	PAGing REQuest Type 1	BTS → MS	Three different PAG_REQ messages were defined for activation of the MS in the case of an MTC. The difference between the messages lies simply in the number of MSs that can be paged simultaneously with one message (PAG_REQ 1 allows paging of two MSs, PAG_REQ 2 allows paging of three MSs, PAG_REQ 3 allows paging of four MSs). Consequently, the according number of IMSIs/TMSIs are contained in a PAG_REQ. Note that the IMSI is not contained in the PAG_REQ if a TMSI is assigned, even though the PAGING message on the A-interface contains both parameters.
22	PAGing REQuest Type 2	BTS → MS	
24	PAGing REQuest Type 3	BTS → MS	
27	PAGing ReSPonse	MS → BTS	PAG_RSP is the first message sent by the MS on the SDCCH to the BTS in an MTC. PAG_RSP corresponds to the CM_SERV_REQ message of a MOC.
28	HaNDover FAIlure	MS → BTS	After an unsuccessful handover initiated by a HND_CMD, the MS sends a HND_FAI over the still existing connection to the old BTS.
29	ASSignment COMplete	MS → BTS	The MS confirms that it successfully changed to the (new) traffic channel, that is, the one previously assigned by an ASS_CMD message.

Table 7.5 (continued)

ID (Hex)	Name	Direction	Description
2B	HaNDover CoMmanD	BTS → MS	Channel assignment for a handover in which the BTS changes is always performed with HND_CMD; in an intra-BTS handover, the HND_CMD can be used. The message contains a description of the new traffic channel and the handover reference.
2C	HaNDover COMplete	MS → BTS	After successful handover initiated by a HND_CMD, the MS responds to the BTS with a HND_COM.
2D	PHYSical INFOrmation	BTS → MS	PHYS_INFO is the only message actually generated by the BTS. It is used in case of a nonsynchronized handover and is sent to the MS on the new channel *Ny1* times. The content of the PHYS_INFO consists of the TA that the MS has to use initially.
2E	ASSignment CoMmanD	BTS → MS	Assignment of a traffic channel in case of an intracell handover or during call setup.
2F	ASSignment FAIlure	MS → BTS	The MS was not successful in changing to the channel specified in the ASS_CMD message. It has, therefore, changed back to the previously used channel and reports the failed access in a ASS_FAI message.
32	CIPHering MODe COMplete	MS → BTS	The MS confirms that a CIPH_MOD_CMD was received and that it has changed to the cipher mode.
35	CIPHering MODe CoMmanD	BTS → MS	The content of the CIPH_MOD_CMD message originates from the VLR. It is part of the ENCR_CMD message on the Abis-interface. The BTS informs the MS with CIPH_MOD_CMD that all data in both, uplink, and downlink are to be encrypted. The only content is the information as to which encryption algorithm A5/X shall be used.
39	IMMediate ASSignment EXTended	BTS → MS	The task of the IMM_ASS_EXT message is similar to that of the IMM_ASS_CMD message. The difference between the two is that the IMM_ASS_EXT message allows assignment of an SDCCH simultaneously for two MSs. That allows the network to reduce the number of messages. It is particularly helpful when the number of available AGCHs is low.
3A	IMMediate ASSignment REJect	BTS → MS	The BSC may answer a CHAN_REQ message with IMM_ASS_REJ if no SDCCHs are available. In this case, no channel is assigned and the MS is informed about a waiting period, during which it may not send a subsequent CHAN_REQ.

Table 7.5 (continued)

ID (Hex)	Name	Direction	Description
3B	ADDitional ASSignment	BTS → MS	There are some cases in which it may become necessary to assign a second halfrate traffic channel when one halfrate channel is already established, for example, to extend the bandwidth of the current connection for data transfer. In that case, the network sends to the MS an ADD_ASS message describing the new channel.
3F	IMMediate ASSignmnent CoMmanD	BTS → MS	The BSC uses the IMM_ASS_CMD to assign an SDCCH to the MS after a CHAN_REQ message was received. IMM_ASS_CMD is always sent on an AGCH. The message has to be distinguished from ASS_CMD, which is used to assign a traffic channel.

Table 7.6
Mobility Management (Skip Indicator/Protocol Discriminator = 05)

ID (Hex)	Name	Direction	Description
01/41	IMSI DETach INDication	MS → BTS	If IMSI attach/detach is allowed in the PLMN, then every time the MS is switched off the MS sends a IMSI_DET_IND to the MSC/VLR. This allows to more quickly reject an incoming call, or apply secondary call treatment, i.e., without sending PAG_REQ's first.
02	LOCation UPDating ACCept	BTS → MS	The MSC/VLR confirms a successful Location Update with a LOC_UPD_ACC. In some cases the LOC_UPD_ACC is used to assign a new TMSI as well.
04	LOCation UPDating REJect	BTS → MS	If a Location Update is not successful, (e.g., HLR is not reachable, IMSI or TMSI are unknown, etc.), then the MSC/VLR terminates the process with a LOC_UPD_REJ.
08/48	LOCation UPDating REQuest	MS → BTS	The MS sends the LOC_UPD_REQ to the MSC/VLR when it changes the Location Area, when Periodic Location Update is active, and when the MS is switched on again (with active IMSI attach/detach). LOC_UPD_REQ is part of the Location Update procedure.
11	AUTHentica-tion REJect	BTS → MS	The AUTH_REJ message is used to inform the MS that authentication was not successful if the MSC/VLR found that the result for SRES from the MS was incorrect.

Table 7.6 (continued)

ID (Hex)	Name	Direction	Description
12	AUTHentication REQuest	BTS → MS	The MSC/VLR sends an AUTH_REQ message during connection setup, in order to authenticate the MS. The only parameter is RAND.
14/54	AUTHentication ReSPonse	MS → BTS	Answer to AUTH_REQ. It contains the authentication result SRES, which was determined by applying the values of K_i and RAND to the algorithm A3.
18	IDENTity REQest	BTS → MS	Although IDENT_REQ generally allows to request all three identification numbers from the MS, (IMSI, TMSI, and IMEI,) it is typically used by the Equipment Identity Register to request the IMEI only.
19/59	IDENTity ReSPonse	MS → BTS	IDENT_RSP is the answer to IDENT_REQ. The MS provides the network with the requested identification numbers (IMSI, TMSI, IMEI), which were requested in the IDENT_REQ message.
1A	TMSI REALlocation CoMmanD	BTS → MS	For every new connection, the VLR assigns a new TMSI to the MS in order to make tracking and interception of a subscriber more difficult. For this purpose, after the ciphering is active, the TMSI_REAL_CMD message is sent to the MS at any arbitrary position within the scenario.
1B/5B	TMSI REALlocation COMplete	MS → BTS	The MS confirms the receipt of a TMSI with a TMSI_REAL_COM.
21	CM SERVice ACCept	BTS → MS	Is used by the MSC if ciphering is not active or after the establishment of a second simultaneous CC connection. CM_SERV_ACC confirms to the MS that the service request, sent to the MSC in a CM_SERV_REQ message, was processed and accepted.
22	CM SERVice REJect	BTS → MS	The service request in which the MS has sent in a CM_SERV_REQ message is rejected by the MSC. The reason (e.g., overload) is provided.
23/63	CM SERVice ABOrt	MS → BTS	Is sent if a MS wants to terminate a MM connection. The CM_SERV_ABO can only be sent during a very narrow time window, because this message can only be used prior to the fist CC message sent.
24/64	CM SERVice REQuest	MS → BTS	The MS sends a CM_SERV_REQ at the beginning of every mobile originated connection in order to provide its identity (IMSI/TMSI) to the NSS, and to specify the service request in more detail (activation SS, MOC, Emergency Call, and SMS).

Table 7.6 (continued)

ID (Hex)	Name	Direction	Description
28/68	CM REeStab-lishment REQuest	MS → BTS	An option in GSM is to allow for a call reestablishment in case of a dropped connection. In these cases, first a CHAN_REQ has to be sent to the BTS and then it is tried with the CM_RES_REQ to reestablish an RR connection for the still existing and active MM and CC connection.
29	ABORT	BTS → MS	Is sent to the MS in order to release all MM connections. A possible reason is that the mobile equipment was identified as stolen (IMEI check). If this is actually the reason for sending ABORT, then the mobile equipment automatically blocks the Subscriber Identity Module. The SIM can, however, after switching off/on be used again.
31/71	MM STATUS	MS ↔ BTS	If one side receives a message for Mobility Management, which contains a protocol error in Layer 3, then an MM STATUS message with the respective error cause is sent. This kind of protocol error may be caused by bit errors on the Air-interface.

Table 7.7
Call Control (Transaction Identifier/Protocol Discriminator = X3)

ID (Hex)	Name	Direction	Description
01/41	ALERTing	MS ↔ BTS	The MSC sends this message in case of a Mobile Originating Call to the MS. In case of a Mobile Terminating Call, the MS sends an ALERT to the MSC. ALERT corresponds to the Address Complete Message (ACM) of ISUP and is responsible for the generation of a ring back tone at the receiving end. ALERT is always sent to that side of the call, which initiated it. This is important for protocol analysis.
02	CALL PROCeeding	BTS → MS	Is sent by the MSC in case of a Mobile Originating Call, in order to inform the MS that the address information which the MS has sent to the MSC in the SETUP message was received and processed. From the perspective of the MSC, CALL_PROC can be regarded as a confirmation that the ISUP Initial Address Message (IAM) was sent. The consequence for the MS is that the MSC does not need, or is not even able to process additional address information.

Table 7.7 (continued)

ID (Hex)	Name	Direction	Description
03	PROGRESS	BTS → MS	If, for a Mobile Originating Call, interworking or transport of inband signaling should become necessary, then the PROGRESS message is sent instead of ALERT. Examples are calls to automated information services or voice-mail boxes. In this case, the PROGRESS message can be regarded as a substitute for ALERT.
05/45	SETUP	MS ↔ BTS	When initiating a Mobile Originating Call, this message is sent by the MS to the MSC. The most important information are the address information of the called party and the type of connection, which is requested (Bearer Capabilities). In case of a Mobile Terminating Call, the MSC sends a SETUP message to the MS. When CLIP (Calling Line Identification Presentation) is active for the called party and is not restricted by the calling party, then the SETUP message also contains the directory number of the caller. The SETUP message is, furthermore, used to activate the Call Waiting tone (Supplementary Service) at the MS.
07/47	CONnect	MS ↔ BTS	The MSC sends this message during a Mobile Originating Call to the MS, to indicate that the connection was successfully established. The MS receiving the CON message corresponds to the MSC receiving the ISUP Answer Message (ANM). The MS sends a CON message to the MSC in case of a mobile terminanting call, as soon as the called party accepts the call.
08/48	CALL CONFirmed	MS → BTS	After receiving a SETUP message during a Mobile Terminating Call scenario, the MS confirms to the MSC in a CALL_CONF that it is able to establish the requested connection (Bearer Service, halfrate/fullrate, baud rate, etc.).
0E/4E	EMERGency SETUP	MS → BTS	This message is sent by the MS in case of an Emergency Call instead of a regular SETUP to carry address information.
0F/4F	CONnect ACKnowledge	MS ↔ BTS	CON_ACK is acknowledgment for a CON message. A call set up is regarded to be successful only after this message was sent. In particular charging starts typically with the CON_ACK message.

Table 7.7 (continued)

ID (Hex)	Name	Direction	Description
10/50	USER INFOrmation	MS ↔ BTS	It is possible in some cases to directly exchange data between the MS and its peer (e.g., ISDN or other MS). The maximum length of the transported payload is 128 octet, within GSM. For transport between GSM and some outside network, this maximum length may be restricted even further, depending on the capabilities of that other network (between 32 octet and 128 octet).
13/53	MODify REJect	MS ↔ BTS	MOD_REJ is the negative response to a MOD message. If the MS is unable to perform the adaptation which was requested by the peer, then the MS or the MSC respectively answers with a MOD_REJ. The reject cause is included in the message.
17/57	MODify	MS ↔ BTS	In some cases, it may become necessary to change the transmission parameters of an existing connection. This applies in particular, when a change from speech to data is made (Bearer Services 61 and 81). The MOD message carries out this task.
18/58	HOLD	MS → BTS	The HOLD message is used to put a call on hold when the user of a MS, while engaged in an active call, receives a second incoming call or wants to set up another call (Multiparty). Then the HOLD message is sent to the MSC. Hold is also the name of the related Supplementary Service.
19	HOLD ACKnowledge	BTS → MS	Acknowledgment by the MSC that a call was placed in the hold state after a HOLD message was received.
1A	HOLD REJect	BTS → MS	The MSC was unable to place a call into hold state. Therefore, the HOLD message is answered with a HOLD_REJ. The reason for this rejection is given in the cause value.
1C/5C	RETRIEVE	MS → BTS	The MS sends this message in order to reactivate a connection which was previously placed on hold.
1D	RETRIEVE ACKnowledge	BTS → MS	The MSC confirms that it has received and processed the RETRIEVE message. The call which was placed on hold is now active again.
1E	RETRIEVE REJect	BTS → MS	It is not possible to switch back to a call that was put on hold. The RETRIEVE request gets a negative response.

Table 7.7 (continued)

ID (Hex)	Name	Direction	Description
1F/5F	MODify COMplete	MS ↔ BTS	MOD_COM is the acknowledgment of a MOD message. Depending on the direction, MOD_COM is sent at different points in a scenario. The MSC sends MOD_COM only after the requested adaptation has been performed. The MSC sends this message already after receiving and accepting the MOD message.
25/65	DISConnect	MS ↔ BTS	Is used either by the MSC or the MS, to terminate an existing CC connection. The DISC message always contains a cause value, which indicates the reason why the connection was disconnected. When the call is terminated regularly, the cause value "16" is sent, which stands for 'normal clear'. Another value in case of problems is e.g., cause 47 = Resources unavailable. Please be advised that when analyzing trace files, even in case of errors the DISC message may carry a normal clear. This is the case when the problem was not detected by call control.
2A/6A	RELease COMplete	MS ↔ BTS	REL_COM is the answer to a REL message and the acknowledgment that the CC resources have been released. REL_COM is always sent by that side, which had previously sent the DISC message. Like for REL, also for REL_COM there exists an ISUP message with the same name.
2D/6D	RELease	MS ↔ BTS	Because of the fact that signaling in GSM is related to ISDN, there are some similarities in the CC protocol between the two. The REL message corresponds directly to an ISUP message with the same name, which in the case of ISDN is responsible for terminating a connection. The same functionality provides this message in GSM, namely to release the CC resources. The relationship is illustrated in Chapter 12, "Scenarios".
31/71	STOP DTMF	MS → BTS	It is possible to use DTMF signaling with a MS. For this purpose, a START_DTMF message is sent to the MSC when the user presses a button on the keypad. This tells the MSC to generate the respective DTMF sound and send it inband to the peer entity (ISDN, PSTN) When the user releases the button, a STOP_DTMF message is sent to the MSC which triggers the MSC to stop sending the respective tone.

Table 7.7 (continued)

ID (Hex)	Name	Direction	Description
32	STOP DTMF ACKnowledge	BTS → MS	Acknowledgment by the MSC that a STOP_DTMF message was received and sending of the DTMF tone was stopped.
34/74	STATUS ENQuiry	MS ↔ BTS	Both MS and MSC may use STATUS_ENQ to inquire about the current state of Call Control in the peer entity. The peer has to answer the STATUS_ENQ with a STATUS message otherwise the connection is torn down.
35/75	START DTMF	MS → BTS	The MS uses START_DTMF to send ASCII coded DTMF tones to the MSC. The only content of a START_DTMF message is the ASCII value of the respective button, which was pressed at the MS. This is for example 31hex when the '1' button was pressed. A START DTMF message can only be sent in a traffic channel during an active connection. Please note that it is not possible to transmit an analog DTMF tone between the MS and the MSC, only the START_DTMF message. The tone, which can be heard at the MS at the same time is generated in the MS. The Glossary provides a detailed description on the transmission of DTMF tones.
36	START DTMF ACKnowledge	BTS → MS	START_DTMF_ACK is the acknowledgment of the MSC that a START_DTMF message was received. When the MSC sends the START_DTMF_ACK, it simultaneously sends an analog DTMF tone which is sent inband in a traffic channel towards the PSTN/ISDN. The duration of the tone is determined by when a STOP_DTMF message is received .
37	START DTMF REJect	BTS → MS	When the MSC is unable to process the START_DTMF, then it sends a START_DTMF_REJ message to the MS. The respective reason is included in the cause value.
39/79	CONGESTion CONTROL	MS ↔ BTS	This message may be used by both sides, in order to activate flow control for data which is transported within USER_INFO messages.
3D/7D	STATUS	MS ↔ BTS	A STATUS message can be sent if protocol errors in the area of Call Control are detected or if a STATUS_ENQ has to be answered. Such an error situation can occur, in particular, when misinterpretations of CC messages occur, because of bit errors (refer also to MM_STATUS and RR_STATUS).

Table 7.7 (continued)

ID (Hex)	Name	Direction	Description
3E/7E	NOTIFY	MS ↔ BTS	The NOTIFY message is used in case of an active connection to inform the peer entity about a incident in the area of Call Control. Example: When a GSM subscriber is placed on Hold because the other party intends to accept or establish another call, then the MSC sends a NOTIFY message to that MS.

Table 7.8
Supplementary Services (Transaction Identifier/Protocol Discriminator = XB)

ID (Hex)	Name	Direction	Description
2A/6A	RELease COMplete	MS ↔ BTS	Although already presented for the Call Control, the REL_COM message shall be separately presented for Supplementary Services. If a connection was established because of a Supplementary Services request, then this connection is released by sending a REL_COM message. [GSM 04.10, GSM 04.80]
3A/7A	FACILITY	MS ↔ BTS	The FACILITY message may be used by both the MS as well as the NSS. The content of this message is transparent data for Supplementary Services. Please note that almost all CC messages contain an optional information element, the 'Facility', with which SS information can be transported without requiring a FACILITY-message. [GSM 04.10, GSM 04.80]
3B/7B	REGISTER	MS ↔ BTS	The REGISTER message is needed for the activation or inquiry of call-independent supplementary services. Example: the activation of Call Forwarding. In this case, sending of a REGISTER message implies that a new Transaction Identifier is assigned and the dialog between MS and the network is established. [GSM 04.10, GSM 04.80]

8

Signaling System Number 7

Signaling System Number 7 (SS7) provides in OSI Layers 1 to 3 the basis for the signaling traffic on all NSS interfaces, as well as on the A-interface.

The relation to GSM is rather hidden at the beginning of the description, but it becomes more and more obvious when the various user parts like SCCP and TCAP/MAP are presented. SS7, together with all its functionality and user parts, forms a much more complex signaling system than LAPD and $LAPD_m$. For that reason, this whole chapter is dedicated to SS7, or rather to its Layers 1 to 3.

8.1 The SS7 Network

A SS7 network consists of directly connected signaling points (SPs), as shown in Figure 8.1(a); SPs that are connected through signaling transfer points (STPs), as shown in Figure 8.1(b); or a combination of SPs and STPs, as shown in Figure 8.1(c). An SP is a network node that has user parts (e.g., SCCP, ISUP) that allow the processing of messages addressed to that SP. The MSC, the BSC, and the exchanges of the PSTN fall into this category. The functionality of the STP typically is related to those of the SP, with the additional capability of being able to relay SS7 messages. Note that it is possible to have a designated STP that has no SP functionality, that is, one that can only relay messages, as shown in Figure 8.1(b).

Samsung Ex. 1032, Page 132 of 417



Figure 8.1(a) Directly connected SPs.

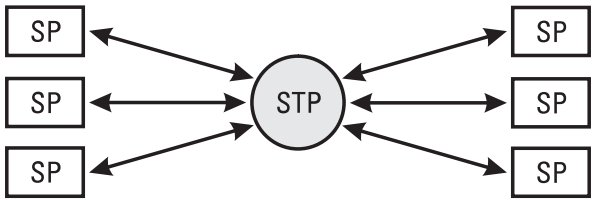


Figure 8.1(b) An STP that interconnects SPs.

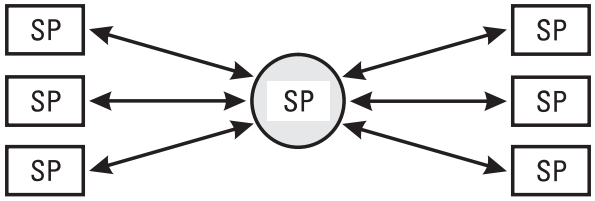


Figure 8.1(c) An STP with SP functionality that interconnects SPs.

8.2 Message Transfer Part

SS7 without user parts consists only of the OSI Layers 1 through 3. Those three layers essentially are represented by the message transfer part (MTP). Parts of the SCCP actually are also part of Layer 3.

The MTP of SS7 performs the following general tasks:

- It provides all the functionality of OSI Layers 1 to 3 required to provide for a reliable transport of signaling data to the various SS7 user parts.
- When problems arise, the MTP takes the necessary measures to ensure that the connection can be maintained or prevents loss of data, for example, by switching to an alternative route.

The MTP can be partitioned into three layers, where the MTP 1 (OSI Layer 1) is responsible for the transfer of single bits or the definition and provision of the necessary electrical and physical means for it.

The MTP 2 (OSI Layer 2) defines the basic frame structure that is used by SS7 for all message types. This frame structure is illustrated in Figure 8.2, which shows the flags that mark beginning and end (as we have seen in LAPD),



Figure 8.2 General format of an SS7 message.

an acknowledgment field with send and receive sequence numbers, a length indicator, an optional information field, and the FCS to transport a checksum (as we also have seen in LAPD).

8.3 Message Types in SS7

Definition of the SS7 message types is another functionality of MTP 2. In Layer 2 of SS7, three different message types are defined: the fill-in signal unit (FISU), the link status signal unit (LSSU), and the message signal unit (MSU). Although no explicit field is available to distinguish among the message types, it is possible to do so based on their different lengths. The length indication (LI) provides that information and relates to the length of the optional data field. The value of the LI is always 0 for FISUs; 1 or 2 for LISUs; and greater than 2 for MSUs.

8.3.1 Fill-In Signal Unit

The FISU (Figure 8.3) is used to supervise the link status when no traffic is available. Both sides poll each other in this idle state. The N(S) and N(R), which in SS7 are called the forward sequence number (FSN) and backward sequence number (BSN) or the forward indicator bit (FIB) and backward indicator bit (BIB), respectively, do not change their values during polling. In addition to the polling functionality, an FISU also can be used to acknowledge receipt of an MSU.

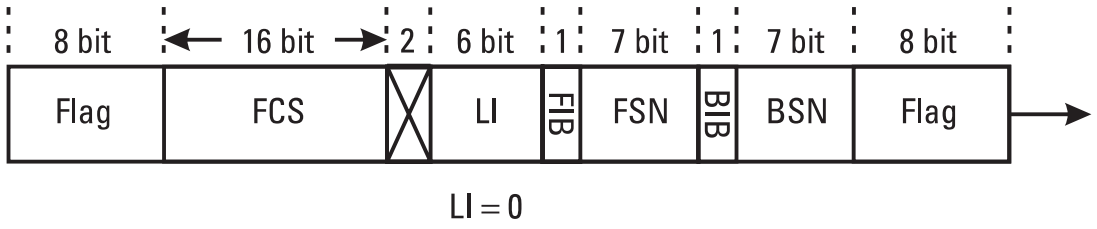


Figure 8.3 Format of the FISU.

8.3.2 Link Status Signal Unit

The LSSU is used only to bring a link into service or to take it out of service and during error situations (e.g., overload), to exchange status information between two SPs or STPs. In Figure 8.4, the status field has a length of 1 byte, but according to ITU definitions it also can be 2 octets long. In any case, only the first three bits of the first byte contain the actual status information. The receiver of an LSSU does not confirm its receipt.

Protocol test equipment usually does not indicate an LSSU as such but displays it according to its status field. For that reason, the status field or its abbreviation can also be used as a subname. Consequently, the term status indication (SI) and the terms SIO, SIOS, and SIB, which are explained in Table 8.1, are used more frequently than LSSU/status field SIOS. Note that, in particular, when SIPOs or SIBs are detected during protocol testing, rather serious problems can be expected at the related SP/STP.

8.3.3 Message Signal Unit

The MSU (Figure 8.5) is used for any type of data transfer between two network nodes. The MSU is the only SS7 message able to carry traffic data (the LSSU does not carry traffic data, only status information), and it is used by all user parts (ISUP, SCCP, OMAP) as a platform particularly for that task. The information field of the MSU consists of the service information octet (SIO)

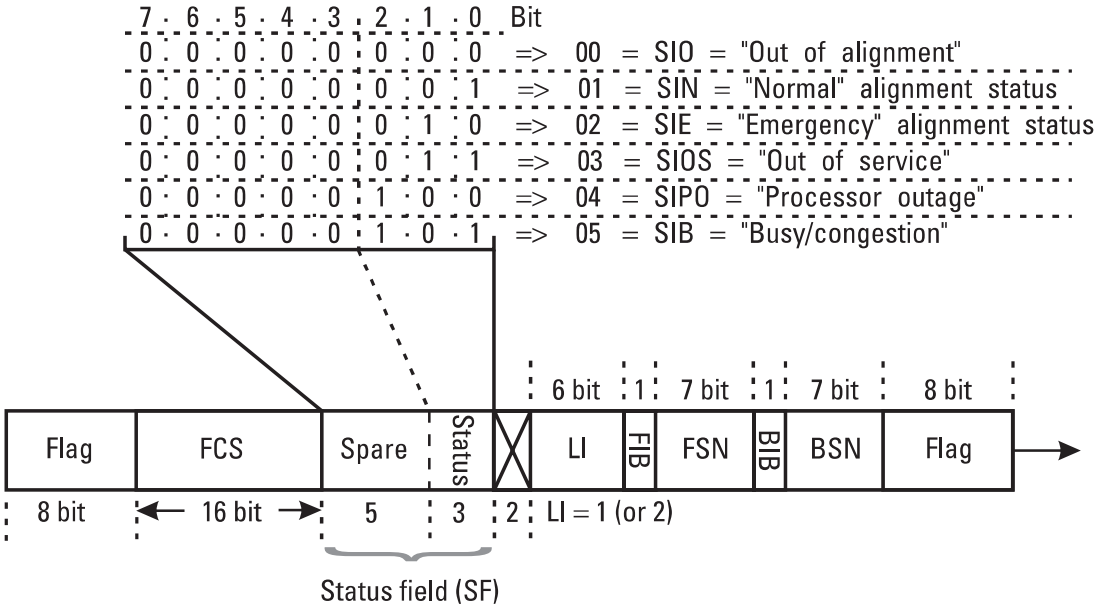


Figure 8.4 Format of the LSSU.

Table 8.1
Status Field Values

Value	Abbreviation	Status	Description
0	SIO	Out of alignment	Start of link alignment
1	SIN	Normal alignment	A connection is brought into service with a normal (long) surveillance time of 8.2 s (see also Section 8.4.2).
2	SIE	Emergency alignment	A connection is brought into service with an emergency (short) surveillance time of about 500 ms. (see also Section 8.4.2).
3	SIOS	Out of service	This indicates in case of an error situation or before a link is taken into service that currently no MSUs can be sent or received.
4	SIPO	Processor outage	When the Layer 2 of an SP or STP detects a problem within the Layer 3 of its own network node it indicates the problem status to the peer entity by sending a SIPO.
5	SIB	Busy/congestion	Signals overload on the originating side. Acknowledgments cannot be sent anymore. Usually, a link failure follows.

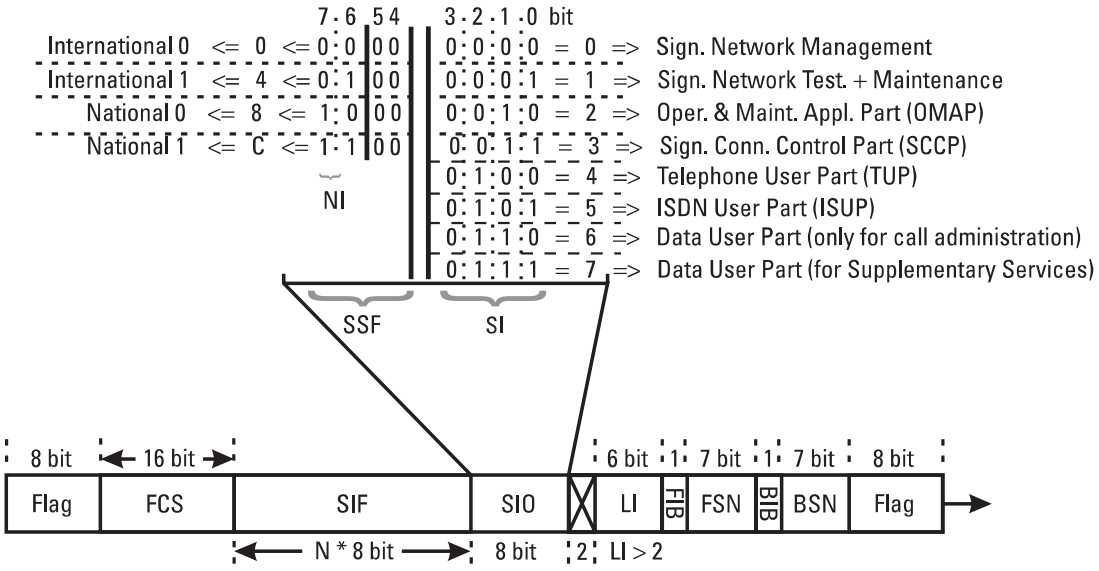


Figure 8.5 Format of the MSU.

and the signaling information field (SIF). The SIO[1] is further partitioned into the subservice field (SSF) and the service indicator (SI), with four bits each. Only the two bits of higher valence in the SSF are necessary to describe the network indicator (NI). The NI is used to distinguish between national and international messages. The SI indicates to which user part an MSU belongs. The four bits of the SI thus determine whether the data of the SIF belong to the SCCP, TCAP, ISUP, and so on, or possibly need to be forwarded to the automatic network management. In contrast to LSSU and FISU, it has to be acknowledged to the peer entity whenever an MSU is received.

8.4 Addressing and Routing of Messages

In an SS7 network, MSUs are not necessarily exchanged between adjacent neighbors (SP/STP). In a GSM system, the MSC and BSC are neighbors; however, the exchange of information between the MSC and the HLR may involve several STPs. SS7 uses so-called point codes for routing and addressing MSUs. Point codes are unique identifiers within an SS7 network. Exactly one point code, a signaling point code (SPC), is assigned to every SP and STP. An MSU has a routing label that contains the point codes of the sender (the originating point code, or OPCs) and the addressee (the destination point code, or DPC). The routing label is, for its part, a component of the SIF. Note that neither FISU nor LSSU possesses a routing label, since those messages are exchanged only between two adjacent nodes.

Figure 8.6 shows the format of a routing label. The OPC defines the sender of the MSU, and the DPC defines its addressee. Note that addressing via SPCs works only on a national basis. The services of higher layers are needed for international addressing, in particular SCCP or ISUP, to provide the necessary features.

The remaining 4 bits of the routing label form the signaling link selection (SLS) field. This parameter is used to balance the load between several SS7 connections of a link group. If, for example, two SS7 connections are available between two network elements, all the even values of the SLS (0, 2, 4,… , 14_{dez}) are assigned to the first link, and the odd values (1, 3, 5,… , 15_{dez}) are assigned to the second link. This fact is important to know in the analysis of SS7 trace files.

1. Note that the service information octet and its abbreviation SIO do not have a relation to the former use of the abbreviation, which stood for status indication/out of alignment. Unfortunately, the standards use the same abbreviation for both.

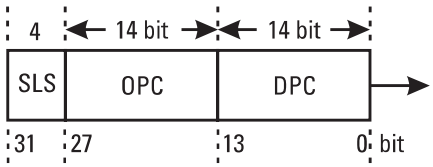


Figure 8.6 Routing label (DPC, OPC, and SLS).

8.4.1 Example: Determination of DPC, OPC, and SLS in a Hexadecimal Trace

In the analysis of hexadecimal trace files, it generally is important to be able to convert DPC and OPC into clear text, to be able to relate the various messages to, for example, a particular MSC or BSC. As shown in Figure 8.6, DPC and OPC are each 14 bits long. The routing label, together with the 4 bits of the SLS, totals 32 bits, or 4 bytes.

Because the OPC and the DPC are 14 bits in length, it is not trivial, particularly with byte (8 bits) or 16-bit-word-oriented presentations, to derive the decimal value of DPC or OPC, as illustrated in Figure 8.7. The sequence of numbers represents the hexadecimal values. The underlined part represents the routing label, that is, the SLS, OPC, and DPC. This information is decoded in clear text. At first sight, the values seem to differ.

It is important when decoding to consider the bitwise sequence of transmission with which the data are received by the system. The binary presentation (left to right) is given in Figure 8.8.

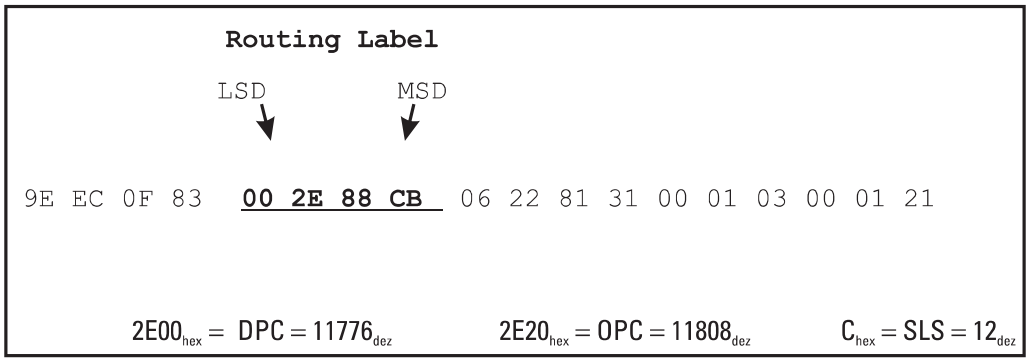


Figure 8.7 Partial trace file and point codes.

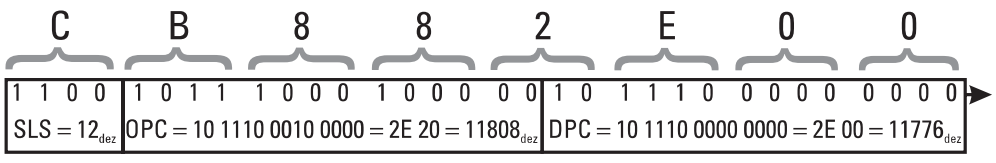


Figure 8.8 Transmission of routing label.

Possible confusion is based on the unusual length (14 bits) of OPC and DPC on the one hand, and, on the other hand, the results from the reversed way of reading/writing (right to left), a problem familiar to most programmers. Misinterpretation can be prevented when these facts are considered.

Other representations of SPCs can be used in various national applications, like the "4-3-4-3" presentation, which refers to the bits that are used per sign. The example in Figure 8.7 reads in the "4-3-4-3" presentation as follows:

$$DPC = 2E00_{hex} = 11776_{dez} = 1011 - 100 - 0000 - 000 = B - 4 - 0 - 0$$

$$OPC = 2E20_{hex} = 11808_{dez} = 1011 - 100 - 0100 - 000 = B - 4 - 4 - 0$$

8.4.2 Example: Commissioning of an SS7 Connection

Every SS7 connection is brought into service as presented in Figure 8.9. In the figure, an A-interface link between BSC and MSC is brought into service.

8.4.2.1 Bringing Layer 2 Into Service

After Layer 1 is established, both sides send an SIOS-LSSU, which indicates that the link is out of service and no MSU can currently be processed.

The process to bring Layer 2 into service starts with sending an SIO-LSSU. Please note the duplex characteristics of SS7. Both terminals are equal, and a link has to be established in *both* directions.

The test period, during which both sides examine the link quality, starts with sending an LSSU-SIN or an LSSU-SIE. Transmitted FISUs must not contain any errors during this test period. The link cannot go into service if an error occurs. The difference between LSSU-SIE and LSSU-SIN is the related surveillance time.

An emergency alignment is used when no alternative SS7 route currently exists and the link needs to be in service as quickly as possible.

8.4.2.2 Bringing Layer 3 Into Service

When the test time is over and no errors were detected, Layer 2 is considered to be in service and Layer 3 initiates further tests. A signaling link test message (SLTM) is used for that purpose, to transmit a number of test bytes to Layer 3 of the peer entity.

If the test bytes are correctly returned to the sender in a signaling link test acknowledgment (SLTA) message, Layer 3 is also considered to be "in traffic." Figure 8.10 shows examples of a SLTM and a SLTA message.

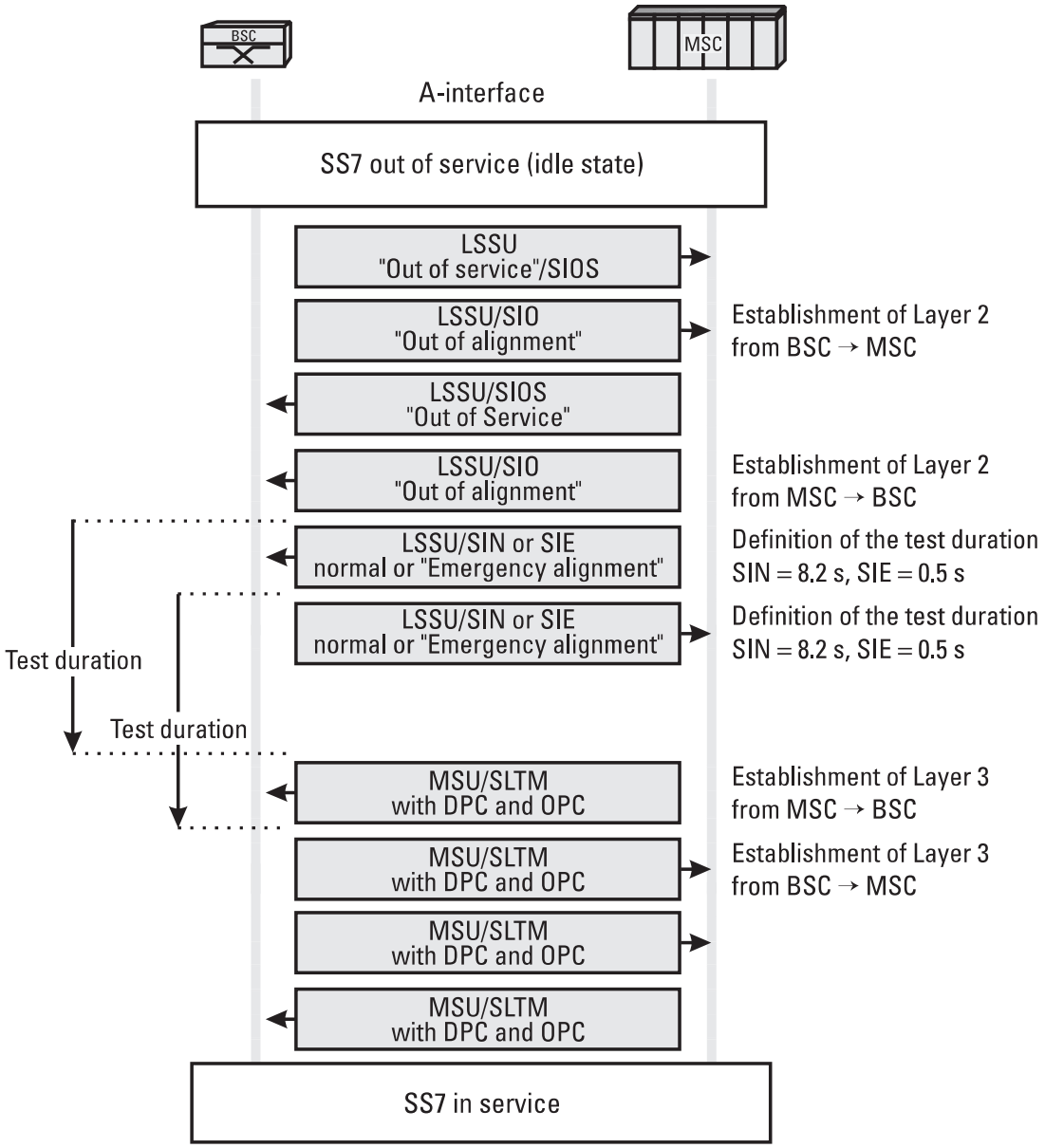


Figure 8.9 Establishment of an SS7 link.

Synchronization of Layer 4 (in this case of the SCCP) follows the link establishment on the A-interface, by applying the reset procedure (described in Chapter 10).

8.5 Error Detection and Error Correction

Layer 2 is responsible for error detection and error correction. To be more specific, within Layer 2, the FSN and the BSN, together with the FCS, take care

```
Signaling link Test Message (SLTM)
    ----0001 Service Indicator          Sig network test & maint mess
    --00---- Sub-Service: Priority      Spare/priority 0 (U.S.A. only)
    10------ Sub-Service: Network Ind   National message
    ******** Destination Point Code     1024
    ******** Originating Point Code     1035
    ******** Signalling Link Code       0
    ----0001 Heading code 0             0x1
    0001---- Heading code 1             0x1
    ----0000 Spare
    0111---- Length indicator           7
    ******** Test pattern               44 43 4E 20 53 53 37




Signalling link Test Ack mess (SLTA)
    ----0001 Service Indicator          Sig network test & maint mess
    --00---- Sub-Service: Priority      Spare/priority 0 (U.S.A. only)
    10------ Sub-Service: Network Ind   National message
    ******** Destination Point Code     1035
    ******** Originating Point Code     1024
    ******** Signalling Link Code       0
    ----0001 Heading code 0             0x1
    0010---- Heading code 1             0x2
    ----0000 Spare
    0111---- Length indicator           7
    ******** Test pattern               44 43 4E 20 53 53 37
```

Figure 8.10 Examples of a SLTM and a SLTA message.

of the error recognition function. Note that the format of those parameters is the same for all three message types (FISU, LSSU, MSU). Refer to Figures 8.3 through 8.5.

SS7 provides two alternative methods of error correction:

- All messages not acknowledged within a specified time frame have to be retransmitted.
- Retransmission occurs only in the case of a negative acknowledgment.

These two basic procedures are described next.

8.5.1 Send Sequence Numbers and Receive Sequence Numbers (FSN, BSN, BIB, FIB)

The 7-bit-long FSN, together with the FIB, forms the send sequence number of an SS7 message. The FSN is incremented by 1 whenever an MSU is sent. The value of the FSN, however, does not change when an LSSU or an FISU is transmitted.

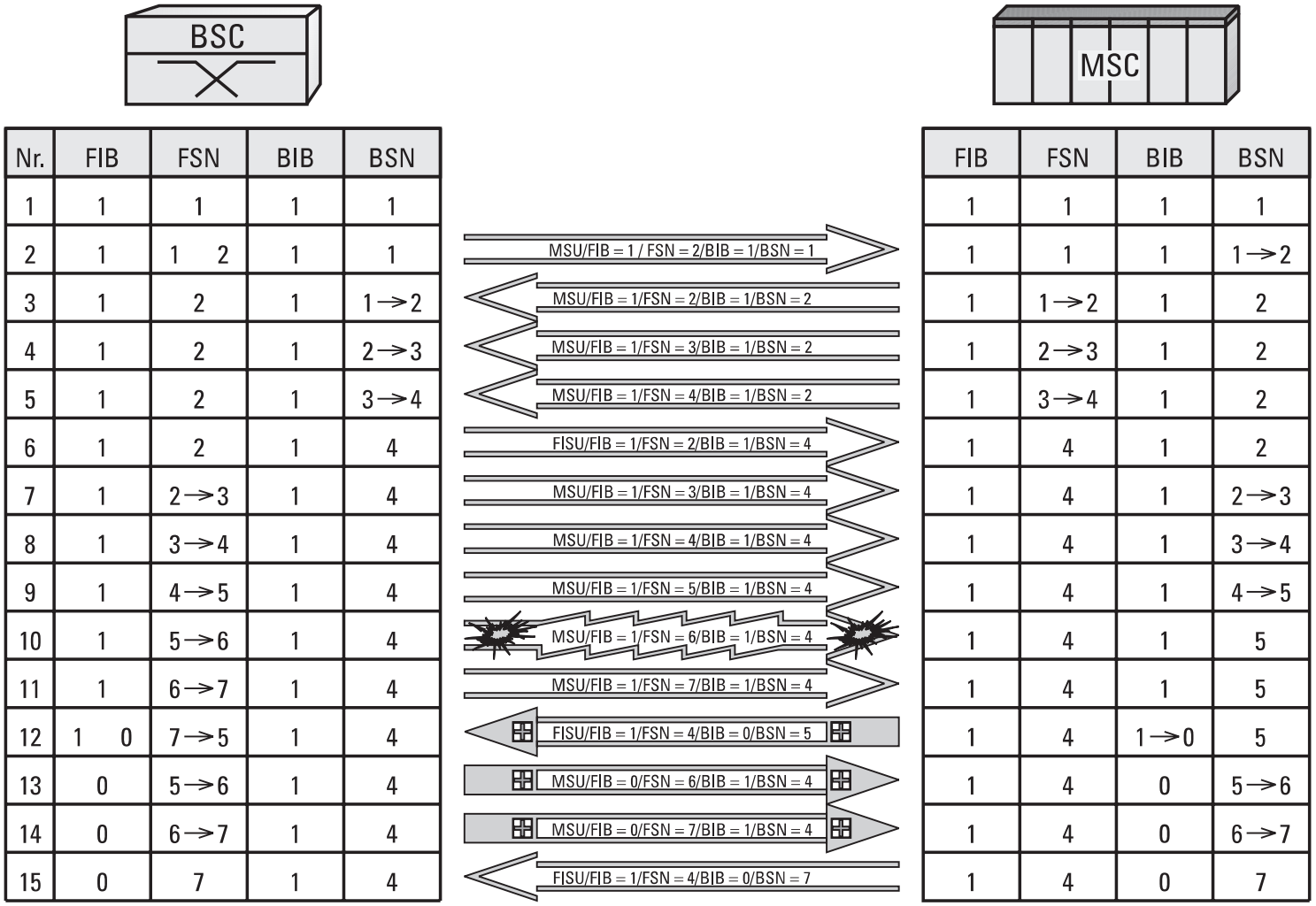
The 7-bit-long BSN and the BIB form the receive sequence number. They are used for positive or negative acknowledgment of a received message. The BIB is used to indicate a problem when a negative acknowledgment has to be returned because of a transmission error. To indicate a transmission error, the value of BIB is simply inverted by the receiving entity, that is, changed from 0 to 1 or from 1 to 0. The inverted value of BIB is sent back to the peer entity together with the BSN of the last error-free received MSU. The peer entity then has to repeat all MSUs with a greater BSN.

FSN/FIB on one side and BSN/BIB on the other together form a functional unit, as Figure 8.11 shows. The example in Section 8.5.2 describes the task of FSN, FIB, BSN, and BIB in more detail.

8.5.2 BSN/BIB and FSN/FIB for Message Transfer

The task of FSN and BSN can best be explained with an example. Refer to Figure 8.11, which shows the exchange of SS7 messages between BSC and MSC. The numbers in the following bulleted list relate to the line numbers in Figure 8.11. The intention is to explain the values of the counters and the principle of error correction.

- Line 1. Let us assume, for simplification purposes, that the link was just brought into service and that the values for FIB, FSN, BIB, and BSN are all 1.
- Line 2. The BSC increments its FSN to a value of 2 and sends an MSU. The other counters do not change. The BSC continues to store



Nr.	FIB	FSN	BIB	BSN
1	1	1	1	1
2	1	1 2	1	1
3	1	2	1	1→2
4	1	2	1	2→3
5	1	2	1	3→4
6	1	2	1	4
7	1	2→3	1	4
8	1	3→4	1	4
9	1	4→5	1	4
10	1	5→6	1	4
11	1	6→7	1	4
12	1 0	7→5	1	4
13	0	5→6	1	4
14	0	6→7	1	4
15	0	7	1	4

FIB	FSN	BIB	BSN
1	1	1	1
1	1	1	1→2
1	1→2	1	2
1	2→3	1	2
1	3→4	1	2
1	4	1	2
1	4	1	2→3
1	4	1	3→4
1	4	1	4→5
1	4	1	5
1	4	1	5
1	4	1→0	5
1	4	0	5→6
1	4	0	6→7
1	4	0	7

Figure 8.11 FSN, FIB and BSN, BIB for error correction.

the contents of the MSU for possible retransmission. The MSC receives the message and checks for errors. When the MSC finds that the message is correct, it increments its BSN counter from 1 to 2.

- Line 3. It happens that the MSC also has to send an MSU. Now the MSC increments its FSN counter from 1 to 2 and transmits this value, together with the new value of BSN (2) to the BSC. The MSC also continues to store the contents of the MSU. After receiving the message, the BSC checks the values for BSN and BIB and finds that the MSC has confirmed the previously sent (under line 2) MSU. The information is contained in the parameter BSN (BSN = 2). Since the MSC received the message without errors, the BSC does not need to continue to store that information and discards it. And because the BSC has received the message from the MSC without error, it increments the value of BSN to 2.
- Line 4. Now the MSC sends another MSU before the BSC is able to acknowledge the MSU. The value of FSN in the MSC increases accordingly to a value of 3, and the value of BSN in the BSC is changed to 3. In addition to the message from line 3, the new MSU has to be stored in the MSC.
- Line 5. The process described under line 4 repeats. The MSC now has to store all three unacknowledged MSUs.
- Line 6. Now the BSC acknowledges that it received the three messages (lines 3, 4, and 5) from the MSC without error. Note the value of BSN (BSN = 4) in the FISU. All three MSUs are acknowledged in one FISU message by confirming the latest correctly received message. Hence, it is not necessary to acknowledge every single message.
- Lines 7, 8, and 9. The BSC transmits three consecutive MSUs to the MSC. It correspondingly increases its value for FSN from 2 to 5. The MSC increments its value for BSN to 5 as well. The BSC needs to store all three MSUs until the MSC confirms proper receipt of them.
- Line 10. The BSC sends another MSU to the MSC, which increases the value of FSN in the BSC to 6. This MSU is corrupted and the MSC detects the error (FCS). Consequently, the value of BSN in the MSC does not change.
- Line 11. Now the BSC sends another MSU to the MSC before the MSC is able to send a negative acknowledgment. Although this message is received without error, the counter for BSN still is not incremented, and its value stays at 6.

- Line 12. Because of the error that occurred in line 10, the MSC inverts its value for BIB from 1 to 0. The new BIB value is sent back to the BSC in an FISU, together with the value for the number of the latest correctly received MSU. When the BSC analyzes this message, it detects from the BIB value that a transmission error occurred and that the MSUs sent under lines 7 through 9 are confirmed. The BSC then inverts its value for FIB and changes its value for FSN from 7 to 5, to retransmit the messages from lines 10 and 11. Note that the message, sent under line 11 and correctly received by the MSC, still has to be sent again.
- Lines 13, 14. With the inverted values of FIB and BIB on the respective sides, the BSC repeats transmission of the messages from lines 10 and 11 to the MSC. This time, both messages are received without error, and the value for BSN in the MSC is increased from 5 to 7.
- Line 15. The MSC confirms receipt of the MSUs (lines 13 and 14, previously lines 10 and 11) by answering with an FISU.

The preceding example can be summarized as follows:

- The counters for BSN/BIB on one hand and FSN/FIB on the other have identical values after positive acknowledgment.
- A corrupted message is indicated by the inversion of the BIB. This procedure also is used in the idle case, when only FISUs are exchanged.
- When one side receives a message with an inverted BIB, it subsequently inverts its FIB and sends it with the next message, to indicate to the peer that it has received the information about the error situation.
- When the values of the counters FSN, FIB, BSN, and BIB are not consistent in a received message (e.g., a jump from 1 to 5), a negative acknowledgment also is returned.
- The counters are not incremented when an FISU or an LSSU is sent.

8.6 SS7 Network Management and Network Test

The various possibilities to configure an SS7 network were presented at the beginning of this chapter. Such a network basically consists of interconnected SPs and STPs, as illustrated in Figure 8.12.

The major task in the operation of a complex network is management or administration of the network. For that purpose, SS7 has dedicated user parts

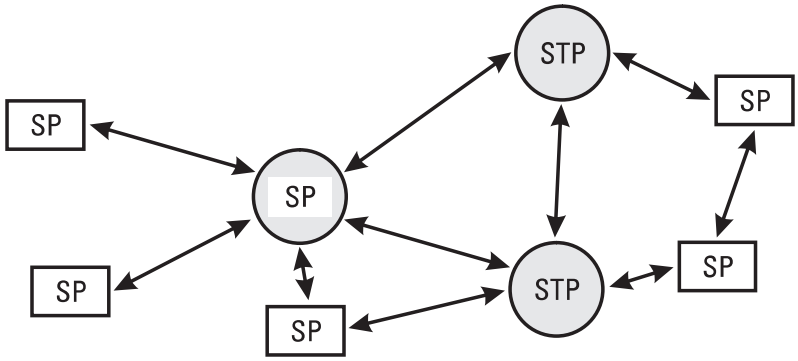


Figure 8.12 Example of an SS7 network.

in Layer 3 that automatically detect error situations and are able to try to correct them autonomously. Errors can be separated into one of three categories:

- Overload on a single SS7 link;
- Outage/bringing into service an SP/STP;
- Outage/bringing into service an SS7 link between SPs or STPs.

SS7 network management has to be able to detect each error situation and to allow for a fix with the appropriate actions. Those actions consist mainly in rerouting signaling data, as well as blocking and unblocking routes. The details of how that is performed are described next.

8.6.1 SS7 Network Test

ITU recommendations deal separately with SS7 network test and SS7 network management. However, they serve similar tasks and thus will be presented together. Table 8.2 shows how SS7 distinguishes network test and network management by assigning two different SIs. The SI is part of the SIO.

Table 8.2
Service Indicators for SS7 Network Management and Network Test

SI (Binary)	User Part
00	Network management
01	Test and maintenance

8.6.2 Possible Error Cases

The messages in the following descriptions frequently are abbreviated. Sections 8.6.5 and 8.6.6 explain the abbreviations

8.6.2.1 Behavior in an Overload Situation

Figure 8.13 illustrates a situation in which an overload situation occurs on the link between the STP and the SP/STP. In that case, both STPs inform their direct neighbors about the limited availability of that connection. The information is sent in TFC messages and TFR messages. Alternative routes will be used after the neighbors are informed about the problem. The changeover procedure (sending of a COO message) is used to actually implement rerouting. When the overload situation has ceased to exist, the neighbors are informed in TFA messages that the link is available again. To actually utilize that link, the changeback procedure has to be executed (sending of a CBD message). In the time period between when the TRC/TFR messages and the TFA messages are sent, the neighbor SPs/STPs periodically check the overload situation by sending RSR or RCT messages. Which of the messages is actually used depends on whether the sender is an SP or an STP. (See the tables at the end of the chapter for explanations of the messages.)

8.6.2.2 Behavior at Outage/Bringing SP/STP Into Service

Figure 8.14 shows the same SS7 network, but this time with the failure of an STP. As with the overload situation, all neighbors have to be informed immediately about the problem. In the case of an outage, that is performed by the sending of TFP messages to all affected SPs and STPs. The rerouting process, as in the overload situation, is done via the changeover procedure. When the failed STP comes back into service, the neighbors first recognize that when the links toward that STP synchronize again. All the neighbor nodes periodically send RST messages during the outage to check the state of the STP. All

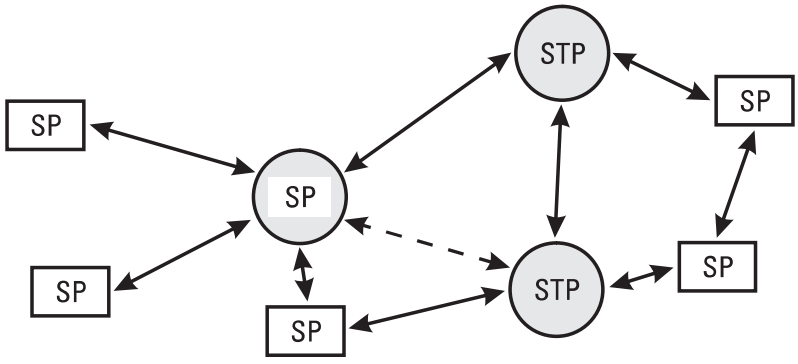


Figure 8.13 SS7 network with overload (dashed link).

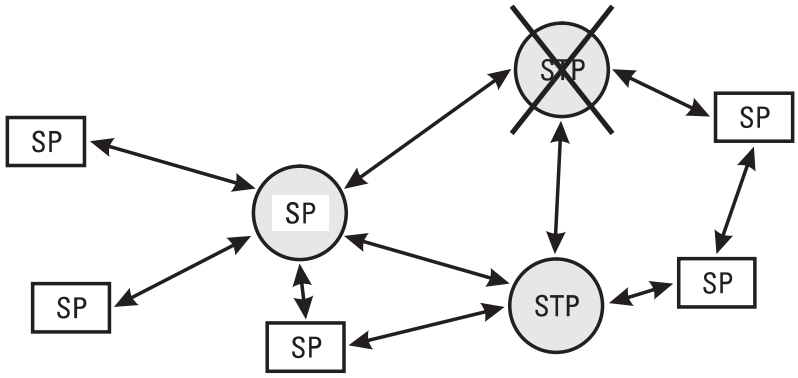


Figure 8.14 SS7 network with STP outage.

the neighbors send TRA messages to the STP when Layer 2 is established again. The STP that got back into service also sends TRA messages to all neighbors (an SP would *not* send those messages). The TRA messages have the purpose of informing all neighbors that the respective routes are available again. Finally, a changeback procedure is used to cancel all the established detours.

8.6.2.3 Behavior When SS7 Link Fails/Is Established

Another possible scenario is the total loss of an SS7 link between an SP and an STP (Figure 8.15). In that situation, the STP has to inform all neighbors about the loss of the connection. That is done with a TFP message. Establishing alternative routes to and from the affected SP is performed by means of the changeover procedure. Both the SP and the STP periodically test the link by sending RST messages during the time period when the link is not available.

The reverse process is executed when the link is brought back into service. The STP sends TFA messages to all affected neighbors, and the alternative routes are canceled by means of the changeback procedure.

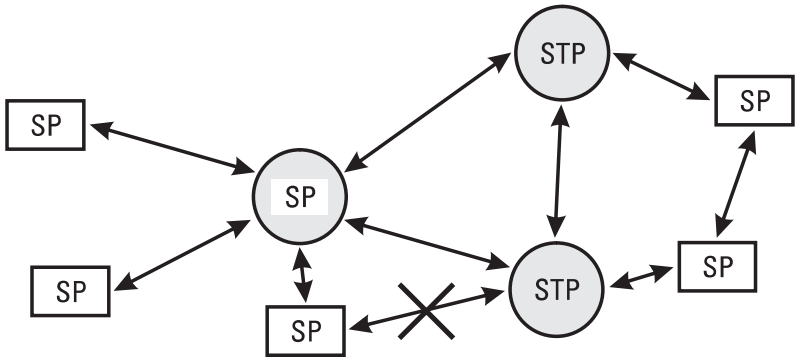


Figure 8.15 SS7 network in which a link has failed.

8.6.2.4 More Error Cases

Other situations may occur, and appropriate measures have to be taken. Such situations include loss of single user parts in an SP, intentional shutdown of an SS7 link by network management, and automatic addition of SS7 links in the case of increasing load or link failures. The tables in the next sections describe the corresponding messages to transmit that information.

8.6.3 Format of SS7 Management Messages and Test Messages

Figure 8.16 presents the format of SS7 management messages and test messages.

The SI is used to differentiate between the user parts for network management and network test.

The SI field of management messages and test messages (both in Layer 3) contains so-called heading codes, which are necessary for message and message-group coding. The SS7 user parts of Layer 4 do not allow for such a functionality. Heading code 0 (H0) defines a whole group, while Heading code 1 (H1) is used to identify a single message within a group. The defined message groups are listed in Table 8.3.

The data part (see Figure 8.16) is optional and not required by all messages.

8.6.4 Messages in SS7 Network Management and Network Test

Figures 8.17(a) through 8.17(d) provide a complete overview of the SS7 messages used for network management and network test. Tables 8.4 and 8.5 list

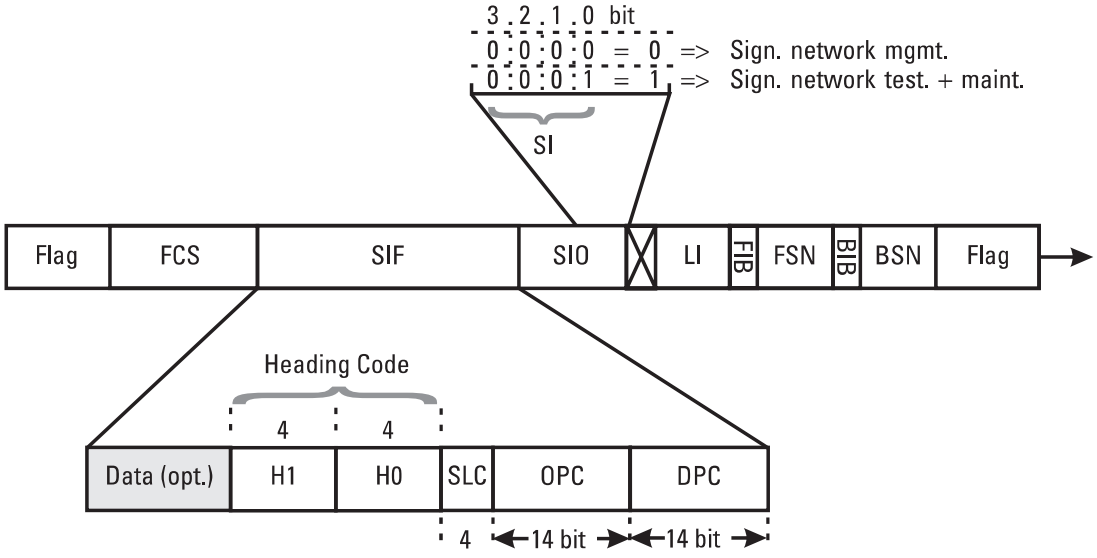


Figure 8.16 Format of SS7 management and test messages.

Table 8.3
Various Message Groups of SS7 Management and Test

H0 (Hex)	Message Group
1	Changeover and changeback
2	Emergency changeover
3	Transfer controlled and signaling route test
4	Transfer prohibited/allowed/restricted
5	Signaling route set test
6	Management inhibit
7	Traffic restart allowed
8	Signaling data link connection
A	User part flow control
1 (test)	Signaling link test

all SS7 network management and test messages, with brief descriptions thereof. Uppercase letters indicate the abbreviations used in this context.

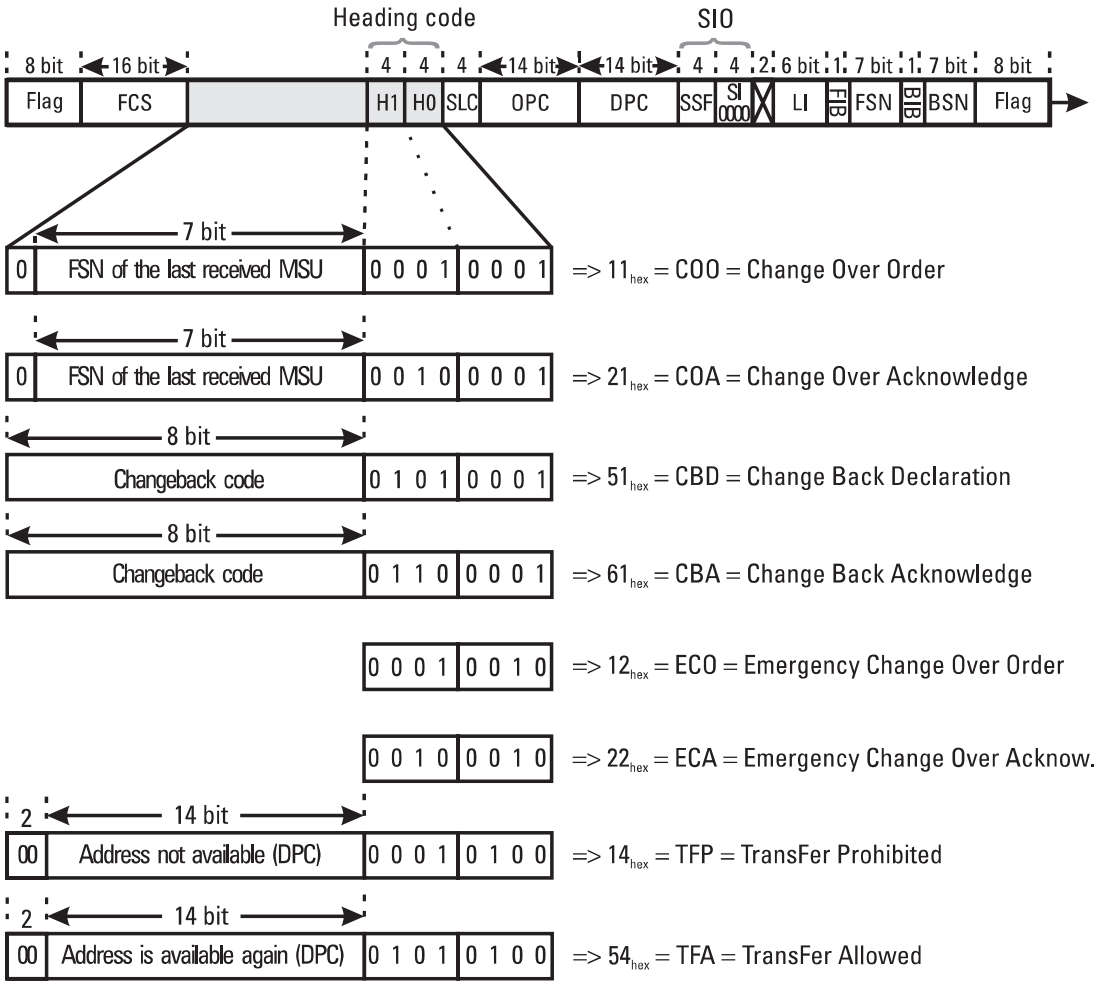


Figure 8.17(a) SS7 network management messages.

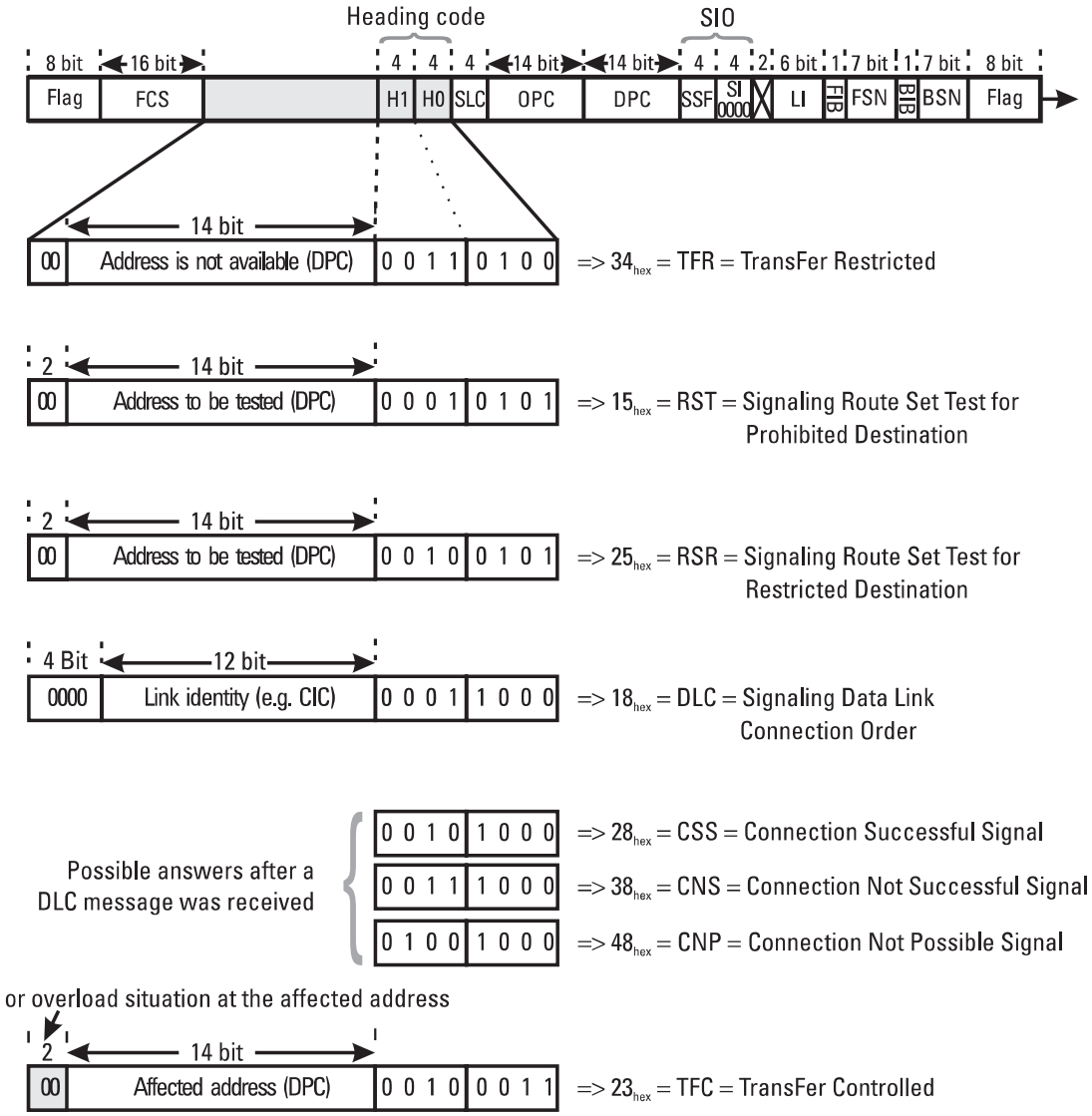


Figure 8.17(b) SS7 network management messages.

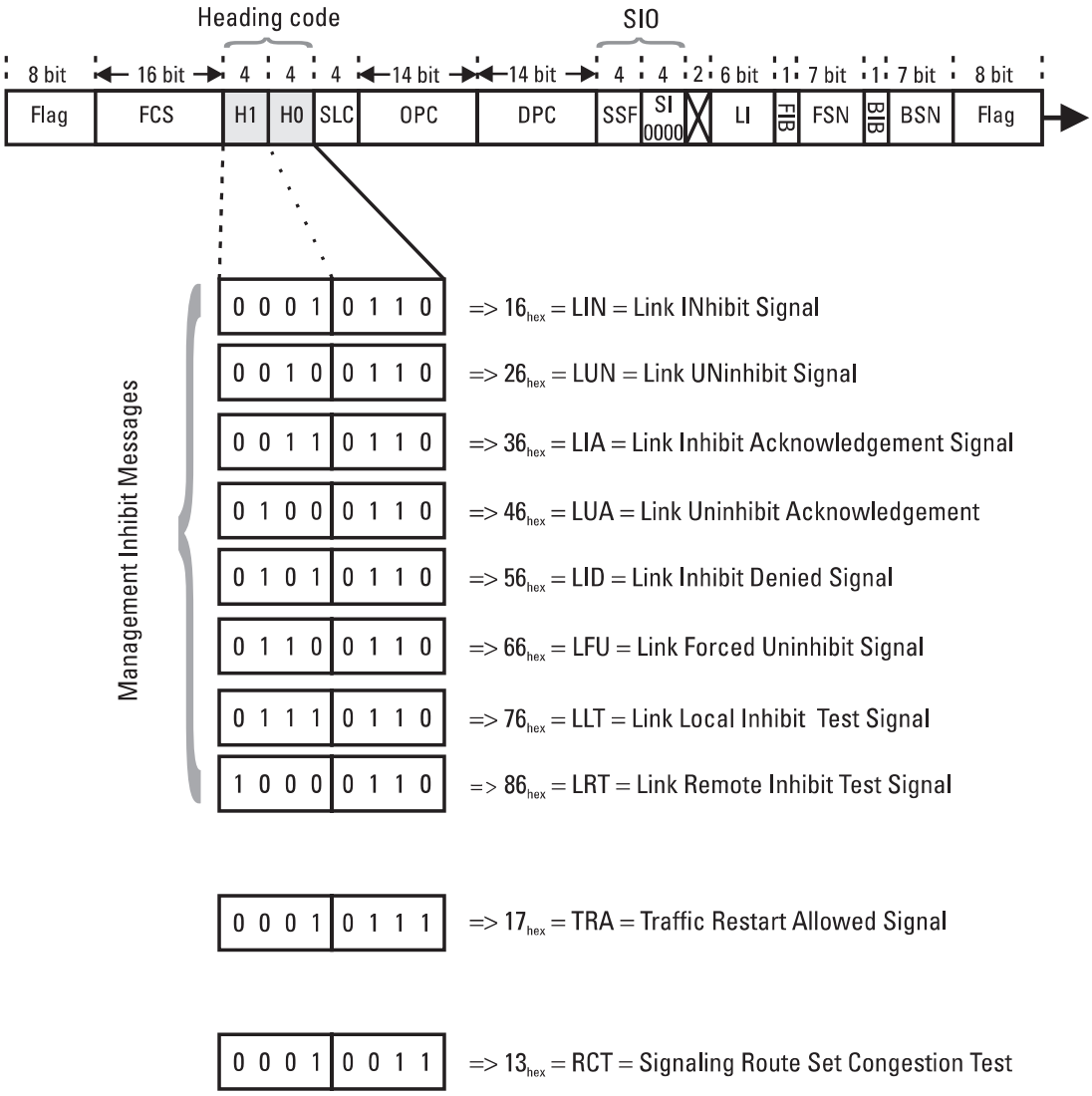


Figure 8.17(c) SS7 network management messages.

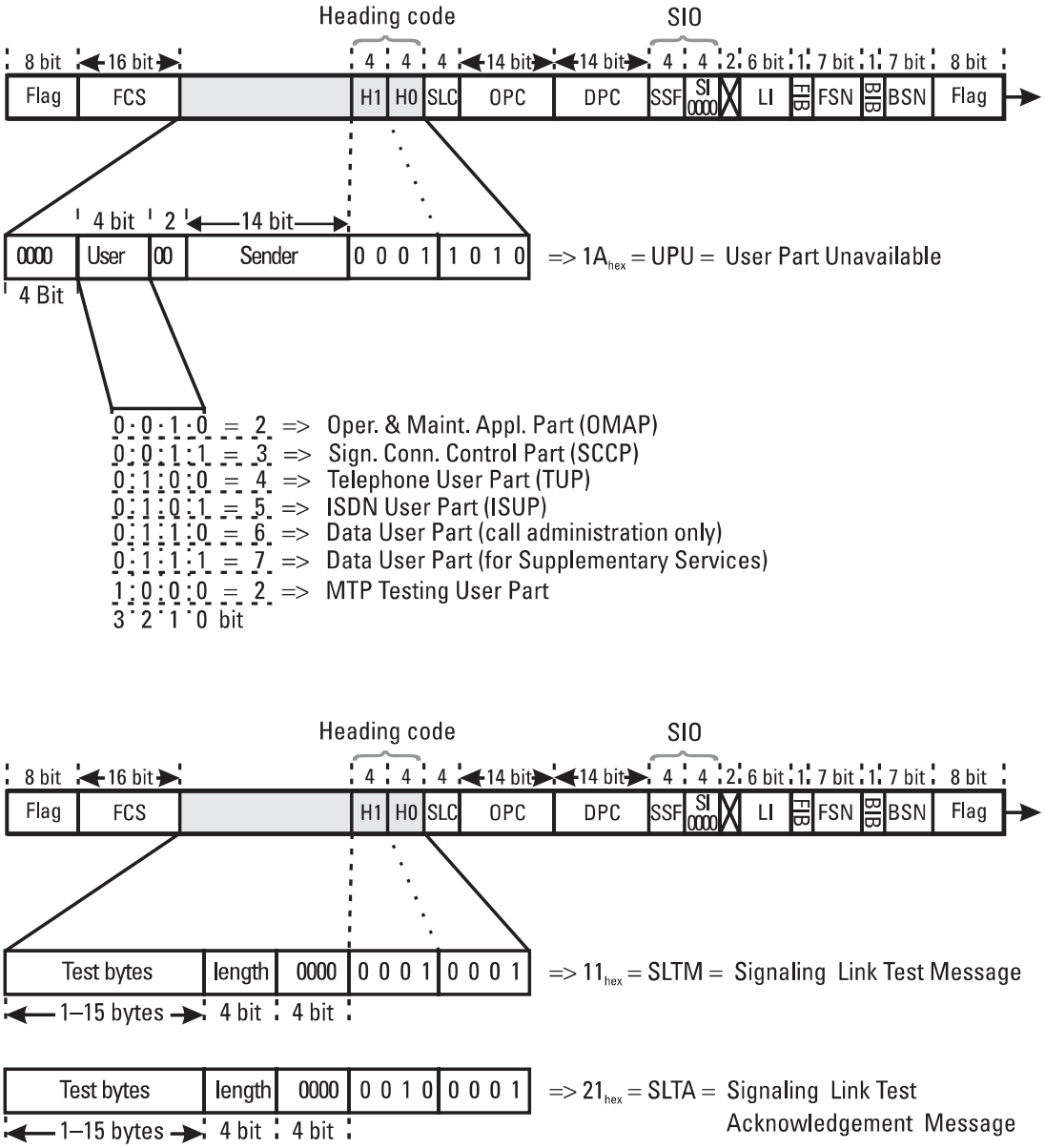


Figure 8.17(d) SS7 Management and test messages.

Table 8.4
Message Types in SS7 Network Management

H1/H0	Abbr.	Name	Description
11	COO	Change Over Order	The COO message is used to re-route the signaling traffic from one link to an alternative link. This is used when a particular signaling link cannot be used anymore. Possible reasons are, intentional shut down, or automatic network management procedures. The COO message always contains the FSN of the last MSU that was received and acknowledged on that link. This allows it to immediately continue with transmission over an alternative link, without loss of data. Both SP or STP can send a COO message.
21	COA	Change Over Acknowledge	The COA message confirms that a COO message was received and processed and that a particular signaling link will no longer be used. A COA message also acknowledges the FSN of the COO message.
51	CBD	Change Back Declaration	The CBD message indicates to the neighbor SP/STP that a previously shut down link, performed by the change over procedure, is now available again and can be used for signaling traffic.
61	CBA	Change Back Acknowledge	Answer to a CBD message. A previously shut down link is now available again and can be used for signaling traffic.
12	ECO	Emergency Change Over Order	It is possible during change over that the FSN of the last correctly received MSU can not be transmitted (e.g., Error situation). In such circumstances the ECO message is used instead of the COO message. The disadvantage of the emergency change over is that it is not possible to determine whether MSU's were lost.
22	ECA	Emergency Change Over Acknowledge	This message acknowledges an ECO message and the switch over to the alternative link(s).
14	TFP	TransFer Prohibited	The TFP message is only used by STPs to inform neighbor SPs or STPs that a certain route to a particular Point Code is not available. The TFP message contains as a parameter the Point Code to which no data can be sent. When a TFP message was received, all the traffic to the affected Point Code has to be routed via alternative routs.
54	TFA	TransFer Allowed	The TFA message is only sent by STPs in order to inform neighbor SPs/STPs about the availability of a route. This message is the counterpart of the TFP message and the TFR message, respectively.

Table 8.4 (continued)

H1/H0	Abbr.	Name	Description
34	TFR	TransFer Restricted	The TFR message is only sent by STPs in order to inform neighboring SPs/STPs about the limited availability of a route to a particular Point Code. Data destined to this Point Code should, when possible, be routed via alternative links. The TFR message is a softer alternative to the TFP message and is used, for example, in the case of overload.
15	RST	Signaling Route Set Test for Prohibited Destination	When an SP/STP receives a TFP message, it periodically sends a RST message to the affected STP, in order to determine if it is available again.
25	RSR	Signaling Route Set Test for Restricted Destination	When an SP/STP receives a TFR message, it periodically sends a RSR message to the affected STP, in order to determine if it is available again.
18	DLC	Signaling Data Link Connection Order	When alternative signaling connections need to be established between SPs/STPs, then a DLC message is sent to the neighbor SP/STP. The most important parameter is the identifier for the channel to be reserved (time slot).
28	CSS	Connection Successful Signal	A positive response when a DLC message is received. The requested channel is available for SS7 and all necessary resources were activated. The generic term for CSS, CNS, and CNP is Signaling Data Link Connection Acknowledgment.
38	CNS	Connection Not Successful Signal	A negative response when a DLC message is received. The requested channel is not available for SS7. The CNS message signals that further attempts to activate such a link can be made, which differentiates it from the CNP message. The generic term for CSS, CNS, and CNP is Signaling Data Link Connection Acknowledgement.
48	CNP	Connection Not Possible Signal	A negative response when a DLC message is received. The requested channel is not available for SS7. The CNP message signals that further attempts to activate such a link are useless, because no connection can be established at all, which differentiates it from the CNS. The generic term for CSS, CNS, and CNP is Signaling Data Link Connection Acknowledgement.

Table 8.4 (continued)

H1/H0	Abbr.	Name	Description
23	TFC	TransFer Controlled	The TFC message is sent by STPs when overload to particular Point Codes occurs. When an STP receives MSUs destined for those point codes, then the STP sends a TFC message to the sender of this MSU as a notification of the overload situation. If further MSUs are received from the same sender, then the TFC message is repeated every eighth time a MSU is received (refer also to the RCT message).
16	LIN	Link INhibit Signal	It is possible that a particular link fails frequently and, hence, must be regarded as insecure. SS7 allows to automatically take such a signaling link out of service. This is done with a LIN message. Please note that this blocks the connection for user signaling only, and that it is still possible to transfer management messages or test messages.
26	LUN	Link UNinhibit Signal	The LUN message is the counter part of the LIN message. A connection that was taken out of service was tested in the meantime, manually or automatically, and shall now be reactivated.
36	LIA	Link Inhibit Acknowledgement Signal	The LIA message is the response when a LIN message was received. A link shall not be available for user signaling anymore.
46	LUA	Link Uninhibit Acknowledgement Signal	The LUA message is the response when a LUN message was received. A connection that was taken out of service is now available again for user signaling.
56	LID	Link Inhibit Denied Signal	Negative response to a LIN message. The connection can not be taken out of service (e.g. because no alternative links are available).
66	LFU	Link Forced Uninhibit Signal	When taking a link out of service, one has to distinguish between the active side, which wants to trigger this action by sending a LIN message, and the side which receives the LIN message. Only the receiving side can send a LFU message, in order to request that this link is brought back to service. (This is a request to send a LUN message.)
76	LLT	Link Local Inhibit Test Signal	The status of the connection is tested by that SP/STP, which originally requested to inhibit the link, by periodically sending a LLT message to the peer entity. When a SP/STP receives a LLT message, it checks whether the link was actually inhibited by that node. If this is the case, no action is undertaken and the status is considered satisfactory. If, however, the link was originally inhibited by that entity which received the LLT message, then there is some inconsistency. In order to resolve this inconsistency, a LFU message is sent as an answer to the other node.

Table 8.4 (continued)

H1/H0	Abbr.	Name	Description
86	LRT	Link Remote Inhibit Test Signal	When an SP/STP receives a LIN message, it expects to periodically receive LLT messages. If this time period, during which the test message was expected expires, then a LRT message is sent to the peer SP/STP.
17	TRA	Traffic Restart Allowed Signal	The TRA message is sent by an SP/STP to a neighboring SP/STP when this neighbor comes back to service, that is, when it can carry data again. When a STP comes to service, this STP also sends TRA messages to all neighbors. This does not apply to an SP.
13	RCT	Signaling Route Set Congestion Test	The RCT message allows an SP/STP to test whether the path to a particular destination STP is available. An RCT message is sent when a TFC message was previously received from the destination STP and the state is uncertain.
1A	UPU	User Part Unavailable	When an SP receives a message for a particular User Part (e.g., SCCP) which is currently not available, then a UPU can be returned to the sender of the original message as a notification about this unavailability of the User Part.

Table 8.5
Message Types in SS7 Network Test

H1/H0	Abbr.	Name	Description
11	SLTM	Signaling Link Test Message	Layer 3 uses the SLTM for the initial test and the periodic test of a SS7 link. The SLTM carries, for this purpose, a sequence of up to 15 test bytes, which the peer needs to correctly receive.
21	SLTA	Signaling Link Test Acknowledge	Every SLTM has to be acknowledged with a SLTA. The SLTA returns the test sequence, previously received in the SLTM, back to the sender.

9

Signaling Connection Control Part

The SCCP uses the layers MTP 1 through 3 of SS7. In GSM, those services are used by a number of subsystems (Figure 9.1). The services of the SCCP are used, in particular, by the base station subsystem application part (BSSAP) on the A-interface and by the transaction capabilities application part (TCAP) together with the mobile application part (MAP) on the various interfaces within the NSS. Note that ISUP also may use the SCCP, but fewer and fewer applications use that combination.

9.1 Tasks of the SCCP

In contrast to the MTP 1 through 3, which is responsible for the transport and address functionality between two network nodes, the SCCP, by means of its Layer 3 functions, offers end-to-end addressing, even across several network nodes and countries. Additionally, the SCCP allows for a distinction among the various applications within a network node; internally, the SCCP refers to these applications as subsystems. Two connection-oriented and two connectionless service classes are available to the users of the SCCP for actual data transfer.

Furthermore, the SCCP comes with its own management functions for administrative tasks, which are independent from those known from the SS7 signaling network management. Although the SCCP is considered a Layer 3 functionality in the ITU Recommendations Q.711 through Q.714, it also provides features that belong to Layer 4, including mechanisms for error detection and an optional segmentation of the data to be transmitted.

Samsung Ex. 1032, Page 159 of 417

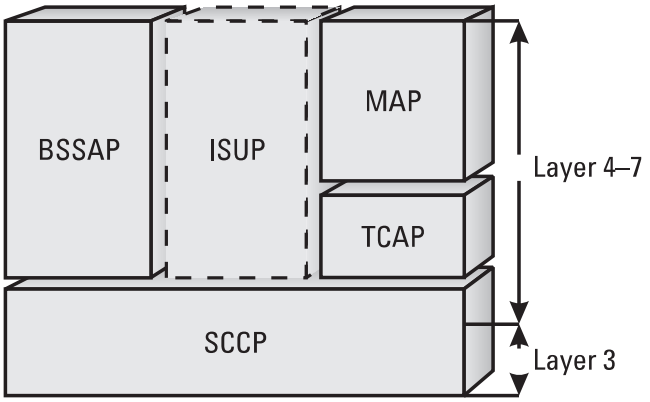


Figure 9.1 The SCCP as a platform for various users.

9.1.1 Services of the SCCP: Connection-Oriented Versus Connectionless

The SCCP offers two connection-oriented and two connectionless service classes to its users. The difference between the two is as follows. Two network nodes establish a virtual connection between the two subsystems for transaction 1, 2, or 3, in case of the connection-oriented mode. The identification of the connection is achieved via reference numbers, the source local reference (SLR) and the destination local reference (DLR). While such a connection is active, it is possible not only to exchange data between the two network nodes but also to address individual transactions.

Figure 9.2 illustrates this relation. The SCCP analyzes the data received from the MTP and forwards the data to the addressed subsystem, where the input data is associated with the various active transactions. Typical examples in GSM for connection-oriented transactions are a location update and a MOC within the BSSAP.

In the case of connectionless service classes, the SCCP provides no referencing; the recipient of a message must assign it to an active process. Examples for connectionless applications are PAGING in the BSSAP, SCCP management, and the TCAP protocol.

Distinguishing between connection-oriented and connectionless service within the SCCP is achieved by a parameter called the protocol class (described in Section 9.3.2.5).

9.1.2 Connection-Oriented Versus Connectionless Service

The difference between connection-oriented and connectionless service can best be explained by the example of sending a letter. The postal service provides the physical means for mail transfer. The individual envelopes correspond to

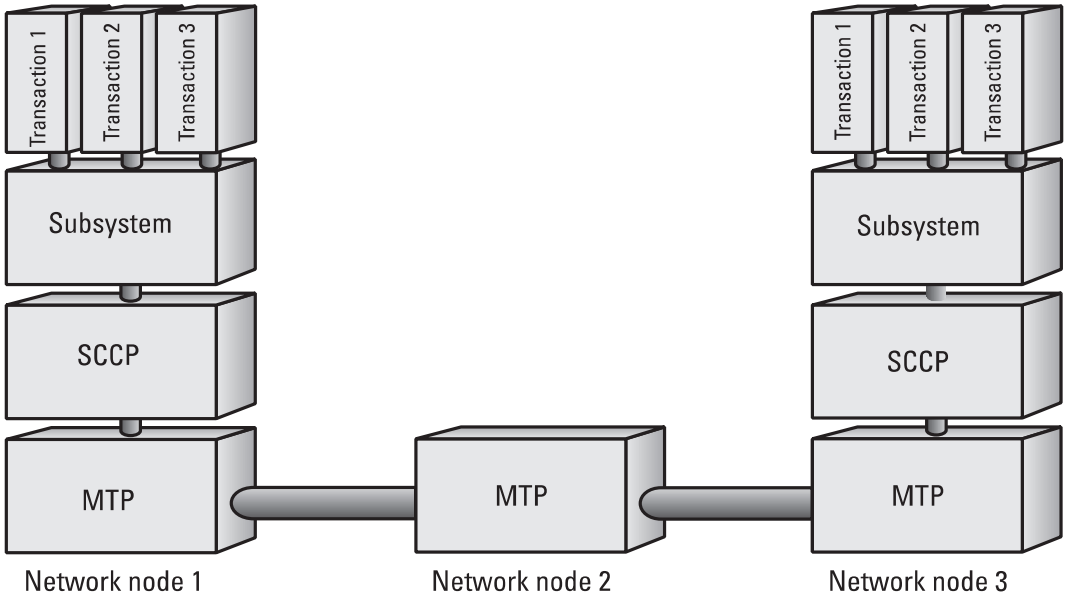


Figure 9.2 Connection-oriented services of the SCCP.

the MSUs, and the letter inside the envelope corresponds to the SCCP message (Figure 9.3).

9.1.2.1 Connection-Oriented Service

When two parties of any particular company correspond via mail, they typically address many issues. References for each issue need to be assigned, so the recipient can distinguish among them. That corresponds to a virtual

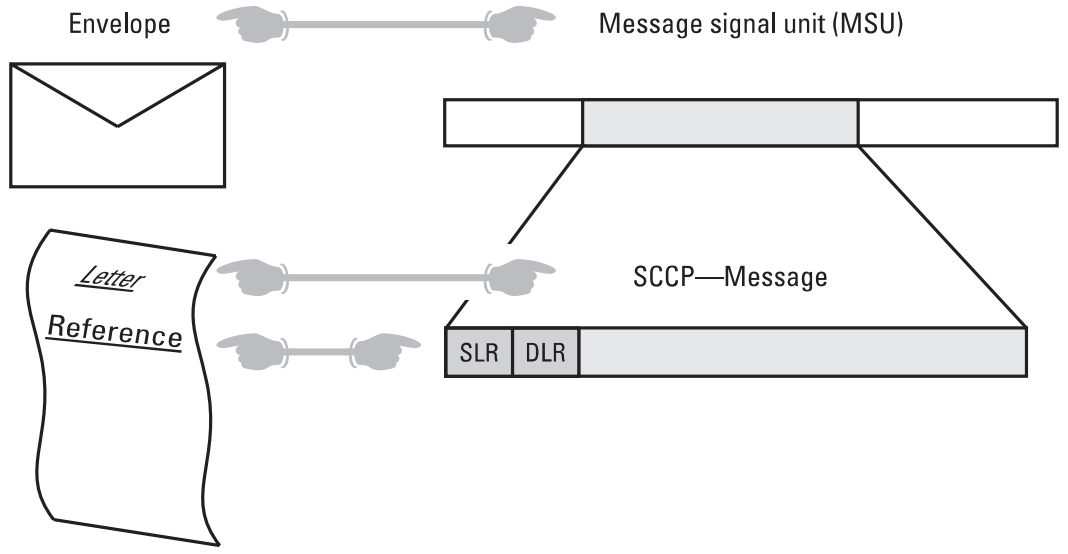


Figure 9.3 The task of SLR and DLR.

connection setup. The various issues that arise could be an unpaid bill or a new order. Each side tries to make the issue clear, for example, by adding a headline or a reference line to establish a unique reference. The function of the reference corresponds to the task of SLR and DLR of connection-oriented services in the SCCP. A virtual connection between sender and recipient is set up in both cases. "Virtual" here means that no permanent, dedicated physical path between the two parties exists.

9.1.2.2 Connectionless Service

A person who vacations in a faraway country typically sends postcards to relatives and friends. Each postcard needs an address to enable delivery, but there is no reference to a specific issue and no answer is expected. It is, therefore, a conversation that does not require an immediate reference or a connection setup.

This comparison is valid only for the SCCP itself. The recipient has the opportunity to include a reference in the data part of the message and hence establish a relation to an issue, even when using the connectionless service classes. (An example is provided in Chapter 11.)

9.2 The SCCP Message Format

The complete SCCP message is hosted, together with the routing label by the SIF of an MSU (Figure 9.4). Only the identifier for the user part SCCP is carried in the SIO outside the SIF. The SCCP is the immediate layer above the MTP, and a wide variety of messages with different formats and tasks are defined for the SCCP. The peculiarities of the SCCP message format will be explained first; the single messages are then described in more detail. Figure 9.5 presents the general format of a SCCP message.

SCCP messages consist of the following parts (refer to Figures 9.4 and 9.5):

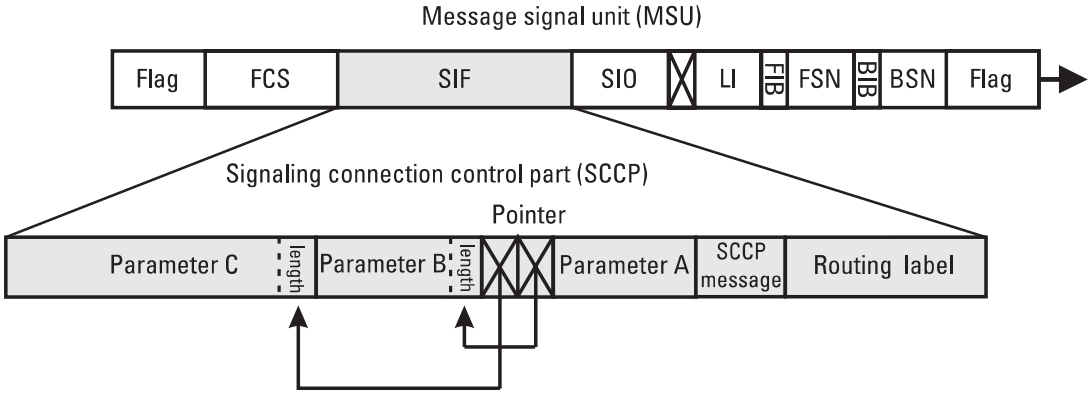


Figure 9.4 The MSU as the transport frame for the SCCP.

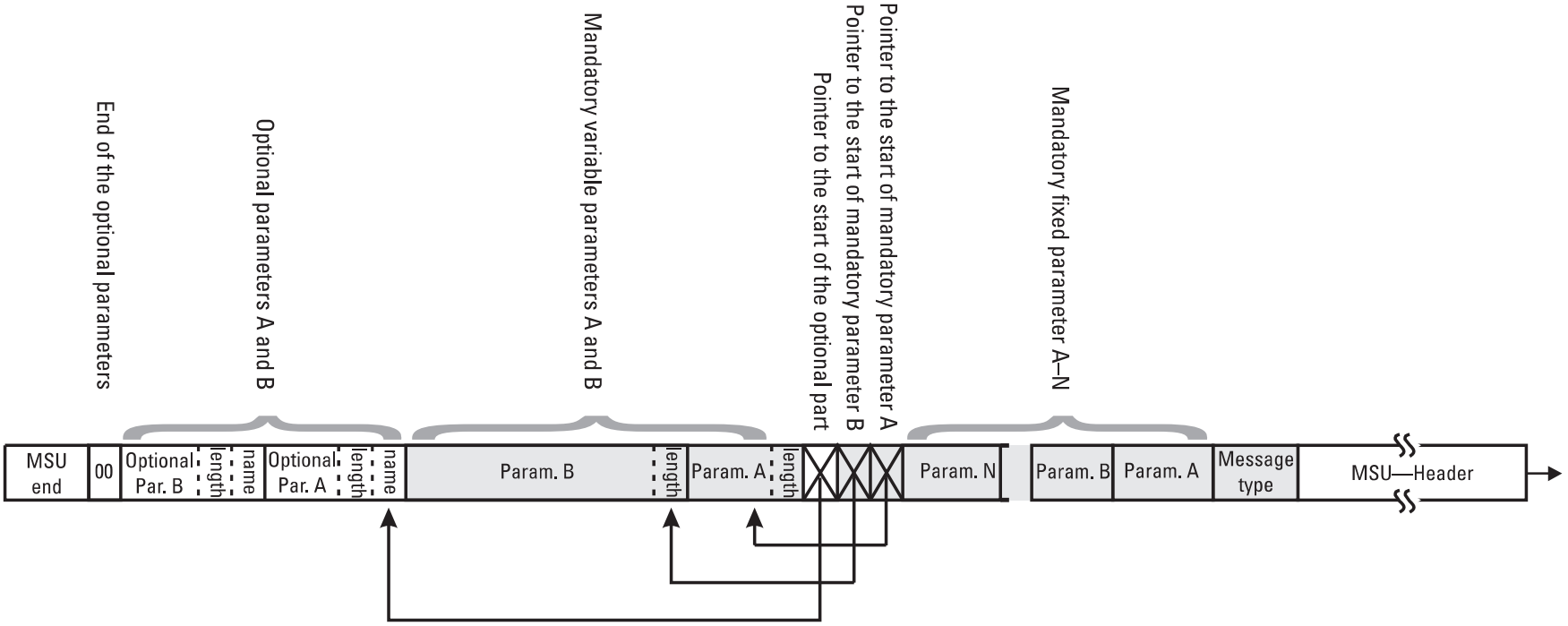


Figure 9.5 General format of an SCCP message.

- Mandatory fixed part. The parameters of this part are mandatory and of fixed length, and their order is fixed. That allows omission of an identifier for the parameter as well as a length indicator.
- Mandatory variable part. The parameters of this part are mandatory and their order is fixed; however, their length may vary, depending on the situation. Again, no identifier is necessary, but a length indicator is required to determine the parameter's position in the message. The length indicator uses an additional byte for each parameter.
- Optional part. All the parameters of this part are optional, that is, a particular parameter may or may not be present in a given message, depending on the circumstances. To enable the recipient of a message to identify the optional parameters, they require an identifier and a length indicator for each such parameter present in the message. Every SCCP message that can contain optional parameters has to have an end-of-optional-parameters (EO) indicator to signal the end of the parameter list (see also Section 9.3.2.3). The code for the EO is 00, which mandates that this value be excluded as a valid identifier.
- Pointer. Every pointer is 1 byte in length. The value of a pointer indicates the distance to the beginning of the field to which it points. One pointer is necessary for every mandatory variable parameter, while only one pointer is necessary for the whole optional part, which points to the start of the optional part, indifferently from the number of parameters contained in that part.

Figure 9.5 presents the general format of a SCCP message. The mandatory part is shaded, while the optional part is in white. (Similar shading is applied to all illustrations of SCCP messages.)

9.3 The SCCP Messages

Figures 9.6(a) and 9.6(b) illustrate those SCCP messages used in GSM.

9.3.1 Tasks of the SCCP Messages

Table 9.1 lists all the SCCP message types that are defined in ITU Recommendations Q.712 and Q.713 *and* used in GSM. The uppercase letters relate to the abbreviations used in this context. Table 9.2 lists the SCCP management messages sent in the data part of UDT messages.

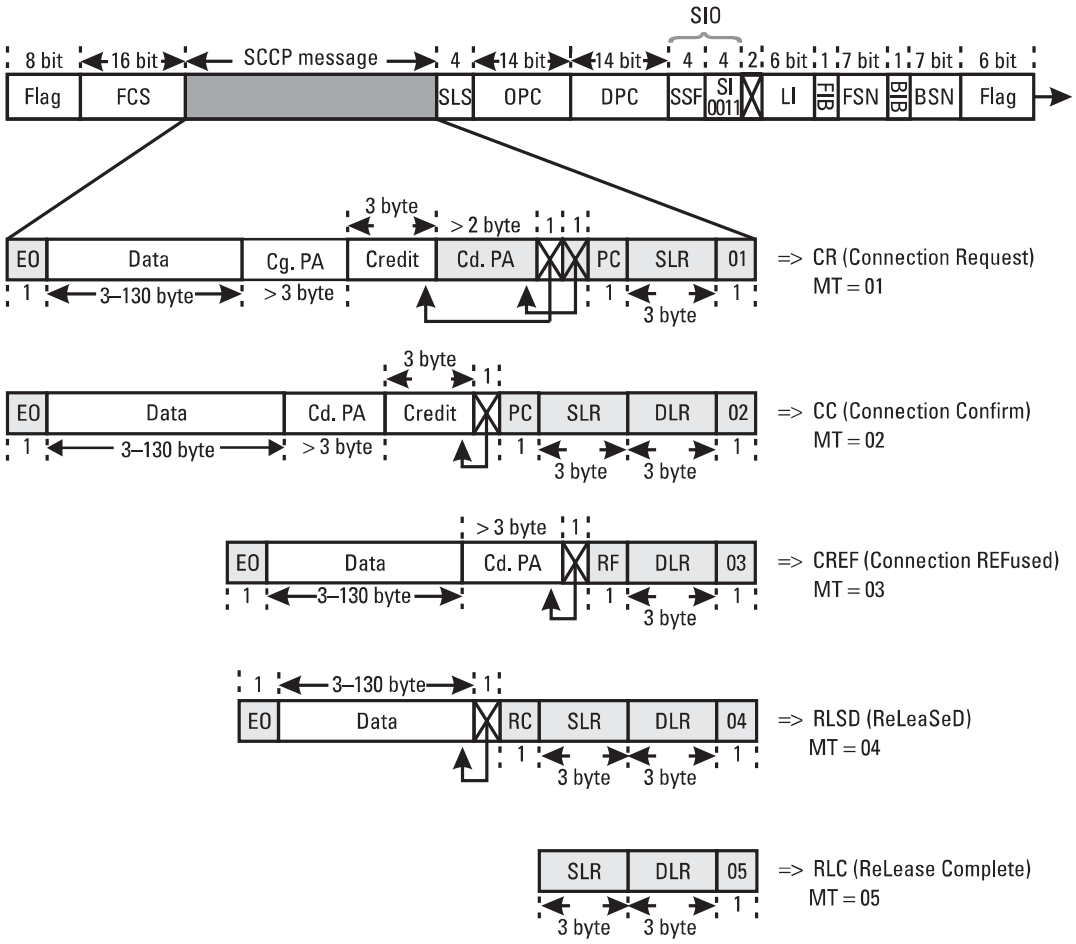


Figure 9.6(a) SCCP messages in GSM (part 1).

9.3.2 Parameters of SCCP Messages

This section presents all the parameters of SCCP messages and describes their task. The same abbreviations are used in the description as in Figure 9.6(a) and 9.6(b). When length information is given for a parameter, it relates only to the parameter itself and not to a possibly necessary length indicator or type field (different from the illustrations).

9.3.2.1 Calling-Party Address and Called-Party Address (>2 Bytes)

The calling-party address (CaPA) and the called-party address (CdPA) have the same format and identify the type of address as well as the address itself. An address may consist of any combination of the following:

- The SPC (2 bytes);
- The SSN (1 byte);
- The global title (> 3 bytes).

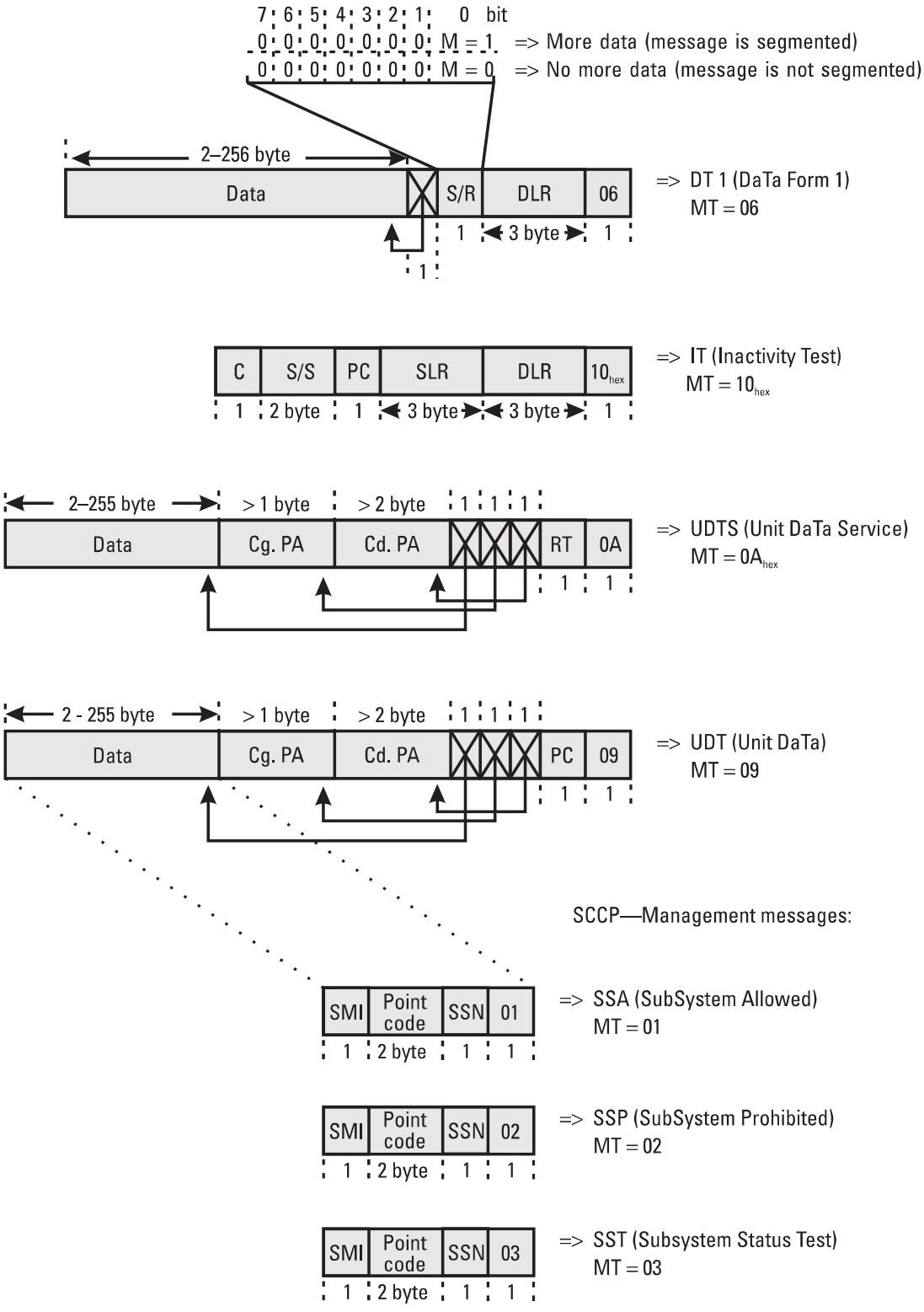


Figure 9.6(b) SCCP messages in GSM (part 2).

Table 9.1
SCCP Message Types

ID (Hex)	Message Type	Connection Oriented?	Description
01	CR (Connection Request)	Yes	Is sent from the BSC to the MSC or vice versa at the beginning of a connection set up, in order to request an SCCP connection. A CR includes in its data part, for example, the whole LOC_UPD_REQ or HND_REQ (BSSAP).
02	CC (Connection Confirm)	Yes	A positive response to CR. Acknowledges receipt of CR and establishment of the requested SCCP connection.
03	CREF (Connection REFused)	Yes	Negative response to CR. The SCCP of a signaling point (BSC or MSC) is unable to provide the requested SCCP connection. A cause value is supplied when the CR is answered by CREF.
04	RLSD (ReLeaSeD)	Yes	The RLSD message is always sent from the MSC to the BSC, in order to release an SCCP connection. The assigned memory resources are released, too.
05	RLC (ReLease Complete)	Yes	The acknowledgement of the receipt of an RLSD message and the confirmation that the assigned SCCP resources were released.
06	DT 1 (DaTa Form 1)	Yes	The entire data transfer between BSC and MSC is performed in DT 1 messages after an SCCP connection was established by a CR and CC. DT 1 messages belong, in contrast to DT 2 messages (which are not used in GSM), to protocol class 2. DT 2 messages belong to protocol class 3 and provide additional mechanisms for error detection.
09	UDT (Unit DaTa)	No	In contrast to the messages presented above, UDT messages provide for connectionless services (protocol class 0 and 1). UDT messages in GSM are used by MAP/TCAP for all data transfer tasks and on the A-interface to convey PAGING messages (among others). Another application of UDT messages is to transmit SCCP management messages.
0A	UDTS (Unit DaTa Service)	No	When the SCCP of a signaling point receives a UDT message with protocol class 1 that can not be processed or forwarded to the addressed subsystem, then a UDTS message is returned to the sender. The original UDT message may then be repeated.

Table 9.1 (continued)

ID (Hex)	Message Type	Connection Oriented?	Description
10	IT (Inactivity Test)	Yes	Every side may periodically send an IT message in order to query the state of an SCCP connection and correct a possible inconsistency of data.

Table 9.2
SCCP Management Messages
(Sent in the Data Part of UDT Messages)

ID (Hex)	Message Type	Connection Oriented?	Description
01	SSA (SubSystem Allowed)	No	Both sides may send it to the respective peer as information that a previously not available subsystem is now available. Examples of subsystems are SCCP management, BSSAP, the VLR, the HLR, or the MSC.
02	SSP (SubSystem Prohibited)	No	An available subsystem has to be taken out of service.
03	SST (SubSystem Status Test)	No	The state of a subsystem which is reported as not available can be queried by sending an SST message.

If all three are present, they appear in exactly the order listed. Figure 9.11 presents the subsystems currently defined for the SCCP. The parameters CaPA and CdPA are necessary for end-to-end addressing of SCCP messages, as indicated in Figure 9.7.

MAP uses all possible combinations, while the BSSAP requires only the SPC and the SSN (= BSSAP) for addressing.

Global Title

A switching exchange or any SCCP network node, particularly for international connection requests, has no information source for routing purposes