VIRTUAL ROAMING SYSTEMS FOR GSM, GPRS AND UMTS

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

VIRTUAL ROAMING SYSTEMS FOR GSM, GPRS AND UMTS

OPEN CONNECTIVITY IN PRACTICE

Arnaud Henry-Labordère

Professor at Ecole Nationale des Ponts et Chaussées, France

WILEY

A John Wiley & Sons, Ltd., Publication

This edition first published 2009

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

Library of Congress Cataloguing-in-Publication Data

Henry-Labordère, A.
Virtual roaming systems for GSM, GPRS and UMTS / Arnaud Henry-Labordère.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-68262-3 (cloth : alk. paper) 1. Roaming (Telecommunication) I. Title.
TK5103.4874.H46 2009
621.382′1–dc22
2009021654

A catalogue record for this book is available from the British Library.

ISBN 9780470994016 (H/B)

Set in 9 on 11 pt Times by SNP Best-set Typesetter Ltd., Hong Kong
Printed in Singapore by Markono Print Media Pte Ltd.

Contents

Preface

Easy roaming is one of the advantages, which made the GSM standard prevail over other standards during the past few years. Customers often think that they can go anywhere and use their services to call, SMS or MMS any mobile in the world, as well as having their data services or Visio 3G. In reality, this is still far from being true. The subject of SMS interworking has been covered in a previous book and there are, in 2009, about 15 suppliers, which claim to be able to provide SMS termination for a large coverage using the principles developed there; unfortunately many offer a 'black hole' solution which is not able to correctly report if the message was delivered.

In the last five years, interest has arisen in generalizing this to 'Open Connectivity', that is full 'Virtual Roaming': being able to use one's phone everywhere, even if there is no bilateral agreement between the 'home network' and the 'visited network'. This is thanks to the use of a 'third party', which has agreements with both and does the invoice clearing as well as the necessary signalling modification, so that this novel arrangement is almost transparent to the two parties concerned. The term 'Open Connectivity' was introduced by the GSM association in 2005 as an equivalent to 'Virtual Roaming'. It covers two services: allowing a (typically small) network to have its subscribers roam in any network ('outbound subscribers virtual roaming'), and allowing a (typically small) network to receive and invoice visitors from other countries. The demand for these services is mostly from the smaller networks, rather than from the larger operators that already have a roaming partner in most countries, as this represents only additional business.

The implementation of 'Virtual Roaming' systems for GSM (2G), GPRS (2.5G), and UMTS (3G) is the subject of this book. It encompasses the well-known 'SMS Hubs' architecture used for SMS interworking as well as voice, data GPRS and 3G virtual roaming.

In terms of roaming, radio access technology is not involved except for the negotiation of common supported features and one can question if this is applicable to the new 4G.

It is too early to come to a definitive conclusion about 4G systems for the 'Long-Term Evolution' of radio access and the 'Evolved Packet System'. The roaming procedures of 4G subscribers to another Evolved Packet System or to a 'legacy system' are today only at the level of High Level Requirements and no practical implementation can be presented. Quoting [2.11] page 8: *'The Evolved Packet System shall provide functionality to support outbound (and inbound) roaming subscribers on (from) other Evolved Packet systems and Legacy networks'*. The latest Release 8 of the 3GPP standard [2.3], covering roaming, mentions 'LTE' only in the title and one can thus assume that a fully new protocol for 4G is a task which is unlikely to be attempted. One can therefore believe that even if the transport network is new, since 2.5G and 3G have generalized the usage of packets inside the core networks to replace circuits, the base procedures will remain the same.

On the other hand, 3G virtual roaming is completely covered as it encompasses the same roaming procedures as 2G and 2.5G (packet data over an IP network such as GRX). There are simply a few different or additional parameters of the MAP and CAMEL protocols which must be relayed properly. The final chapter gives existing solutions for mobile ↔ fixed convergence in the expected future 4G standards: roaming costs can be drastically reduced as all communications between the Home Network and some remote visited country can use IP while providing a transparent service to the users.

After spending the last few years on SMS and its interworking, this is the generalization to voice and data virtual roaming for which work was started in 2002 (first patent in 2003). It then became a very real subject through the interest of the GSM association. This book is intended for people in charge of commercial or technical roaming with the 1200 existing mobile operators worldwide, for engineers developing virtual roaming systems and associated Value Added Services, and also for mobile telecommunications SS7 courses. Virtual roaming is a very comprehensive application of MAP, CAMEL, TCAP, SCCP and GTP, which allows these various topics to be put into a common perspective that is very useful for consolidating a detailed understanding.

We have also integrated various original solutions which are useful for making virtual roaming effective or for developing general software for Roaming Hubs. This book is for developers (they will find the traces invaluable), students and the roaming specialists of all the mobile operators. It assumes that they have a background in the protocols used, notably SS7. There are many excellent books which have covered the subject and this one explains systems and applications.

Chapter 1 is an introduction to the standard roaming procedure and to the principle of virtual roaming: open connectivity for inbound visitors and multi-IMSI systems for outbound subscribers.

The less obvious business model, such as GPRS virtual roaming (a new subject), is also presented. The brief illustrated explanation of the SS7 standard protocol layers will be useful for nonspecialists but a good knowledge of roaming procedures and SS7 is required. The trace examples and personal study of the references will enable the necessary knowledge base to be obtained.

Chapter 2 describes Virtual Roaming, including the prepaid case with CAMEL parameter transformations, SMS, Supplementary Services and USSD implementations in a comprehensive way. It also includes the equipment checking procedures to implement control of stolen handsets with a virtual roaming agreement and the small difference for UMTS. It also contains a brief presentation of the GSM standard ↔ IS 41 transformations for inter-standard roaming, allowing a CDMA subscriber to roam almost seamlessly (they have to have a GSM handset but keep the same service) in a GSM network. Much pioneering work (commercially offered as ‘Pick-to-roam’, etc.) was done many years ago for this case because of the large demand from CDMA users (Korea, USA) for roaming. It briefly explains the Roaming Hub architecture when a virtual visitor with a number from an IS 41 network wants to use a GSM phone with the virtual roaming service. The subject of transparent protocol conversion and interworking covers an important part of the world market as 18 % of mobiles are IS 41. In the particular case of SMS interworking, no one in 2009 is providing a transparent service.

Chapter 3 is for the connection of customers of the Roaming Hub: how Mobile Network operators must configure their network to route virtual visitors’ traffic to the Roaming Hub. Also, for the Roaming Hub operator: how a multiple Point Code Roaming Hub works in detail to connect customers with National or International Point Codes. It also includes an introduction to SIGTRAN configuration, since many SCCP gateways provide a SIGTRAN M3UA or M2PA interface, which makes the implementation of powerful Roaming Hubs quite simple.

This chapter is the most technical of the book. It will be very useful for operations staff configuring their SCCP gateway or virtual roaming agreements and also for software developers of Roaming Hub systems as they must include some advanced SCCP functions in order to simplify the provisioning of new customers. The connection, according to the proposed method of the GSM association, is explained as well as compatibility with more advanced schemes such as those in Chapter 3.

Chapter 4 describes the method of networking several Roaming Hubs so they cooperate for a larger coverage as well as for Mobile Number Portability resolution. We use our original TCAP-based Hub end-to-end addressing so that a given Hub can force a path to a given destination mobile network through a given final Hub. It is mandatory in a Mobile Number Portability context.

Chapter 5 describes ‘hosted Roaming Hubs’, which may have several GTs provided by different networks. It raises special problems for which detailed original solutions are given.

We go beyond the core subject of Roaming Hubs with the chapters that follow, because they concern other services which could be offered by a supplier that uses the strategic position in the middle of SS7 signalling, and also explain some of my research subjects in recent years.

Chapter 6 is about offering Location-based Services (geo-localization) to visitors. It gives the solution of the network side in full detail with a fuller implementation of the algorithm than in [5.1]. The communication with Base Station Controllers to get measurements uses 'Connection Oriented' SCCP, which is not so well known as 'Connectionless' SCCP, so the full details and traces are included to show how it works. We have also explained how the 'spyware' methods embedded in the handset work. As the little-known details are explained, this chapter would make the book worth having in itself. There are many documents and books on the subject, but none of them gives so many details for developers of LBS core platforms, including how to get location alerts when a subscriber is nearing an area.

Chapter 7 methods are for outgoing call procedures to reduce the charges received from roaming partners; even if it is not directly relevant to virtual roaming, it can be used to increase the interest of virtual outbound roaming. The integration of CAMEL-based methods, Call Back and local calls is original and gives an elegant global solution.

Chapter 8 covers Over The Air (OTA) provisioning of SIM cards. It is appropriate because of the need to load 'SIM Tool Kits' to implement 'multi-IMSI' outbound subscribers' virtual roaming. Preferred networks can also be set for cost optimization. Our aim is to provide a reference document in a few pages with full practical development details that are not well-known in general. We give the computation and formatting for Cryptographic Checksum, as well as the structure of the main files of the SIM card directory. The various steps of the ciphering are shown and will provide complete understanding, so this part will be a reference for any engineer wanting to use or even develop an OTA SIM server. Many practical details are given, which could allow anyone to develop a SIM card OTA and verify step by step that the payload is correct, as well as the data selected and the checksum or ciphering result.

Chapter 9 is about the OTA provisioning of handsets to set their Internet access using GPRS. Special accesses can then be easily provided for roamers. The solution presented is very original as there is an automatic learning of the profile type (two main modes exist), without relying on an accurate IMEI (model type) → profile type, which is impractical (more than 13 000 model types). Even if NSS engineers know the purpose, they often ignore the details.

We finish with the perspective for 4G, although the specific standards concerning roaming are not yet available. Chapter 10 presents an existing solution for optimized roaming with roamers using a PC or an Internet-connected phone with a VoIP connection to their Home Network. This is a recent idea and the originality is that it does not use a '3G key modem' for data connection in order to avoid the high charges of GPRS data, but instead uses a fixed line or Wi-Fi connection that a roamer gets at their hotel or work place abroad. This is in line with the High Level Requirements of 4G, although the various existing solutions are not standardized, but the solutions presented do work with existing 2G and 3G networks.

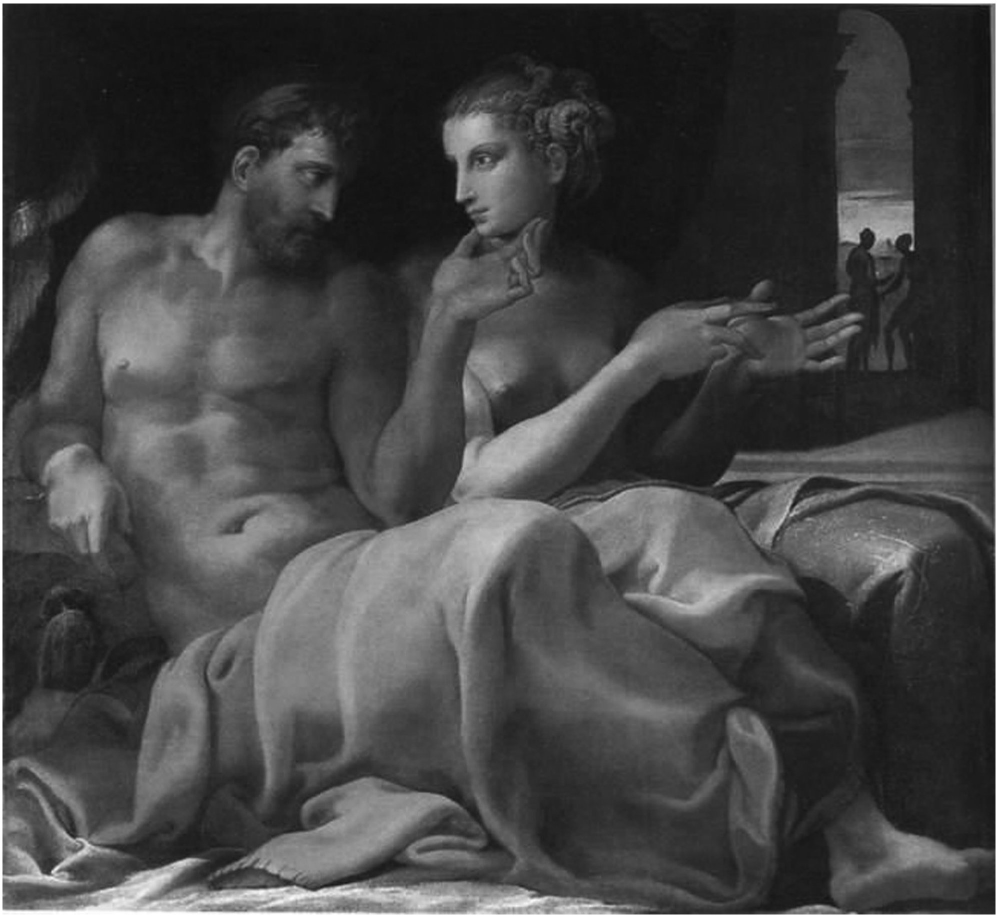
We also give an overview of the IMS architecture that has an impact on virtual roaming. It is a subject which will be of significance for some years, in particular using high bandwidth HSPDA to make Visio calls using the Packet Domain, and there are ways of making regular calls without IPV6 or 'presence servers', with a much better quality than H324-M, which is limited to 64 Kbits/sec on a fixed network.

As it is an efficient teaching method, in Chapter 11 we show many selected traces so that they can be used as a highly practical course. For the specialists, it is probably the most useful part of this book as it immediately answers many practical questions if they want to develop a solution.

We have provided a comprehensive list of abbreviations, which the reader can use when they meet one of the many acronyms that they may not know: in addition, this avoids including the explanation in the text.

Virtual Roaming is the objective and it has been ongoing since 1999; starting with SMS then MMS interworking. As it is big business, many suppliers have entered these two markets, but several implementations are very poor as they lack the Quality of Service which can only be provided by the SS7 signalling transparency. It is the aim of this book to explain a full Roaming Hub solution, including principles for bridging between the two main standards, GSM and IS 41, and the full provision of all existing mobile services in a virtual roaming situation, in the soon to arrive reality of an all IP network. The billing issues are not addressed much, except in Chapter 1, which does not mean that they are considered easy or not important, but simply that the technology and problems are remote from the rest of the book.

A course at France Telecom, when they launched the implementation of their Virtual Roaming system at the end of 2008, gave me the opportunity to prepare this practical text book. Their experts deserve many thanks for their advice and quality checking of the Roaming Hub software as do the RD of HALYS, which developed it. I would like also to thank the referees and the editor.



Francesco Primaticcio, Italian (Mantua, active France), 1504–1570, *Ulysses and Penelope*, about 1560, oil on canvas, 121.3 × 170.2 cm, Purchased with funds from the Libbey Endowment, Gift of Edward Drummond Libbey, 1964.60. Photo Credit: Toni Marie Gonzalez, Toledo Museum of Art. Reproduced by permission.

'Penelope telling Ulysses her ordeals while he was roaming away'

Painting of Primatice (Francesco Primaticcio)

VIRTUAL ROAMING

BY THE SAME AUTHOR

‘Méthodes et Modèles de la Recherche Opérationnelle, Vol. 3’ (with Arnold Kaufmann), Dunod, 1973, translated to English ‘Integer and Mixed Programming’, Addison Wesley (1976), Russian (MIR, 1975), Spanish (CCSA, 1975), Romanian (1976).
‘Exercices et Problèmes de Recherche Opérationnelle’, Masson, 1976.
‘Analyse de données’, Masson, 1976.
‘Recherche Opérationnelle’, Presses des Ponts et Chaussées, 1981.
‘Cours de Recherche Opérationnelle’, Presse des Ponts et Chaussées, 1995, Vol. 1, linear and nonlinear programming, graphs, Vol. 2, optimal control, game theory.
‘SMS and MMS interworking in Mobile Networks’, (with Vincent Jonack), Artech Publishing House, 2004.

Abbreviations and Acronyms

A

A3	Authentication algorithm A3
A38	A single algorithm performing the functions of A3 and A8
A5/1	Encryption algorithm A5/1
A5/2	Encryption algorithm A5/2
A5/X	Encryption algorithm A5/0-7
A8	Ciphering key generating algorithm A8
AA19	Standard GSM contract between two operators for the charging of the SMS-MT sent to their own subscribers by the other operator
AB	Access Burst
AC	– Access Class (C0 to C15) – Application Context
ACC	Automatic Congestion Control
ACCH	Associated Control CHannel
ACK	ACKnowledgement
ACM	– Accumulated Call Meter (a zone of a SIM card) – Address Complete Message (Response to a ISUP Call setup)
ACMmax	Maximum of the Accumulated Call Meter
ACSE	Association Control Service Element
ACU	Antenna Combining Unit
ADC	– ADministration Centre – Analogue to Digital Converter
ADD	Automatic Device Detection (inclusion of IMEIsv in Update Location)
ADN	Abbreviated Dialling Number
ADPCM	Adaptive Differential Pulse Code Modulation
AE	Application Entity
AEC	Acoustic Echo Control
AEF	Additional Elementary Functions
AGCH	Access Grant CHannel
Ai	Action indicator
AMPS	Advanced Mobile Phone System (Analogue mobile Radio system)
ANSI	American National Standards Institute
AoC	Advice of Charge
AoCC	Advice of Charge Charging supplementary service
AoCI	Advice of Charge Information supplementary service
APLMN	Associated Public Land Mobile Network

APN	Access Provider Name
ASE	Application Service Element
ASN.1	Abstract Syntax Notation One
ARFCN	Absolute Radio Frequency Channel Number
ARQ	Automatic ReQuest for retransmission
ASP	Application Service Provider (Content Provider for Internet services)
ATT (flag)	ATTach
AU	Access Unit
AuC	Authentication Centre
AUT(H)	AUThentication

B

BA	BCCH Allocation
BAIC	Barring of All Incoming Calls supplementary service
BAOC	Barring of All Outgoing Calls supplementary service
BCC	Base Transceiver Station (BTS) Colour Code
BCCH	Broadcast Control CHannel
BCD	Binary Coded Decimal
BCF	Base station Control Function
BCIE	Bearer Capability Information Element
BER	Bit Error Rate
BFI	Bad Frame Indication
BI	all Barring of Incoming call supplementary services
BIB	Backward Indicator Bit
BIC-Roam	Barring of Incoming Calls when Roaming outside the home PLMN country supplementary service
Bm	Full-rate traffic channel
BN	Bit Number
BO	all Barring of Outgoing call supplementary services
BOIC	Barring of Outgoing International Calls supplementary service
BOIC-exHC	Barring of Outgoing International Calls except those directed to the Home PLMN Country supplementary service
BS	– Basic Service (group) – Bearer Service
BSG	Basic Service Group
BSC	Base Station Controller GSM 2G
BSIC	Base transceiver Station Identity Code
BSIC	CELL BSIC of an adjacent cell
BSN	Backward Sequence Number
BSS	Base Station System (GSM 2G)
BSSAP	Base Station System Application Part
BSSAP-LE	Base Station System Application Part-Location Extension
BSSMAP	Base Station System Management Application Part
BSSOMAP	Base Station System Operation and Maintenance Application Part
BTS	Base Transceiver Station GSM 2G

C

C	Conditional
CA	Cell Allocation

CAI	Charge Advice Information
CAMEL	Customised Application for Mobile Network
CB	Cell Broadcast
CBC	– Cell Broadcast Centre
	– Ciphering Block Chaining (used in the 3DES algorithm)
CBCH	Cell Broadcast CHannel
CBMI	Cell Broadcast Message Identifier
CC	– Country Code
	– Call Control
CCBS	Completion of Calls to Busy Subscriber supplementary service
CCCH	Common Control CHannel
CCF	Conditional Call Forwarding
CCH	Control CHannel
CCITT	Comité Consultatif International Télégraphique et Téléphonique (The International Telegraph and Telephone Consultative Committee)
CCM	Current Call Meter
CCP	Capability/Configuration Parameter
CCPE	Control Channel Protocol Entity
Cct	Circuit
CDMA	Code Division Multiple Access
CDR	Call Detailed Record (billing record)
CDUR	Chargeable DURation
CED	Called Station Identifier
CEIR	Central Equipment Identity Register
CEND	End of Charge Point
CEPT	Conférence des administrations Européennes des Postes et Télécommunications
CF	– Conversion Facility
	– all Call Forwarding services
CFB	Call Forwarding on mobile subscriber Busy supplementary service
CFNRc	Call Forwarding on mobile subscriber Not Reachable supplementary service
CFNRy	Call Forwarding on No Reply supplementary service
CFU	Call Forwarding Unconditional supplementary service
CHP	CHarging Point
CHV	Card Holder Verification information
CI	– Cell Identity
	– CUG Index
CIC	Circuit Identification Code
CIR	Carrier to Interference Ratio
CKSN	Ciphering Key Sequence Number
CLI	Calling Line Identity
CLIP	Calling Line Identification Presentation supplementary service
CLIR	Calling Line Identification Restriction supplementary service
CM	Connection Management
CMD	CoMmanD
CMM	Channel Mode Modify
CNF	CoNFirmation (Answer to a REQ (Request))
CNG	CalliNG tone
CNTR	Counter (control for OTA SIM security)
COLI	COnnected Line Identity
COLP	COnnected Line identification Presentation supplementary service

COLR	COnnected Line identification Restriction supplementary service
COM	COMplete
COMP	128 Authentication and Ciphering algorithm used for A3 and A8 (GSM)
COMP	128-2 Improved algorithm used for UMTS
CONNACK	CONNect ACKnowledgement
C/R	Command/Response field bit
CRC	Cyclic Redundancy Check (3 bit)
CRE	Call RE establishment procedure
CS	Domain Circuit Service Domain (includes MSCs)
CSPDN	Circuit Switched Public Data Network
CT	– Call Transfer supplementary service – Channel Tester – Channel Type
CTR	Common Technical Regulation
CUG	Closed User Group supplementary service
CW	Call Waiting supplementary service

D

DA	Destination Address
DAC	Digital to Analogue Converter
DAMPS	Digital AMPS (the TDMA mobile radio system)
DB	Dummy Burst
DCCH	Dedicated Control CHannel
DCE	Data Circuit terminating Equipment
DCF	Data Communication Function
DCN	Data Communication Network
DCS1800	Digital Cellular System at 1800 MHz
DES	Data Encryption Standard (used for security of OTA SIM)
3DES	Triple DES (with two keys)
DET	DETach
DISC	DISConnect
DL	Data Link (layer)
DLCI	Data Link Connection Identifier
DLD	Data Link Discriminator
Dm	Control channel (ISDN terminology applied to mobile service)
DMR	Digital Mobile Radio
DNIC	Data network identifier
DP	Dial/Dialled Pulse
DP	Destination Point (of an IN service)
DPC	Destination Point Code
DRX	Discontinuous reception (mechanism)
DSE	Data Switching Exchange
DSI	Digital Speech Interpolation
DSS1	Digital Subscriber Signalling No 1
DTAP	Direct Transfer Application Part
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi Frequency (signalling)
DTX	Discontinuous transmission (mechanism)
DVB-H	Digital Video Broadcast-Handheld (MULTICAST method for mobile TV)

E

EA	External Alarms
EBSG	Elementary Basic Service Group
ECM	Error Correction Mode (facsimile)
Ec/No	Ratio of energy per modulating bit to the noise spectral density
ECT	Explicit Call Transfer supplementary service
EDGE	Enhanced Data Rates for GSM Evolution (2.75 intermediate generation allowing much higher rates without UMTS: 170 Kbits/sec for Visio)
EEL	Electric Echo Loss
EIA	Electronic Industries Equipment
EIR	Equipment Identity Register
EL	Echo Loss
EMC	ElectroMagnetic Compatibility
eMLPP	enhanced Multi-Level Precedence and Pre-emption service
EMMI	Electrical Man Machine Interface
EPROM	Erasable Programmable Read Only Memory
ERP	Ear Reference Point
ERP	Equivalent Radiated Power
ERR	ERRor
ESME	External Short Message Entity (an ASP or ISP) connected by SMPP
ESN	Electronic Serial Number
ESP	Encapsulating Security Payload
ETR	ETSI Technical Report
ETS	European Telecommunication Standard
ETSI	European Telecommunications Standards Institute
E164	Format of the ‘ordinary’ telephone numbers with a ‘Country Code’ (CC) and a Network Destination Code (NDC)
E212	Format of the ‘IMSI’ telephone numbers with a ‘Mobile Country Code’ (MCC) and a Mobile Network Code (MNC)
E214	Format of a Destination Address, a mix of E164 and E212

F

FA	– Full Allocation – Fax Adaptor
FAC	Final Assembly Code
FACCH	Fast Associated Control CHannel
FACCH/F	Fast Associated Control Channel/Full rate
FACCH/H	Fast Associated Control Channel/Half rate
FB	Frequency correction Burst
FCCH	Frequency Correction CHannel
FCS	Frame Check Sequence
FDM	Frequency Division Multiplex
FDN	Fixed Dialling Number
FEC	Forward Error Correction
FER	Frame Erasure Ratio
FH	Frequency Hopping
FIB	Forward Indicator Bit
FISU	Fill In Signal Units

FN	Frame Number
FR	Full Rate
FSG	Foreign Subscriber Gateway
FSN	Forward Sequence Number
ftn	forwarded-to number

G

GCR	Group Call Register
GGSN	GPRS Gateway Support Node, in GPRS-equipped network, provides the interface between an operator’s own IP network and the external IP network (GRX mostly)
GMLC	Gateway Mobile Location Centre
GMSC	Gateway Mobile-services Switching Centre
GMSK	Gaussian Minimum Shift Keying (modulation)
GPA	GSM PLMN Area
GPRS	General Packet Radio Service
GRX	The Intranet IP network used by mobile operators to exchange GPRS data. It is operated on a cooperative basis by the main international carriers.
GSA	GSM System Area
GSM	Global System for Mobile communications
GSM MS	GSM Mobile Station
GSM PLMN	GSM Public Land Mobile Network
GSM-R	GSM Railway adaptation (fast mobility)
GT	Global Title (E164 numbering address)
GTT	Global Title Translation
GUI	Graphic User Interface

H

H223	Multiplexing protocol for Visio, voice and control
H245	Control protocol in H223 for H324-M communications
H263,H264	Visio encoding standard for H324-M
H324-M	Standard for Visio calls 3G using 64 Kbits and ISUP
HANDO	HANDOver
HDLC	High level Data Link Control
HLC	High Layer Compatibility
HLR	Home Location Register
HMAC	Hash Message Authentication
HOLD	Call hold supplementary service
HPLMN	Home PLMN
HPU	Hand Portable Unit
HR	Half Rate
HSN	Hopping Sequence Number
HSPDA	High Speed Downlink Packet Access (gives 250 Kbits useful data for Visio)
HU	Home Units

I

I	Information frames (RLP)
IA	Incoming Access (closed user group SS)
IA5	International Alphabet 5

IAM	Initial Address Message
IAP	Internet Access Provider (provides the access for a modem or a permanent IP connection to the Internet, not necessarily a Portal or Content Provider)
IC	Interlock Code (CUG SS)
ICB	Incoming Calls Barred (within the CUG)
ICC	Integrated Circuit(s) Card
IC (pref)	Interlock Code of the preferential CUG
ICM	In-Call Modification
ID	IDentification/IDentity/IDentifier
IDN	Integrated Digital Network
IE	(signalling) Information Element
IEC	International Electrotechnical Commission
IEI	Information Element Identifier
IETF	Internet Engineering Task Force
I-ETS	Interim European Telecommunications Standard
IGP	International Gateway Provider (SCCP access to the SS7 network)
IGW	International SCCP Gateway (synonym of IGP).
IMEI	International Mobile station Equipment Identity
IMEIsv	International Mobile station Equipment Identity with software version
IMS	IP Multimedia System
IMSI	International Mobile Subscriber Identity
IN	Interrogating Node
INAP	Intelligent Network Application Part
InitialDP	CAMEL service to start an IN Service
IOT	Inter Operator Tariff
IP	Internet Protocol
IR21	International Roaming 21 document (description of the detailed numbering plan as standardized by the GSM association)
ISC	International Switching Centre
ISD	Abbreviation for Insert Subscriber Data
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider (content provider for Internet services)
ISUP	ISDN User Part (of signalling system No. 7)
ITC	Information Transfer Capability
ITU	International Telecommunication Union
IVR	Interactive Voice Response
IWF	InterWorking Function
IWMSC	InterWorking MSC
IWU	InterWorking Unit

K

k	Windows size
K	Constraint length of the convolutional code
Kc	Ciphering key
Ki	Individual subscriber authentication key
KiC	Key for Ciphering (OTA SIM)
KiD	Key for RC/CC/DS signature (OTA SIM)
KiK	Key for protecting KiC and KiD

L

L1	Layer 1
L2ML	Layer 2 Management Link
L2R	Layer 2 Relay
L2R BOP	L2R Bit Orientated Protocol
L2R COP	L2R Character Orientated Protocol
L3	Layer 3
LA	Location Area
LAC	Location Area Code
LAI	Location Area Identity
LAN	Local Area Network
LAPB	Link Access Protocol Balanced
LAPDm	Link Access Protocol on the Dm channel
LBS	Location Based Services
LCN	Local Communication Network
LCS	Location Services
LCSC	LCS Client
LCSS	LCS Server
LE	Local Exchange
LEMF	Law Enforcement Monitoring Facility
LI	– Length Indicator – Line Identity – Lawful Interception
LLC	Low Layer Compatibility
Lm	Traffic channel with capacity lower than a Bm
LMSI	Local Mobile Station Identity
LMU	A Location Measurement Unit with only Air interface
LMU	B Location Measurement Unit integrated in a BTS.
LND	Last Number Dialled
LNP	Local Number Portability
LPLMN	Local PLMN
LR	Location Register
LSSU	Link Status Signal Units
LSTR	Listener Side Tone Rating
LTE	Local Terminal Emulator
LTE	Long Term Evolution (the new radio access standard of the 4G)
LU	– Local Units – Location Update
LV	Length and Value

M

M	Mandatory
MA	Mobile Allocation
MACN	Mobile Allocation Channel Number
MAF	Mobile Additional Function
MAH	Mobile Access Hunting supplementary service
MAI	Mobile Allocation Index
MAIO	Mobile Allocation Index Offset

MAP	Mobile Application Part
MC	Message Centre (in the IS 41 network, equivalent of a GSM SMSC)
MC	MultiCall (simultaneous bearer services)
MCC	Mobile Country Code
MCI	Malicious Call Identification supplementary service
MD	Mediation Device
MDL	(mobile) Management (entity) Data Link (layer)
MDN	Mobile Destination Number (IS 41)
ME	– Maintenance Entity – Mobile Equipment
MEF	Maintenance Entity Function
MF	– MultiFrame – Mediation Function
MFSMWR	MTU_FORWARD_SHORT_MSG_WWW_REQ
MFSMC	MTU_FORWARD_SHORT_MSG_CNF
MFSMHI	MTU_FORWARD_SHORT_MSG_HO_IND
MFSMWRSP	MTU_FORWARD_SHORT_MSG_WWW_RSP
MGT	Mobile Global Title
MHS	Message Handling System
MIC	Mobile Interface Controller
MIP	Mobile IP
MLC	Mobile Location Centre
MLU	Mobile Location Units
MM	– Man Machine – Mobility Management
MMD	Multi Media Domain
MME	Mobile Management Entity
MMI	Man Machine Interface
MMS	Multimedia Messaging Service
MM1	Protocols using IP standards (HTTP) to exchange MMS between the mobile phone and the MMSC
MM4	In the MMS architecture, protocol to send MMS from one MMSC to another (interconnection), basically SMTP (email)
MM5	In the MMS architecture, protocol to interrogate the HLRs
MM7	Protocols using IP standards so Content Provider sends MMS to an MMSC
MMT	Mobile Money Transfer
MNC	Mobile Network Code
MNO	Mobile Network Operators
MNP	Mobile Number Portability
MO	Mobile Originated
MOC	Mobile Originated Call
MO-LR	Mobile Originating Location Request
MoU	Memorandum of Understanding
MPC	Mobile Positioning Centre
MPEG 4	Visio encoding standard for H324-M (alternative to H263 or H264)
MPH	(mobile) Management (entity) PHysical (layer) [primitive]
MPTY	MultiParTY (Multi ParTY) supplementary service
MRP	Mouth Reference Point
MS	Mobile Station

MSC	Mobile services Switching Centre, Mobile Switching Centre: • Anchor MSC Mobile Switching Centre, that is the first to assign a traffic channel to an MS • Serving MSC MSC which currently has the MS obtaining service at one of its cell sites • Tandem MSC Previous Serving MSC in the handoff chain
MSCM	Mobile Station Class Mark
MSCU	Mobile Station Control Unit
MSISDN	Mobile Station International ISDN Number
MSRN	Mobile Station Roaming Number
MSU	Message Signal Units
MT	Mobile Terminated
MT	(0,1,2) – Mobile Termination
MT-LR	Mobile Terminating Location Request
MTC	Mobile Terminated Call
MTM	Mobile-To-Mobile (call)
MTN	Maintenance Regular Message
MTP	Message Transfer Part
MTP2	MTP Layer 2 (Link control level)
MTP3	MTP Layer 3 (Network control sub-level (handles Point Codes)
MU	Mark Up
MULTICAST	‘MULtiple broadCAST’, broadcast such as that used in Digital TV (DVB-H). The content is broadcast to any number of receivers as in classical TV, thus it is much more economical than the UNICAST currently used.
MUMS	Multi User Mobile Station
MVNO	Mobile Virtual Network Operator
MWD	Message Waiting Data (indication in an HLR)
M2PA	MTP2 Peer-to-Peer Adaptation Layer
M2UA	MTP2 User Adaptation Layer
M3UA	MTP3 User Adaptation Layer

N

N/W	Network
NAMPS	Narrow AMPS
NB	Normal Burst
NBIN	A parameter in the hopping sequence
NCC	Network (PLMN) Country Code
NCELL	Neighbouring (of current serving) Cell
NCH	Notification CHannel
NDC	Network Destination Code
NDUB	Network Determined User Busy
NE	Network Element
NEF	Network Element Function
NET	Norme Européenne de Télécommunications
NF	Network Function
NFC	Near Field Technology (contactless communication of handset)
NGN	Next GeNeration (IP-based equipment and networks)
NI	Network Indicator
NIC	Network Independent Clocking

NI-LR	Network Induced Location Request
NM	Network Management
NMC	Network Management Centre
NMSI	National Mobile Station Identification number
Node B	The UMTS 3G equivalent of a BTS (GSM 2G)
NPI	Number Plan Identifier
NPS	Network Planning System
NSAP	Network Service Access Point
NSS	Network Vendors
NT	– Network Termination – Non Transparent
NTAAB	New Type Approval Advisory Board
NUA	Network User Access
NUI	Network User Identification
NUP	National User Part (SS7)

O

O	Optional
OA	– Outgoing Access (CUG SS) – Origin Address
O&M	Operations & Maintenance
OACSU	Off Air Call Set Up
OCB	Outgoing Calls Barred within the CUG
OD	Optional for operators to implement for their aim
OLR	Overall Loudness Rating
OMC	Operations & Maintenance Centre
OML	Operations and Maintenance Link
OPC	Originating Point Code
OR	Optimal Routing
OS	Operating System
OSI	Open System Interconnection
OSI RM	OSI Reference Model
OSSS	Originating SMS Supplementary Service

P

P-CSCF	Proxy Call Session Control Function
PABX	Private Automatic Branch eXchange
PAD	Packet Assembly/Disassembly facility
PCH	Paging CHannel
PCM	Pulse Code Modulation
PD	– Protocol Discriminator – Public Data
PDN	Public Data Networks
PH	– Packet Handler – PHysical (layer)
PHI	Packet Handler Interface
PI	Presentation Indicator
PICS	Protocol Implementation Conformance Statement
PIN	Personal Identification Number

PIXT	Protocol Implementation eXtra information for Testing
PLMN	Public Lands Mobile Network
PNE	Présentation des Normes Européennes
POI	Point Of Interconnection (with PSTN)
PoR	Proof of Receipt (OTA SIM)
PP	Point-to-Point
PPE	Primitive Procedure Entity
Pref CUG	Preferential CUG
PRN	Abbreviation for the MAP primitive Provide Roaming Number
Ps	Location probability
PS	Domain Packet Service Domain (includes SGSN)
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
PUCT	Price per Unit Currency Table
PW	PassWord

Q

QA	Q (Interface) Adapter
QAF	Q Adapter Function
QoS	Quality of Service

R

R	Value of Reduction of the MS-transmitted RF power relative to the maximum allowed output power of the highest power class of MS (A)
RA	RAndom mode request information field
RAB	Random Access Burst
RAC	Routing Area Code (for GPRS coverage)
RACH	Random Access Channel
RAI	Routing Area Information (for GPRS coverage)
RAND	RANDom number (used for authentication)
RBER	Residual Bit Error Ratio
RCP	Remote Control Point (the SCCP function of a MSC (Alcatel term)
RDI	Restricted Digital Information
REC	RECommendation
REJ	REJect(ion)
REL	RELease
REQ	REQuest
RF	Radio Frequency
RFC	Radio Frequency Channel
RFCH	Radio Frequency CHannel
RFN	Reduced TDMA Frame Number
RFU	Reserved for Future Use
RH	Roaming Hub
RLP	Radio Link Protocol
RLR	Receiver Loudness Rating
RMS	Root Mean Square (value)
RNC	Radio Network Controller UMTS 3G (equivalent to BSC (GSM 2G))
RNTABLE	Table of 128 integers in the hopping sequence

ROSE	Remote Operation Service Element
RP	Reply Path
RPOA	Recognised Private Operating Agency
RR	Radio Resource
RSE	Radio System Entity
RSL	Radio Signalling Link
RSZI	Regional Subscription Zone Identity
RTE	Remote Terminal Emulator
RTCP	Real Time Control Protocol
RTP	Real Time Protocol (used to carry 3G H323 Visio sessions)
RTSP	Real Time Streaming Protocol (distributes a multimedia stream (e.g. TV) on an IP connection.
RXLEV	Received signal level
RXQUAL	Received Signal Quality

S

S/W	SoftWare
SABM	Set Asynchronous Balanced Mode
SACCH	Slow Associated Control CHannel
SACCH/C4	Slow Associated Control CHannel/SDCCH/4
SACCH/C8	Slow Associated Control CHannel/SDCCH/8
SACCH/T	Slow Associated Control CHannel/Traffic channel
SACCH/TF	Slow Associated Control CHannel/Traffic channel Full rate
SACCH/TH	Slow Associated Control CHannel/Traffic channel Half rate
SAP	Service Access Point
SAPI	Service Access Point Indicator
SB	Synchronization Burst
SC	– Service Centre (used for SMS) – Service Code
SCE	Service Creation Environment (scripting for IN or IVR)
SCP	Service Control Point
SCCP	Signalling Connection Control Part
SCF	Service Control Function
SCH	Synchronization Channel
SCLC	SCCP ConnectionLess Control
SCMG	SCCP Management
SCN	Sub Channel Number
SCOC	SCCP Connection Oriented Control
SCF	Service Control Function
SCP	Service Control Point
SCRC	SCCP Routing Control
SCTP	Stream Control Transmission Protocol (TCP with multihoming)
SDCCH	Stand-alone Dedicated Control CHannel
SDL	Specification Description Language
SDP	Service Data Point
SDT	SDL Development Tool
SDU	Service Data Unit
SE	Support Entity

SGSN	Support GPRS Service Node. In GSM 2.5 G with GPRS, it has both circuit and IP interfaces, and provides the GPRS service to a visiting mobile phone. It can deliver SMS-MT.
SEF	Support Entity Function
SF	Status Field
SFH	Slow Frequency Hopping
SGP	SIGTRAN Gateway Point (IP ↔ TDM conversion)
SI	– Screening Indicator – Service Interworking – Supplementary Information
SID	SIlence Descriptor
SIGTRAN	Signal Transport (Working Group which works on SS7/IP)
SIF	Signalling Information Field
SIM	Subscriber Identity Module
SIO	Service Information Octet
SIP	Session Initiated Protocol (the VoIP protocol)
SLC	Signalling Link Code
SLPP	Subscriber LCS Privacy Profile
SLR	Send Loudness Rating
SLS	Signalling Link Selection
SLTA	Signalling Link Test Message Acknowledgment
SLTM	Signalling Link Test Message (polling between adjacent Point Codes)
SM	Short Message
SME	Short Message Entity
SMF	Service Management Function
SMIL	Synchronized Multimedia Integration Language (to code animated sequences for MMS)
SMG	Special Mobile Group
SMLC	Serving Mobile Location Centre
SMS	Short Message Service
SMSC	Short Message Service Centre
SMSCB	Short Message Service Cell Broadcast
SMSDPTP	SMS Delivery Point to Point
SMSDBCKW	SMS Delivery Backward
SMSDFWD	SMS Delivery Forward
SMS-SC	Short Message Service – Service Centre
SMS/PP	Short Message Service/Point-to-Point
Smt	Short message terminal
SM-AL	Short Message Application Layer
SM-TL	Short Message Transfer Layer
SM-RL	Short Message Relay Layer
SM-RP	Short Message Relay Protocol
SN	Subscriber Number
SNM	Signalling Network Management
SNR	Serial NumbeR
SOA	Suppress Outgoing Access (CUG SS)
SOR	Steering Of Roaming
SP	– Service Provider – Signalling Point – SPare

SPC	Signalling Point Code
SPC	Suppress Preferential CUG
SRES	Signed RESponse (authentication)
SRI	Abbreviation for the MAP primitive Send_Routing_Info
SRI_SM	Abbreviation for the MAP primitive Send Routing Info for Short Message
SRF	Service Resource Function
SS	– Supplementary Service – System Simulator
SSC	Supplementary Service Control string
SSF	– Subservice Field – Service Switching function (the IN part of an MSC, may have its own GT)
SSN	Sub-System Number
SST	Sub-System Test (polling between SCCP sub-systems)
SSTA	Sub-System Test Acknowledgement
SS7	Signalling System No. 7
SSP	Service Switching Point
STMR	SideTone Masking Rating
STP	Signalling Transfer Point
SU	Signal Unit
SUA	SCCP User Adaptation Layer
SVN	Software Version Number
SWP	Single Wire Protocol

T

T Timer	Transparent Signalling messages are transmitted without any content change
TA	– Terminal Adaptor – Timing Advance (between an MS and its serving BTS)
TAC	Type Allocation Code, six digits (first of IMEI) of a handset model
TAF	Terminal Adaptation Function
TAR	Toolkit Application Reference (OTA SIM)
TBR	Technical Basis for Regulation
TC	Transaction Capabilities
TCAP	Transaction Capability Application Part
TCH	Traffic CHannel
TCH/F	A full rate TCH
TCH/F2.4	A full rate data TCH (≤2.4 Kbit/s)
TCH/F4.8	A full rate data TCH (4.8 Kbit/s)
TCH/F9.6	A full rate data TCH (9.6 Kbit/s)
TCH/FS	A full rate Speech TCH
TCH/H	A half rate TCH
TCH/H2.4	A half rate data TCH (≤2.4 Kbit/s)
TCH/H4.8	A half rate data TCH (4.8 Kbit/s)
TCH/HS	A half rate Speech TCH
TCI	Transceiver Control Interface
TC-TR	Technical Committee Technical Report
TDMA	Time Division Multiple Access
TE	Terminal Equipment
Tei	Terminal endpoint identifier
TFA	TransFer Allowed

TFP	TransFer Prohibited
TI or TID	Transaction Identifier (in the TCAP protocol)
TLV	Type, Length and Value
TMN	Telecommunications Management Network
TMSI	Temporary Mobile Subscriber Identity
TN	Timeslot Number
TOA	Time of Arrival
TON	Type Of Number
TP	Transfer Protocol (in the MAP protocol)
TRX	Transceiver
TS	– Time Slot – Technical Specification – TeleService
TSC	Training Sequence Code
TSDI	Transceiver Speech & Data Interface
TTCN	Tree and Tabular Combined Notation
TUA	TCAP User Adaptation Layer
TUP	Telephone User Part (SS7)
TV	Type and Value
TXPWR	Transmit PoWeR; Tx power level in the MS_TXPWR_REQUEST and MS_TXPWR_CONF parameters

U

UA	User Adaptation
UDI	Unrestricted Digital Information
UDT	Unit Data Message (of SCCP)
UDUB	User Determined User Busy
UE	User Equipment
UI	Unnumbered Information (Frame)
UIC	Union Internationale des Chemins de Fer
UL	Abbreviation for UPDATE LOCATION
UMA	Unlicensed Mobile Access
UNICAST	‘UNIque broadCASTing’: TV broadcast method where each receiver has a dedicated channel (can be used for ‘on demand’) and the content is ‘streamed’
UPCMI	Uniform PCM Interface (13 bit)
UPD	Up to date
USSD	Unstructured Supplementary Service Data
UUS	User-to-User Signalling supplementary service
UTRAN	UMTS Terrestrial Radio Access Network (3G) equivalent to BSS (2G)

V

VAD	Voice Activity Detection
VAP	Videotex Access Point
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service
VLR	Visitor Location Register
VMS	Voice Mail System
VMSC	Visited MSC
VPLMN	Visited PLMN

VPN	Virtual Private Network
VoIP	Voice over IP protocol
VSC	Videotex Service Centre
V(SD)	Send state variable
VTX host	The components dedicated to Videotex service

W

WAN	Wide Area Network
WAP	Wireless Application Protocol
WBXML	Wireless 'Binary' XML
WML	Wireless Markup Language
WLL	Wireless Local Loop
WLNP	Wireless Local Number Portability
WS	Work Station
WPA	Wrong Password Attempts (counter)

X

XID	eXchange Identifier
XML	Extensible Markup Language
XRES	Expected Response (from the USIM card when computing A3)

Z

ZC	Zone Code

1

‘Virtual Roaming’ Purpose and Principles

Ἄνδρα μοι ἔννεπε, Μοῦσα, πολύτροπον, ὃς μάλα πολλὰ πλάγχθη, ἐπεὶ Τροίης ἱερὸν πτολίεθρον ἔπερσεν·

O Muse, tell me the story of the man of many tricks, who roamed far and wide after he destroyed the sacred city of Troy.

Odysseus, Homer

1.1 Mobile Services Affected by Virtual Roaming

‘Open Connectivity’ is a term which emerged in 2006 as an equivalent to ‘Virtual Roaming’. There were about 800 GSM networks worldwide in 2008 and 1200 mobile networks in total (TDMA, CDMA, IDEN, etc.). The number of bilateral agreements that need to have total service connectivity is therefore very high and the idea arose to replace many bilateral agreements (N × N-1)/2 by agreements with a number M of aggregating ‘virtual roaming suppliers’.

The ‘virtual Roaming Hub’ is a system which provides all the roaming services between two mobile networks A and B which do not have direct roaming agreements.

These services include:

- all voice services (making and receiving calls);
- all Visio 3G services;
- all SMS services (sending and receiving);
- transparent CAMEL prepaid charging scheme (T-CSI, O-CSI, SMS-CSI, GPRS-CSI, …);
- GPRS data services (2.5G and 3G) (these will become even more important in the future);
- location-based services;
- VMS ‘anti-tromboning’;
- stolen equipment checking.

Which Companies Will Use a Virtual Roaming Service?

First: the new mobile operators. It allows them to get revenues (currencies) from the roaming visitors which they can receive with the service, and also from their outbound subscribers in many possible foreign networks.

Second: large mobile operators. With very little work (agreements, testing, billing), they can increase their inbound visitors’ business by including small–medium operators, and get additional coverage for their outbound subscribers.

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice   Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

Which Companies Will Operate a Virtual Roaming Hub?

The 'Roaming Hub supplier' can be an SS7 carrier with a VAS business (SMS interworking, etc.) or a regular GSM operator ('Hosting') which has many roaming agreements and wants to draw new revenues by allowing smaller operators ('Hosted') to use its roaming agreements.

Frequently, in an international group of mobile operators, the largest may buy a Roaming Hub and provide the service to the others. It is technically possible for the Roaming Hub to be hosted in another country (as explained in Chapter 4).

1.2 Virtual Roaming Hub for Inbound Visitors' Service (Single IMSI)

Figures 1.1 to 1.4 show the registration principle and the incoming call scenario.

They are based on a Network B which is willing to handle visitors from A, but the 'A network' does not have roaming with VPLMN B. The help of the Roaming Hub is then used. The visitors of 'A' use their standard SIM card with a single IMSI, and there is no special provisioning for them *individually* in B or A.

1.2.1 Registration Principle for a Virtual Visitor

The UPDATE LOCATION (a signalling message of the MAP network) is sent from Network B to the Roaming Hub which has Network A as part of its registered PLMNs. The Roaming Hub has its own address in the SS7 network and must have roaming with both the VPLMN (network visited) and the HPLMN (Home network of the visitor).

The principle is that all the SS7 messages, which would normally go from B to A, are forced to go through a 'Roaming Hub', shown on the right of the diagrams that follow:

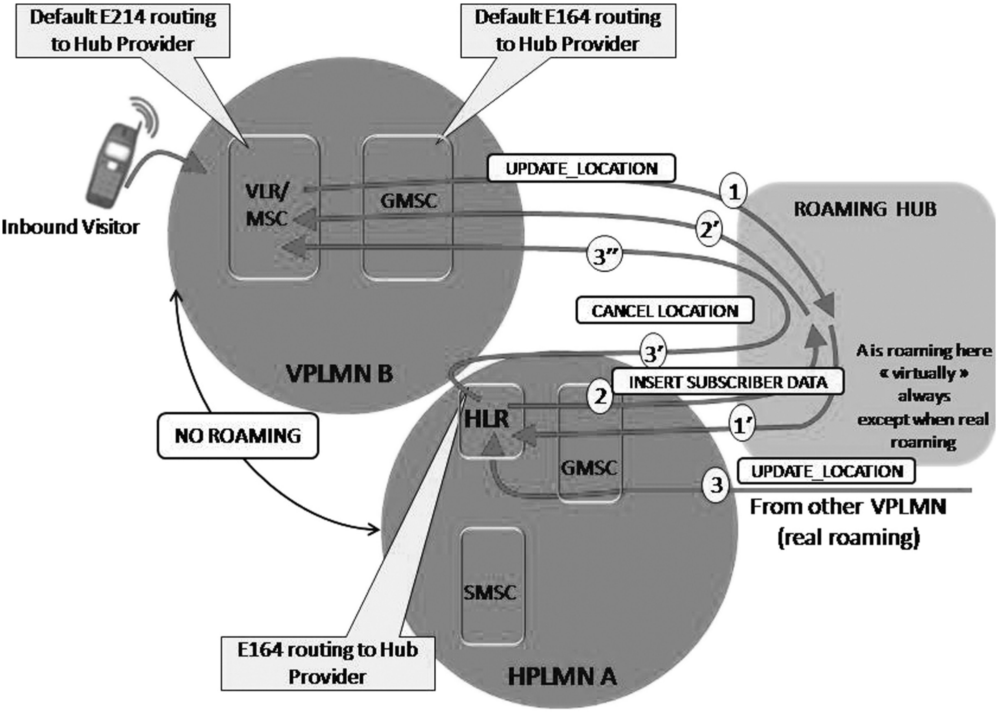

Default E214 routing to Hub Provider
Default E164 routing to Hub Provider
Inbound Visitor
VLR/ MSC
GMSC
UPDATE_LOCATION
1
2'
3''
ROAMING HUB
CANCEL LOCATION
3'
VPLMN B
INSERT SUBSCRIBER DATA
2
HLR
1'
A is roaming here « virtually » always except when real roaming
NO ROAMING
GMSC
3
UPDATE_LOCATION
From other VPLMN (real roaming)
SMSC
E164 routing to Hub Provider
HPLMN A

Figure 1.1 Registration principle for a virtual visitor

- The UPDATE LOCATION (1) is relayed from B to A (1′).
- The INSERT SUBSCRIBER DATA (2) is relayed from A to B (2′). This MAP message includes the customer profile and their ordinary number (MSISDN).
- In (3) the mobile is registering in a network other than B. A CANCEL LOCATION (3′) would be sent by the HLR to the Roaming Hub and then to the VLR in VPLMN B (3″).
- Network A considers that its subscriber is roaming in the VLR = Roaming Hub, not in VPLMN B!

1.2.2 CAMEL Prepaid Outgoing Call of a Virtual Visitor

CAMEL is the protocol used to exchange messages between an MSC and a HLR to charge prepaid customers.

Take the case of a prepaid subscriber of A, roaming in B and trying to make a call (1). The CAMEL INITIAL DP (2) which is sent to their system (called Service Control Point) is relayed through the Roaming Hub (2′). A CONTINUE (3) is sent back (credit available), so the call is performed (4). The call does not go through the Roaming Hub as it uses the ISUP telephone network, not the SS7 signalling network.

1.2.3 SMS-MO Sending for a Virtual Visitor

When subscriber A sends an SMS-MO (1), it is relayed to their network A's SMSC through the Roaming Hub, which sends it (1′) to their SMSC. This SMSC sends the SMS-MT (2), and if a STATUS REPORT (acknowledgment) was requested, sends it to subscriber A through the Roaming Hub (3) and (3′).

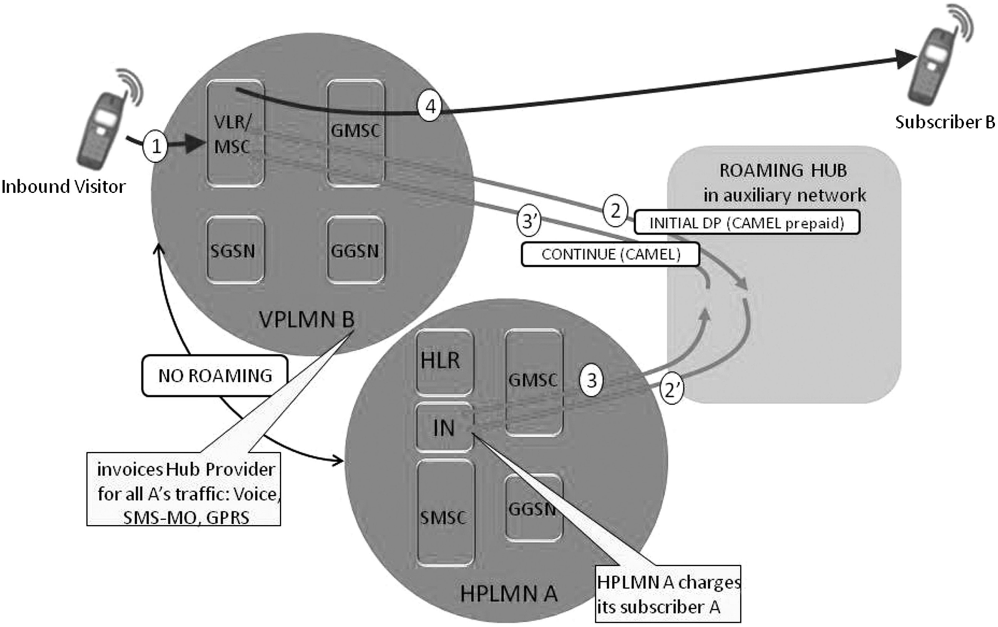

Inbound Visitor
1
VLR/ MSC
GMSC
4
Subscriber B
SGSN
GGSN
VPLMN B
ROAMING HUB in auxiliary network
2
INITIAL DP (CAMEL prepaid)
3'
CONTINUE (CAMEL)
NO ROAMING
HLR
GMSC
3
2'
IN
SMSC
GGSN
HPLMN A
invoices Hub Provider for all A's traffic: Voice, SMS-MO, GPRS
HPLMN A charges its subscriber A

Figure 1.2 CAMEL prepaid outgoing call of a virtual visitor

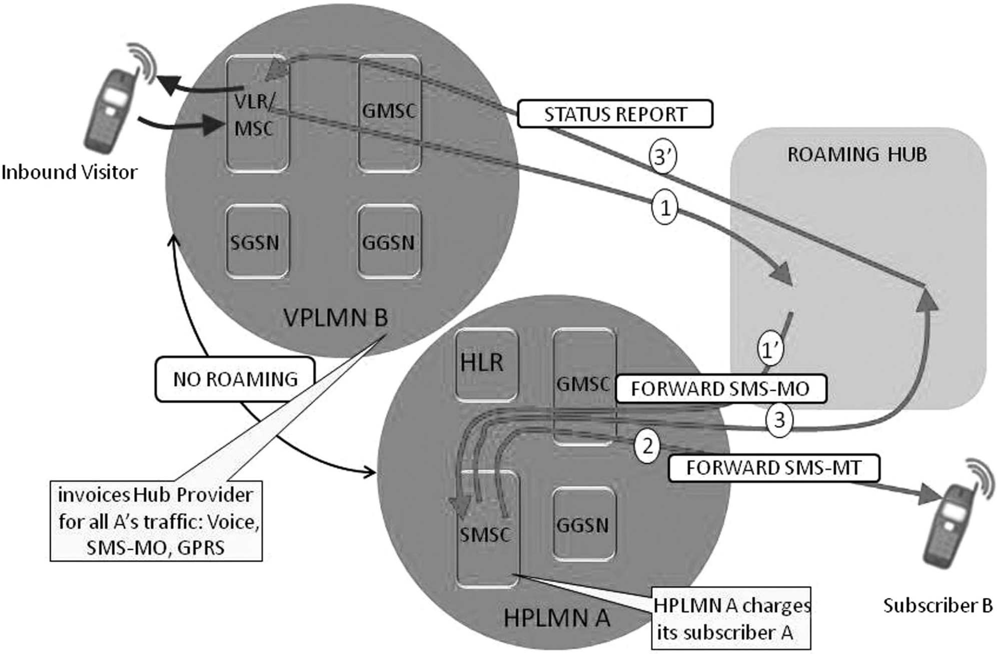


Figure 1.3 SMS-MO sending for a virtual visitor

1.2.4 GPRS Access (Data Services) for a Virtual Visitor

The registration procedure in the visited SGSN is identical to UPDATE LOCATION except that it will use UPDATE LOCATION GPRS. This is done at the 'attach GPRS' phase. Now when the subscriber tries to access a data service, it will 'Activate a PDP context' which involves setting up a data connection with the GGSN in their HPLMN A. It uses the GTP protocol and the 'Activate PDP context' is sent using the GRX data network (1) *through the Roaming Hub* with a change of IP addresses to the HPLMN GGSN (1′). Then the HPLMN GGSN makes (and charges its customer) the connection to the requested service (Internet, MMS, etc.).

1.2.4.1 Billing Principle

The VPLMN B will charge its Roaming Hub supplier based on tickets (measuring the data volume between the 'Activate PDP connect' and the 'PDP disconnect' phases). The Roaming Hub supplier will then charge the HPLMN A, which then charges its customer. Prepaid GPRS roaming is possible because when the prepaid user makes a connection to a data service, their 'Activate PDP context' triggers a CAMEL INITIAL DP GPRS to the IN machine of the Home network (through the Roaming Hub), very similar to INITIAL DP for a voice call. The IN machine gives a limit to the visited SGSN that is a 'Max Transferred data volume' as well as a 'Max Elapsed time' limit using the CAMEL APPLY CHARGING GPRS message sent to the GGSN. When there is a 'PDP disconnect', the SGSN sends to the IN machine the effective 'Transferred data volume' and 'Elapsed time' of the 'session' in a CAMEL APPLY CHARGING REPORT GPRS. The SGSN counts the volume, and stops and disconnects if the limit is reached before the user interrupts the session.

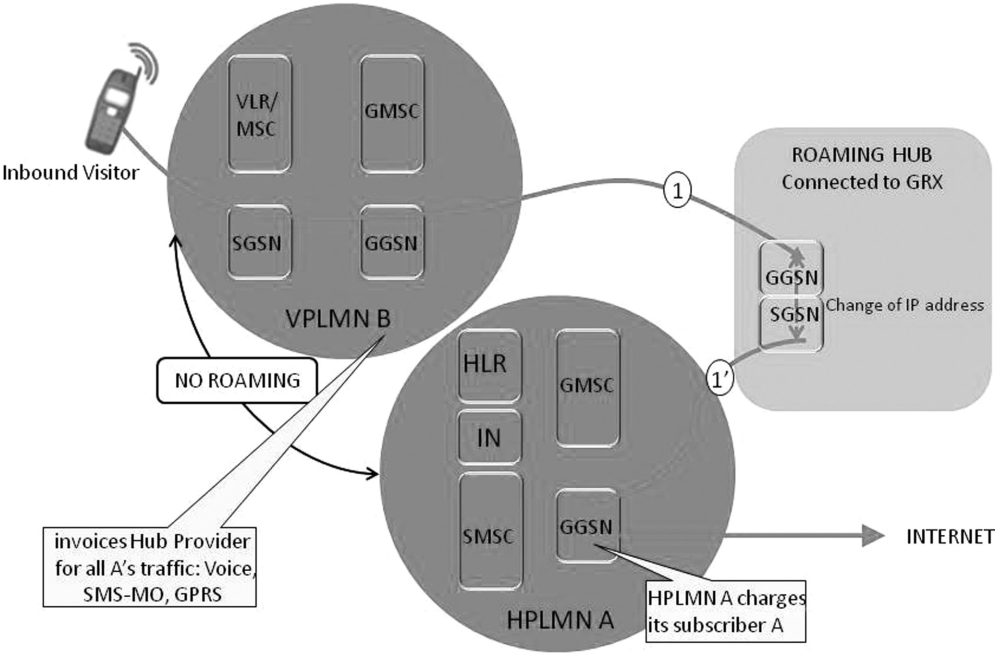


Figure 1.4 GPRS access

1.2.4.2 Business Model: Data Services of the Roaming Hub

The business model for GPRS data revenue is the same as for the sending of SMS-MO *by visitors of B*; it is not the same as that of an 'SMS Hub' (which charges B for the sending of SMS to other networks such as A, *by the subscribers of B*). The customer VPLMN B *receives* money from a GPRS Roaming Hub supplier while it *pays* an 'SMS Hub' service. So there is a very attractive business model for the VPLMNs which will be customers: they do not invest anything and they receive revenues! Assume that VPLMN B does have a connection to the GRX data network, but does not have an agreement with HPLMN A for GPRS roaming.

The VPLMN B, if it had a roaming agreement with A, would charge HPLMN A for the traffic (GPRS or SMS-MO) sent by its subscriber. If there is a Roaming Hub supplier in the path, it will be charged by VPLMN B. In order to have a connection with HPLMN A, the Roaming Hub makes an agreement with a mobile operator C (the 'third party') that has many GPRS data roaming agreements *including A*. This agreement also provides for an IP address of the Roaming Hub belonging to the range of C, so that any data traffic sent by the RH is identified by A as coming from one of its roaming partners that is C.

The Roaming Hub supplier prepares the data service invoice elements (sent to HPLMN A by C) and the credit elements (and payments) sent to the VPLMN B. With the difference, it pays C as agreed and keeps the margin. An example will illustrate this:

- A virtual visitor of B makes an internet connection and sends 1 Mega octet which transits through the Roaming Hub.
- The Roaming Hub supplier creates a billing ticket for HPLMN A at the rate 'roaming in C' (this is the principle).

- Network C (their partner) sends this ticket, charged at 3 euro, to HPLMN A (this is their agreed rate for traffic C → A).
- C charges the Roaming Hub supplier 1 euro (this is the rate that they have agreed).
- The Roaming Hub supplier creates a credit note and pays B with 0.5 euro as agreed.

The end paying party is always the subscriber (of HPLMN A) who pays 5 euro to A.

- HPLMN A has a margin of 2 euro.
- 'Third party' C has a margin of 1 euro (less the small GRX charge).
- The Roaming Hub supplier has a margin of 1.5 euro (less the small GRX charge).
- The customer VMPLN B of the virtual roaming data service has received 0.5 euro (it did not have to make any developments or Capital Expenditure) less the small GRX charge.

The Roaming Hub supplier receives all its revenues from its partner C. So this is a very secure business model for C, which receives its revenue from its usual roaming partners. Situations which have occurred in other markets (voice), where a mobile network C incurs call charges and is not paid by an 'aggregator', cannot happen. For the above figures summarizing the various business models for a Roaming Hub supplier, for an 'SMS Hub' (which is also known as SMSeXchange) and for voice call termination (international voice carrier), the payment chain is shown in Table 1.1.

Table 1.2 shows other cases.

Table 1.1 Payment chain for Voice and Data services of inbound visitors

Type of Service	End paying party	It pays	Paid Party pays	Next Party paid	Next Party paid
GPRS raw data (Figure 1.4)	Subscriber of HPLMN A	HPLMN A	Mobile Network C	Roaming Hub	VPLMN B
Outgoing Voice traffic (4 of Figure 1.2)	Subscriber of HPLMN A	HPLMN A	Mobile Network C	International voice carrier	Network visited by subscriber B

Table 1.2 Payment chain for other cases

Type of Service	End paying party	It pays	Paid Party pays	Next Party paid	Next Party paid
SMS (SMSeXchange) (Figure 2.18)	SMS-MO sending subscriber which belongs to 'HPLMN nominal' (visitor of VPLMN A)	HPLMN nominal	SMSeXchange	HPLMN auxiliary	VPLMN A (originating) and VPLMN C (if SMS-MT charged by C)
MMS (MMSeXchange) (Figure 2.18 also)	Subscriber of HPLMN nominal	HPLMN nominal	MMSeXchange	HPLMN auxiliary	VPLMN A (originating) and VPLMN C (if SMS-MT charged by C)
(1) Voice traffic (reception of call while roaming) (Figure 1.5)	Visitor of VPLMN B which is a subscriber of HPLMN A	HPLMN nominal	International voice carrier	Terminating network or carrier	VPLMN B (by the carrier as the Roaming Hub is not involved)

1.2.5 Incoming Call

When a call is received for subscriber A who is roaming in network B, the Roaming Hub will allow network A to get the roaming number in the VPLMN B.

(1) is the call received by the Virtual Visitor of (B). It arrives at the GMSC of A which interrogates the HLR with a SEND ROUTING INFO (2) in order to get the 'Roaming Number' in B. The HLR interrogates the Roaming Hub, because it is the VLR, with a PROVIDE ROAMING NUMBER (3), which is relayed to B, giving the response (4), which is returned (5) to the GMSC.

If the subscriber is prepaid, the IN (SCP) is interrogated (6) with an INITIAL DP. Then the GMSC makes the ISUP call directly (7) to its subscriber; it does not go through the Roaming Hub.

This is shown in Figure 1.5.

1.3 Virtual Roaming Hub for Outbound Subscribers: Multi-IMSI

To get worldwide coverage quickly, some mobile operators ('nominal HPLMN') may use multi-IMSI cards. The virtual Roaming Hub allows the subscriber concerned to receive calls or SMSs to their ordinary number, *whichever IMSI is selected*, even if they have more than two.

The virtual Roaming Hub is thus the key system for a *seamless service*. It is even better if the phone handsets have a SIM Tool Kit which makes the IMSI selection automatically.

The 'nominal HPLMN' needs simply to agree with the operator providing the other IMSIs (the 'auxiliary HPLMN') to have an SS7 rerouting to their Roaming Hub.

The important virtual inbound visitor service is obviously independent of whether, for outbound subscribers, a single IMSI or dual IMSI is used in the SIM cards.

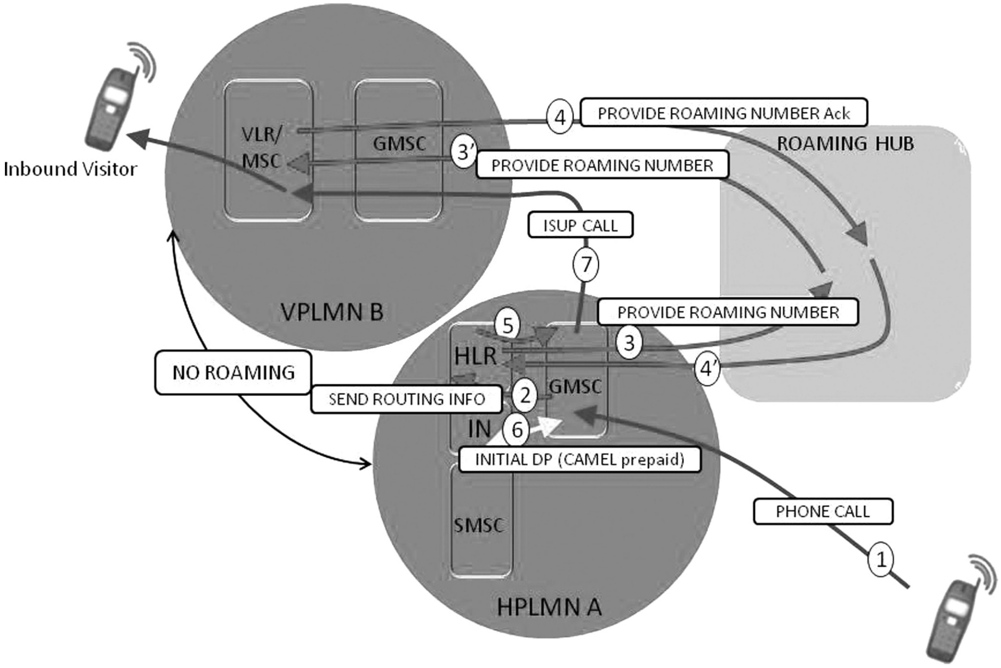


Figure 1.5 Incoming call

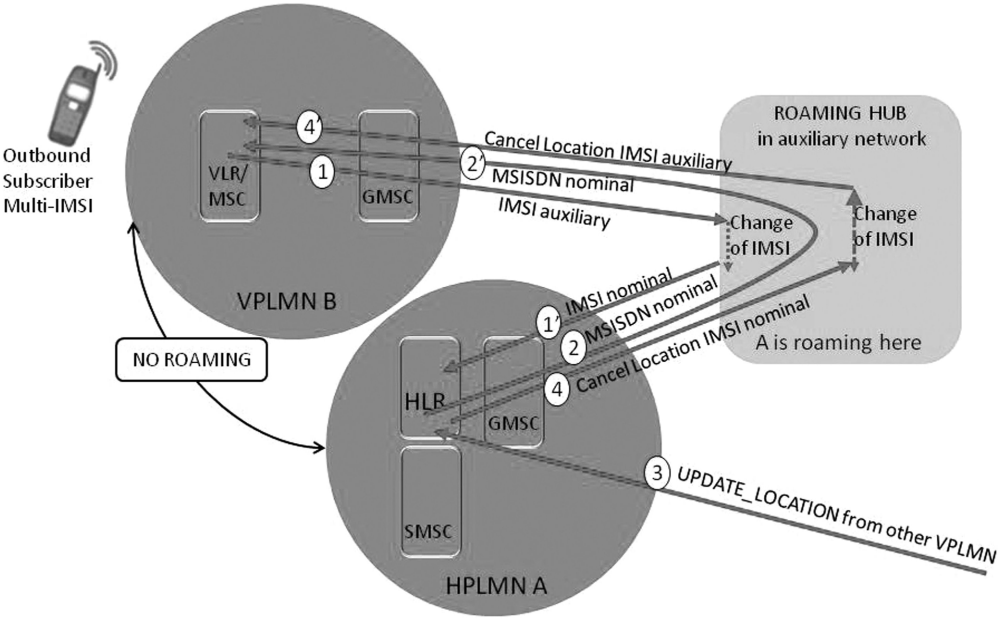


Figure 1.6 Location registration principle for multi-IMSI

For the outbound subscriber service, the Virtual Roaming Hub supports both the following:

- Dual IMSI (the 'Hosted Operators' users select the IMSI of the 'Hosting Operator' while abroad in some countries): no particular network setup is required in the visited networks, just the existing setup for the 'Hosting Operator'.
- Multiple IMSI.

Figure 1.6 shows the location registration principle for multi-IMSI.

The key difference with the first case is that there is an *automatic change of IMSI* performed by the Roaming Hub. When the outbound subscriber A attempts to register in the VPLMN B, their 'nominal IMSI' will fail (no roaming), so either they manually change the SIM card to use the 'auxiliary IMSI' which has the agreement with the visited network, or a 'SIM Tool Kit' in their special SIM card does it. A SIM or USIM card (UMTS) is a programmable device which can have additional logic added (see Chapter 8). The sequence is as follows:

- At (1) the registration is attempted with the 'auxiliary IMSI', the message called UPDATE LOCATION goes to the Roaming Hub.
- At (1′) with a table for each subscriber, it is changed to the 'nominal IMSI' and sent to the HLR in the HPLMN A of the subscriber.
- The profile of the subscriber is sent back (2) to the Roaming Hub and contains the 'nominal MSISDN'.
- But the 'nominal MSISDN' is left the same when sent back (2′) to the VLR in VPLMN (B), because in all the calls, SMS and other procedures, the VPLMN controls the 'IMSI auxiliary' (it has a roaming agreement with it), not the MSISDN.

As a result, any call or SMS sent by the virtual multi-IMSI visitor will still have the *correct origin number*. This is the main 'trick' of the 'multi-IMSI' system. The VPLMN will send the charge to the 'auxiliary HPLMN', which must have a billing system capable of dispatching the charge to the HPLMNs which use its 'auxiliary IMSI'.

1.4 Brief Introduction to Standard Bilateral Roaming Procedures

Although we assume some prerequisites, we will explain the notations and diagrams that we use with the standard procedures, and show the details that are the core of the MAP transformations which will be used for Virtual Roaming. Here E214 stands for an E214 type of address, computed from the IMSI by replacing the MCC (France = 208) and the MNC (SFR = 10) by the CC (France = 33) and the MGT (SFR = 609). E164 is the normal address such as that used by mobiles (their MSISDN) or network equipment. When only the IMSI is known, such as in the initial registration procedure, the E214 must be used, as well as in some other cases. The E214 and E164 addresses that belong to an operator start with the same CC-MGT; their lengths are different (not important) but they contain two different 'Numbering Plan' indicators. The equipment's 'SCCP Gateways' use this difference and have different routing tables for each.

In Figure 1.7 we see three layers of the SS7 protocol stack: MAP, TCAP and SCCP.

INSERT SUBSCRIBER DATA will copy the subscriber profile from the HLR to the VLR. In particular, it includes the MSISDN, the ordinary telephone number which will be used:

- as the origin in calls;
- as the origin in SMSs sent by the subscriber (SMS-MO).

Prepaid Subscribers' Case

For prepaid subscribers, their credit must be checked for each call they make, using the CAMEL protocol, so their profile in the VLR includes 'VLR CAMEL Info' with the GT of the 'Service Control Point'.

There can be many SCPs (Service Control Points) for the different subscribers and many HLRs. The information SCP and MAP HLR are those corresponding to the particular subscriber. This will raise a particular difficulty if the VPLMN has a Roaming Hub setup.

At the end of the procedure, the HLR GT is sent by the HLR to the VLR. It could be used to directly address the HLR in procedures such as READY FOR MS and PURGE MS; in reality the E214 address based on the IMSI is used.

Roaming Hub software must have full signalling transparency. In Figure 1.7 we have summarized the content of the SCCP layer addresses, the types of TCAP messages (BEGIN, CONTINUE, END) and the main parameters of the MAP layer. As the Roaming Hub in certain configurations, such as 'Alias GT mode', must change some MAP parameters, it means that the basic principle of the software is to 'chain TCAP transactions' so that incoming MAP parameters (inside TCAP) may be changed and transmitted in a new TCAP transaction. One can see that the UPDATE LOCATION was sent by the VLR to the HLR using the E214 address of the HLR (for example 336891234567890). But the HLR does not send its answer (an INSERT SUBSCRIBER DATA) in a TCAP CONTINUE using this CdPa as its 'Calling Party address'. Instead the HLR *replaces* it by its 'E164 address' (for example 33689000150).

For the rest of the dialogue to the HLR (INSERT SUBSCRIBER DATA Ack sent by the VLR to the HLR), this E164 address will be used instead of the E214 address used initially.

So it would not be normal for any SCCP Gateway of the SS7 network to ever receive an SCCP Calling Party address which is E214. Some SCCP Gateway performs the control and will bar the SCCP message if the CgPa is E214. So the Roaming Hub must be able to relay forward the SCCP Calling Party (after an eventual 'Alias GT' transformation).

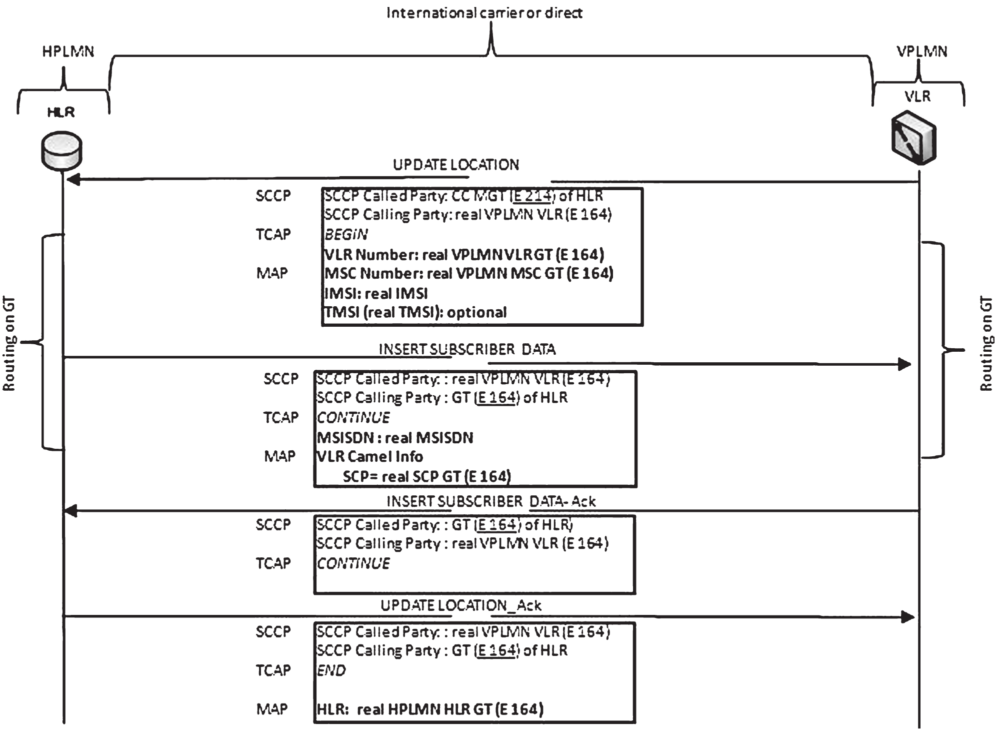

International carrier or direct
HPLMN
HLR
VPLMN
VLR
UPDATE LOCATION
SCCP
TCAP
MAP
SCCP Called Party: CC MGT (E 214) of HLR
SCCP Calling Party: real VPLMN VLR (E 164)
BEGIN
VLR Number: real VPLMN VLR GT (E 164)
MSC Number: real VPLMN MSC GT (E 164)
IMSI: real IMSI
TMSI (real TMSI): optional
Routing on GT
Routing on GT
INSERT SUBSCRIBER DATA
SCCP
TCAP
MAP
SCCP Called Party: : real VPLMN VLR (E 164)
SCCP Calling Party : GT (E 164) of HLR
CONTINUE
MSISDN : real MSISDN
VLR Camel Info
SCP= real SCP GT (E 164)
INSERT SUBSCRIBER DATA- Ack
SCCP
TCAP
SCCP Called Party: : GT (E 164) of HLR
SCCP Calling Party : real VPLMN VLR (E 164)
CONTINUE
UPDATE LOCATION_Ack
SCCP
TCAP
MAP
SCCP Called Party: : real VPLMN VLR (E 164)
SCCP Calling Party : GT (E 164) of HLR
END
HLR: real HPLMN HLR GT (E 164)

Figure 1.7 Update location registration procedure

1.5 Principles of the SS7 Protocol Layers Used in Roaming Procedures

Figure 1.8 details the exchange of Figure 1.7 by using the analogy of multiple envelopes which address the various layers. This concerns the case where two international SCCP Gateways, #1 and #2, are used in the path from the VPLMN (Visited Network) to the HPLMN (Home Network of the Visitor), and the MTP layer ('Point Code' layer) is involved in the routing of messages.

To illustrate the successive layers acting as successive envelopes of the same message, we have inverted the order of the layers of Figure 1.7, which will, however, be followed throughout the book:

- MTP ('Point Code network layer') (not shown in general);
- SCCP ('GT network layer');
- TCAP ('Transaction layer');
- MAP, CAMEL ('Application layer') below.

There is a good summary of SS7 in [5.1] Chapter 2.

1.5.1 Need to Have Standardized Messages: the MAP and CAMEL Protocols

In (1) the handset is turned on and transmits the IMSI number of the subscriber (from the SIM or USIM card). As result, the visited equipment MSC/VLR needs to register the mobile in its HLR in the home country. The VLR codes a MAP message called 'UPDATE LOCATION' with the IMSI and its GT

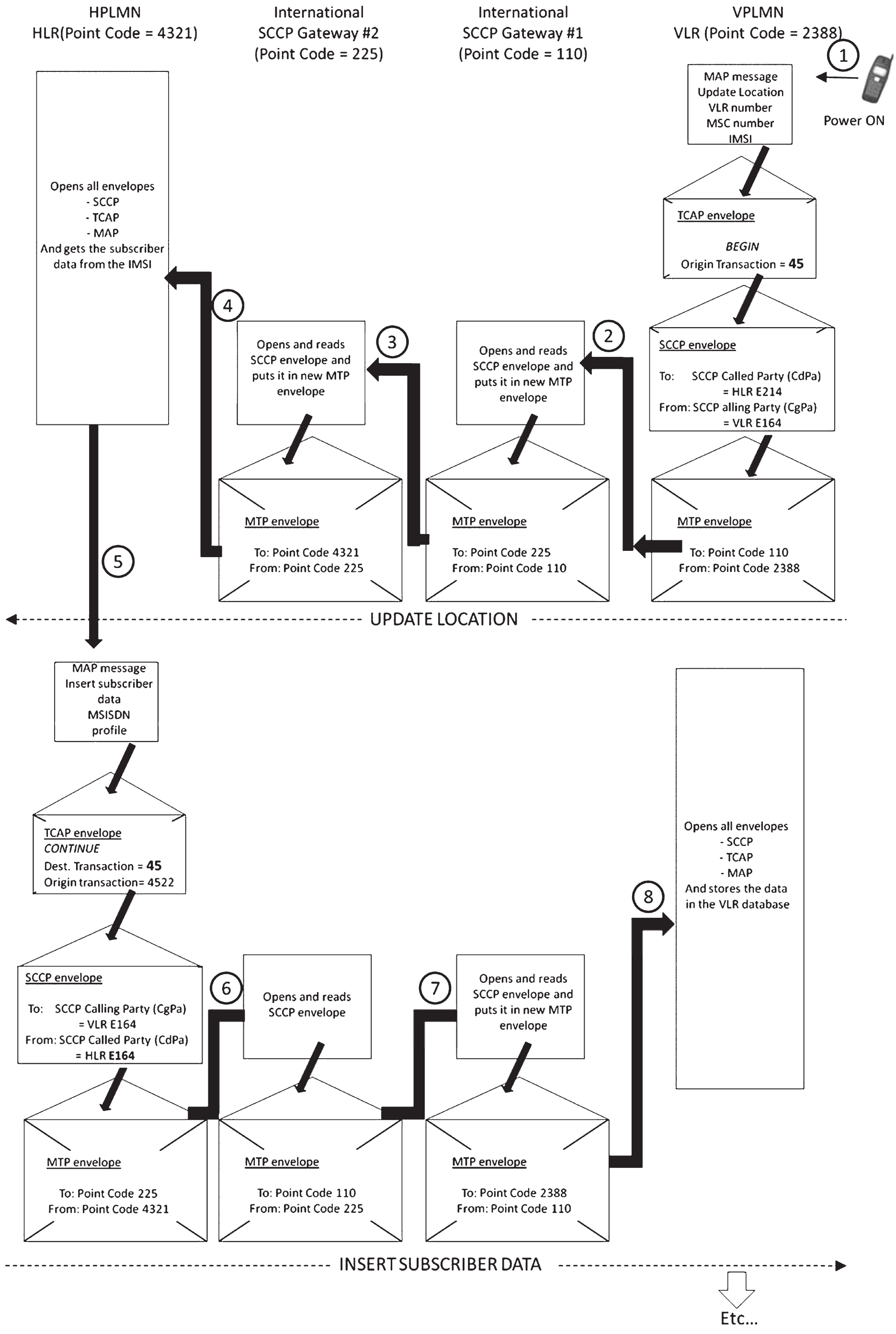


Figure 1.8 Multiple envelope principle of SS7

(different GTs are possible for the VLR and MSC subsystems). To be understood by the remote HLR, interoperability is required and the very complex MAP protocol standard [2.3] is used. In Chapter 2, for the CAMEL procedures for prepaid subscribers, there is also a standard [2.4] for the coding of CAMEL messages.

1.5.2 Need to Exchange Them with Transactions: the TCAP Protocol

The VLR needs to establish a session with the distant HLR, called a 'TCAP transaction', because the UPDATE LOCATION that it sends will be replied to by the profile of the subscriber in several successive data exchanges with an acknowledgment. Besides special errors, the TCAP protocol includes three main transaction types: BEGIN, CONTINUE and END.

The VLR allocates a new 'Origin Transaction ID' (45 in Figure 1.8) and inserts the MAP UPDATE LOCATION in a TCAP envelope with 'BEGIN'.

1.5.3 Packet Protocol to Transfer Data between Two Different Networks: SCCP

The VLR needs to send this TCAP envelope to the distant HLR. From the IMSI and a table, it builds the E214 GT address of the HLR. An SCCP envelope is created with this address as 'To' and the VLR sets its own GT address (E164) as 'From', and these are used to transport the previous TCAP envelope.

1.5.4 Packet Protocol to Transfer SCCP Blocks between Equipment: MTP or SIGTRAN

At this stage, the 'From' is a GT and the MSC/VLR, in general, does not have a direct route with the HLR. To allow this case and have the addressing simplicity of the GT system, a 'Point Code' layer is provided which uses 'Point Code' local addresses assigned to all equipment (in association with a Global Title address). The MSC/VLR (its Point Code is 2388) uses a table of Global Title routes to get the Point Code 110 of the International Gateway #1 which provides the SS7 route to the HLR's network. The previous SCCP envelope is inserted in an MTP envelope with 'To: 110' and 'From: 2388' and sent (2).

Upon receiving it, the International Gateway opens the MTP envelope to read the SCCP envelope and sees 'To: HLR E214 GT'. From its GT routing table it finds the address (the international Point Code) of the International SCCP Gateway partner #2, which provides the end route to this network. It creates a new MTP envelope with 'From: 110' and 'To: 225' and sends (3) it to the IGW#2, which by the same method will send (4) the MTP envelope to the HLR.

The HLR opens all the successive envelopes until it gets the MAP UPDATE LOCATION with the IMSI of the customer and the MSC and VLR GTs. It uses them to register the customer so the calls and SMSs can be sent to these GTs.

Then the HLR needs to send the 'profile' of the subscriber to the VLR. It creates an INSERT SUBSRCRIBER DATA MAP message with the first block of the profile and inserts it (5) in a TCAP envelope, which has Destination Transaction ID = 45 of the type CONTINUE.

The 'answer' of the HLR will be sent to the VLR (6), (7) and (8) in the same way as above. The VLR will Ack (see Etc. at the bottom of Figure 1.8) the reception of the INSERT SUBSCRIBER DATA with another CONTINUE. We leave the reader to complete the sequence until at the end the HLR will send a TCAP END, which terminates the transaction.

1.5.5 The Lower Layers, not a Concern for Virtual Roaming Systems

The ‘Point Code’ layer can be either MTP3 or SIGTRAN (M3UA, see Chapter 3). The Roaming Hub architecture is independent of the lower layers (MTP2 when TDM E1 circuits are used, M2PA when SIGTRAN is used with MTP3, SCTP/IP with M3UA). So the detailed diagrams of the next chapter, which explain the architecture, will only show layers down to the SCCP layer, as the MTP layer operation has nothing remarkable to be explained.

2

Architecture of Virtual Roaming Systems

The Triumph TR3 was the last car designed for hairy-chested drivers.
'The Triumph TRs', Graham Robson, 1978

2.1 SCCP, MAP, CAP and GTP Transformation Principle in the Roaming Hub

Figure 2.1 will be used to explain the transformation of MAP parameters in the case of virtual roaming by visitors of an HPLMN in a VPLMN. If the VPLMN and the HPLMN had an agreement, it would be a classical exchange of MAP messages, as in Figure 1.7, starting with an UPDATE_LOCATION sent by the VPLMN, the HLR sending back the profile of the subscriber INSERT SUBSCRIBER DATA, then sending the UPDATE LOCATION Ack which contains the GT of the HLR.

Some parameters, MAP or CAMEL, which carry the GT, are changed. The rule is simple: *inside the network of Roaming Hubs, the real GT is set*. (Or equivalently: (1) when a message is sent from the network to a HPLMN or VPLMN, the parameters are eventually transformed, and (2), when a message enters the network with coded parameters, they are translated to the real GT.)

As a consequence, *a parameter is never modified twice*.

HI is the 'Hub Indicator' of the Roaming Hub, for example +33151. So the addressing of the SCP or the HLR made by the VPLMN will always be routed to the Roaming Hub for any value of OI_hplmn.

The transformation of addresses to the Real GT is, for symmetry reasons, made:

- in the Roaming Hub (EXIT) for the flow from VPLMN to HPLMN;
- in the Roaming Hub (ENTRY) for the flow from HPLMN to VPLMN.

The detailed explanations are valid for a very general case with several Roaming Hubs in the chain. The signalling between two Roaming Hubs in order to be able to control the route from the ENTRY is explained in Chapter 3. The case is further generalized in Chapter 4 for a Roaming Hub having several 'Virtual Hub Indicators'.

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

2.1.1 Setup of Virtual Visitor Roaming in the VPLMN

The GMSC must be configured so that all the GTs for Mobiles for which the VPLMN does not have roaming are routed to the Roaming Hub. This concerns the E214 and E164 addresses of their HLRs, the E164 addresses of the SMSC, etc. Chapter 5 will show the various methods of configuring the GT. This can have several possible values depending on the connection mode, but all must be routed to the Roaming Hub by international addressing or by a direct connection.

Any E164 address, for which there is no roaming, must be routed to the Roaming Hub (ENTRY).

We present a very general case with a network of Roaming Hubs: the one adjacent to the VMPLMN is called Roaming Hub (ENTRY) with a GT called HI_E (Hub Indicator ENTRY); the one adjacent to the HPLMN is called Roaming Hub (EXIT) with a GT called HI_X (Hub Indicator EXIT). The simpler case, of course, is a single Roaming Hub ($HI_E = HI_X = HI$).

2.1.2 Required SCCP Address Transparency of the MAP, CAMEL and TCAP Layers of the SS7 Stack

Looking at Figure 1.7, we see that the HLR responds with an INSERT SUBSCRIBER DATA (ISD) to the UPDATE LOCATION (UL) received from the VLR. This ISD is sent in an SCCP message using as CdPa the CgPa received in the UL (including the GT of the VLR). But the CgPa is not the CdPa of the UL (the E214 address of the HLR); the HLR replaces it by its own GT (E164). When we include a Roaming Hub in the path, this CgPa = GT E164 of the HLR must be received by the Roaming Hub at the application layer from TCAP then MAP transformed (Alias GT mode) or relayed transparently (MTP tunnelling mode) for the SCCP addressing of the ISD to the VLR.

To operate correctly, the Roaming Hub then needs to have the TCAP and MAP or CAMEL layers to pass the SCCP CgPa received in the TCAP CONTINUE transparently to the Roaming Hub application, like those which carry the ISD sent by the HLR.

If you need a reminder of the TCAP protocol, see Section 5.2.

2.2 Procedures for the Virtual Roaming Visitors' Service (Single IMSI)

We will explain the procedures in a logical order, starting with the main services:

- voice and SMS: the registration procedure;
- reception of a call or an SMS-MT while roaming;
- outgoing call in the prepaid case with CAMEL;
- SMS-MO and also the SMS-MO prepaid case.

But in order for the services to work fully, as if there was a bilateral roaming agreement, we will have:

- READY FOR SM;
- PURGE MS.

Then, to offer their data services to the virtual roaming visitors, there will be:

- a GPRS registration procedure, very much like the previous one;
- a connection to a data service (Internet, MMS, etc.): it uses the GTP protocol in the GRX network (the private IP network for mobile data services) and not MAP or CAMEL. The Roaming Hub must implement the GTP protocol to behave as a relaying GGSN (GPRS Gateway Service Node).

There are several solutions to connect the VPLMN. In order to have a coherent CdPa (Calling Party Address SCCP) from the VPLMN, we will assume that the recommended method of Section 3.2 is used: any E214 (e.g. for UPDATE LOCATION) or E164 address (e.g. to send SMS-MO to the HPLMN SMSC), which the VPLMN does not have roaming with, *is translated to the full E164 address* of the

Roaming Hub (ENTRY). This means that, on the other hand, an address such as HI_X + OI_vmpln + NNI_scp is left (because the GT HI_X has roaming with the VPLMN).

2.2.1 *The UPDATE LOCATION Registration Procedure (MAP sent to the HLR)*

When a mobile is turned on, its HLR must have the location (the MSC Number and VLR Number that it is visiting) and send the profile to the HLR. In order for the standard procedure to work through a Roaming Hub, some changes must be made in the MAP parameters. Although only one INSERT SUBSCRIBER DATA is represented, there can be four in practice.

The MAP parameter identifying a particular subscriber for the HLR is the IMSI.

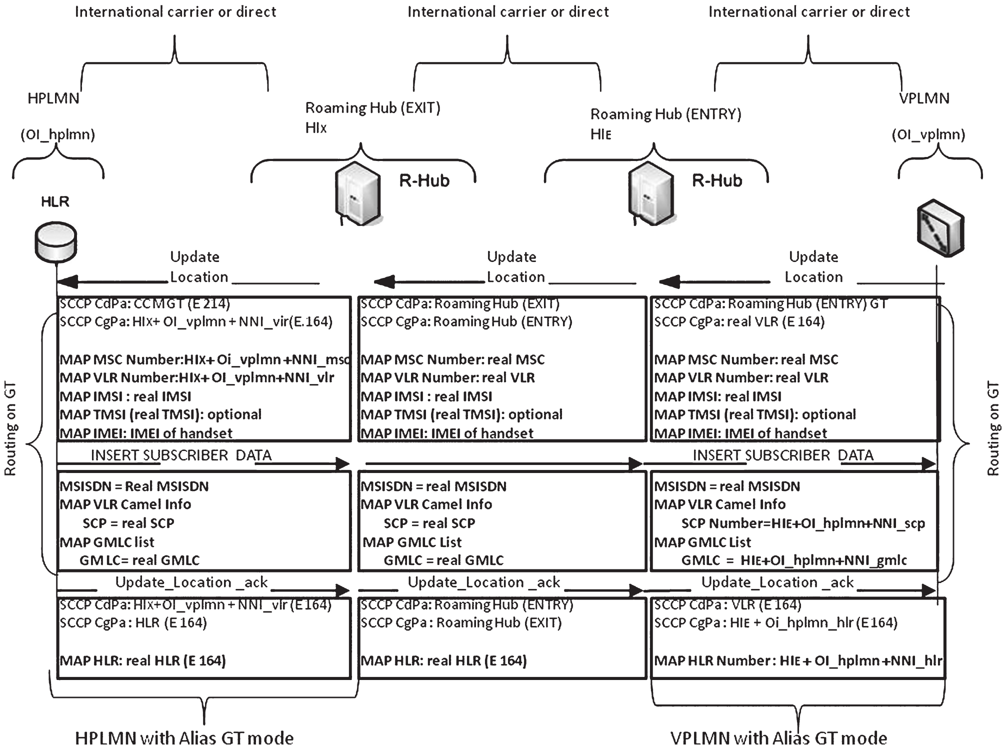

International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
HLR
Update Location
Update Location
Update Location
SCCP CdPa: CCMGT (E 214)
SCCP CgPa: HIX+ OI_vplmn + NNI_vir(E.164)
MAP MSC Number:HIX+ Oi_vplmn +NNI_msc
MAP VLR Number:HIX+ OI_vplmn+NNI_vlr
MAP IMSI : real IMSI
MAP TMSI (real TMSI): optional
MAP IMEI: IMEI of handset
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)
MAP MSC Number: real MSC
MAP VLR Number: real VLR
MAP IMSI : real IMSI
MAP TMSI (real TMSI): optional
MAP IMEI: IMEI of handset
SCCP CdPa: Roaming Hub (ENTRY) GT
SCCP CgPa: real VLR (E 164)
MAP MSC Number: real MSC
MAP VLR Number: real VLR
MAP IMSI: real IMSI
MAP TMSI (real TMSI): optional
MAP IMEI: IMEI of handset
Routing on GT
INSERT SUBSCRIBER DATA
INSERT SUBSCRIBER DATA
Routing on GT
MSISDN = Real MSISDN
MAP VLR Camel Info
SCP = real SCP
MAP GMLC list
GM LC= real GMLC
MSISDN = real MSISDN
MAP VLR Camel Info
SCP = real SCP
MAP GMLC List
GMLC = real GMLC
MSISDN = real MSISDN
MAP VLR Camel Info
SCP Number=HIE+OI_hplmn+NNI_scp
MAP GMLC List
GMLC = HIE+OI_hplmn+NNI_gmlc
Update_Location _ack
Update_Location _ack
Update_Location _ack
SCCP CdPa: HIx+OI_vplmn + NNI_vlr (E164)
SCCP CgPa : HLR (E 164)
MAP HLR: real HLR (E 164)
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa : Roaming Hub (EXIT)
MAP HLR: real HLR (E 164)
SCCP CdPa : VLR (E 164)
SCCP CgPa : HIE + Oi_hplmn_hlr (E164)
MAP HLR Number : HIE + OI_hplmn +NNI_hlr
HPLMN with Alias GT mode
VPLMN with Alias GT mode

Figure 2.1 The UPDATE LOCATION registration procedure (MAP sent to the HLR)

In order to be consistent, the HLR and SCP sent to the VPLMN are also transformed so that the VPLMN will address them by a GT of the Roaming Hub (ENTRY) HI_E. It allows the Roaming Hub (ENTRY) to use the 'static method 2' of Table 2.3 to set the real GT.

The virtual visitor may have 'Location Based Services' provided by their HPLMN with a list of GMLC (Gateway Mobile Location Centre) GTs. These addresses must also be transformed as shown.

Example:

IMSI = 605031234567890
R-Hub HI = 3315099
Translation IMSI (E.212 → E.214): MCC → 33, MNC → 15099
R-Hub ENTRY GT = +3315099 (E.164)

Note that the TMSI could be sent by the VPLMN and used by the HLR to return this TMSI to the incoming SEND ROUTING INFO for SM. In this case, the FORWARD SM-MT will contain only the TMSI. However, the Roaming Hub which had also received the IMSI would be able to identify the destination HPLMN of this SMS-MT.

If the VPLMN has the Automatic Device Detection feature, it will inform the HLR of the type of handset (IMEI) so that a new profile for Internet services can be automatically loaded. The Roaming Hub, being in the signalling path, could then provide useful data for the provisioning of handsets as explained in Chapter 9.

As shown in the introduction in Section 1.4, an E164 HLR address received from the PLMN for the INSERT SUBSCRIBER DATA must be properly transmitted as an E164 address to the VLR.

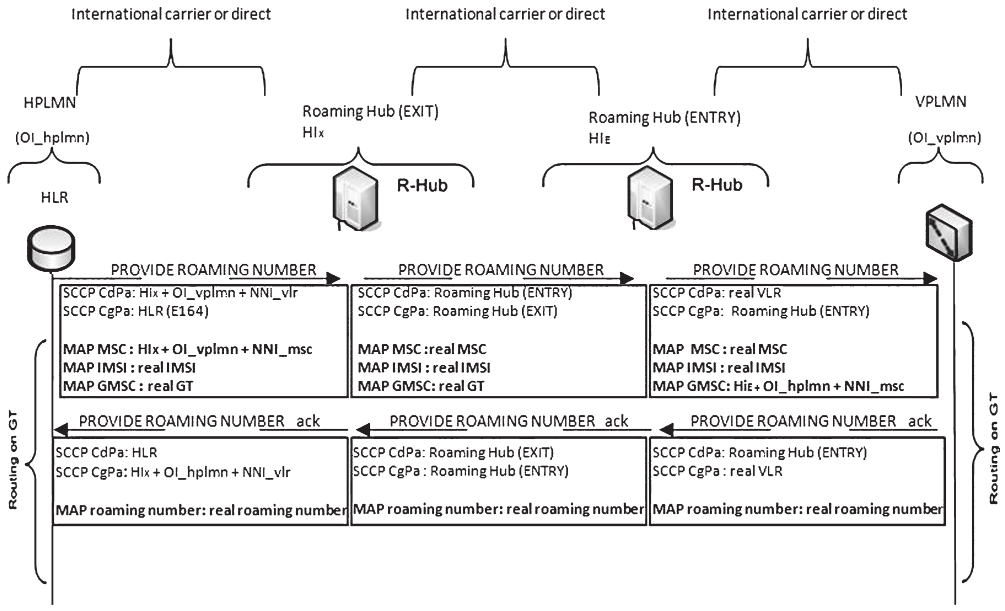
2.2.2 *Outgoing Calls for Post-paid Visitors*

MAP or CAMEL signalling is not involved. The virtual subscriber makes a call. An MOC (Mobile Originated Call) ticket will be generated, which must be passed to the Roaming Hub for clearing and indirect charging to the VPLMN.

2.2.3 *Reception of Calls while Roaming (MAP Sent to the VLR)*

The HLR in the HPLMN has VLR = HI_X + OI_vplmn + NNI_vlr which it received in the UPDATE LOCATION parameters. So the PROVIDE ROAMING NUMBER sent by the HLR when a call is made to the subscriber has this address directly in the SCCP Called Party Address, because it starts with HI_X, the GT of the Roaming Hub (EXIT). Figure 2.2 shows the process.

The MAP parameter identifying a particular subscriber for the VLR is the IMSI.



SCCP CdPa: HIx + OI_vplmn + NNI_vlr
SCCP CgPa: HLR (E164)
MAP MSC : HIx + OI_vplmn + NNI_msc
MAP IMSI : real IMSI
MAP GMSC : real GT

SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa: Roaming Hub (EXIT)
MAP MSC : real MSC
MAP IMSI : real IMSI
MAP GMSC: real GT

SCCP CdPa: real VLR
SCCP CgPa: Roaming Hub (ENTRY)
MAP MSC : real MSC
MAP IMSI : real IMSI
MAP GMSC: HIE + OI_hplmn + NNI_msc

SCCP CdPa: HLR
SCCP CgPa: HIx + OI_hplmn + NNI_vlr
MAP roaming number: real roaming number

SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa : Roaming Hub (ENTRY)
MAP roaming number: real roaming number

SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa : real VLR
MAP roaming number: real roaming number

Figure 2.2 Reception of calls while roaming (MAP sent to the VLR)

Some vendors (Alcatel, Siemens) use different GTs for the MSC and the VLR. In PROVIDE ROAMING NUMBER, it is the VLR GT which is used for the SCCP addressing, while in the MAP parameters it is the MSC.

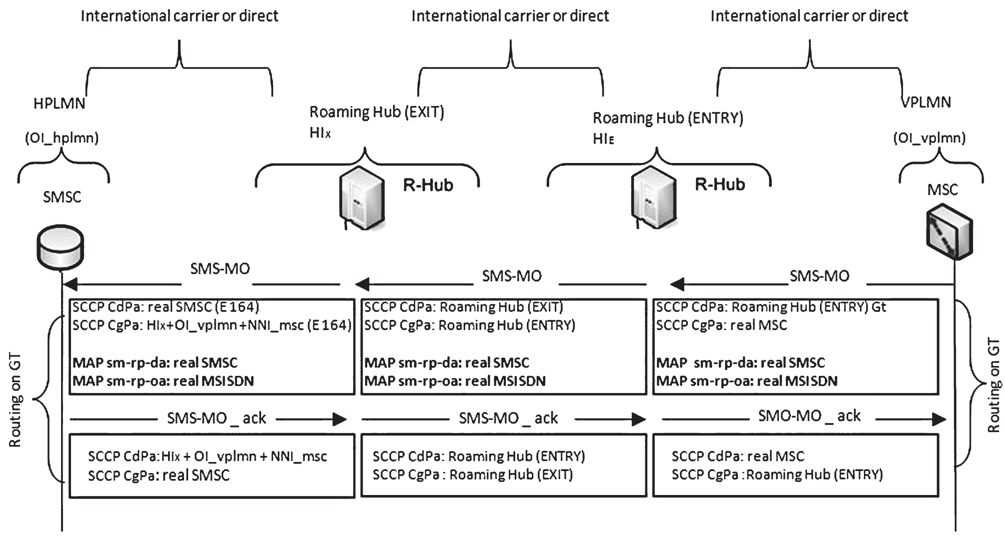

International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
SMSC
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
MSC
SMS-MO
SMS-MO
SMS-MO
SCCP CdPa: real SMSC (E 164)
SCCP CgPa: HIx+OI_vplmn+NNI_msc (E 164)
MAP sm-rp-da: real SMSC
MAP sm-rp-oa: real MSISDN
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)
MAP sm-rp-da: real SMSC
MAP sm-rp-oa: real MSISDN
SCCP CdPa: Roaming Hub (ENTRY) Gt
SCCP CgPa: real MSC
MAP sm-rp-da: real SMSC
MAP sm-rp-oa: real MSISDN
SMS-MO _ ack
SMS-MO _ ack
SMO-MO _ ack
SCCP CdPa: HIx + OI_vplmn + NNI_msc
SCCP CgPa: real SMSC
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa : Roaming Hub (EXIT)
SCCP CdPa: real MSC
SCCP CgPa : Roaming Hub (ENTRY)
Routing on GT
Routing on GT

Figure 2.3 Outgoing SMS-MO

2.2.4 *Outgoing SMS-MO (MAP to the SMSC)*

The SIM card of the roaming visitor contains the GT of their SMSC. The VMSC sets the GT of the destination SMSC in the parameter sm-rp-da of the SMS-MO.

As the GT will be changed by the setup of the VPLMN with the Roaming Hub, the Roaming Hub must relay the SMS-MO to the GT obtained from the MAP parameter sm-rp-da.

The Roaming Hub (EXIT) sets the SCCP CdPa to the real SMSC which it has received in the MAP parameters, as shown in Figure 2.3.

The MAP parameter identifying a particular sending subscriber for the SMSC is the MSISDN of the sender in the 'sm_rp_oa' parameter or the IMSI, which maybe included if the MSC or the SGSN supports number portability.

If the subscriber is prepaid with a CAMEL profile including the 'SMS-CSI', an Initial DP SMS will be sent exactly as for voice.

2.2.5 *Reception of SMS-MT while Roaming (MAP sent to MSC)*

As shown, the SMSC of the HPLMN will send the SMS. To do this, it interrogates the HLR of the destination number to get the IMSI and the Visited MSC GT: it will get VMSC = HI_X + OI_vplmn + NNI_msc. So the procedure shown in Figure 2.4 will be very much like the sending of the PROVIDE ROAMING NUMBER in Figure 2.2.

The MAP parameter identifying a particular subscriber for the MSC is the IMSI.

One notices that the parameter Service Centre address must be changed. It is used for the billing process of the AA19 SMS charging agreement, and as the HPLMN and VPLMN do not have a roaming agreement, HI + OI_hplmn + NNI_smsc must be sent to the VPLMN so that it charges the Roaming Hub (ENTRY) for the SMS-MT termination.

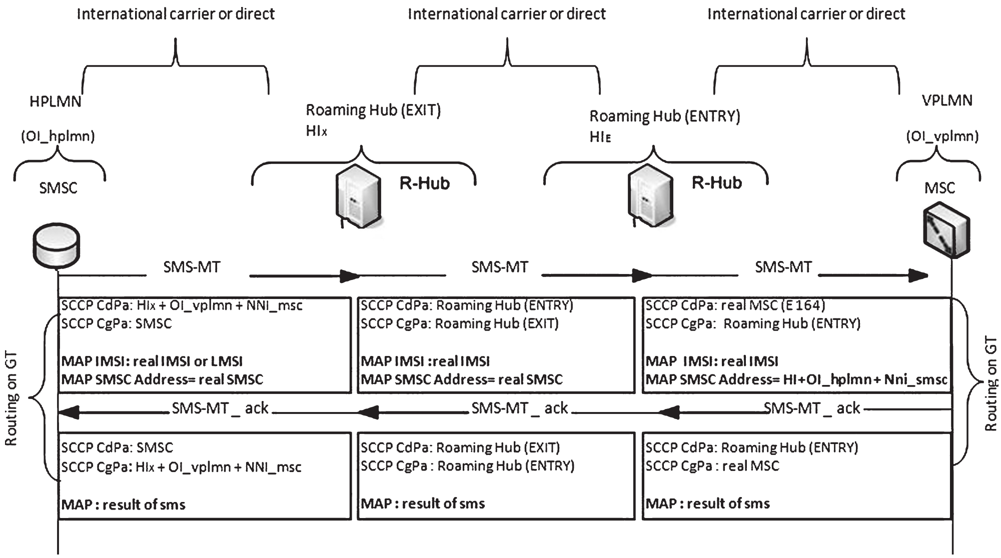

International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
SMSC
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
MSC
SMS-MT
SMS-MT
SMS-MT
SCCP CdPa: HIx + OI_vplmn + NNI_msc
SCCP CgPa: SMSC
MAP IMSI: real IMSI or LMSI
MAP SMSC Address= real SMSC
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa: Roaming Hub (EXIT)
MAP IMSI :real IMSI
MAP SMSC Address= real SMSC
SCCP CdPa: real MSC (E 164)
SCCP CgPa: Roaming Hub (ENTRY)
MAP IMSI: real IMSI
MAP SMSC Address= HI+OI_hplmn+ Nni_smsc
SMS-MT _ ack
SMS-MT _ ack
SMS-MT _ ack
SCCP CdPa: SMSC
SCCP CgPa: HIx + OI_vplmn + NNI_msc
MAP : result of sms
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa : Roaming Hub (ENTRY)
MAP : result of sms
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa : real MSC
MAP : result of sms
Routing on GT
Routing on GT

Figure 2.4 Reception of SMS-MT while roaming

2.2.5.1 Case of 'Reply Path' Setting

It is possible that a sending SMSC (other), which is not the HPLMN above *but must also be a customer of the Roaming Hub*, could send an SMS-MT with the Reply Path set back to itself; it will reach the subscriber if this SMSC has a roaming agreement with HPLMN (in addition to the agreement with the Roaming Hub). In this case, the OI_hplmn is OI_hplmn (other), and the reply SMS-MO from the subscriber will go to this SMSC (other) by the Reply Path mechanism.

2.2.6 READY FOR SM Procedure (MAP to the HLR)

When the SMS memory of a handset is emptied or it is switched on again, the VLR or the SGSN sends a MAP READY FOR SM to the HLR, for the HLR to ALERT the SMSC. The Roaming Hub has the GT of the real HLR (E164) memorized in the MAP-UPDATE-LOCATION. It is used to send the SM READY to the real HLR GT (implementation dependent). *This is a case where the HLR E164 address returned in the UPDATE LOCATION is used*. The MAP parameters do not include the VLR or SGSN GT.

The MAP parameter identifying a particular subscriber for the HLR is the IMSI.

It works the same as PURGE MS (see Figure 2.7).

2.2.7 Outgoing USSD (MAP to the HLR)

A USSD 'call' is performed when one dials a number such as *888#; 888 is a USSD service code declared in the HLR. *There is no parameter in the MAP protocol to identify the particular subscriber*: it also uses TCAP to carry the IMSI in the destination_ref field. The diagram is the same as for outgoing supplementary services (see Figure 2.5).

2.2.8 Reception of USSD 'Push' while Roaming (MAP Sent to MSC)

A lesser known service is the possibility that some USSD service of the HPLMN 'pushes' a USSD message to the virtual visitor (for example: a question which the USSD answers).

The mechanism is the same as for an SMS-MT, except that an UNSTRUCTURED-SS REQUEST (conversational) or NOTIFY (just a 'push') is sent to the MSC by the USSD service.

2.2.9 Outgoing Supplementary Services (Call Forwarding or Barring) (MAP to the HLR)

These are the services used when a call forwarding or cancellation of forwarding is performed with the handset. *There is no parameter in the MAP protocol to identify the particular subscriber*; it is a TCAP parameter in the 'dialogue part', called 'destination_reference' where the IMSI is coded. This parameter is also used in Section 4.3.2 to carry the final destination of traffic between several Roaming Hubs. As you can see, the destination reference is not used between the Roaming Hubs to carry the IMSI as it must carry the final Roaming Hub destination as explained in Chapter 4 where the TCAP manipulation necessary between two Roaming Hubs is explained.

Also, the HLR may control the field 'origin-reference' in the TCAP dialogue part: it contains the GT (transformed) corresponding to the originating VLR.

2.2.9.1 Without Get Password

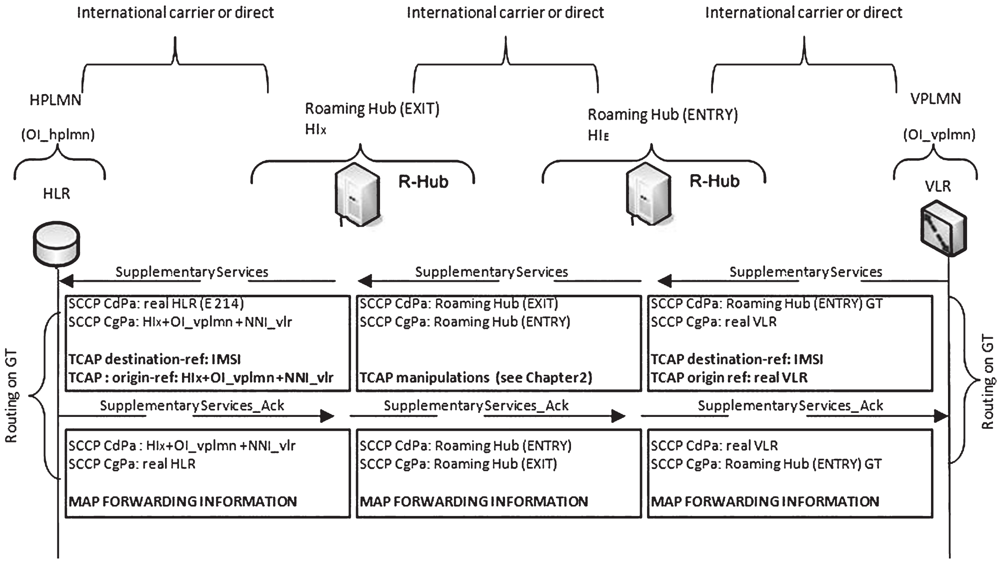

International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
Roaming Hub (EXIT)
HIx
Roaming Hub (ENTRY)
HIE
VPLMN
(OI_vplmn)
HLR
R-Hub
R-Hub
VLR
SupplementaryServices
SupplementaryServices
SupplementaryServices
SCCP CdPa: real HLR (E 214)
SCCP CgPa: HIx+OI_vplmn+NNI_vlr
TCAP destination-ref: IMSI
TCAP : origin-ref: HIx+OI_vplmn+NNI_vlr
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)
TCAP manipulations (see Chapter2)
SCCP CdPa: Roaming Hub (ENTRY) GT
SCCP CgPa: real VLR
TCAP destination-ref: IMSI
TCAP origin ref: real VLR
SupplementaryServices_Ack
SupplementaryServices_Ack
SupplementaryServices_Ack
SCCP CdPa : HIx+OI_vplmn +NNI_vlr
SCCP CgPa: real HLR
MAP FORWARDING INFORMATION
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa: Roaming Hub (EXIT)
MAP FORWARDING INFORMATION
SCCP CdPa: real VLR
SCCP CgPa: Roaming Hub (ENTRY) GT
MAP FORWARDING INFORMATION
Routing on GT
Routing on GT

Figure 2.5 Outgoing Supplementary Services

2.2.9.2 Get Password Request by the HLR

The handsets have a menu for the activation of 'call barring' (e.g. bar reception of all calls). Most HLRs secure the procedure by asking for a password which is recorded in the HLR. The SS ACTIVATE and

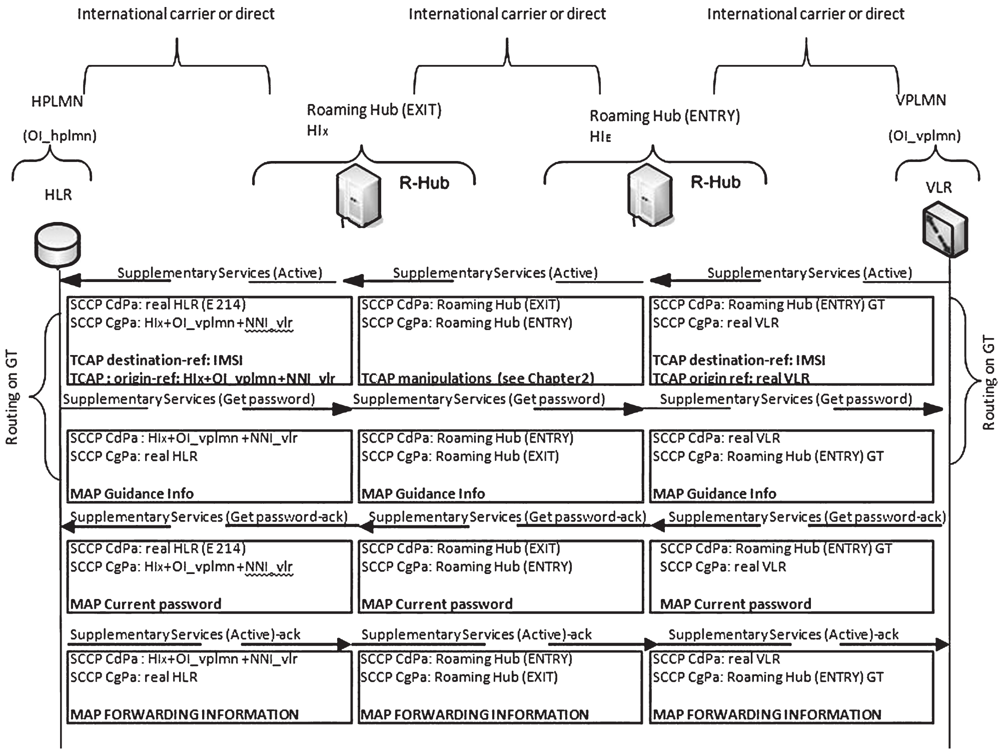

International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
HLR
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
VLR
Routing on GT
Routing on GT
SupplementaryServices (Active)
SupplementaryServices (Active)
SupplementaryServices (Active)
SCCP CdPa: real HLR (E 214)
SCCP CgPa: HIx+OI_vplmn+NNI_vlr
TCAP destination-ref: IMSI
TCAP : origin-ref: HIx+OI_vplmn+NNI_vlr
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)
TCAP manipulations (see Chapter2)
SCCP CdPa: Roaming Hub (ENTRY) GT
SCCP CgPa: real VLR
TCAP destination-ref: IMSI
TCAP origin ref: real VLR
SupplementaryServices (Get password)
SupplementaryServices (Get password)
SupplementaryServices (Get password)
SCCP CdPa : HIx+OI_vplmn +NNI_vlr
SCCP CgPa: real HLR
MAP Guidance Info
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa: Roaming Hub (EXIT)
MAP Guidance Info
SCCP CdPa: real VLR
SCCP CgPa: Roaming Hub (ENTRY) GT
MAP Guidance Info
SupplementaryServices (Get password-ack)
SupplementaryServices (Get password-ack)
SupplementaryServices (Get password-ack)
SCCP CdPa: real HLR (E 214)
SCCP CgPa: HIx+OI_vplmn+NNI_vlr
MAP Current password
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)
MAP Current password
SCCP CdPa: Roaming Hub (ENTRY) GT
SCCP CgPa: real VLR
MAP Current password
SupplementaryServices (Active)-ack
SupplementaryServices (Active)-ack
SupplementaryServices (Active)-ack
SCCP CdPa : HIx+OI_vplmn +NNI_vlr
SCCP CgPa: real HLR
MAP FORWARDING INFORMATION
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa: Roaming Hub (EXIT)
MAP FORWARDING INFORMATION
SCCP CdPa: real VLR
SCCP CgPa: Roaming Hub (ENTRY) GT
MAP FORWARDING INFORMATION

Figure 2.6 Outgoing Supplementary Services Active with ‘GET PASSWORD’

the request for and sending of the password are contained within a single TCAP transaction. The full dialogue through the Roaming Hub is given in Figure 2.6. The GET PASSWORD request by the HLR and the sending of a password can be repeated several times. So the pattern of this type of dialogue is like that of an UDPDATE LOCATION.

2.2.10 PURGE MS Procedure (MAP to the HLR)

When the user has not used their phone for a long time (implementation dependent, about two weeks), the VLR or the SGSN will send a MAP PURGE MS to the HLR which erases the last entry of the visited VLR or SGSN. So if any call or SMS is then attempted to this user, the HLR will immediately return a user error = 29 meaning ‘detached HLR’. It is the E214 address of the HLR which is used by the VLR or the SGSN as derived from the IMSI.

The MAP parameters include the VLR or SGSN GT which issues the service. The MAP parameter identifying a particular subscriber for the HLR is the IMSI.

It is the same if the PURGE MS is sent by an SGSN, except that the parameter name is SGSN instead of VLR.

2.2.11 2.5G and 3G: UPDATE LOCATION GPRS (MAP to the HLR)

This is exactly the same procedure as previously, except that it is the SGSN which makes the registration instead of the VLR as shown in Figure 2.8.

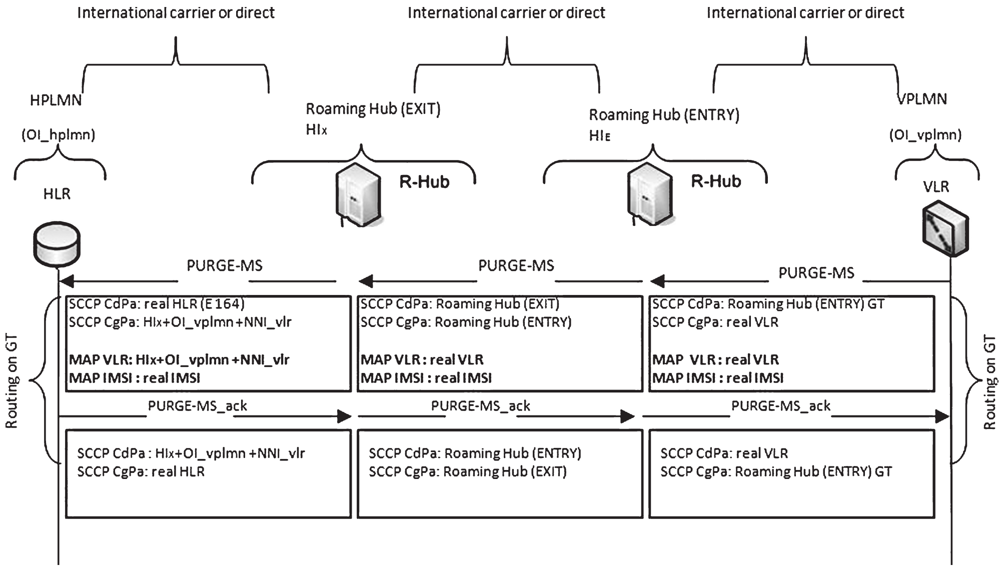

International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
HLR
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
VLR
PURGE-MS
PURGE-MS
PURGE-MS
SCCP CdPa: real HLR (E 164)
SCCP CgPa: HIx+OI_vplmn+NNI_vlr
MAP VLR: HIx+OI_vplmn+NNI_vlr
MAP IMSI : real IMSI
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)
MAP VLR : real VLR
MAP IMSI : real IMSI
SCCP CdPa: Roaming Hub (ENTRY) GT
SCCP CgPa: real VLR
MAP VLR : real VLR
MAP IMSI : real IMSI
PURGE-MS_ack
PURGE-MS_ack
PURGE-MS_ack
SCCP CdPa : HIx+OI_vplmn +NNI_vlr
SCCP CgPa: real HLR
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa: Roaming Hub (EXIT)
SCCP CdPa: real VLR
SCCP CgPa: Roaming Hub (ENTRY) GT
Routing on GT
Routing on GT

Figure 2.7 PURGE MS procedure

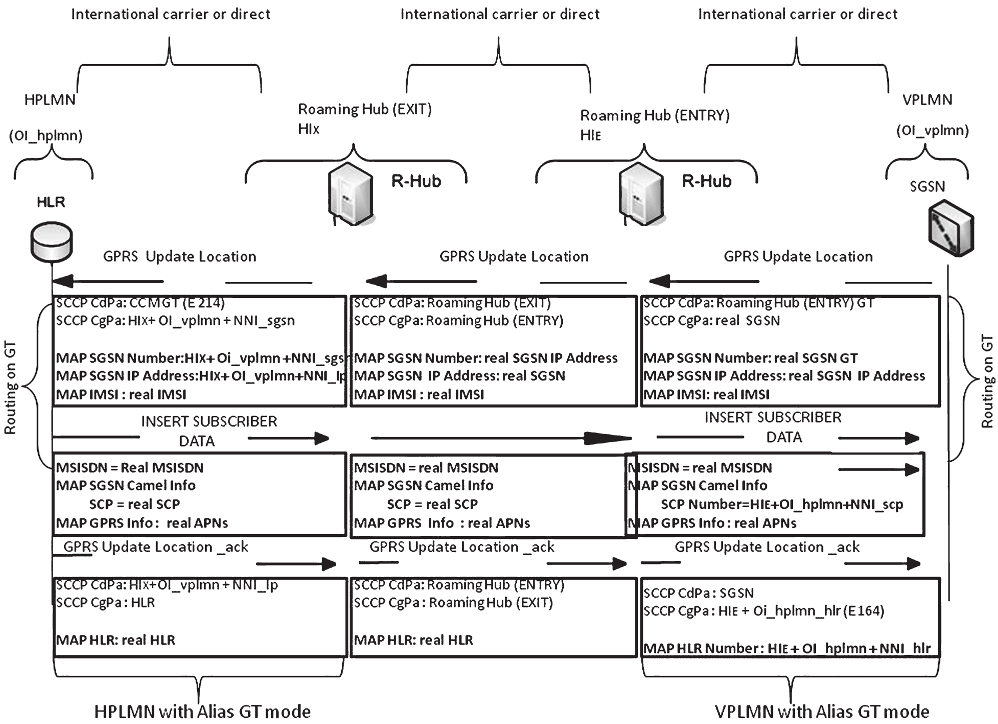

International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
HLR
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
SGSN
GPRS Update Location
GPRS Update Location
GPRS Update Location
SCCP CdPa: CCMGT (E 214)
SCCP CgPa: HIX+ OI_vplmn + NNI_sgsn
MAP SGSN Number:HIX+ Oi_vplmn +NNI_sgs
MAP SGSN IP Address:HIX+ OI_vplmn+NNI_Ip
MAP IMSI : real IMSI
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)
MAP SGSN Number: real SGSN IP Address
MAP SGSN IP Address: real SGSN
MAP IMSI : real IMSI
SCCP CdPa: Roaming Hub (ENTRY) GT
SCCP CgPa: real SGSN
MAP SGSN Number: real SGSN GT
MAP SGSN IP Address: real SGSN IP Address
MAP IMSI: real IMSI
INSERT SUBSCRIBER DATA
INSERT SUBSCRIBER DATA
MSISDN = Real MSISDN
MAP SGSN Camel Info
SCP = real SCP
MAP GPRS Info : real APNs
MSISDN = real MSISDN
MAP SGSN Camel Info
SCP = real SCP
MAP GPRS Info : real APNs
MSISDN = real MSISDN
MAP SGSN Camel Info
SCP Number=HIE+OI_hplmn+NNI_scp
MAP GPRS Info : real APNs
GPRS Update Location _ack
GPRS Update Location _ack
GPRS Update Location _ack
SCCP CdPa: HIx+OI_vplmn + NNI_Ip
SCCP CgPa : HLR
MAP HLR: real HLR
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa : Roaming Hub (EXIT)
MAP HLR: real HLR
SCCP CdPa : SGSN
SCCP CgPa : HIE + Oi_hplmn_hlr (E164)
MAP HLR Number : HIE + OI_hplmn + NNI_hlr
HPLMN with Alias GT mode
VPLMN with Alias GT mode
Routing on GT
Routing on GT

Figure 2.8 UPDATE LOCATION GPRS

The MAP parameter identifying a particular subscriber for the HLR is the IMSI.

The SGSN profile will contain a list of APNs (Access Provider Names) which identifies the GGSN that the handset can connect to. The example contains four APNs in the same GGSN which can have different charging schemes.

MSISDN: +37493123456
IMSI: +283058000123456

```
value InsertSubscriberDataArg ::=
{
  subscriberStatus serviceGranted,
  teleserviceList
  {
    short Message MT-PP,
    short Message MO-PP
  },
  gprsSubscriptionData
  {
    completeDataListIncluded NULL,
    gprsDataList
    {
      {
        pdp-ContextId 6,
        pdp-Type IETF allocated address: IPv4,
        qos-Subscribed ′15821F′H,
        vplmnAddressAllowed NULL,
        apn TEST.VIVACELL.AM
      },
      {
        pdp-ContextId 5,
        pdp-Type IETF allocated address: IPv4,
        qos-Subscribed ′15821F′H,
        vplmnAddressAllowed NULL,
        apn MMS.VIVACELL.AM
      },
      {
        pdp-ContextId 4,
        pdp-Type IETF allocated address: IPv4,
        qos-Subscribed ′15821F′H,
        vplmnAddressAllowed NULL,
        apn WAP.VIVACELL.AM
      }
    }
  },
  networkAccessMode bothMSCAndSGSN
}
{
  gprsSubscriptionData
  {
    gprsDataList
```

```
      {
        {
          pdp-ContextId 2,
          pdp-Type IETF allocated address: IPv4,
          qos-Subscribed ′15821F′H,
          vplmnAddressAllowed NULL,
          apn INET.VIVACELL.AM
        }
      }
    }
  }
```

2.2.12 2.5G and 3G: Outgoing Create PDP Context (GTP to the HPLMN GGSN)

When a mobile switches on with GPRS roaming coverage of an SGSN, the UPDATE LOCATION GPRS occurs as above and it becomes 'GPRS attached' in the HLR. It can send and receive SMS by GPRS. However, there is as yet no data connection. For this, it goes into some 'gallery' menu and a Create PDP Context procedure is executed, which establishes a data packet connection with its HPLMN GGSN through the VPLMN GGSN and the Roaming Hub (as the two do not have a bilateral roaming agreement).

The main transformation is to change the SGSN IP address to the Roaming Hub IP address (which has a data roaming agreement with the HPLMN and the VPLMN) as shown in Figure 2.9.

The GTP parameter identifying a particular subscriber for the GGSN is the IMSI. The CAP uses the GRX network, not the SS7 network.

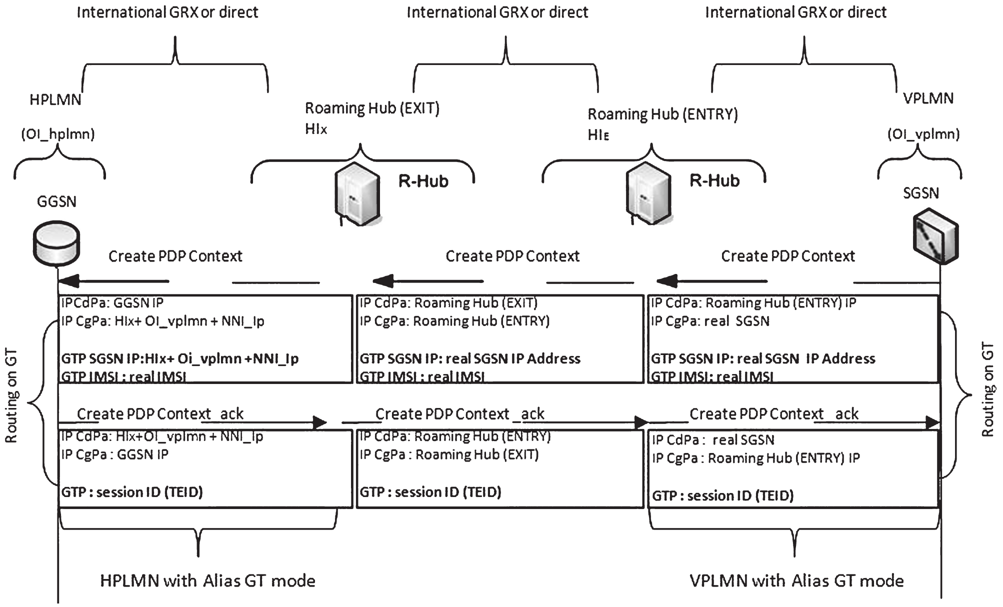


Figure 2.9 Outgoing Create PDP Context

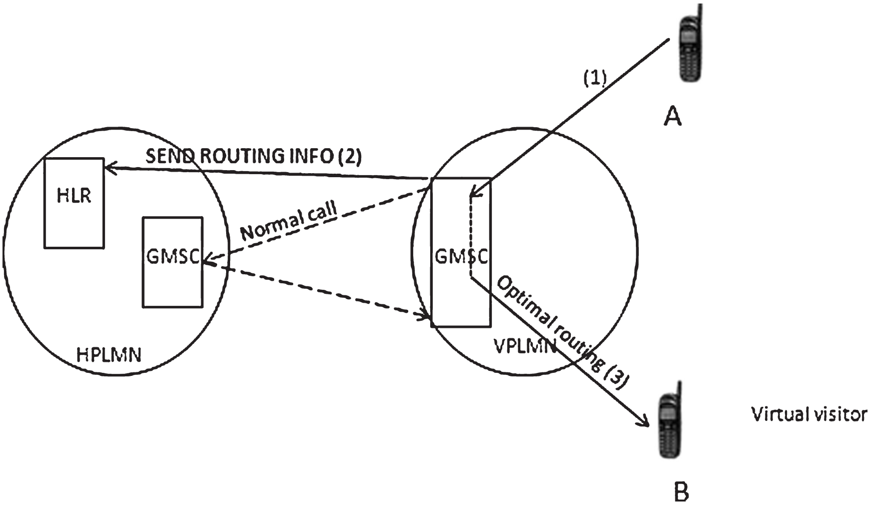


Figure 2.10 Optimal call reception routing

2.2.13 Extended Service: Optimal Call Reception Routing (MAP to the HLR)

The VPLMN may wish to attract visitors to B by offering 'Optimal Routing' [2.9], so it sets its GMSC to offer the service, shown in Figure 2.10. The visitors, called from A in the network offering the service, do not have a forward and back 'tromboning' to their HPLMN, so the charge for receiving any call could be cancelled.

To achieve this, the GMSC VPLMN must be able to make a SEND ROUTING INFO (2) to the HLR HPLMN in order to get the roaming number. If the returned VMSC is in its own network, it performs a direct local call (3).

This raises exactly the same issue or solution in the case of MNP as for the SEND ROUTING INFO FOR SM.

2.2.14 Extended Service: Optimal Routing to VMS (MAP to the GMSC)

The VPLMN may wish to attract visitors by offering Optimal Routing to the VMS in the home country.

The reception of VMS messages by B becomes much cheaper; to do this, the MSC VPLMN must be able to make a RESUME CALL HANDLING to the GMSC HPLMN with the forwarded number = VMS. The 'tromboning' is interrupted and the call is transferred locally (4) in the HPLMN to the VMS, as shown in Figure 2.11.

2.2.15 Extended Service SMSeXchange: Visitor Receiving SMS-MT from All the VPLMN Subscribers

The virtual visitor expects to receive the SMSs sent by the subscribers of the VPLMN that the visitor has chosen. These SMSs will come from the SMSC of the VPLMN: there are no interworking issues for the MAP FORWARD-SM-MT as the destination MSC is the VPLMN where the virtual visitor is currently. The SEND ROUTING INFO FOR SM must be able to interrogate the HLR of the VLMN with MNP (Mobile Portability problem). This MNP will be covered in detail in Chapter 4.

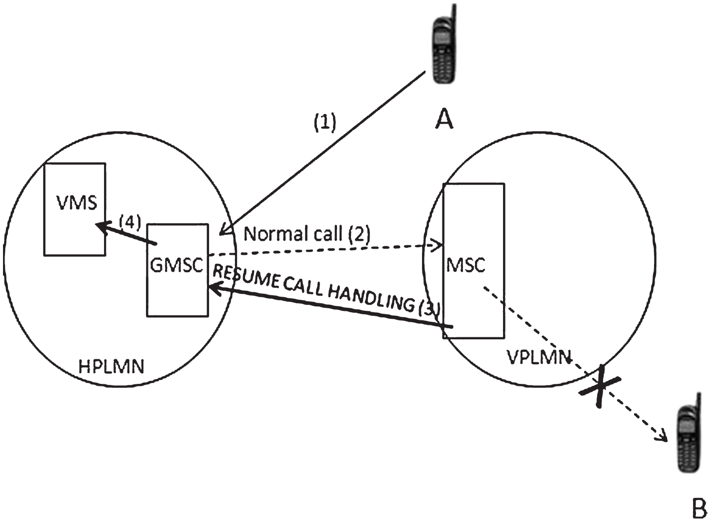


Figure 2.11 Optimal routing to VMS

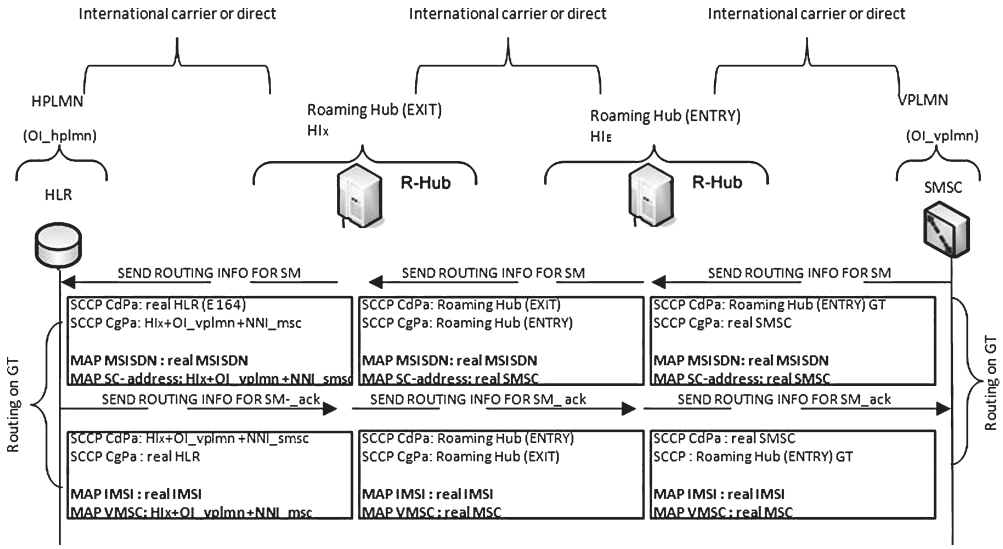

International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
HLR
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
SMSC
SEND ROUTING INFO FOR SM
SEND ROUTING INFO FOR SM
SEND ROUTING INFO FOR SM
SCCP CdPa: real HLR (E 164)
SCCP CgPa: HIx+OI_vplmn+NNI_msc
MAP MSISDN : real MSISDN
MAP SC- address: HIx+OI_vplmn+NNI_smsc
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)
MAP MSISDN: real MSISDN
MAP SC-address: real SMSC
SCCP CdPa: Roaming Hub (ENTRY) GT
SCCP CgPa: real SMSC
MAP MSISDN: real MSISDN
MAP SC-address: real SMSC
SEND ROUTING INFO FOR SM-_ack
SEND ROUTING INFO FOR SM_ ack
SEND ROUTING INFO FOR SM_ack
SCCP CdPa: HIx+OI_vplmn +NNI_smsc
SCCP CgPa : real HLR
MAP IMSI : real IMSI
MAP VMSC: HIx+OI_vplmn+NNI_msc
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa: Roaming Hub (EXIT)
MAP IMSI : real IMSI
MAP VMSC : real MSC
SCCP CdPa : real SMSC
SCCP : Roaming Hub (ENTRY) GT
MAP IMSI : real IMSI
MAP VMSC : real MSC
Routing on GT
Routing on GT

Figure 2.12 Extended service SMSeXchange

For MNP, the Roaming Hub must provide the search procedure described in Chapter 4: the MSISDN does not allow the address of the HLR to be found directly if two HPLMNs from the same country have MNP, (such as all western Europe), unless a simple Roaming Hub (ENTRY) has a relation with all the networks of an MNP country that are clients of the service. If the HPLMN does not have MNP, this service is immediately provided.

The details of this service are shown in Figure 2.12.

2.2.16 *Extended Service: Allowing the VPLMN to ‘Push’ USSD to the Virtual Visitors*

One can also think of allowing the USSD platform of the VPLMN to ‘push’ USSD messages to the visitors (a questionnaire: are you happy with our network?).

Provided that the SMSeXchange service is opened, it is the same as sending SMS-MT to the visitors, except that in the HPLMN, the SCCP CgPa will be: HI_X + OI_vplmn + NNI_ussd in the SEND-ROUTING-INFO-FOR-SM, which allows the VPLMN to know the visited MSC. The USSD platform of the VPLMN will then send an UNSTRUCTURED SS REQUEST (or NOTIFY) to the visitor.

2.2.17 *Extended Service: Providing the Control of Stolen Handsets in the VPLMN*

The MAP CHECK_IMEI is used (the IMEI is a unique identifier for each handset). See Chapter 9 where the procedure to transmit the CHECK_IMEI to the EIR in the HPLMN is detailed.

2.2.18 *Outgoing Call, SMS or GPRS for Prepaid Visitors (CAMEL to the SCP)*

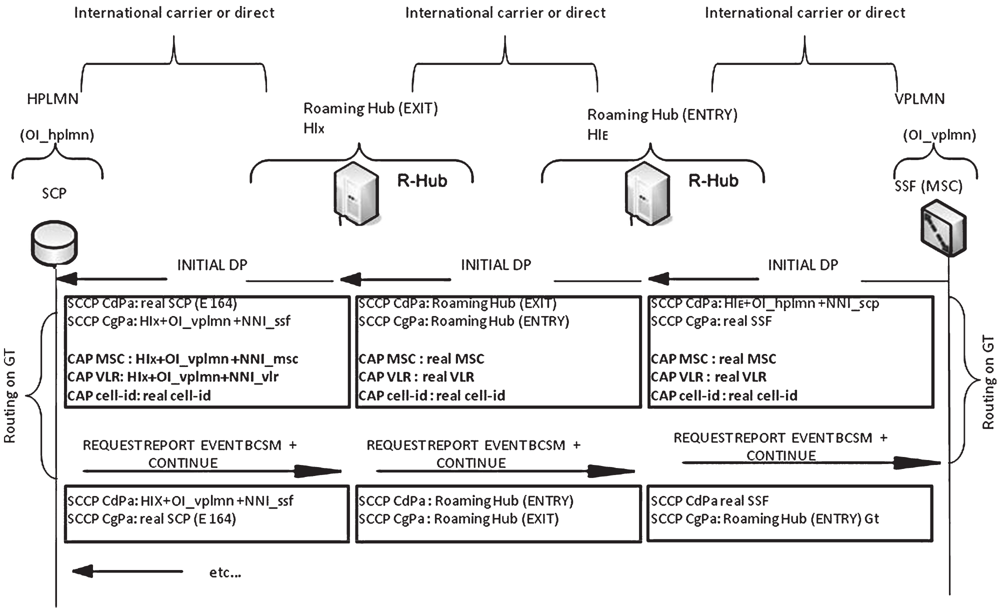
A visitor may be registered as prepaid. Whenever they make a call, a CAMEL message INITIAL DP is sent from the VPLMN to their home SCP. There can be many SCPs and the INITIAL DP must be sent to the right one.

For a post-paid subscriber, an outgoing call by a virtual visitor does not use the Roaming HUB.

In the UPDATE LOCATION PROCEDURE, the Roaming Hub must memorize the GT of the real SCP and sets it up from the IMSI whenever it receives the IDP from the VPLMN.

The MAP parameter identifying a particular subscriber for the SCP is the Calling Party Number but the IMSI is also included.

Details of the process are shown in Figure 2.13.


International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
SCP
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
SSF (MSC)
INITIAL DP
INITIAL DP
INITIAL DP
Routing on GT
Routing on GT
REQUEST REPORT EVENT BCSM + CONTINUE
REQUEST REPORT EVENT BCSM + CONTINUE
REQUEST REPORT EVENT BCSM + CONTINUE
etc...

SCCP CdPa: real SCP (E 164)
SCCP CgPa: HIx+OI_vplmn +NNI_ssf

CAP MSC : HIx+OI_vplmn+NNI_msc
CAP VLR: HIx+OI_vplmn+NNI_vlr
CAP cell-id: real cell-id

SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa: Roaming Hub (ENTRY)

CAP MSC : real MSC
CAP VLR : real VLR
CAP cell-id : real cell-id

SCCP CdPa: HIE+OI_hplmn +NNI_scp
SCCP CgPa: real SSF

CAP MSC : real MSC
CAP VLR : real VLR
CAP cell-id : real cell-id

SCCP CdPa: HIX+OI_vplmn +NNI_ssf
SCCP CgPa: real SCP (E 164)

SCCP CdPa : Roaming Hub (ENTRY)
SCCP CgPa : Roaming Hub (EXIT)

SCCP CdPa real SSF
SCCP CgPa: Roaming Hub (ENTRY) Gt

Figure 2.13 Outgoing call, SMS or GPRS for prepaid visitors

The GT of the SCP: HI$_X$ + OI_hplmn + NNI_scp is left as it is because this address (belongs to Roaming Hub (ENTRY)) has roaming with the VPLMN.

In the Roaming Hub (EXIT), the correct SCP GT is set in SCCP CdPa, using the table built from the INSERT SUBSCRIBER DATA which was received in the UPDATE LOCATION registration procedure.

Note that the cell-id is transparently relayed without transformation.

For SMS and GPRS charging it is the same: INITIAL DP sms, INITIAL DP gprs, CONTINUE sms, CONTINUE gprs, etc. belong to the 'CAMEL Phase 3' set of CAMEL services.

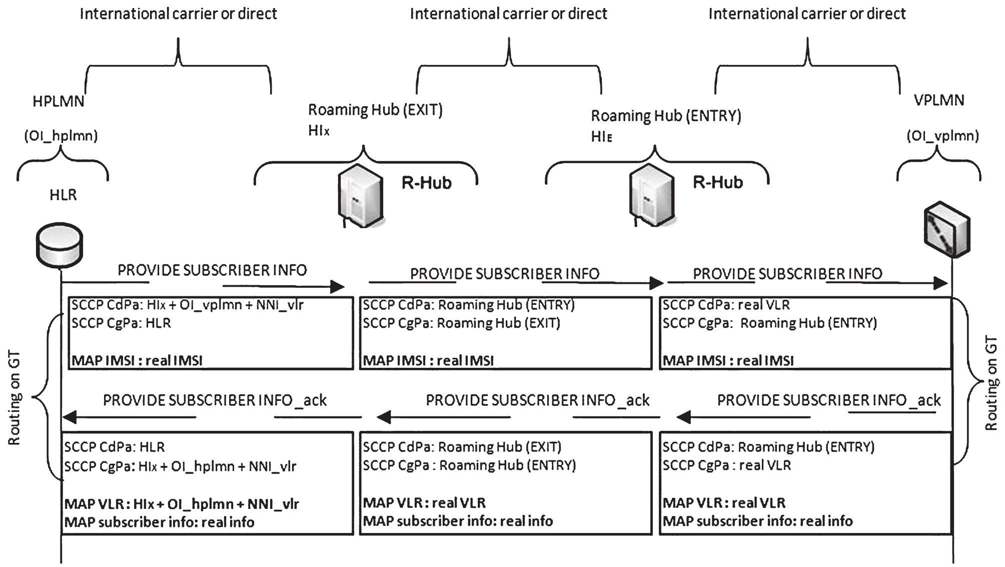
2.2.19 Reception of Calls while Roaming for a Prepaid Subscriber

For charging purposes for a prepaid subscriber, the GMSC of the HPLMN that receives the call should have the VLR GT as well as some subscriber information. The GMSC interrogates the HLR with a SEND ROUTING INFO. The HLR sends a PROVIDE ROAMING NUMBER as above, then, for a prepaid subscriber, sends a PROVIDE SUBSCRIBER INFO. The result is returned by the HLR to the GMSC, which will trigger, if the subscriber is prepaid, an INITIAL DP to the SCF which includes these results. This procedure is shown in Figure 2.14.

2.3 Restriction of Virtual Roaming by the Roaming Hub

Virtual roaming between a HPLMN and VPLMN may be restricted pair-wise for:

- GPRS roaming (bar UPDATE LOCATION GPRS);
- CAMEL roaming (no prepaid roamer from HPLMN allowed in the VPLMN);
- SMS interworking (VPLMN subscribers cannot send SMS to HPLMN visitors).



International carrier or direct
International carrier or direct
International carrier or direct
HPLMN
(OI_hplmn)
HLR
Roaming Hub (EXIT)
HIx
R-Hub
Roaming Hub (ENTRY)
HIE
R-Hub
VPLMN
(OI_vplmn)
PROVIDE SUBSCRIBER INFO
PROVIDE SUBSCRIBER INFO
PROVIDE SUBSCRIBER INFO
SCCP CdPa: HIx + OI_vplmn + NNI_vlr
SCCP CgPa: HLR
MAP IMSI : real IMSI
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa: Roaming Hub (EXIT)
MAP IMSI : real IMSI
SCCP CdPa: real VLR
SCCP CgPa: Roaming Hub (ENTRY)
MAP IMSI : real IMSI
PROVIDE SUBSCRIBER INFO_ack
PROVIDE SUBSCRIBER INFO_ack
PROVIDE SUBSCRIBER INFO_ack
SCCP CdPa: HLR
SCCP CgPa: HIx + OI_hplmn + NNI_vlr
MAP VLR: HIx + OI_hplmn + NNI_vlr
MAP subscriber info: real info
SCCP CdPa: Roaming Hub (EXIT)
SCCP CgPa : Roaming Hub (ENTRY)
MAP VLR: real VLR
MAP subscriber info: real info
SCCP CdPa: Roaming Hub (ENTRY)
SCCP CgPa : real VLR
MAP VLR: real VLR
MAP subscriber info: real info
Routing on GT
Routing on GT

Figure 2.14 Reception of calls while roaming for a prepaid subscriber

2.3.1 GPRS Barring

The GPRS barring function is straightforward: the Roaming Hub analyses the operation UPDATE LOCATION GPRS, recognizes an IMSI of the HPLMN and makes an immediate Ack to the VPLMN with a refuse reason, while the UPDATE LOCATION GPRS is not even transmitted to the HPLMN (local barring).

2.3.2 SMS Interworking Barring

The SMS interworking barring is more complex: one needs to bar the SEND ROUTING INFO FOR SM *request* sent by the VPLMN SMSC to the HLRs of the HPLMN. It is not so simple if the HPLMN belongs to a country with Mobile Number Portability implemented because the MSISDN belonging to the HPLMN range of numbers cannot be used as a criterion. So it is the response SEND ROUTING INFO FOR SM *confirmation* (Ack) from the HPLMN which must be modified to indicate barring.

2.3.3 CAMEL Roamers Barring

This is quite complicated, as one must let the post-paid customers roam and the 'prepaid' roamers can only be recognized from the VLR CAMEL Subscription information received in the UPDATE LOCATION procedure. Figure 2.15 shows one of the correct methods.

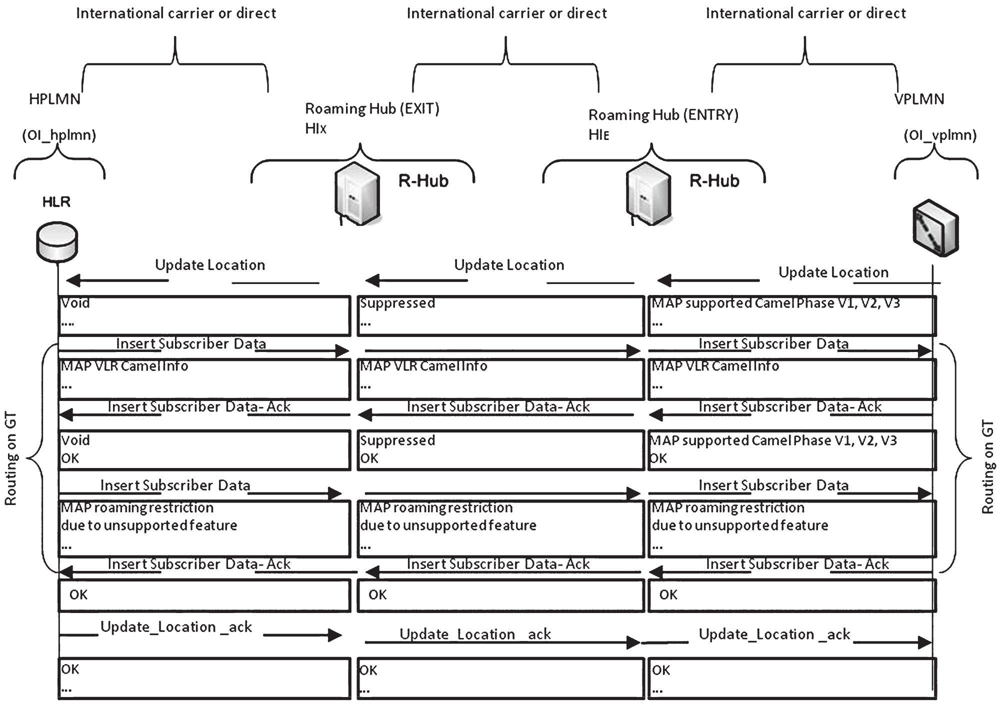


Figure 2.15 MAP CAMEL subscription information method

The UPDATE LOCATION procedure is 'successful' (no rejection in the Roaming Hub). However, a prepaid roamer is barred in the HPLMN because of the 'roaming restriction' sent by their HLR (which we want): they cannot receive calls or SMS-MT. Also, as there is a 'roaming restriction' in the VLR of the VPLMN, they cannot use their phone for anything but emergency usage.

2.4 Procedures for the Virtual Roaming Visitors' Service (Multi-IMSI)

The procedure is the same whether the subscriber uses two SIM cards or a single 'dual IMSI' SIM card with an STK (SIM Tool Kit), which is more convenient.

The normal SIM card is called the 'nominal' and the other one that the subscriber uses while roaming is called the 'auxiliary'. For an STK solution, the normal IMSI is the 'nominal' and the other, which will be used in roaming (automatically) if the 'nominal' does not have the roaming agreement, is called the 'auxiliary IMSI'.

There is a particular setup for the sending of this SMS-MO.

The SMSC GT in the SIM auxiliary or the IMSI auxiliary file for SMSC is the 'Roaming Hub' GT, *not* the SMSC of the 'auxiliary' mobile network.

With regard to the MSISDN which will be returned to the VPLMN when the UPDATE LOCATION procedure is performed using the 'auxiliary SIM' or 'auxiliary IMSI', it will always be the 'nominal MSISDN', so that outgoing calls show this number in the CLI (Calling Line Identification). This is because the Roaming Hub will redirect the UPDATE LOCATION performed by the 'auxiliary IMSI' or 'auxiliary SIM' to the 'nominal HPLMN' after replacing it with the 'nominal' IMSI.

We will not explain all the procedures of the 'inbound visitor (single-IMSI case)' again, only the main ones to show the principle of the IMSI exchange or destination SMSC exchange performed by the Roaming Hub in this 'multi-IMSI case'. We will leave the rest for the exercises at the end of the book.

2.4.1 Setup for the Roaming Hub in the 'Auxiliary Mobile Network'

The Roaming Hub is in the 'auxiliary network', which is the network with many roaming agreements. One piece of equipment can provide the service for several 'nominal networks'. In Chapter 5 we develop the useful case where the Roaming Hub is not 'physically' at the auxiliary network site but is in another country, with the signalling being relayed.

The IMSI's auxiliaries must be reserved, however *MSISDNs will not be assigned* (they are not used), with preferably a consecutive range of IMSIs as it simplifies the creation of the E214 'ingoing table'.

2.4.1.1 Connecting the Virtual Roaming Hub in the Auxiliary Network: E214 and E164 Incoming Route Table Creation

The Roaming Hub is like a new HLR 'proxy' only for these IMSIs; we call it a 'proxy' because it does not hold the profiles of these auxiliary IMSIs, only the real VLR and MSC that they are currently visiting in some VPLMN. The auxiliary IMSIs *are not declared at all* in the HLR auxiliary.

It is also a new MSC-VLR (the same GT as for the HLR can be used), which the 'HLR nominal' believes that its virtual outbound subscribers are visiting.

As any HLR is addressed for most MAP services with its E214 address (CC + MGT + Serial Number of the IMSI), the GMSC of the auxiliary network will configure the 'incoming table E214' so that the Roaming Hub receives the MAP messages addressed to its HLR function for all the 'auxiliary IMSIs'. Also, the E164 'incoming table' pointing to the 'HLR + MSC-VLR' Roaming Hub must be created.

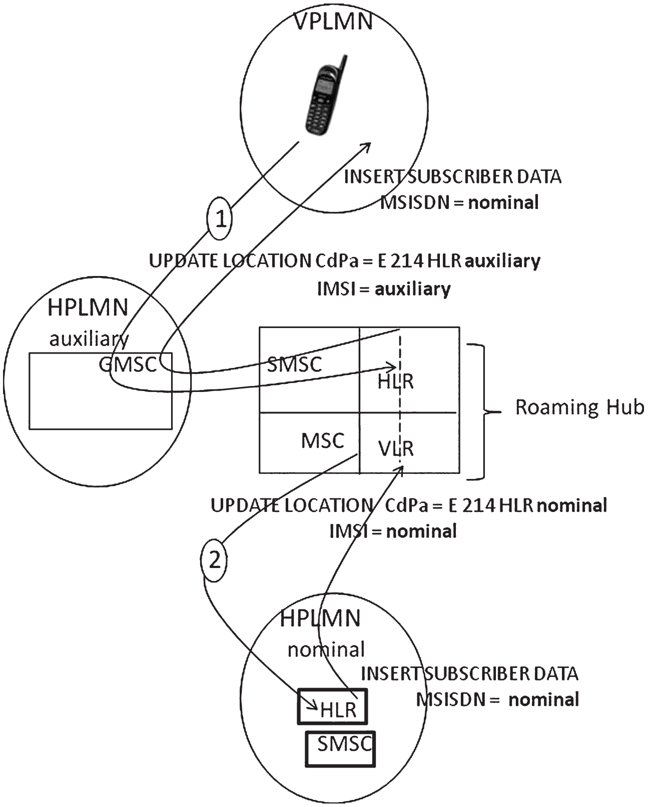


Figure 2.16 Architecture of the multi-IMSI Roaming Hub: UPDATE LOCATION

When the IMSI auxiliary is active, the UPDATE LOCATION is sent (1) to a HLR of a HPLMN auxiliary. The setup sends it (2) to the Roaming Hub. It replaces the IMSI auxiliary by the IMSI nominal, and the VMSC-VLR GT belonging to the VPLMN by the Roaming Hub GT, and sends to the HLR nominal. The profile in the INSERT SUBSCRIBER DATA is routed back through the Roaming Hub but the MSISN = nominal (although the original IMSI = auxiliary!).

2.4.1.2 Manufacturing the Dual IMSI Cards (if the STK Solution is Used)

Pairs of IMSI auxiliary and IMSI nominal (the main one) must be given to the card manufacturer, as well as the SMSC = SMSC nominal for the IMSI nominal file (when it can be used), but with SMSC auxiliary = Roaming Hub for the IMSI auxiliary file. It should be specified that these last two fields are ‘OTAble’ as is the SIM Tool Kit so that changes are possible.

2.4.2 Setup in the Roaming Hub of the Correspondence ‘Auxiliary IMSI → Nominal IMSI’

For each virtual outbound subscriber of the nominal network, the correspondence of their IMSI nominal with the IMSI auxiliary must be created in the Roaming Hub at the auxiliary network site. The setting of the nominal SMSC GT (because it is set in the SMS-MO procedure) is done once for the nominal network.

2.4.3 The SEND AUTHENTICATION Procedure

The procedure verifies, before the UPDATE LOCATION, that the subscriber is the real owner of the IMSI. A handshake procedure called 'A3' is used: the HLR and the SIM card execute a common algorithm with their common Ki key to compute the result of the same random number and the results are compared.

The important detail is that although the IMSI auxiliary is sent by the SIM card (1), the A3 check is done with the Ki of the nominal IMSI (2) which has been replaced by the Roaming Hub. This procedure is shown in Figure 2.17.

The set of parameters is different for 2G and 3G subscribers and there is an older version of this MAP service, SEND PARAMETERS, which is still sometimes used when a roaming connection is tested for the first time.

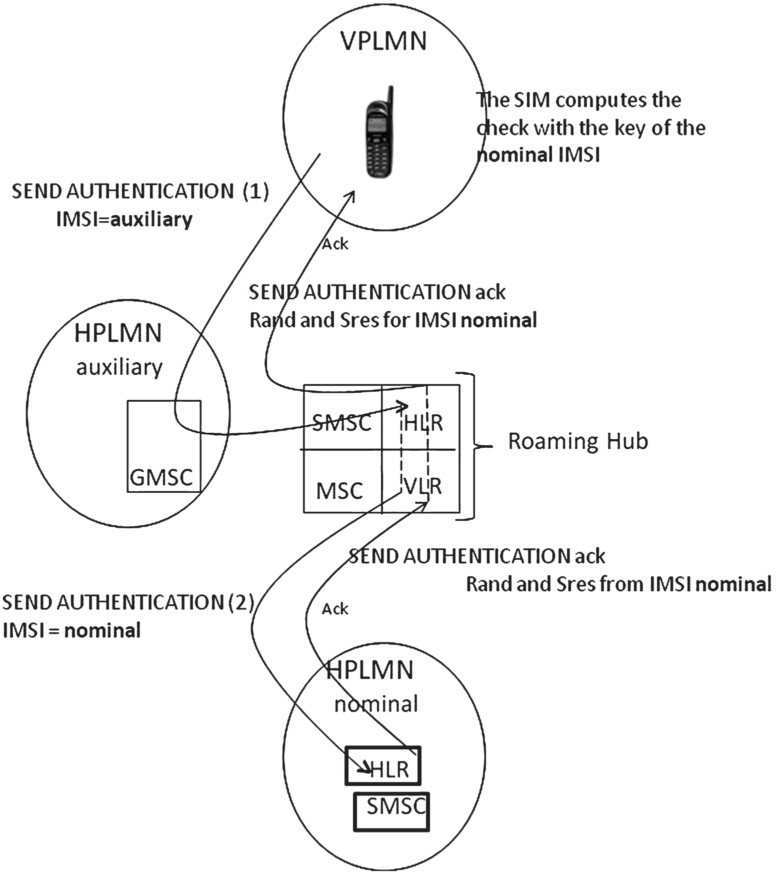


Figure 2.17 SEND AUTHENTICATION multi-IMSI procedure

2.4.3.1 Difference between 2G and 3G

The authentication and ciphering algorithm, COMP128, used (example SRAND → SRES) in GSM was weak as the real key length, 128, had 'unused parts'. There is a better algorithm, COMP128-2, in UMTS. There are also additional parameters in the authentication vector returned by the HLR.

Additional specific services exist in the INSERT SUBSCRIBER DATA containing the profile sent by the HLR to the VLR, but in the Roaming Hub they will be transparently handled as it does not need additional features.

2.4.3.2 Segmented TCAP Dialogues

In 3G, the authentication vector may be very long and the requesting VLR may have a dialogue in several segments, until the dialogue is closed.

2.4.4 The UPDATE LOCATION Registration Procedure (MAP Sent to the HLR Nominal)

As seen in Figure 2.16, the MSISDN nominal is returned transparently from the HLR to the VPLMN, in the INSERT SUBSCRIBER DATA. But the Roaming Hub uses the internal table to change the IMSI:

IMSI auxiliary → IMSI nominal

while the rest is the same (in particular for prepaid outbound subscribers as in the virtual visitor case).

2.4.5 Reception of Calls while Roaming (MAP Sent to the VLR)

The call arrives at the GMSC of the HLMN nominal, which will proceed as in the case of virtual visitors. The PROVIDE ROAMING NUMBER is sent to the 'VLR' = Roaming Hub which will change:

IMSI nominal → IMSI auxiliary

and will, acting as the HLR, interrogate the real VLR to obtain the real Roaming Number in the HPLMN. The ISUP call will then go directly from the HPLMN nominal to the real VLR.

2.4.6 Outgoing SMS-MO (MAP to the SMSC): Generalization of SMSeXchange

This is explained in [2.1] and also by Figure 2.18. It is the most complicated call flow of those in this book, although there is no other way as we want:

- the SMS sent to show Origin Address = MSISDN nominal;
- while having the additional destinations provided by the roaming agreements of the auxiliary network.

The exercise at the end of the book will help. The Service Centre to which the SMS-MO (1) is sent = *the Roaming Hub GT when the IMSI auxiliary is active*. It is *not the Service Centre nominal* (it would not reach it because VPLMN is assumed not to have roaming with the HPLMN nominal. It is *not the Service Centre of the auxiliary HPLMN*, because the Origin Address in the SMS-MO is 'nominal' and *the SMS-MO would be rejected* by this Service Centre.

2.4.6.1 No MNP in the Country of the Outbound Roaming Subscriber

The 'SMSC' in the Roaming Hub changes the Roaming Hub GT → GT of SMSC nominal, based on a table OA MSISDN nominal → SMSC GT (*because there is no MNP*), then behaves as an MSC to send the SMS-MO (2) to the SMSC nominal. The SMSC accepts it *because the Origin Address is one of its subscribers.*

However the SMSC nominal may not have many agreements. But the Roaming Hub extends the coverage; it works as an SMSeXchange for the SMSC nominal (see Figure 2.18):

- The SEND ROUTING INFO FOR SM is sent to the Roaming Hub (3).
- The Roaming Hub sends it to the destination network (4) which responds (5) giving the VMSC GT.
- Following the SMSeXchange transparency principle, this response is relayed (6) to the SMSC nominal with the real visited VMSC GT.

If the SMSC nominal does not have roaming with this GT, the setup in the HPLMN nominal will route the FORWARD SM MT to the Roaming Hub (7) then to the destination VPLMN (8).

As a result, the outbound virtual subscriber, visiting a VPLMN they do not have real roaming with, will be able to send an SMS to many other networks which their HPLMN does not have roaming with, but the HPLMN auxiliary does.

This general case involves *at least* five mobile networks: VPLMN of A, HPLMN auxiliary, with the Roaming Hub, HPLMN nominal of A, HPLMN of B, VPLMN of B, and is the most complex data flow case which exists. If the last VPLMN network of destination B charges the AA19 SMS-MT termination charge, it will be sent to the HPLMN auxiliary, which will pass it to the HPLMN nominal.

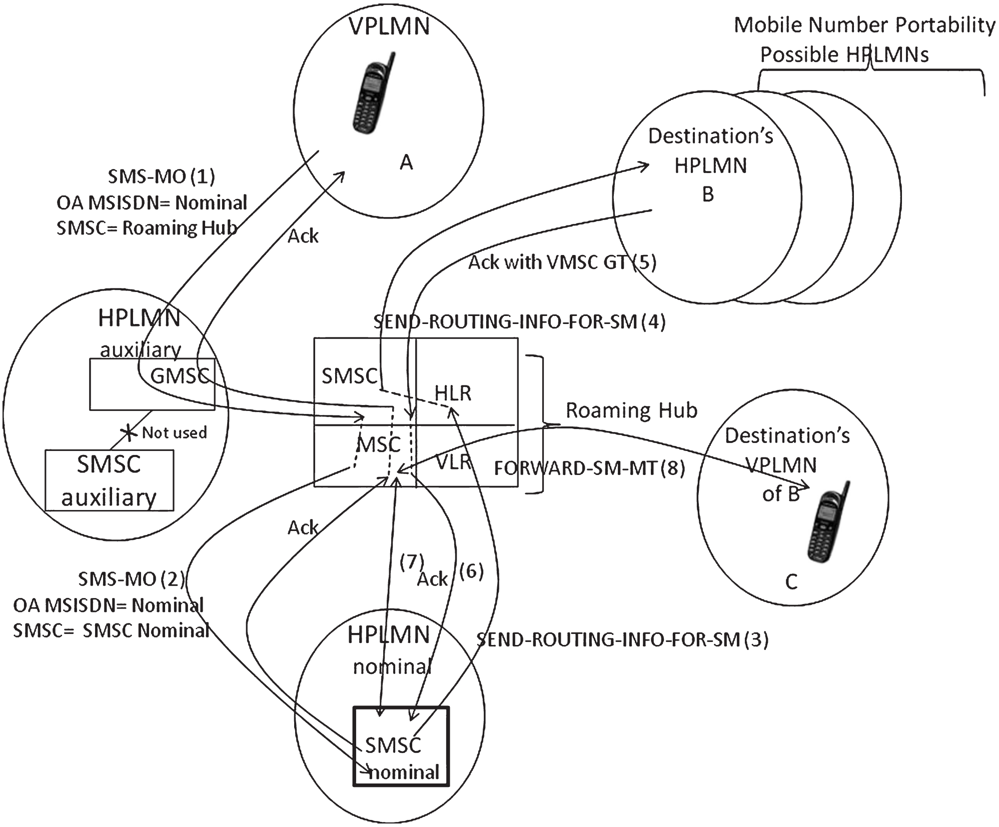


Figure 2.18 Using the SMSeXchange function for the virtual outbound subscriber's multi-IMSI

There could be more than five networks involved if, in addition:

- the Roaming Hub is ‘hosted’ (Chapter 5);
- the destination HPLMN B has mobile number portability and there is a network of Roaming Hubs (Chapter 4).

There are, then, *real observed cases with eight mobile networks involved* (hosted Roaming Hub case and two searches necessary to access the HPLMN B in addition to the first attempt). It would make an interesting billing question if the various MAP services involved were all charged by participants.

2.4.6.2 MNP in the Country of the Outbound Roaming Subscriber: Mandatory ‘Address Resolution’ by the Roaming Hub

In fact, it is even more complicated because of the (eventual) Mobile Number Portability in the country of the HPLMN nominal. MAP V3 for the FORWARD SM MO (1) has a parameter which is the IMSI, but unfortunately few networks implement it and if there are several HPLMN customers of the same Roaming Hub, *one could not know which SMSC GT to set*. The only solution is that the Roaming Hub will determine which HPLMN the OA belongs to, by interrogating (2) the HLRs of the concerned country and getting the IMSI of the OA, which allows the right SMSC GT to be found. This is shown in Figure 2.19.

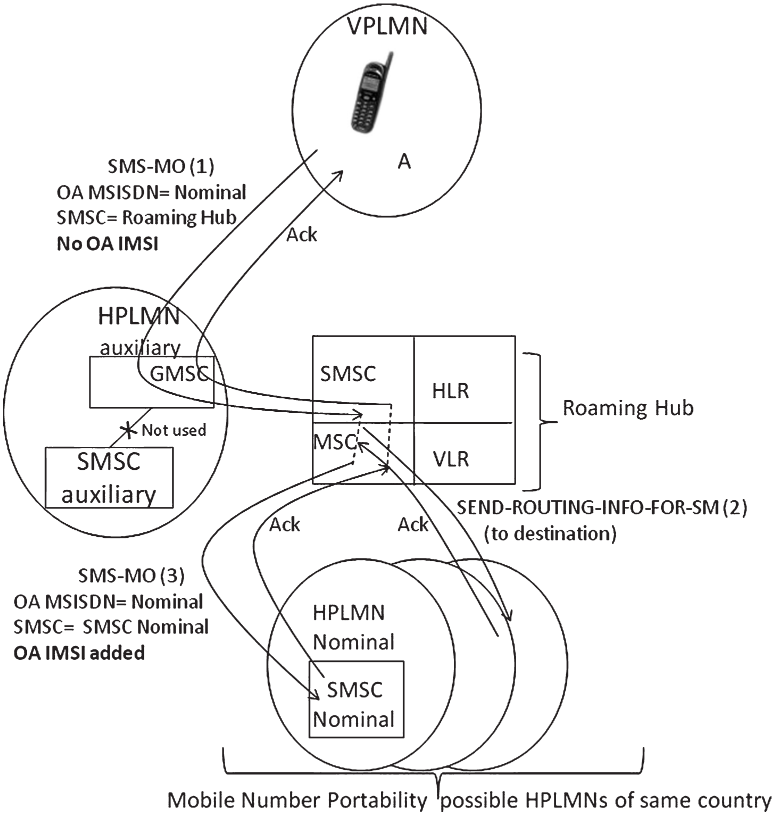


Figure 2.19 Necessary address resolution of the sender in an SMS-MO multi-IMSI

To be rigorous, the Roaming Hub will add the IMSI of OA in the FORWARD SM MO V3 (3) that it sends to the chosen SMSC. All this together makes this outgoing SMS-MO for multi-IMSI subscribers the most complicated.

Note that by interrogating the HLR, the VMSC returned should be the Roaming Hub GT, and the Roaming Hub can find the real VMSC from a table. If the Calling Party GT is different, this shows an SMS fraud: systems connected to the SS7 network sending SMS-MO to an SMSC with a faked OA which belongs to it. So, as a by-product, the Roaming Hub provides protection.

As in the MAP implementation of the HPLMN nominal, there could be more networks and more senders involved: those corresponding to the range, and those corresponding to the network A belongs to. There could, then, be more than 10 networks in total involved in the SMS-MO + SMS-MT procedure if there is MNP for the sender and for the destination.

2.4.7 Reception of SMS-MT while Roaming (MAP Sent to MSC)

Does the multi-IMSI virtual roamer receive SMS-MT from networks which their nominal network does not have roaming with? *No, in general*, unless the sending network has opened all the SCCP routes as many European operators do for the sending of SMS. But this virtual roamer will be able to keep receiving SMS-MT from all the roaming partners of their nominal network. It may appear abnormal as, on the other hand, the reception of calls, from any network, works.

It is because the sending SMSC interrogates the HLR with the nominal MSISDN, so if the SCCP route is not opened with the nominal network, it cannot work. *In particular, a virtual visitor multi-IMSI is not able (in general) to receive SMS-MT from subscribers of the VPLMN they are currently using.*

2.5 IS 41 ↔ MAP GSM Inter-standard Roaming Hubs

About 18 % of the world’s mobile users use systems based on the IS 41 standard (CDMA, TDMA), mostly in the USA and Korea, and usage is growing in Africa and Asia as a cheaper alternative to GSM. The main drawback is the impossibility of roaming in GSM-covered countries.

A well-known solution is to borrow a GSM phone that has many roaming agreements and to have a Roaming Hub which makes the protocol conversion (see Figure 2.20). This type of solution has existed since about 2000, before the GSM world got interested in Virtual Roaming, and was extended [2.2] to Optimal Routing to VMS as explained in Chapter 7. IS 41 to GSM roaming was specified in J-STD-038 but it does not cover the forwarding of received calls in a GSM network to the VMS (in the IS 41 network). This is because IS 41 does not provide an automatic ‘Forward-to-number’ in the VLR customer’s profile, but relies on an IS 41 Redirect request (the equivalent of a MAP RESUME CALL HANDLING) to transfer the call to the VMS.

2.5.1 Initial Registration Procedure GSM Network → IS 41

IS 41 and GSM are very different protocols and Figure 2.21 shows the transformation done by an ‘Inter-standard’ Roaming Hub for MAP. The functions of each protocol message are different and they also have a very different method of coding (IS 41 does not use ASN1 coding).

Table 2.1 shows the approximate correspondence for the main services involved in roaming.

2.5.2 Reception of Calls while Roaming (IS 41 Virtual Visitor) and VMS Forwarding

Figure 2.22 shows the reception of calls (IS 41 virtual visitor) with an inter-standard Roaming Hub.

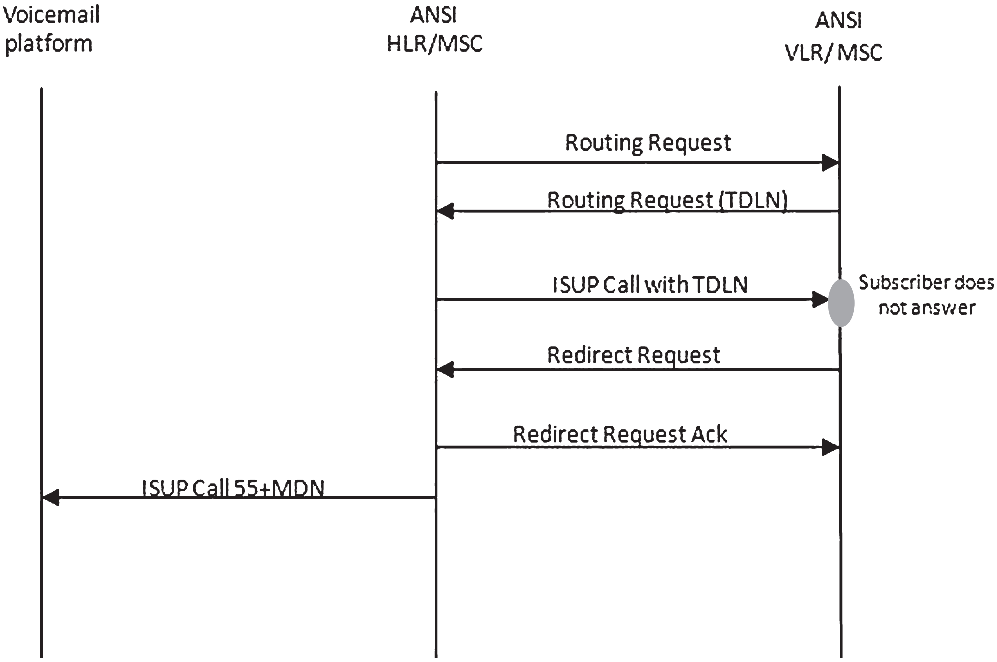


Figure 2.20 Standard Call Forward to Voicemail in IS 41

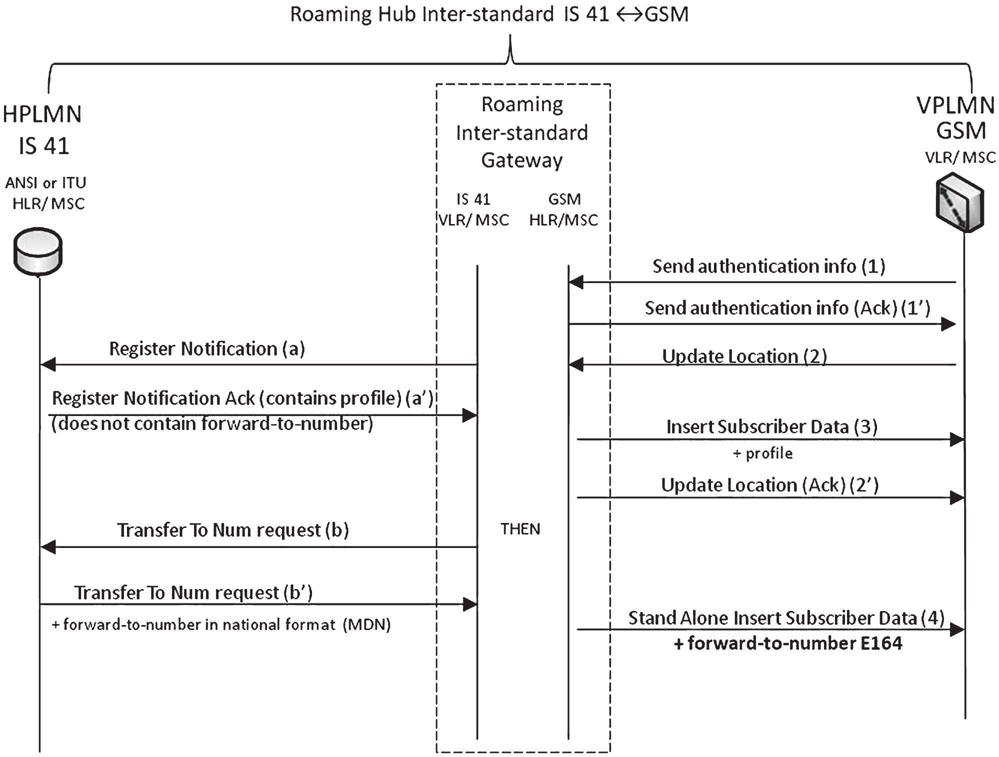

Roaming Hub Inter-standard IS 41 ↔GSM
HPLMN IS 41
ANSI or ITU HLR/MSC
Roaming Inter-standard Gateway
IS 41 VLR/MSC
GSM HLR/MSC
VPLMN GSM
VLR/MSC
Send authentication info (1)
Send authentication info (Ack) (1′)
Register Notification (a)
Update Location (2)
Register Notification Ack (contains profile) (a′)
(does not contain forward-to-number)
Insert Subscriber Data (3)
+ profile
Update Location (Ack) (2′)
Transfer To Num request (b)
THEN
Transfer To Num request (b′)
+ forward-to-number in national format (MDN)
Stand Alone Insert Subscriber Data (4)
+ forward-to-number E164

Figure 2.21 Inter-standard IS 41 ↔ MAP GSM Roaming Hub

Table 2.1 Correspondence between GSM MAP and IS 41 protocol

GSM MAP	IS 41
REGISTER NOTIFICATION request	UPDATE LOCATION request
REGISTER NOTIFICATION (with profile) Ack	INSERT SUBSCRIBER DATA indication + UPDATE LOCATION Ack
REGISTRATION CANCELLATION request	CANCEL LOCATION request
TRANSFER TO NUMBER request	OUTGOING SUPPL. SERVICES request (call forwarding)
TRANSFER TO NUMBER Ack	OUTGOING SUPPL. SERVICES Ack
ROUTING REQUEST request	PROVIDE ROAMING NUMBER request
ROUTING REQUEST Ack (with TLDN)	PROVIDE ROAMING NUMBER Ack (with MSRN)
REDIRECT REQUEST	RESUME CALL HANDLING
SMS REQUEST	SEND ROUTING INFO FOR SM
SMS DELIVERY POINT TO POINT	FORWARD SHORT MESSAGE
SMS NOTIFICATION	ALERT SERVICE CENTRE

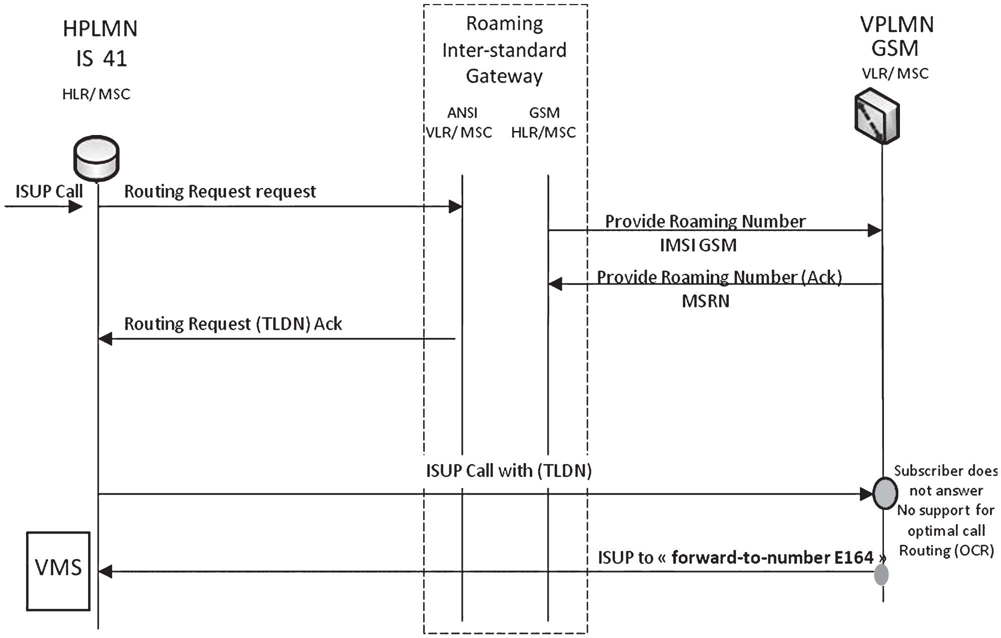


Figure 2.22 Reception of calls (IS 41 virtual visitor) with an inter-standard Roaming Hub

2.6 Various MAP and CAMEL Transformation Methods

As seen in the previous examples, the SCCP addresses and the GT in the MAP parameters are modified. Some SCCP address recoveries can be obtained from the unmodified MAP parameters (such as IMSI); other SCCP recoveries need to use a table.

Table 2.2 MAP parameters used to derive the SCCP Called Party Address

Service Name	SCCP Called Party Address to HPLMN	SCCP Called Party Address to MSC or VLR
MAP UPDATE LOCATION	HLR: E214 computed from IMSI	–
MAP READY FOR SM	HLR: E214 computed from IMSI	–
MAP PURGE MS	HLR: E214 computed from IMSI, but VLR or SGSN GT must be carried ‘translated’	–
MAP SMS-MO	SMSC: E164 from sm-rp-da	–
MAP PROVIDE ROAMING NUMBER	HLR: E214 computed from IMSI	VLR: E164 from MSC number
MAP SEND ROUTING INFO FOR SM	HLR: E164 searched with the MSISDN in the case of MNP (Chapter 4)	–
MAP SEND ROUTING INFO	HLR: E164 searched with the MSISDN in the case of MNP (Chapter 4)	–

2.6.1 Called SCCP Address from Transparent MAP Parameters

In this case there is no need to perform a translation of the MAP parameters as in the next section. This is shown in Table 2.2.

2.6.2 MAP and SCCP Translations from Tables

There are various methods used, which are called ‘Alias GT mode 0 to 5’, such that a ‘Roaming Hub’ equivalent GT is translated to the Real GT. There is a limit in MAP and CAMEL of 16 digits for any GT (15 according to the GSM standard, but most systems accept 16). But for SCCP, the addresses with most systems can go to 22 or more.

It must be possible for a HPLMN to trace the GT visited by its subscribers, so the HI + OI + NNI system was designed: the real GT is translated and the result will then be no longer than 15 digits in such a case.

HI	6 digits
OI_vplmn	5 digits
NNI	4 digits (necessary for the China networks!)

These are the various possible setups for the parameters:

Roaming Hub (ENTRY) GT
HI + OI_hplmn + NNI_scp
HI + OI_hplmn + NNI_hlr
HI + OI_vplmn + NNI_msc
HI + OI_vplmn + NNI_vlr
HI + OI_vplmn + NNI_ssf (prepaid visitors)
HI + OI_vplmn + NNI_sgsn (data services for the visitors)
HI + OI_vplmn + NNI_ip (the IP address of an SGSN: data services for the visitors)

and for extended services:

Table 2.3 Different connection methods for a Roaming Hub

	0 (dynamic) also called 'Network Extension'	1(no table)	2 (static) (GSM association)	3(dynamic)	4(no table) (same as real roaming) HPLMN adjacent to Roaming Hub	5(no table) (*almost* same as real roaming) HPLMN NOT adjacent to Roaming Hub
SCCP Cdga	Roaming Hub(EXIT)	HI + Real GT	HI + OI-vplmn-NNI_xxx	HI + empty	Real GT	HI + empty
MAP MSC Number	Roaming Hub(EXIT)	HI + Real GT	HI + OI-vplmn-NNI_msc	HI + empty	Real GT	Real GT
MAP VLR Number	Roaming Hub(EXIT)	HI + Real GT	HI + OI-vplmn-NNI_vlr	HI + empty	Real GT	Real GT
MAP HLR Number	Roaming Hub(ENTRY)	HI + Real GT	HI + OI-hplmn + NNI-hlr	HI + empty	Real GT	Real GT

HI + OI_vplmn + NNI_smsc (SMS from the VPLMN to the HPLMN visitors)
HI + OI_vplmn +NNI_ussd (push USSD from the VPLMN to the HPLMN visitors)
Hi + OI_hplmn +NNI_gmlc

There are two types of table, depending on the method chosen by the HPLMN:

- **Static:** this gives the real GT from the OI + NNI, and no individual dynamic table creation is necessary. But the table is updated (automatically) only when a new GT is found.
- **Dynamic:** in the UPDATE LOCATION procedure the Roaming Hub builds the table of IMSI → Real GT (VLR, SGSN or HLR) while it replaces it by its own GT.
- **No table:** the real GT is carried after the GT (HI of the roaming Hub): it needs a small GT (three or four digits) to pass a GT of up to 11 or 12 digits as MAP GT length is limited to 16 digits, when the mode = 1. However, the processing of tickets allows requests from the HPLMN to be answered on the real location of its subscribers.

Table 2.3 shows the various connection methods.

Method 4 is exactly like a real bilateral roaming setup as frequently the HPLMN will also want to have the virtual roaming service for visitors of the VPLMN which offers the same service to it. Only the financial clearing scheme is different and involves the Roaming Hub supplier as an intermediary.

2.7 Appendix of Chapter 2

2.7.1 List of MAP Services

The only MAP services concerned are between systems in different networks. MAP services between two systems in the HPLMN or the VPLMN do not transit through a Roaming Hub and are not in the list shown in Table 2.4. 'AC' means 'Application Context' as standardized in the GSM specifications.

Table 2.4 List of standard MAP services

AC Name	AC Version	Operations	Handling by a Roaming Hub and comments
locationCancellationContext	V1,V2,V3	cancelLocation	**Transparently relayed**
equipmentMngtContext	V1,V2	CheckIMEI (CHECKIMEI) **(stolen handset checking service)**	**MAP manipulation** contains IMEI: addressing is to the EIR GT E164, which is mapped to RHEntry GT of the VPLMN MNO. So EIR checking is available in the virtual visited networks if checkIMEI is available in the MNO. The RH Entry inserts the real EIR GT
imsiRetrievalContext	V2	SendIMSI **(Maintenance operation)**	**Transparently relayed** (AC not opened in general in HPLMN)
infoRetrievalContext	V2,V3	sendAuthenticationInfo	**Transparently relayed** **Note: full support of 3G**
interVlrInfoRetrievalContext	–	sendIdentification	No (not relevant to the RH function)
handoverControlContext	–	prepareHandover	No (not relevant to the RH function)
		forwardAccessSignalling	No (not relevant to the RH function)
		sendEndSignal	No (not relevant to the RH function)
		processAccessSignalling	No (not relevant to the RH function)
		prepareSubsequentHandover	No (not relevant to the RH function)
mwdMngtContext	–	readyForSM	**Transparently relayed**
msPurgingContext	V2	purgeMS	**Transparently relayed**
shortMsgAlertContext	V2	AlertServiceCentre (SMSeXchange service)	**MAP Address manipulation** useful for SMS interworking VPLMN → HPLMN VPLMN SC to be alerted changed from RHF to VPLMN (table)
resetContext	–	reset	No (not relevant to the RH function)
networkUnstructuredSsContext	V1,V2	ProcessUnstructuredSS-Request (USSDPROCESS)	**Transparently relayed**
		unstructuredSS-Request	″
		unstructuredSS-Notify	″
tracingContext	V2	activateTraceMode	″
		deactivateTraceMode	″
networkFunctionalSsContext	V1,V2	SS (register)	″
		SS (erase)	″
		SS (activate)	″
		SS (deactivate)	″
		SS (registerPassword)	″
		SS (interrogate)	″
		SS (getPassword)	″

Table 2.4 (*continued*)

AC Name	AC Version	Operations	Handling by a Roaming Hub and comments
shortMsgMO-RelayContext	V1,V2,V3	MO-forwardSM (and MT in V1,V2) (SMS)	**MAP Address manipulation** SC Address of VPLMN changed
shortMsgMT-RelayContext	V3	Mt-forwardSM (SMS)	**MAP Address manipulation** SC Address of HPLMN changed
shortMsgMT-VGCS-RelayContext	–	mt-forwardSM-VGCS	No
shortMsgGatewayContext	V1,V2,V3	SendRoutingInfoForSM **(SMSeXchange service)**	**MAP Address manipulation** in the REQ, SC Address of HPLMN changed In CNF, GT of VMSC must be changed
		ReportSM-DeliveryStatus **(SMSeXchange service)**	**MAP Address manipulation** in the REQ, SC Address of HPLMN changed
		InformServiceCentre **(SMSeXchange service)**	**Transparently relayed**
networkLocUpContext	V1,V2,V3	UpdateLocation (UL)	**MAP manipulation** The two GTs of the MSC and VLR will be changed depending on the 'Alias GT mode' used CAMEL Phase supported changed to Minimum of (VPLMN, HPLMN)
	V3	forwardCheckSs-Indication	No (not relevant to the RH function)
	V3	restoreData	**Transparently relayed**
	V1,V2,V3	insertSubscriberData	**MAP manipulation** the 'VLR CAMEL info' is extracted to get the SCF GT of this subscriber for the forwarding of IDP, IDP SMS the VLR CAMEL info or the SGSN
	V1,V2,V3	activateTraceMode	**Transparently relayed**
gprsLocationUpdateContext	V3	UpdateGprsLocation (ULGPRS)	**MAP manipulation** The GT of the SGSN and IP address will be changed, depending on the 'Alias GT mode' used CAMEL Phase supported changed to Minimum of (VPLMN, HPLMN)
	V3	insertSubscriberData	**MAP manipulation** the 'SGSN CAMEL info' is extracted to get the SCF GT of this subscriber for the forwarding of IDP GPRS
	V3	activateTraceMode	**Transparently relayed**
subscriberDataMngtContext	V1,V2,V3	insertSubscriberData	**MAP manipulation** GT of SCP modified to be RH
		deleteSubscriberData	**Transparently relayed**

(*continued overleaf*)

Table 2.4 (*continued*)

AC Name	AC Version	Operations	Handling by a Roaming Hub and comments
roamingNumberEnquiryContext	V1,V2,V3	ProvideRoamingNumber	**MAP manipulation** GT of interrogating HPLMN changed depending on the Alias GT mode (call to virtual roamer by HPLMN)
locationInfoRetrievalContext	V1,V2,V3	SendRoutingInfo **(Optimal Routing service)**	**MAP manipulation** GT of GMSC VPLMN changed
gprsNotifyContext	V3	noteMsPresentForGprs	A Roaming Hub will never be considered as the GGSN of Virtual visitors, so this MAP service is irrelevant
gprsLocationInfoRetrievalContext	V3	SendRoutingInfoForGprs **(Optimal Routing of Network activated GPRS services!)**	**MAP manipulation** (this function is not yet opened for most HLR and is used for future Network activated PDP context HPLMN → virtual roaming visitor GGSN GT of HPLMN changed GGSN IP Address changed
failureReportContext	V3	failureReport	Not implemented
callControlTransferContext	V3,V4	ResumeCallHandling **(Optimal routing service)**	**Transparently relayed**
subscriberInfoEnquiryContext	V3	provideSubscriberInfo	**MAP manipulation** In the CNF, the GT and cell must be changed
anyTimeEnquiryContext	V3	anyTimeInterrogation	**MAP manipulation** In the CNF, the GT and cell must be changed
anyTimeInfoHandlingContext	V3	anyTimeSubscriptionInterrogation	**MAP manipulation** In the CNF, the GT and cell must be changed
		anyTimeModification	No
ss-InvocationNotificationContext	V3	ss-InvocationNotification	No
groupCallControlContext	V3	prepareGroupCall	No
		processGroupCallSignalling	No
		forwardGroupCallSignalling	No
		sendGroupCallEndSignal	No
reportingContext	V3	setReportingState	No
		statusReport	No
		remoteUserFree	No
callCompletionContext	V3	registerCC-Entry	No
		eraseCC-Entry	No
istAlertingContext	V3	istAlert	No
ServiceTerminationcontext	V3	istCommand	No
locationSvcEnquiryContext	V3	ProvideSubscriberLocation **(LCS service)**	**MAP manipulation** The GTs of the authorized GMLC must have been modified in the customer profile in the UL phase and the GT of the MLC is replaced by RH GT in provideSubscriberLocation

Table 2.4 (*continued*)

AC Name	AC Version	Operations	Handling by a Roaming Hub and comments
″	V3	SubscriberLocationReport **(LCS service)**	″
locationSvcGatewayContext	V3	SendRoutingInfoForLCS	No (not relevant to the RH function)
mm-EventReportingContext	V3	Note MM-Event	No (not relevant to the RH function)
subscriberDataModificationNotificationContext	V3	noteSubscriberDataModified	No
authenticationFailureReportContext	V3	authenticationFailureReport	No
secureTransportHandlingContext	V3	secureTransportClass1	No (not relevant to the RH function)
		secureTransportClass2	No (not relevant to the RH function)
		secureTransportClass3	No (not relevant to the RH function)
		secureTransportClass4	No (not relevant to the RH function)
resourceManagementContext	V3	releaseResources	No (not relevant to the RH function)
	V4	Reset	Transparently relayed (used by the HLR to inform the VLRs and SGSNs that it has lost the registrations)
	V4	Forward Check SS Indication	Transparently relayed (used by the HLR to inform the VLR that it has lost the forwarding conditions of subscribers)

2.7.2 Additional MAP Services V1 Which Must be Supported

Table 2.5 MAPV1 services

AC Name	AC Version	Operations	Handling and comments
No (V1)	V1	Send Parameters	Old equivalent V1 of SendAuthenticationInfo. Actually sent by Orange France VLRs to some RPs HLRs. Format and Operation Code very different from SendAuthentication. **It must be implemented**
No (V1)	V1	AlertSCwithoutResult **(SMSeXchange service)**	Old equivalent V1 of AlertServiceCentre. Some old HLRs still use it. **It must be implemented**
No (V1)	V1	Begin Subscriber Activity	Used to send the IMSI associated with USSD, Supplementary Services, etc.

2.7.3 List of CAMEL Services

Table 2.6 List of CAMEL services

AC Name	Phase CS	Operations	Handling by a Roaming Hub and comments
cap-gsm-ssf-to-gsm-scf	1	**Initial DP (IDP) (SSF→ SCF)**	**CAP manipulation** The GTs of the VPLMN will be changed as well as cell info, depending on the 'Alias GT mode' used
″	1	Request Report BCSMEvent	**Transparently relayed**
″	1	Continue	″
″	1	Continue with arguments	″
″	1	Release Call	″
″	1	Cancel	
″	1	Event Report BCSM	″
″	1	Play Announcement	″
″	1	Connect To Resource	″
″	1	Establish Temporary Connection	″
″	1	Disconnect Forward Connection	″
″	1	Disconnect Forward connection with arguments	″
″	1	Connect	″
″	1	Apply Charging	″
″	1	Apply Charging Report	″
″	1	Activity Test	″
″	1	Reset Timer	″
″	4	**Initiate Call Attempt (ICA) (SCF→ SSF)**	(**calls initiated by SCF**: see Chapter 7, Section 7.2.4 for the 'Call Back' application)
″	4	Furnish Charging Information	″
″	4	Call Gap	″
″	4	Move Leg	″
″	4	Split leg	″
″	4	Disconnect leg	″
″	4	Entity Released	″
″	4	Play Tone	″
″	4	Call Information Report	″
″	4	Call Information Request	″
″	4	Send Charging Information	″

Table 2.6 (*continued*)

AC Name	Phase CS	Operations	Handling by a Roaming Hub and comments
″	4	Prompt and Collect User Information	″
–	–	–	–
Cap-gsm-scf-to-gsm-srf	1	Assist Request Instructions	Intelligent Peripheral procedure: unlikely to transit between 2 networks
″	1	Specialized Resource Report	″
–	–	–	–
cap3-sms-AC(acE = 61)	3	**Initial DP SMS (IDPsms)** **(SSF→ SCF)**	**CAP manipulation** **Forward:** The GTs of the VPLMN will be changed as well as cell info, depending on the ‘Alias GT mode’ used
″	3	Request Report SMS Event	**Transparently relayed**
″	3	Continue SMS	″
″	3	Release SMS	″
″	3	Event Report SMS	″
″	3	Connect SMS	″
″	3	Furnish Charging Information SMS	″
″	3	Reset Timer SMS	″
–	–	–	–
CAP-gprsSSF-gsmSCF-AC(acE = 50)	3	**Initial DP GPRS (IDPgprs)** **(SSF→ SCF)**	**CAP manipulation** **Forward**: The SGSN Number and SGSN Address will be changed as well as RAI, depending on the ‘Alias GT mode’ used
″	3	Request Report GPRS Event	**Transparently relayed**
″	3	Continue GPRS	″
″	3	Release GPRS	″
″	3	Event Report GPRS	″
″	3	Connect GPRS	″
″	3	Apply Charging GPRS	″
″	3	Apply Charging Report GPRS	″
″	3	Cancel GPRS	″
″	3	Activity Test GPRS	″
″	3	Furnish Charging Information GPRS	″
″	3	Reset Timer GPRS	″
″	3	Send Charging Information GPRS	″
″	3	Entity Released GPRS	″

2.7.4 List of GTP Services

If the Roaming Hub offers the Internet data connection service, it will use the services of the GTP protocol shown in Table 2.7.

Table 2.7 List of GTP services

Direction	GTP version	Operations	Handling by a Roaming Hub and comments
SGSN → GGSN	0	**Create PDP Context**	**IP manipulation** The IP address of the originating SGSN will be changed to the IP of the RH
SGSN → GGSN	0	**Update PDP Context**	**IP manipulation** The IP address of the originating SGSN will be changed to the IP of the RH
SGSN → GGSN	0	**Delete PDP Context**	**IP manipulation** The IP address of the originating SGSN will be changed to the IP of the RH
GGSN → SGSN	0	**PDU Notification Request**	**IP manipulation** The IP address of the originating GGSN will be changed to the IP of the RH
SGSN → GGSN	0	**PDU Notification Reject Request**	**IP manipulation** The IP address of the originating SGSN will be changed to the IP of the RH

References and Further Reading

Virtual Roaming Architectures

[2.1] Henry-Labordère, A., ‘Système de mobiles à deux cartes SIM’, Patent FR 07 52 559 European patent application.

[2.2] Singh, Lokdeep, ‘Method and system for optimal call routing in GSM foreign mode for CDMA to GSM roaming’, US patent application.

Latest GSM Protocol Standards used Currently in Roaming Hub Technology

[2.3] ETSI TS 129 002 v8.8.1 (2009-02), ‘Digital cellular telecommunications systems (Phase 2+)’, Universal Mobile Telecommunications System (UMTS); LTE; Mobile Application Part (**MAP**) specification (3GPP TS 29.002 version 8.8.1 **Release 8**).

[2.4] ETSI TS 129 078 v7.4.0 (2007-10), ‘Digital cellular telecommunications systems (Phase 2+)’, Universal Mobile Telecommunications System (UMTS); Customized Applications for Mobile Enhancement Logic (**CAMEL**) Phase X (3GPP TS 29.078 version 7.4.0 **Release 7**).

[2.5] ETSI TS 129 060 v8.8.0 (2009-06), ‘GPRS Tunnelling Protocol (**GTP**) across the Gn and Gp interface’, (3GPP TS 29.060 version 8.8.0 **Release 8**).

IS 41 Protocol Standards

[2.6] TIA/EIA SP-3558, ‘Cellular Radiotelecommunications intersystem operation’, Chapters 1 to 5 (5 gives the specification of the MAP IS 41 services).

Common Protocol Layers GSM-IS 41

[2.7] ITU-T Recommendations Q771, Q772, Q773, Q774, Q775 (**TCAP**).

[2.8] ITU-T Recommendations Q711, Q712, Q713, Q714 (**SCCP**).

Service Architectures

[2.9] ETSI TS 123 079 v7.0.0 (2007-06), ‘Digital cellular telecommunications systems (Phase 2+)’, Universal Mobile Telecommunications System (UMTS); Support of **Optimal Routing** (**SOR**), Technical Realization (3GPP TS 23.079 version 7.0.0 **Release 7**).

[2.10] Noldus, Rogier, ‘CAMEL, Intelligent Networks for the GSM, GPRS and UMTS Network’, Wiley editor, 2006.

Future High-level Requirements for LTE

[2.11] ETSI TS 122 278 v8.8.0 (2009-06), ‘Universal Mobile Telecommunication System (UMTS); **LTE**; Service Requirement for the Evolved Packet System (EPS)’ (3GPP TS 22.278 version 8.8.0 **Release 8**).

3

Connecting the VPLMN MNOs to a Virtual Roaming Supplier

A duck's legs are truly short, but what would lengthening bring to it?

Zhuang Zi (Tchouang Tseu)

3.1 MNO Configuration vs Roaming Hub Supplier Configuration

We consider first in Sections 3.1 to 3.4 what *must be configured in the VPLMN MNO*. Section 3.3 gives two methods to configure the E212 → E214 tables for virtual roaming visitors.

Section 3.5 and all the following sections are about the *configuration of the Roaming Hub supplier* and describe what must be configured to connect the MNO according to one of the possibilities. It will be clearer to take the supplier's viewpoint and say 'they' for the MNO, as the supplier will give the instructions and explanations and eventually a detailed user guide for the particular vendor that the MNO is using.

Very importantly, there is no need with either method to make any 'MAP or CAMEL manipulation' in the MNO's equipment (and the software is not designed for it any way): in Figure 3.1, we do not show the *MAP or CAMEL level, as it remains unchanged when transmitted to the Roaming Hub*.

3.2 Connection to the Roaming Hub Service, MNO Point of View: Using the 'Alias GT' Method

This 'Alias GT' method is the most flexible commercially, as the MNO and the Roaming Hub (ENTRY) which provides the service *are not necessarily adjacent*; that is, the Roaming Hub does not need to be the international SCCP gateway of the MNO.

3.2.1 Basic Services: Voice and SMS

We now consider the virtual visitor service that an MNO wants to offer, the details of which are given in Chapter 1. The following principles are derived from it.

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

3.2.1.1 CC-MGT of HPLMNs Must Be Translated to the Roaming Hub GT

The CC-MGT is the initial piece of all the equipment of the HPLMN (33-689 for Orange France, 33-609 for SFR etc.):

- *Any Main Global Title (MGT) E164 that the MNO does not have roaming with must be translated* to a GT of the Roaming Hub (ENTRY). This is a consequence of offering the SMS-MO service to the virtual visitor. *The SCCP setup is in the GMSC* and it does not concern all the NDCs of the virtual visiting network at this stage.

In Figure 3.1, the SMS-MO is sent to the SMSC GT ('Message Centre') in the SIM card. The GT starts with the CC-MGT of the HPLMN, and will then be routed to the Roaming Hub (ENTRY).

3.2.1.2 E212 → E214 of HPLMNs Created to Route to Roaming Hub

This table is used for the addressing of the HLRs for all MAP services which are based on the IMSI address:

- All the translations E212 → E214 (in particular to route the UPDATE LOCATION) must be set to provide an E214 address which points to its Roaming Hub (ENTRY). *The setup must be done in each MSC/VLR SCCP table* of the MNO.

This setup can be done for each virtual visiting network opening, *one by one*. Depending upon the NSS vendor, there can also be a full default setup for any network the MNO does not have roaming with. So, if the Hub Indicator (the CC-MGT) of the Roaming Hub is 33-191, the E212 → E214 table

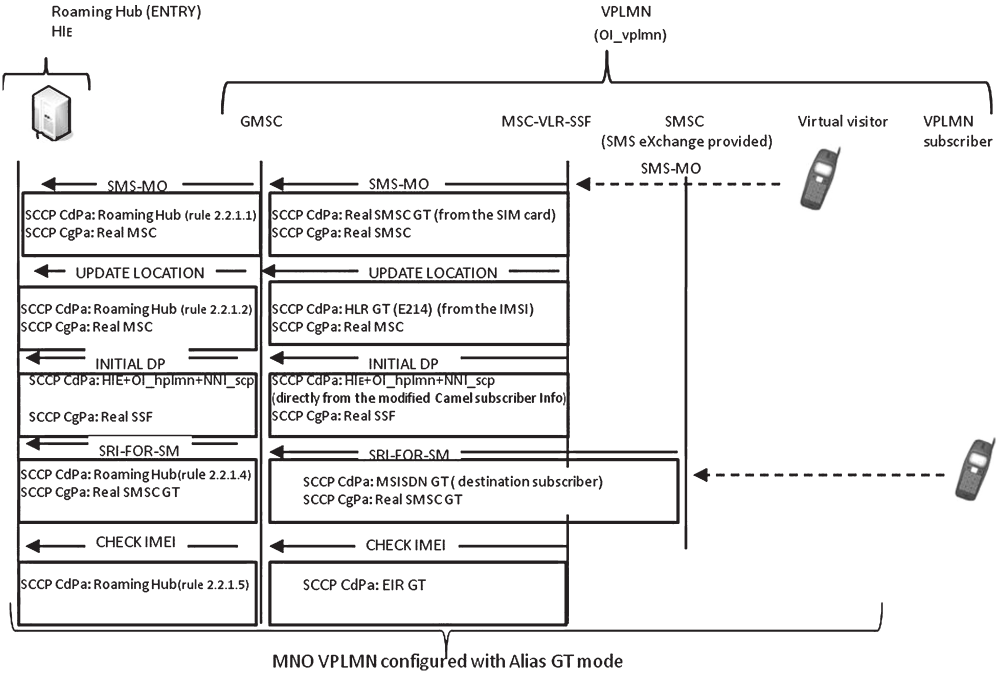

Roaming Hub (ENTRY)
HIE
VPLMN
(OI_vplmn)
GMSC
MSC-VLR-SSF
SMSC
(SMS eXchange provided)
Virtual visitor
VPLMN
subscriber
SMS-MO
SMS-MO
SMS-MO
SCCP CdPa: Roaming Hub (rule 2.2.1.1)
SCCP CgPa: Real MSC
SCCP CdPa: Real SMSC GT (from the SIM card)
SCCP CgPa: Real SMSC
UPDATE LOCATION
UPDATE LOCATION
SCCP CdPa: Roaming Hub (rule 2.2.1.2)
SCCP CgPa: Real MSC
SCCP CdPa: HLR GT (E214) (from the IMSI)
SCCP CgPa: Real MSC
INITIAL DP
INITIAL DP
SCCP CdPa: HIE+OI_hplmn+NNI_scp
SCCP CgPa: Real SSF
SCCP CdPa: HIE+OI_hplmn+NNI_scp
(directly from the modified Camel subscriber Info)
SCCP CgPa: Real SSF
SRI-FOR-SM
SRI-FOR-SM
SCCP CdPa: Roaming Hub(rule 2.2.1.4)
SCCP CgPa: Real SMSC GT
SCCP CdPa: MSISDN GT (destination subscriber)
SCCP CgPa: Real SMSC GT
CHECK IMEI
CHECK IMEI
SCCP CdPa: Roaming Hub(rule 2.2.1.5)
SCCP CdPa: EIR GT
MNO VPLMN configured with Alias GT mode

Figure 3.1 Configuration of the MNO for the virtual roaming supplier

which would be created to allow a virtual roaming visitor of HPLMN Now(Sudan) with E212 = 283-05 would be:

283-05 → 33-191

3.2.1.3 Prepaid Virtual Visitors' Configuration (CAMEL)

In Figure 3.1, why did the Roaming Hub dynamically change the VLR CAMEL subscription information of the INSERT SUBSCRIBER DATA to HI_E + OI_hplmn + NNI_scp? From the above, if we had left the original SCP address, it would have been translated by the GMSC and sent to the Roaming Hub (ENTRY) when an Initial DP would be performed.

But for CAMEL subscribers, most MSC/VLR create controls such that they have roaming with the SCP:

- when the UL is performed;
- when a prepaid CAMEL call is made.

So, in *each MSC/VLR*, the CAMEL table of visitors must be provisioned and the CC-MGT of the accepted SCP entered. The dynamic change of all SCP GT to HI_E + OI_hplmn + NNI_scp allows there to be a single value SCP GT range = CC-MGT of HI_E for all CAMEL virtual visitors.

This is the recommended method, although another is possible with a different implementation of the Roaming Hub which would not change the SCP GTs of the virtual roaming visitors. The other reason why this method should be used is that it is mandatory for the 'multi-IMSI' outbound subscriber service *as the visited network does not make any change in its configuration to receive the visitors*: they use another IMSI which is already its roaming partner. With this recommended method, you can see that the SSF function in the MSC-VLR *directly provides the Roaming Hub (ENTRY) GT* as the destination of the INITIAL DP.

3.2.1.4 Setting up the 'SMSeXchange Service' if it is Provided by the Roaming Hub Supplier

This is the case when the supplier provides many destinations for SMS-MT through their own SMS-MT termination agreements. The SEND ROUTING INFO sent by their SMSC must be rerouted to the Roaming Hub; their CdPa address is any MSISDN. To have the SMSeXchange service, they must configure their GMSC (or their SMSC if it has a GT translation capability) so that *any NDC* (not just the MGT as in Section 3.2.1) that the MNO *does not have roaming with* is translated to a GT of the Roaming Hub (ENTRY). So this strategy makes the default configuration for the E164 GT very simple.

In Figure 3.1 you see that the SMSC created a destination GT = the MSISDN of the destination number and that after the GMSC translation, it becomes the Roaming Hub GT.

3.2.1.5 Control of Stolen Handsets: Checking of the IMEI Service

In order to provide this service to the virtual visitor, the MNO will configure each HPLMN and Relay EIR. Based on the rule in Section 3.2.1.1, the GT will be replaced by the GMLC with the Roaming Hub (ENTRY). Next, the Roaming Hub will analyse the IMSI in the CHECK_IMEI (in the TCAP dialogue part) and use a table to find the real EIR GT and set it as the Called Party SCCP.

3.3 Details of E212 → E214 MNO Configuration with the GT Translation Methods

3.3.1 Alias GT E214

This method was developed in [3.5] and is usable in most cases even without a more elaborate GT translation:

(1) Create a *default* E164 (if possible, otherwise do it to reach virtual roaming) outgoing table (always possible) so that all the E164 addressing will go to the Roaming Hub when there is no direct roaming agreement:
 – 33 602 123456 → **32 04** 33 602 123456 → Point Code of *adjacent SCCP Gateway*.
(2) Create, one by one, the entries of a default E212 → **E214** table (if possible):
 – 20801…sn → 3204…. → Point Code of *adjacent SCCP Gateway*.
 All the SCCP E214 and E164 go to the Roaming Hub GT (called HI) 3204.

3.3.2 Alias GT E164

This can be used with the recent software releases of the GMSC.

Example:

- Huawei GMSC (e.g. Comium Ivory Coast);
- Siemens SR11 (e.g. Africell Sierra Leone).

The procedure is:

(1) Create a **default** E164 outgoing table so that all the E164 addressing will go to the Roaming Hub full GT when there is no direct roaming agreement:
 – 33 602 123456 → **33 152 000 123** → Point Code of *adjacent SCCP Gateway.*
(2) Create a default E212 → **E164** table for all the destinations you do not roam with:
 – MCC MNC…sn → **33 152 000 123** (E164 not E214!) → Point Code of *adjacent SCCP Gateway*;
 – E212 → E164 fixed GT of the Roaming Hub → Point Code of *adjacent SCCP gateway*.
 All the SCCP also go to the Roaming Hub full GT 33152000123.

3.4 Connection to the Roaming Hub Service, MNO Point of View: Using the ‘MTP Transparent Tunnelling’ Method

This assumes that there is no Global Title translation in the GMSC software, and that the MNO has a Point Code, national or international, *adjacent* to the international SCCP gateway which *is also the Roaming Hub*. The configuration is *exactly the same as when a GMSC has several SS7 suppliers* and MTP routes to each:

(1) In the GMSC, create an MTP route to the Point Code ‘a’ of the Roaming Hub through the linkset of *the SCCP Gateway hosting the Roaming Hub*. Ask your IGW to do the same to your PC = ‘u’.
(2) Create one by one the ‘virtual roaming’ agreements in your GMSCs (example: Orange France):
 – CC = 33, NDCs = 602, 607–608, 630–633, 637, 642–643, 645, 654, 670–689 (E164);
 – MCC = 208, MNC = 01 (IMSI E212).
(3) Create the normal E164 outgoing tables; make all the CC-NDC point to the Point Code ‘a’ of the Roaming Hub.
(4) Create the E212 → E214 table, so that 20801.SerialNumber is translated to 33689.SerialNumber, and make the E214 GT point to the Point Code ‘a’ of the Roaming Hub.

3.5 Roaming Hub Supplier Point of View: Different Modes of Connection of the MNO Clients

It is well known that the SS7 network includes two embedded network layers. SCCP uses Global Titles (e.g. 23675500001) and the prefix CC-NDC 236-75 that uniquely identifies a network and allows a hierarchical addressing Country-Operator. MTP (or M3UA in SIGTRAN) uses Point Codes, which can be either International unique Point Codes, or National significance Point Codes.

The mobile operators can use an International Gateway (either addressed with its National Point Code if they have a direct connection, or with its International Point Code, if they use a 'transit' through another carrier). This is the most frequent case.

They can also directly address the foreign partner or their International Gateway, but they need to have their own International Point Code. It is supposed to reduce the SS7 carrier charges, but is now little used because whenever they make a roaming agreement, an MTP route must be created between their International PC and the destination International Point Code (an International GW or the mobile network directly if they also have an International Point Code).

There are two types of connections for Mobile Network MNOs so that their SCCP messages reach their Roaming Hub.

3.5.1 GT Translations

This is very flexible because it is possible to *make a full default setup*, which is not possible with the other method, and also it requires only one Point Code (National or International) in the Roaming Hub. Different variants are detailed below.

3.5.2 MTP Transparent Tunnelling

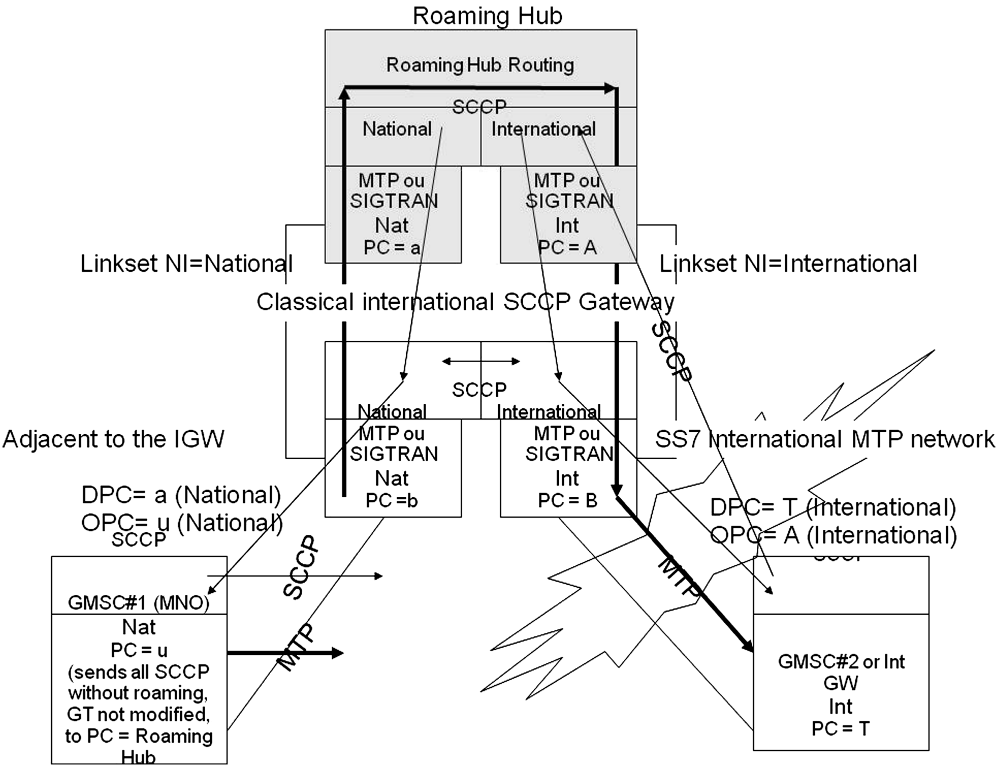


Figure 3.2 MTP transparent tunnelling connection of MNOs

3.5.2.1 MTP Level

This is necessary if no GT translation is possible in the GMSC of the MNO, so that the SCCP CdPa GT is *the standard unmodified E214 or E164* of the destination network (roaming is not supposed to exist). It must go to the Roaming Hub, *which is assumed to be connected with a classical SCCP International GW* (that is, the connection between National and International traffic is not possible between the MTP (or SIGTRAN) layers. In Figure 3.3, this is illustrated by a separation between two MTP (or SIGTRAN) blocks:

(1) GMSC#1 is 'adjacent' to the IGW (its international SS7 provider), and *uses a National PC*. The GMSC must set an MTP route to PC National = 'a' of the Roaming Hub through the linkset to its adjacent PC = 'b' for all the destinations it has virtual roaming with (for real roaming it would be PC = 'a'). This is a simple MTP layer setup in the GMSC, done once for all.

A National PC is needed for the Roaming Hub.

The Roaming Hub should create a *national MTP route to the list of all the GMSC* (such as HMSC#1) with National Point Codes. We will see that this can be avoided if the Roaming Hub has a special SCCP address translation facility.

It may not need to set all these Point Codes in the list of Responding Point Codes in its SCCP layer (national) so as to respond to their SSTs, as usually no SSTs are generated between GMSCs and their IGW (it is not useful and uses resources).

(2) GMSC#2 has an International PC = T and is thus not necessarily adjacent to the IGW. To use the Roaming Hub service, the GMSC must create *a new end-to-end MTP route* to the PC International = 'A' of the Roaming Hub, and will send the 'nonreal roaming SS7 traffic' to this PC = 'A' instead of 'B'.

An international PC is necessary as it is the only way for the Roaming Hub to receive-send SCCP with GMSC#2.

The Roaming Hub *should* create an *international MTP route to the list of all the GMSC* (such as GMSC#2) with International Point Codes. This may also be avoided with the special SCCP address translation facility.

It may not need (see national case) to set all these Point Codes in the list of Responding Point Codes in its SCCP layer (international).

3.5.2.2 SCCP Level

The Roaming Hub setup is simplified because it is associated with an IGW which takes care of the routing based on the GT. So to send SCCP traffic to GMSC#2, *the Roaming Hub routing does not need to know* its International Point Code, or its National Point Code for the traffic to GMSC#1. *All the international SCCP could be sent to either the National or the International Point Code* of the IGW because it is an SCCP Gateway and can transfer from a National Network to an International Network. Then there is a single list of destination networks all reachable by one of the preferred Point Codes of the IGW.

There can also be two lists in the Roaming Hub: the destinations reachable by National Point Codes and those by International ones; it avoids SCCP transfers in the IGW between these two networks and the Roaming Hub uses one of the two linksets.

3.5.3 National Point Code ↔ International Point Code Routing

Figure 3.1 shows what the Roaming Hub does. SCCP traffic (e.g. UPDATE LOCATION) for virtual visitors of Network#2 is sent by Network#1. It reaches the Roaming Hub routing layer from the 'National side' SS7. From the IMSI in the MAP layer, the HPLMN can be determined, and if a distinct list of the International networks exists, traffic could be sent directly to the International side of the IGW.

The entire route goes through the IGW which concentrates the SS7. The Roaming Hub must have two Point Codes, National and International, if all the possible cases are to be handled.

3.6 Implementation of a Roaming Hub with Several Point Codes

3.6.1 Architecture Principle for Multiple Point Codes

As described previously, it is necessary for the Roaming Hub to address either the National or International Point Code of the IGW in order to be reached directly by MNO using ‘MTP Tunnelling’. The information requirement is to be able to have customers with different connections but the same Point Code (could happen). So the Roaming Hub must use a different Point Code, based on the destination.

The Roaming Hub has up to four lists of customers (more if customers with identical National Point Codes must be handled).

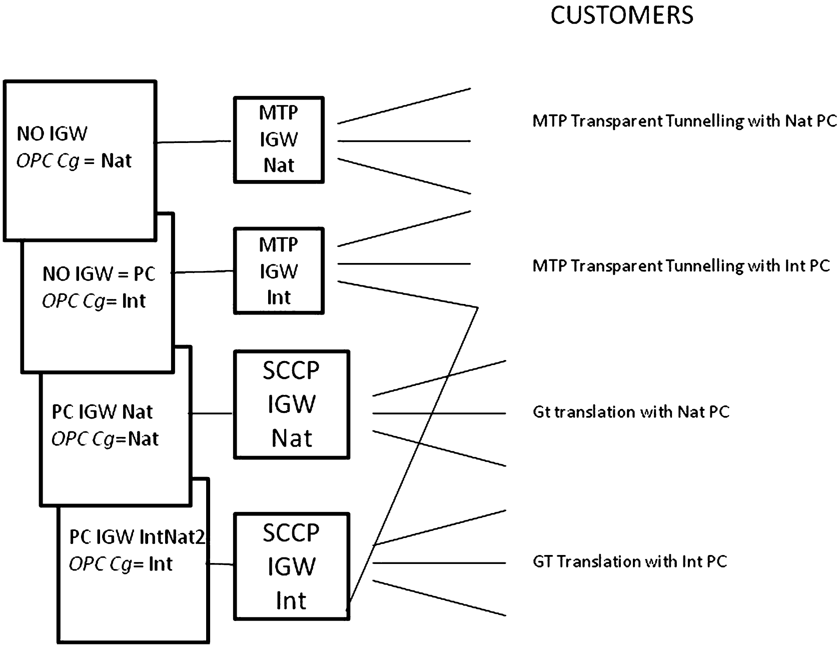


Figure 3.3 Sets of customers based on connection mode

Sending SCCP to an ‘MTP Transparent Tunnelling’ with an International PC can be achieved in three ways:

(1) Directly to its PC (the Roaming Hub acts as an IGW), origin = International.
(2) Through the IGW International, origin = International (the IGW will set its own OPC).
(3) Through the IGW National, origin = National (it will be passed to IGW International).

Cases (2) and (3) are simpler to administrate. For (1), the International Point Code of each distant GMSC must be positioned and addressed. In (1) and (2), the physical links do not need to be direct to the Roaming Hub; they are concentrated in the IGW MTP function.

Using several National Point Codes also allows different networks to be addressed with the same National Point Code, as this can happen, but the linksets should be direct to the Roaming Hub.

3.6.2 Details of Operation

A *single SCCP instance* (arbitrarily OPC = National) *and MTP3* can be used with all the linksets with the various Point Codes declared. A special address translation mechanism uses an ‘Intermediate layer’ between SCCP and MTP3 (or M3UA).

All the routing below uses ‘routing on GT’.

3.6.2.1 Outgoing SCCP (Roaming Hub → Distant Mobile Network)

The routing function of the Roaming Hub decides the Origin Point Code (OPC Cg) to be used, and passes it in the Calling Party address of SCCP, *which it normally should not do* (the Calling Party PC must be left empty), while setting the Destination Point Code (the International Gateway Point Code or the direct Point Code of the distant customer).

The SCCP layer must be set so that this PC *is included* (here OPC Cg) in the Called Party address (*not done normally*). Note that when SCCP creates the MTP3 message, its own OPC (National) is used.

As seen previously, because the routing is on GT, the SCCP *takes out the DPC* from the SCCP Cd Pa.

The intermediate layer MTP3-SCCP is used, the purpose of which is to perform the final coding of the MTP3 message. It uses an initialization table which gives the NI Cg of all the OPC Cg which can be used by the Roaming Hub.

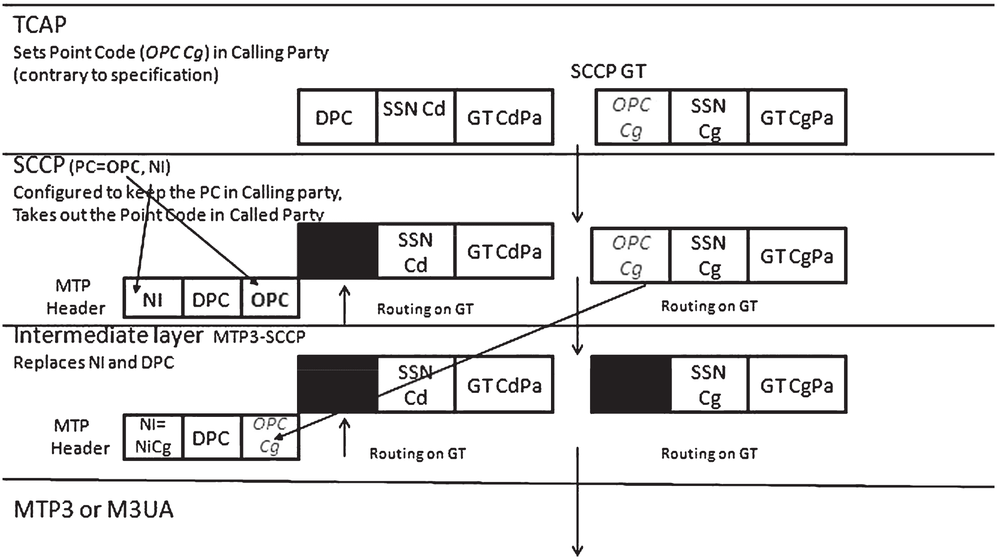


Figure 3.4 Outgoing SCCP for multiple Point Codes Roaming Hub, several National, several International, and several Nation Spare

When the intermediate layer receives a message from SCCP, it analyses the OPC Cg in the SCCP Calling Party address header, and matches with the entries in the table to find the NICg (can be international). It modifies the MTP3 header to have NI = NICg and replaces OPC by OPC Cg, while taking out the OPC Cg from the SCCP CgPa to comply with the standard (no Point Code in SCCP CgPa when there is ‘routing on GT’).

3.6.2.2 Incoming SCCP (Roaming Hub ← Distant Mobile Network): Impossibility of Using a Standard SCCP

Assuming the SCCP comes from an international Point Code, the NI is International and the DPC = PC Int of the Roaming Hub (the SCCP unique stack has been chosen to be PC = Nat).

The linkset configuration for the International Point Code will *need to disable the NI control,* so that traffic to NI international is still passed to the upper layer while the MTP3 layer receives an initialization from SCCP with ‘National’.

The intermediate layer changes ‘routing on GT’ to ‘routing on PC + SSN’ (so that the SCCP knows that it is the destination) and passes it to the upper layers, and inserts the PC Nat in the SCCP CdPa.

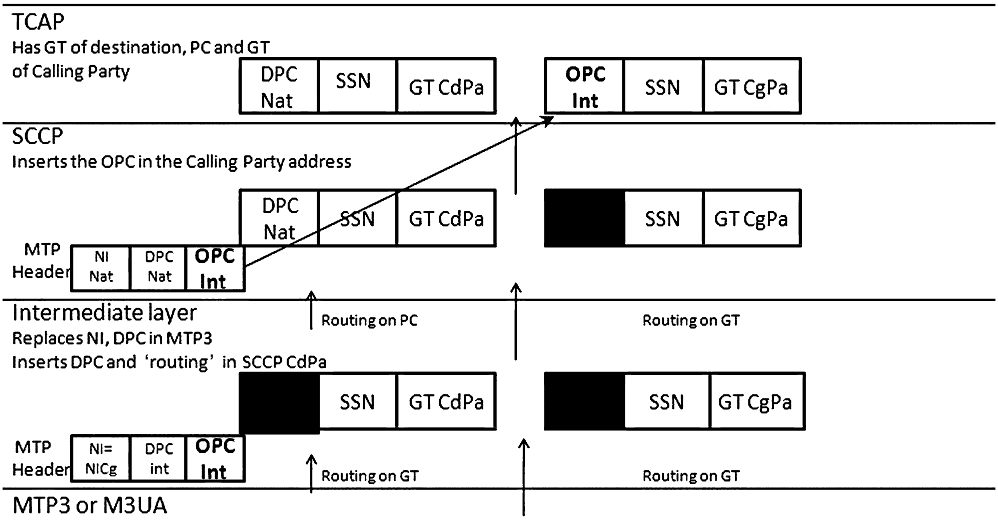


Figure 3.5 Incoming SCCP International → National SCCP example: *does not work*

At the TCAP trace level, you can see an OPC in the Calling Party Address: it is set by the SCCP layer from the OPC *at MTP3 level*, not from an empty (most of the time) OPC in the GT Calling Party address.

Also at the TCAP trace level, the DPC in the Called Party Address *must always be the SCCP stack Point Code as must the DPC in the MTP3 header*. If either of the two is different from the SCCP stack, it will be refused by SCCP (Network Failure reject).

But the TCAP *must have the original MTP3 DPC*, otherwise the Response to the incoming TCAP would not find the matching linkset:

- DPC Nat → OPC (which is International) (does not exist).

So the solution is to bypass the SCCP for the Incoming SCCP, *so that the original DPC can be passed to TCAP*. Remember that the SCCP does not do much for Class 0 and Class 1 (Connectionless SCCP). It has an active function for Connection Oriented as it manages ‘Connection Ids’ very much like TCAP Transaction Ids.

3.6.2.3 Correct Solution: Bypass of SCCP from MTP3 → TCAP

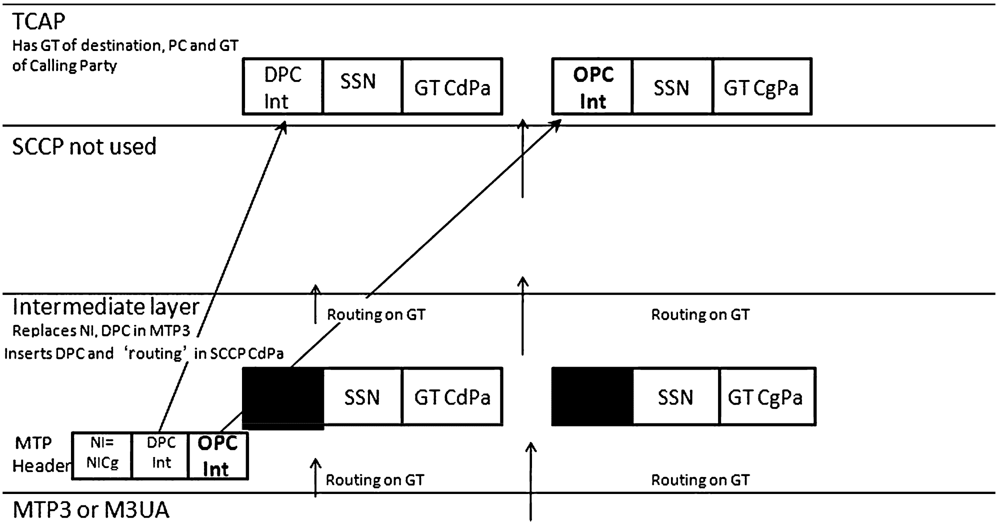


Figure 3.6 Incoming SCCP International → National SCCP example: **ByPass SCCP**

The Intermediate layer sets the DPC in the SCCP Called Party Address and in the SCCP Calling Party Address and sends directly to TCAP. So, the response can be sent correctly to this DPC, because this linkset exists: DPC (International) → OPC (which is International).

3.6.2.4 Case of SST and SSA

We will still use SCCP for the SST and SSA function, as well as for the 'Connection Oriented' (Class 2) SCCP as it is always addressed to the Point Code of the SCCP stack.

The International SCCP GW, in general, does not send SST (it would load the network). But if there is a direct connection to an International PC, it could happen. The SST sent to the Roaming Hub International PC = '*A*' inside the *Data Parameter* should be *changed* to Nat PC = '*a*' of the SCCP layer for the incoming SST, and *should be replaced* by 'International PC = 'A' in the SSA received from SCCP. As there is no way to know which PC it is really, the solution is to memorize the PC polled by the SST and to insert it in the Data Parameter field of the SSA received from the SCCP, which answers sequentially when it receives several SSTs.

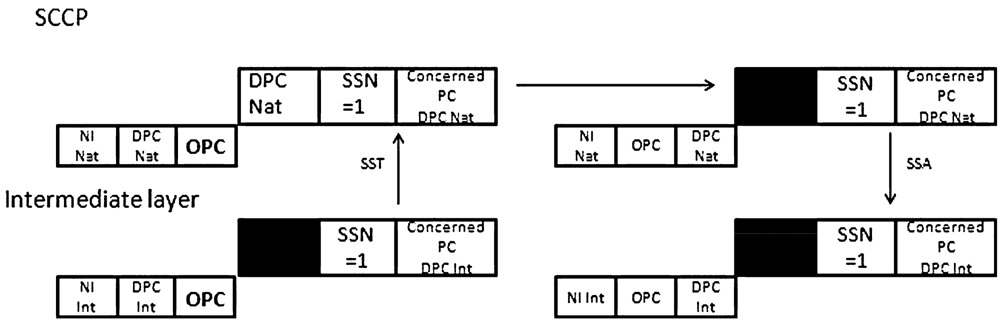


Figure 3.7 SCCP management message transformations

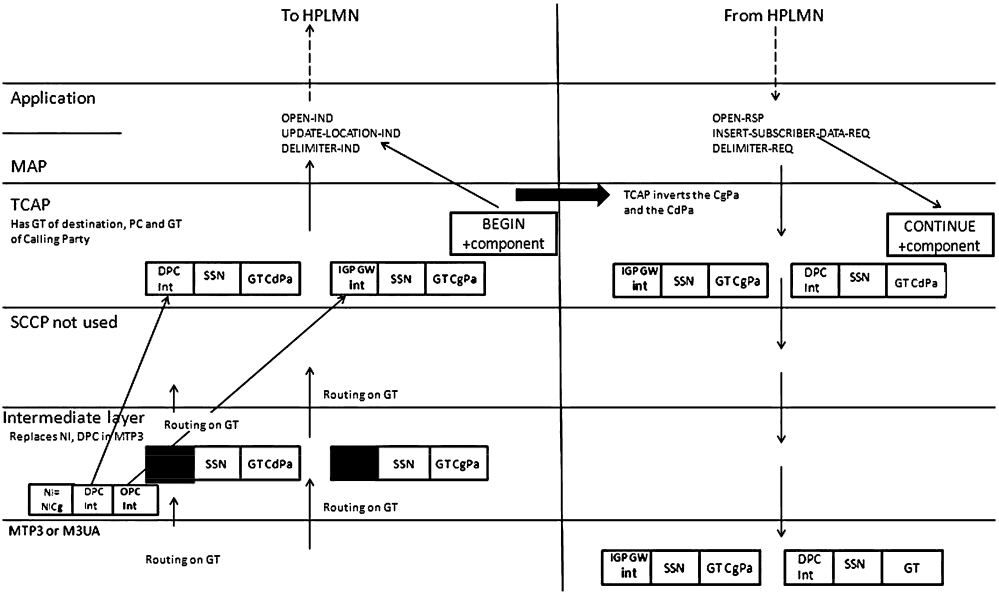


Figure 3.8 Origin Point Code substitution in the Roaming Hub

3.6.3 Origin Point Code Substitution to Avoid Creating MTP Routes to all the MNOs

Some customers using the ‘MTP transparent tunnelling’ connection method may wish to send all their international SCCP traffic directly to the Roaming Hub and reserve their GMSC only for the national SCCP. In the case of Orange France, that means more than 100 Point Codes to declare: all the HLRs, MSCs, SMSCs, etc.

Entering and updating the list regularly would be a very onerous task for the Roaming Hub supplier.

How can declaring all the MNOs’ Point Codes at the MTP level be avoided?

In Figure 3.6, consider an MTP message arriving from one of the MNOs and the MTP route is *not declared to this MNO*: it does not prevent the message coming in if the MNO has declared the MTP route *to the Roaming Hub*. Assume it contains a TCAP BEGIN with an UPDATE LOCATION.

When the application answers with a TCAP CONTINUE in the same TCAP transaction, the Calling Party address SCCP with the Point Code = OPCint becomes the Called Party address. If there was no MTP route opened to this OPCint, *it would not be sent*. The trick is to have the intermediate layer test of whether the *OPCint* is one of the PCs of the IGW; if not, replace it by one of them (the national or the international, depending on the Network Indicator of the MTP level).

The way it works is illustrated in Figure 3.8.

3.7 SS7 Stack Architecture for a Robust Integrated System with Several Point Codes

3.7.1 Layered Architecture Diagram

An ‘integrated system’ needs to have most functions of an MSC-VLR-SSF and will simultaneously run MAP and CAMEL (using TCAP), as well as BSSAP running directly with SCCP. If one also wants

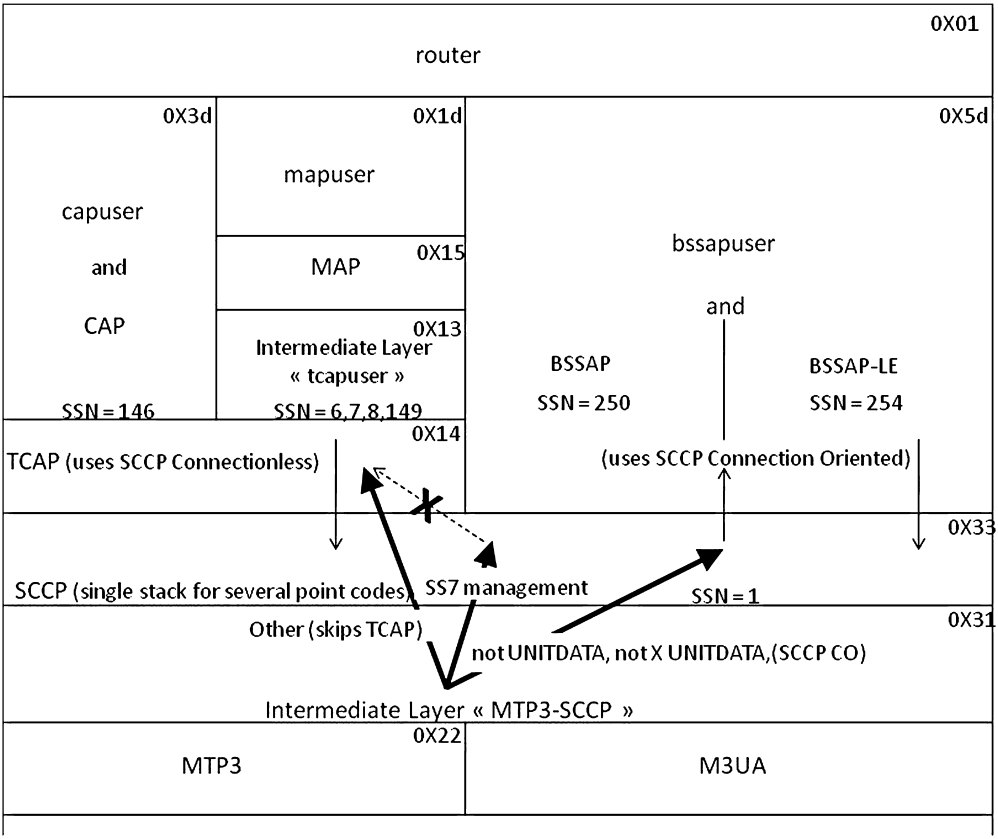


Figure 3.9 SS7 stack integrated architecture for multiple Point Codes and SCCP CO and CL

to have several Point Codes for SCCP, it requires a very special SS7 stack. An implementation example is given in Figure 3.9.

3.7.2 Intermediate Layer MTP3-SCCP

The UNITDATA and XUNITDATA incoming SCCP messages must ‘skip’ the SCPP layer, and go directly to TCAP reception, while the SCCP Connection Oriented need to use SCCP. The SCCP management (SubSystemNumber = 1) goes to the SCCP layer also.

3.7.3 Intermediate Layer TCAPuser

This layer is a useful addition to the standard SS7 stack in order to add timers to the *incoming* MAP transactions, as TCAP provides timers (and time-outs) only for the outgoing transactions sent by upper layers. This absence of timers can create congestion (lack of incoming TCAP contexts) in the case when the sending equipment (e.g. MSC) does not complete a segmented TCAP transaction (dialogue with empty component, then nothing). In this case, the receiving ‘MAP user’ may not be ‘triggered’ and the TCAP context remains hung up.

The intermediate layer’s purpose is to add a timer in the incoming transactions and close them if necessary.

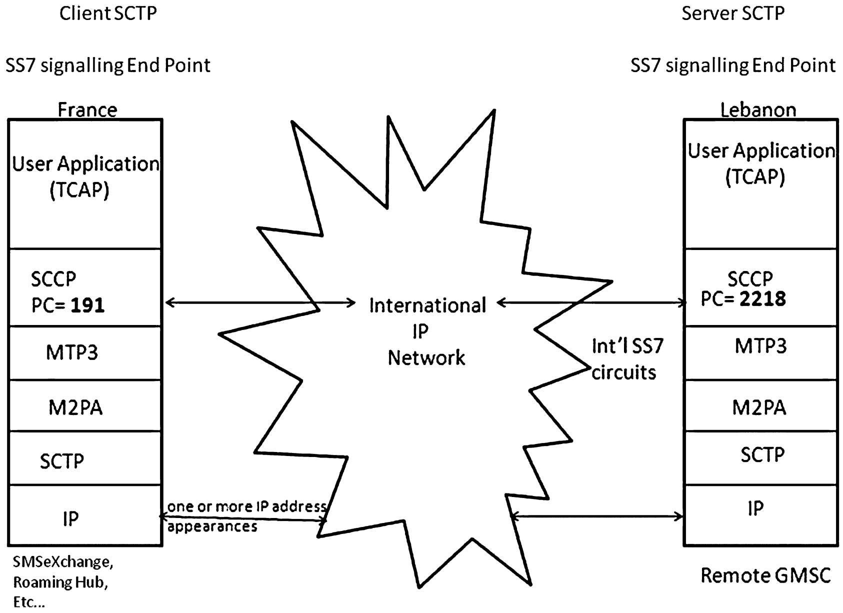


Figure 3.10 SIGTRAN based 'peer-to-peer' connection using M2PA

3.8 SIGTRAN Introduction and Practical Configuration

3.8.1 SIGTRAN the all IP SS7 Signalling Connection for 2.5G, 3G and 4G

IP connections are standard in all servers, while SS7 over E1 requires special hardware. This is the cost reduction and performance incentive which led to the development of SIGTRAN (Special Interest Group on TRANslations). It allows SS7 to be exchanged over cheaper IP connections [3.1].

In Figure 3.10, we use one mode of SIGTRAN, MTP3 [3.3] and M2PA [3.4], which is a straightforward equivalent of classical TDM links using E1s, with each 'link' being replaced by an IP connection. In this mode, the two connected systems are almost symmetrical, so it is suitable for the replacement of long-haul E1 connections of the SS7 international network. To connect Roaming Hubs together, SIGTRAN is the suitable mode.

To explain SIGTRAN in practical terms, we will first show how we would set up the connection between the two systems of Figure 3.10 if we were using E1, then modify it to use SIGTAN M2PA 'peer to peer'.

Figure 3.11 shows the signalling diagram which allows an 'AS' (Application Server) with SIGTRAN connections to exchange SS7 with distant SS7 equipment such as a GMSC in a remote GSM network. This example uses the M3UA mode of SIGTRAN which is intended to connect most often the HLR, MSCs and SMSCs to the GMSC of a mobile network.

3.8.2 Example of an E1 (TDM) Connection Configuration with Dialogic Software

We assume the reader has more familiarity with the setup of E1 connections. They use a 'linkset' between two *adjacent* Point Codes (PC a = **191** and PC b = ***3421*** in Figure 3.2). Each linkset is made of up to 16 'signalling links', which are 64 Kbit channels, each identified by a 'Signalling Link Code'. The Dialogic setup for this linkset is as follows.

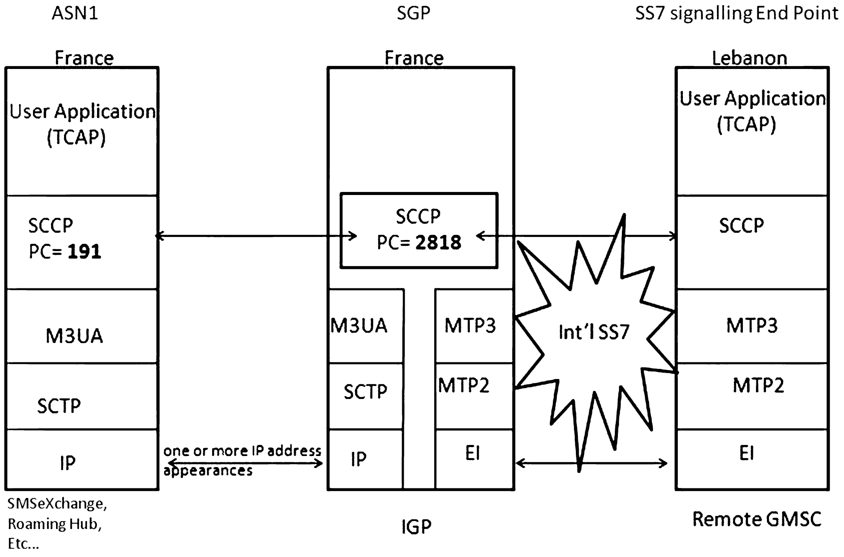


Figure 3.11 SIGTRAN-based International Gateway with M3UA

* **191** is the local Point Code, ***3421*** the Distant Point Code

* 1) Define LINKSETS: 2 SS7 links on this linkset with **3 Signalling** Links

* MTP_LINKSET <linkset_id> <adjacent_spc> <num_links> <flags> <local_spc> <ssf>

MTP_LINKSET 0 ***3421*** **3 0x0000 191 0x08** /* this is the MTP3 setup*/

* 2) Define **3** signalling LINKS with Signalling Link Codes 4, 5, 6 on time slots, 16,17,18:

* MTP_LINK <link_id> <linkset_id> <link_ref> <slc> <board_id> <blink[0..3]> <stream> <timeslot> <flags>

MTP_LINK 0 0 0 4 0 1 0 16 0x00000006 /* this is the MTP2 setup */

MTP_LINK 1 0 1 5 0 1 1 17 0x00000006

MTP_LINK 2 0 2 6 0 1 2 18 0x00000006

3.8.3 SCTP (Stream Control Protocol): Principle [3.2]

This is the equivalent of TCP, that is error control, resequencing of packets and congestion control. But TCP is byte oriented, while SCTP is 'frame oriented' (short blocks). The main unsuitability of TCP for carrying signalling SS7 messages from different sources is that it uses a 'single stream' between two end points. In the cases of loss of messages or sequence violation, this means that TCP will hold up delivery of all data of this 'monolithic stream' until the correct sequence is restored. Also, the timers of TCP (in seconds) make it unsuitable for real-time transmission: subsecond timers are necessary.

SCTP was designed to alleviate these defects which made TCP unsuitable for SS7 transmission.

SCTP allows what is called 'multi-homing' communications with one or both extremities, having several IP addresses (main user difference with TCP). It was designed in 2000 (RFC 2960). It allows *several 'streams'*, which are independent, within a 'connection' (referred to as an '*association*'). In TCP, a 'stream' is a sequence of bytes; in SCTP, a 'stream' is a sequence of messages (very short or very long). Routing to one IP address is independent of all the others so that if there is a restore for one IP address, it does not affect the others.

In the SIGTRAN stack, each SCTP ‘association’ corresponds to an SS7 link (managed by the MTP2 LINK Level protocol of the ‘TDM stack’. Each ‘association’ will handle the error correction independently without delays for the others between the same Signalling End Points, which is exactly what a classical SS7 link/E1 does with the MTP2 protocol.

In practice, several ‘IP addresses’ for a given End Point are created by defining different IP Ports for each ‘association’.

3.8.4 *Example of MTP3/M2PA/SCTP Configuration with the Dialogic SIGTRAN Software*

This starts similarly to the E1 connection configuration; except that the ‘flag’ in the MTP_LINK definition is 0x***80***000006 instead of 0x00000006 to show that it will be implemented by an SCTP association using M2UA (MTP2 User Adaptation layer). Also there is no Time Slot, SLC or processor SS7 (‘blink’) assigned.

```
* 191 is the local Point Code, 3421 the Distant Point Code
* 1) Define LINKSETS: 2 SS7 links on this linkset with 3 Signalling Links
* MTP_LINKSET <linkset_id> <adjacent_spc> <num_links> <flags> <local_spc> <ssf>
MTP_LINKSET 0  3421  3  0x0000  191  0x08        /* this is the MTP3 setup*/
* 2) Define 3 signalling LINKS with Signalling Link Codes 4,5,6 on time slots, 16,17,18 :
* MTP_LINK   <link_id> <linkset_id> <link_ref>  <slc>  <board_id> <blink[0..3]> <stream>
<timeslot> <flags>
MTP_LINK 0 0 0 0 0 1 0 0 0x80000006          /* this is the MTP2 setup */
MTP_LINK 1 0 1 0 0 1 0 0 0x80000006          /* to adapt to M2PA */
MTP_LINK 2 0 2 0 0 1 0 0 0x80000006
```

The specific parameters to create the correspondence between the SS7 links and the required three SCTP associations are below. Three different IP addresses (three different ports 3565, 3566, 3567) are used so that there are three different streams, one for each ‘association’ (the three ‘SS7 links’ equate to an IP ‘stream’.

```
CNSYS:IPADDR=192.168.0.211,DAUD=Y;          /* 192.168.0.211 main IP address */
* SNSLI:SNLINK=,IPADDR=,SG=,[SS7MD=,][IPADDR2=][HPORT=][PPORT=][SNEND=];
* The SNEND parameter specifies whether the host’s end is acting as a Client or Server (C or S) for
SCTP
HPORT and PPORT are the Host’s and Peer SCTP ports (same by default)
SNSLI:SNLINK=1,IPADDR=192.168.0.212,SS7MD=ITU14,SG=1,PPORT=3565,SNEND=C,SNTY
PE=M2PA,M2PA=1;
SNSLI:SNLINK=2,IPADDR=192.168.0.212,SS7MD=ITU14,SG=1,PPORT=3566,SNEND=C,SNTY
PE=M2PA,M2PA=1;
SNSLI:SNLINK=3,IPADDR=192.168.0.212,SS7MD=ITU14,SG=1,PPORT=3567,SNEND=C,SNTY
PE=M2PA,M2PA=1;
```

3.8.5 *Example: M3UA/SCTP Configuration with the Dialogic SIGTRAN Software*

3.8.5.1 Config File: AS Side

```
********************************************************************
CNSYS:IPADDR=192.168.0.213,PER=0,DAUD=Y;
SNAPI:AS=1,OPC=191,RC=5,TRMD=LS,SS7MD=ITU14;
```

```
SNSLI:SNLINK=1,IPADDR=192.168.0.212,HPORT=2905,PPORT=2905,SNEND=C,SG=1,SS7MD
=ITU14;
SNRTI: SNRT = 1, DPC = 2818;
SNRLI: SNRL = 1, SNRT = 1, SG= 1;
```

There are two differences between the AS side and the SG side:

- At the M3UA level, the AS sends a **DAUD** (Destination Audit) of the M3UA protocol.
- At the SCTP level, AS is 'Client', and SG is 'Server' for the SCTP 'association' establishment.

3.8.5.2 Config File: SG Side

```
CNSYS:IPADDR=192.168.0.212,PER=0;
SNAPI:AS=1,OPC=2818,RC=5,TRMD=LS,SS7MD=ITU14;
SNSLI:SNLINK=1,IPADDR=192.168.0.213,HPORT=2905,PPORT=2905,SNEND=S,SG=1,SS7MD
=ITU14;
SNRTI:SNRT=1,DPC=191;
SNRLI:SN
```

3.9 Standard MTP3 Load Distribution Algorithm

SIGTRAN will simplify as well as improve the performance. However, in the MTP3/M2PA case, if the number of links in a linkset is not correct, there could be congestion. So it is useful to explain the MTP3 load distribution over the different links, whether SIGTRAN or TDM is used.

3.9.1 Distribution of Traffic on the Various Links of a Given Linkset

The SCCP layer creates a cyclic Signalling Link Selector (SLS) from 0 to 15 (in nonconnected mode, which we assume here). This is why there is a maximum of 16 links in a given linkset.

The MTP3 layer to which SCCP sends the block to be sent has N links (1 ≤ N ≤ 16), and assigns the link number L by:

- L = SLS mod N

For example, in a complete SLS cycle of 16 sending, if N = 3, L = 1 for SLS = 0, 3, 6, 9, 12 and 16 and L = 2 for SLS = 1, 4, 7, 10 and 13.

One sees that for a given number of links N *which does not divide exactly into 16* (that is a power of 2), *the traffic is not evenly balanced on the links*. For example, where N = 3 above, link 1 will be used six times and link 2 only five times in a complete 16 SLS cycle.

This is well known, but it is useful to give the interesting values of the number of links, which while not being divisors of 16:

- decrease the maximum traffic per link;
- do not decrease the maximum traffic per link.

3.9.2 Load of the Most Loaded Link(s)

Let us look at U(x) the 'echelon function':

- U(x) = 0, x = 0
- U(x) = 1, x > 0

P(x) is the function yielding the value of the integer part of x (that is P (4.2) = 4.

The load of the most loaded link (measured as the number of times that a link is used in a 16 SLS cycle) is:

- Max = P (16/N) + U (16 modulo N)

For example for N = 7, the formula gives Max = 3 (check with the cycle being 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1) and the first two links perform three transmissions while the others perform only two.

Plot of the function Max:

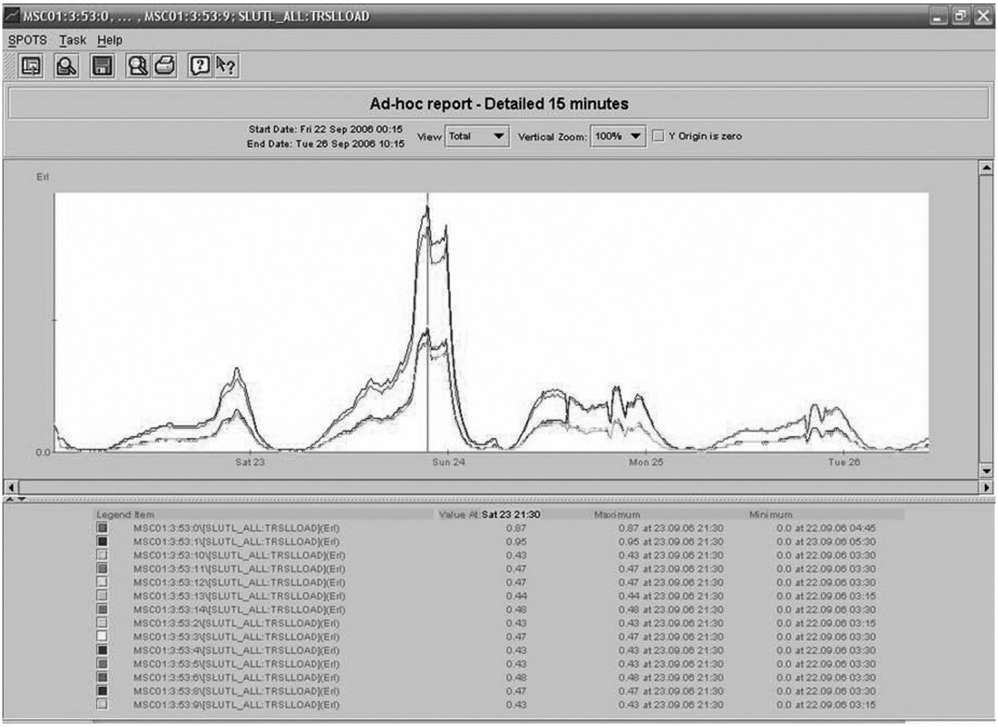
N = 1,	Max = 16
N = 2,	Max = 8
N = 3,	Max = 6
N = {4,***5***}	Max = 4
N = {6,***7***}	Max = 3
N = {8,***9,10,11,12,13,14,15***}	Max = 2
N = 16	Max = 1

Seven links are no better than six.

Ten links are no better than eight.

In the plotting of the Max function, the special values of number of links in bold italic ***5, 7, 9, 10, 11, 12, 13, 14, 15*** should not be used as they cost links without decreasing the load of the most loaded link(s).

The case explained here is real and can be visualized by certain analysers which give these load curves on each link.



Ad-hoc report - Detailed 15 minutes

Start Date: Fri 22 Sep 2006 00:15
End Date: Tue 26 Sep 2006 10:15
View: Total
Vertical Zoom: 100%
□ Y Origin is zero

Legend Item	Value At: Sat 23 21:30	Maximum	Minimum
▨ MSC01:3:53:0\[SLUTL_ALL:TRSLLOAD](Erl)	0.87	0.87 at 23.09.06 21:30	0.0 at 22.09.06 04:45
■ MSC01:3:53:1\[SLUTL_ALL:TRSLLOAD](Erl)	0.95	0.95 at 23.09.06 21:30	0.0 at 23.09.06 05:30
□ MSC01:3:53:10\[SLUTL_ALL:TRSLLOAD](Erl)	0.43	0.43 at 23.09.06 21:30	0.0 at 22.09.06 03:30
▨ MSC01:3:53:11\[SLUTL_ALL:TRSLLOAD](Erl)	0.47	0.47 at 23.09.06 21:30	0.0 at 22.09.06 03:30
□ MSC01:3:53:12\[SLUTL_ALL:TRSLLOAD](Erl)	0.47	0.47 at 23.09.06 21:30	0.0 at 22.09.06 03:30
□ MSC01:3:53:13\[SLUTL_ALL:TRSLLOAD](Erl)	0.44	0.44 at 23.09.06 21:30	0.0 at 22.09.06 03:15
▨ MSC01:3:53:14\[SLUTL_ALL:TRSLLOAD](Erl)	0.48	0.48 at 23.09.06 21:30	0.0 at 22.09.06 03:30
□ MSC01:3:53:2\[SLUTL_ALL:TRSLLOAD](Erl)	0.43	0.43 at 23.09.06 21:30	0.0 at 22.09.06 03:15
□ MSC01:3:53:3\[SLUTL_ALL:TRSLLOAD](Erl)	0.47	0.47 at 23.09.06 21:30	0.0 at 22.09.06 03:30
■ MSC01:3:53:4\[SLUTL_ALL:TRSLLOAD](Erl)	0.43	0.43 at 23.09.06 21:30	0.0 at 22.09.06 03:30
▨ MSC01:3:53:5\[SLUTL_ALL:TRSLLOAD](Erl)	0.43	0.43 at 23.09.06 21:30	0.0 at 22.09.06 03:30
▨ MSC01:3:53:6\[SLUTL_ALL:TRSLLOAD](Erl)	0.48	0.48 at 23.09.06 21:30	0.0 at 22.09.06 03:30
■ MSC01:3:53:8\[SLUTL_ALL:TRSLLOAD](Erl)	0.47	0.47 at 23.09.06 21:30	0.0 at 22.09.06 03:30
□ MSC01:3:53:9\[SLUTL_ALL:TRSLLOAD](Erl)	0.43	0.43 at 23.09.06 21:30	0.0 at 22.09.06 03:15

Figure 3.12 Distribution of load on TDM E1 signalling links

Here 14 links are configured, so, as you can see, on the first two links the load is higher than on the others. Indeed, if you apply the formula L = SLS mod N with N = 14, you have the following sequence: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, **0**, **1**.

So the links 0 and 1 are used twice and the others only once.

3.10 SCCP Class 1 (Sequenced Connectionless Protocol)

3.10.1 The 'Sequence Control' Number

The above discussion of the load distribution on the different links of a linkset is interesting in order to understand how SCCP Class 1 [2.8] works and also that it must be implemented fully in a Roaming Hub.

Table 3.1 Comparison of SCCP Class 0 and Class 1 messages between the SS7 layers

	Class 0		Class 1	
SS7 stack layers	Service sent to the upper layer	Service sent to the lower layer	Service sent to the upper layer	Service sent to the lower layer
Application (MAP user layer)		MAP-DIALOGUE-REQ: **OPEN** **No QOS parameter** (means class 0)		MAP-DIALOGUE-REQ: **OPEN** **QOS parameter = Seq Ctrl required** (means class **1**)
MAP (TCAP user layer)	MAP-DIALOGUE-IND: **OPEN** **No QOS parameter (means class 0)**	TCAP-MSG_DIALOGUE_REQ **QOS = Seq Ctrl NOT required** (means class **0**)	MAP-DIALOGUE-IND): **OPEN** **QOS = Seq Ctrl required** (means class **1**)	TCAP-MSG_DIALOGUE_REQ **QOS = Seq Ctrl required** (means class **1**)
TCAP	TCAP-MSG_DIALOGUE_IND **QOS** = No **Seq Ctrl required** (means class 0)	SCP_MSG-TX-REQ N-UNITDATA: RETURN_OPTION (**no** SEQ_CTRL)	TCAP-MSG_DIALOGUE_IND **QOS = Seq Ctrl required** (means class **1**)	SCP_MSG-TX-REQ N-UNITDATA: RETURN_OPTION **SEQ_CTRL = seq0–31**

SCCP (N-UNITDATA parameters)	SCP_MSG-TX-IND
	N-UNITDATA:
	RETURN_OPTION
	No SEQ_CTRL
		MTP_MSG_TX_REQ
		Return Option
		Class = 0
		SLS = 0–15 from **internal SCCP counter**
			SCP_MSG-TX-IND
			N-UNITDATA:
			RETURN_OPTION
			SEQ_CTRL = **SLS**
				MTP_MSG_TX_REQ
				Return Option
				Class = 1
				SLS = 0–15 = **seq0–31** modulo 16 **from received TCAP**

MTP3 or M3UA	MTP_MSG_TX_IND Return Option Class = 0 **SLS** = 0–15		MTP_MSG_TX_IND Return Option Class = 1 **SLS** = 0–15	Sends on link# SLS modulo number_of_links

Take the example of Chapter 5, Section 5.2.2 (b), and assume that the VLR which sends the UPDATE LOCATION wants to speed up the process, so that the HLR does not wait for the CONTINUE from the VLR to send the next block of the profile. It will work *if the different blocks of INSERT SUBSCRIBER DATA reach the VLR in the proper sequence*. As there are multiple paths between the two nodes in the SS7 networks and *several links in parallel*, the ordinary 'Class 0' connectionless SCCP, which is just a 'datagram' service, does not achieve this objective: two messages sent quickly in the order 1 then 2 could arrive in the reverse order. So the VLR which initiates the UPDATE LOCATION will select instead 'Class 1' so that different SCCP messages sent in order will reach the destination HLR in the same order, and the messages sent by the HLR also reach the VLR in the same order.

The initiating application, which needs 'Class 1 SCCP', creates a 'Sequence Control' number (from 0–31) which is passed as a parameter to the TCAP layer when the transaction is opened, then from TCAP to SCCP (the presence of this parameter is what indicates 'Class 1'). As SCCP is requested as 'Class 1', instead of using the next value of an internal counter as SLS, SCCP *uses this received value* modulo 16 (it yields an SLS (from 0–15)) and passes it to MTP3 or M3UA. This SLS is included in the MTP3 message and allows the MTP3 layer to compute the outgoing link number to be used. At each SCCP transit, the protocol being 'Class 1', SCCP uses *the SLS value received from an incoming MTP3 message as the SLS* for the next outgoing link. Assume there are no alternate routes for address translations, then all messages with the same 'Sequence Control' will follow the same sequence of link numbers on the path between the two distant nodes and the sequence will be received in order by this simple SCCP Class 1 scheme.

3.10.2 Messages between the SS7 Protocol Layers when SCCP Class 1 is Used

In the standard Application Programming Interfaces for TCAP, there are two primitives: one to send 'Dialogue' messages (BEGIN, CONTINUE, END), and one to send 'Components' (Invoke, Return Result, Reject). The request for Class 1 is set in the 'Dialogue' message sent by the TCAP user layer to TCAP.

References and Further Reading

[3.1] Jim Darrock, 'Introduction to Sigtran', Artesyn Communication products.

[3.2] RFC 2760, IETF, Stream Transmission Protocol.

[3.3] RFC 3332, IETF, MTP3 User Adaptation Layer.

[3.4] RFC 4165, IETF, MTP2 User Peer-to-Peer Adaptation Layer.

[3.5] Henry-Labordère, A., 'Système de transmission d'informations entre les téléphones mobiles d'opérateurs non liés par des accords d'itinérance', Patent FR 03 07710, Patent BE 2003/0378.

4

Networks of Roaming Hubs and SMSeXchanges

> *It is clear where the future of sustainable energy lies: a litre of petrol gets polymerized after a few years and costs a third what a bottle of more than decent "rosé de Provence" wine costs, which can be used more than 20 years later.*
>
> *Gaston Bouchignard, 1968*

4.1 Cooperation of Several Roaming Hubs

To provide the widest coverage, several Roaming Hubs, each with their set of agreements, can cooperate. There can be, then, several paths to reach a Mobile Network (redundancy) and the Mobile Portability issue (SMS and Optimal Routing) can be completely resolved in an elegant fashion. Technically, it is necessary for the Roaming Hubs to have a way to perform 'End-to-End' routing to a given distant (not necessarily adjacent) Roaming Hub and we give the solution to this.

The objective is that the customers (MNOs) have a fully transparent service which encompasses the MNP cases while their SMSC equipment, GMSC, remains standard. The MNP must be handled by the Roaming Hub.

4.2 Problem Raised by Mobile Number Portability (MNP)

4.2.1 Reminder: Example of MNP Implementation

In [5.1] Chapter 4, the various implementations are explained. Figure 4.1 shows the 'level N' method used in Europe and Hong Kong (first to implement MNP in 1999). Each mobile network has a copy of a daily updated database, which contains the list of ported numbers and which network they are ported to.

A frequent confusion (surprisingly even with engineers that know SS7 quite well, but not the MNP implementations), is that 'if there is MNP implemented, the SCCP message sent to any of these networks will be answered'. This confusion leads to the (wrong) conclusion that MNP is not an issue, for example for the sending of SMS to a foreign network, and that whatever MSISDN is addressed, an answer will be received from the HLR.

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

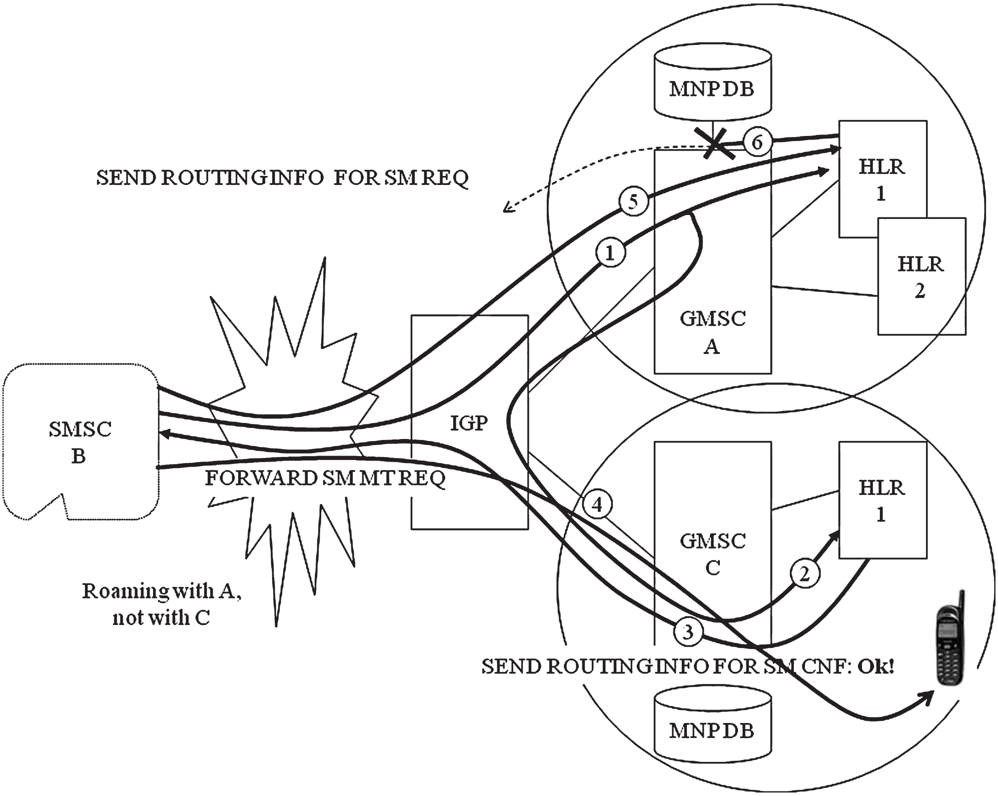


Figure 4.1 MNP implementation at 'level N' (Europe example)

One must think of what 'opening roaming agreements' means for the SCCP routing. Take SMSC B which:

- has at least *one* roaming agreement in the distant country, meaning that it must have opened *all* the NDC number ranges of this country, *even those it does not have roaming with,* according to the IREG principles;
- is addressing an MSISDN belonging to a range of numbers allocated to network A but ported to Network C (Network B cannot know because it does not have a database of MNP of its foreign partners!);
- does not have a roaming agreement with network A (this means that an SCCP *from A → B is not sent*, but that the incoming route *B → A is opened*); opening a roaming agreement A ↔ B from A's point of view means creating the route A → B;
- has a roaming agreement with network C (this means that SCCP C → B is sent).

The SEND ROUTING INFO FOR SM request (1) reaches GMSC A because all forward SCCP routes are opened. Network A checks the MSISDN, finds it is ported to C and reroutes the SEND ROUTING INFO FOR SM request (2) to network C (the SCCP Calling Party is B). As the MSISDN was 'ported in' to C, it does answer to the SCCP Called Party B. And the SEND ROUTING INFO FOR SM confirmation (3) reaches B, *because the SCCP route C → B is opened.* It contains a GT of A, and SMSC B can successfully send the FORWARD SM MT request (4) to C and get the confirmation.

The following happens for an MSISDN of A which is not ‘ported out’ to a network which B does not have an agreement with:

- The SEND ROUTING INFO FOR SM request (4) still reaches A.
- But the SEND ROUTING INFO FOR SM confirmation (5) is not sent back to B (route A → B not opened).
- The SEND ROUTING INFO FOR SM ‘times out’ in SMSC B because of no response. The same would happen if an MSISDN of C (which B has roaming with) was ported to a network which B does not have roaming with.

Conclusion: B receives and answers if and only if the destination number, *whatever range it belongs to*, is a subscriber of a network which B has roaming with.

4.2.2 *Implementation of the Network Search with Distributed Roaming Hubs*

The example is a network of Roaming Hubs providing the SMS termination service or Optimal Routing to an MNO (Sudan), so it can send SMSs to many destinations (UK mobile networks in the example). The destination number is a Vodafone range number ‘ported out’ to O2, and no Roaming Hub has roaming with all the eight UK operators.

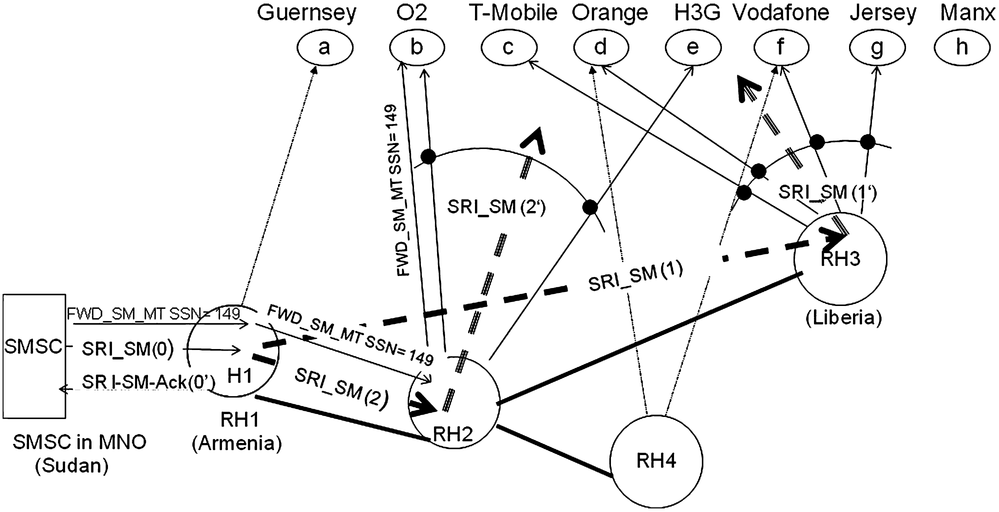


Figure 4.2 Dynamic network searches for number portability

Each Roaming Hub *knows the full graph of agreements of the partners’ Roaming Hubs* so that a global routing computation can be done. The MNO SMSC on the left sends blindly a SEND ROUTING INFO FOR SM request (abbreviated SRI_SM) to its Roaming Hub (ENTRY) #1; it does not need to be concerned by MNP.

Roaming Hub#3 has the largest number of agreements in the UK (four) and it includes Vodafone (most likely, as the portability rate is much lower than 50% in UK). Roaming Hub#4 also reaches Vodafone (with a smaller probability of the number if ported out) because it has agreements with only two networks (Vodafone and Orange). The procedure is as follows:

(1) Roaming Hub#1 chooses Roaming Hub#3 and forwards the SEND ROUTING INFO FOR SM (1), which sends it blindly to the UK (1′). Because the destination subscriber does not belong to a reachable network from Roaming Hub#3, it will ‘time out’ and ‘backward time out’ the request from Roaming Hub#1.
(2) For Roaming Hub#1, Roaming Hub#4 is not considered as the next choice because its two destinations were already searched in the previous request.
(3) Roaming Hub#1 chooses Roaming Hub#2, the last remaining covering H3G and O2. It sends SEND ROUTING FOR INFO request (2) to Roaming Hub#2 which sends it blindly to the UK (2′) and, this time, receives an answer because the destination subscriber belongs to O2. This SEND ROUTING INFO FOR SM Ack is sent back to the MNO SMSC (0′) with an IMSI, VMSC GT and eventually SGSN GT of O2 UK. The total time has been longer, of course (14 sec in the example), than if it had worked on the first search made by the Roaming Hub network (2 sec).
At this stage, the ‘search part’ is completed. If the MSISDN was ported out to Manx Telecom, it would fail with a time-out from Roaming Hub (ENTRY) #1 because it is not reachable from any of the Roaming Hubs.
(4) If successful, the SMSC of MNO will send the FORWARD SM MT to Roaming Hub (ENTRY) #1. The SubSystem Number (SSN) = 149 (SGSN) if an SGSN GT has been returned in order to send the SMS-MT using GPRS. *The Roaming Hub must leave the SSN transparent.*

The standard time-out value for the MAP SEND ROUTING INFO FOR SM request or SEND ROUTING INFO request is 30 sec. To allow two search failures + one success, the Roaming Hub will use a shorter timer (12 sec recommended), so that the software in the sending SMSC or GMSC does not ‘time out’ at 30 sec. The detailed search algorithm is given in [4.2].

4.3 Use of the TCAP Dialogue Part to Provide an End-To-End Routing Capability

We explain now the original idea [4.1], which allows a system to have ‘end-to-end’ routing when SCCP or MTP takes a single predefined path to reach a destination. The reader will now understand why end-to-end routing is necessary so that the various Roaming Hubs can really cooperate.

4.3.1 TCAP Dialogue and Component Parts

TCAP is explained in [5.1] Chapter 2. It includes two parts:

- the ‘dialogue’ part with the SCCP addresses (Called and Calling), the Application context (in > V1), and a ‘TCAP User Information’;
- the ‘component’ part which may be of four types:
  - Invoke (1);
  - Return Result (2);
  - Return Error (3);
  - Reject (4).

The SCCP address TCAP parameter allows addressing of the ‘adjacent’ system. The ‘TCAP User Information’ (exists only if MAP version > 1) is structured as:

- destination reference (standard);
- extension container (also called ‘Ellipsis’): this last field is vendor proprietary.

For example the destination reference is used to carry the IMSI of the mobile (in E164 format) in a MAP REGISTER-SS so the HLR knows which mobile is making a call transfer.

The origin reference may be necessary and has the GT of the original MSC for control.

In [4.1] an original solution is developed to allow the originating Hub to force the sending of a request from a given Roaming Hub FINAL to the HPLMN. This is necessary to implement the search in the three cases when a destination mobile is addressed by its MSISDN:

- SMSeXchange: the originating SMSC wants to send an SMS to a number with Mobile Number Portability. A SEND ROUTING INFO FOR SM is sent and the parameter is MSISDN with a search explained below.
- SMSeXchange: the originating SMSC wants to notify the HLR to ask to be alerted if an SMS-MT delivery failed and the reachability or memory full condition has changed. As it will follow the previous MAP request, the search could be avoided, but still the Roaming Hub FINAL which reaches the HLR must be addressed.
- Optimal routing (the classical solution [2.9]): The originating GMSC needs to query the HLR to get the Roaming Number and trigger an optimal routing; it sends a SEND ROUTING INFO with the MSISDN.

4.3.2 Example of Use of the 'Destination Reference'

This is the trace of the MAP Protocol as specified in the GSM specifications. It shows how the information is set up, in particular dest_ref = 23156000999 which is the GT of the Roaming Hub FINAL.

```
MAP-OPEN-REQ(1)           → Corresponds to preparation of the TCAP dialogue
dest_address(Q713)(1)     → Parameter for SCCP: adjacent Roaming Hub
L = 013
Data: Route on GT, Global Title included(0x13),
Signalling Point Code (ITU) = 1-096-3 ( 2819)
Subsystem Number = HLR(6),
Global Title:
Translation Type = 0,
Numbering Plan = ISDN/Telephony(E164),
Nature Address Indicator = International number,
Address information = 37493297311 /* Adjacent Roaming Hub in Armenia */
dest_ref(GT E164 final or IMSI)(2) – END-To-END routing: Roaming Hub FINAL
L = 007
Data: Ext = No extension
      Ton = International
      Npi = ISDN
      Address = 23156000999 /* final Roaming Hub in Liberia */
orig_address(Q713)(3)                → Parameter for SCCP: origin Roaming Hub
L = 011
Data: Route on GT, Global Title included(0x12),
      No SPC in address
      Subsystem Number = MSC(8),
      Global Title:
      Translation Type = 0,
      Numbering Plan = ISDN/Telephony(E164),
      Nature Address Indicator = International number,
      Address information = 249950008800 /* sending Roaming Hub */
MAPorCAP_Application_Context(11)
L = 009
Data: (Hex) 060704000001001403
```

```
         MAP_ShortMsgGatewayPackage_v1_or_v2 MAP V3
MAPPN_ellipsis(57) /* END-To-END routing : carries the final MAP version and message reference for tracing */
L = 015
Data: (Hex) 820A4F474114423A49472908830101
         HALYS_ellipsis(1) Message Reference Number = f474144124a394749280
         HALYS_ellipsis(2) Final MAP version = 1
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
MAP-SEND-ROUTING-INFO-FOR-SM-REQ(1) → Preparation of the TCAP component 'invoke'
MAPPN_timeout(45)
L = 002
Data: timeout value = 22 sec
MAPPN_invoke_id(14)
L = 001
Data: 1
MAPPN_msisdn(15)
L = 007
Data: Ext = No extension
         Ton = International
         Npi = ISDN
         Address = 33677123456 /* Destination (French) number which may be 'ported' */
MAPPN_sm_rp_pri(16)
L = 001
Data: (1):High Priority
MAPPN_sc_addr(17)
L = 007
Data: Ext = No extension
         Ton = International
         Npi = ISDN
         Address = 249950008800 /* Sending Roaming Hub */
MAPPN_GPRS_Support_Indicator(118)
L = 000
 - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
MAP-DELIMITER-REQ(5) /* Sends the dialogue and the component to TCAP which sends to SCCP. */
```

4.3.3 Example of Use of the Origin_Reference

This is another standard field inside the TCAP user information. It is used to carry 'post Roaming Hub (FINAL) addresses', such as:

- SCP GT (the Roaming Hub (FINAL) will set the address of the destination SCP);
- HLR GT (in the case of MNP in nonregulated countries, it is implemented by the Roaming Hub at 'level N-2' (see [5.1] Chapter 4)). The Roaming Hub (FINAL) will be able to interrogate the HLRs of the country one by one, and the GT to interrogate is passed in origin_reference.

4.3.4 Avoiding Unnecessary MAP (or CAMEL) Version Negotiations

The solution requires that the TCAP user information parameter is accepted. So the dialogue between two Roaming Hubs which have 'End-to-End' routing must be at least MAP V2 and we use MAP V3 in the example (exists for the MAP primitive used).

The addressed network may not accept this and a MAP version negotiation would be created. But as the Roaming Hub ENTRY knows the final version, it includes it in the TCAP user information 'ellipsis' (V1 in the example) and it is used by the Roaming Hub FINAL.

In addition, a unique 'Message Reference' can be included to facilitate the tracing between the Roaming Hubs.

4.3.5 Compatibility with Roaming Hubs not Capable of 'End-to-End' Routing

The GSMa system has not covered the MNP requirement, so many Roaming Hub designs will not provide End-to-End routing unless they incorporate the method explained here (patent).

In this case, the Roaming Hub can work with them by not including the TCAP dialogue modification and will not be able to use them for the MNP resolution. For their incoming traffic, there is no issue and they can use the full benefits of a Roaming Hub network with our design.

References and Further Reading

[4.1] Henry-Labordère, A., 'Système de transmission avec coopération de plusieurs mandataires pour la réalisation de l'itinérance virtuelle pour les opérateurs de mobile', European patent 07 301 371.6.

[4.2] Henry-Labordère, A. and Diallo, Madiagne, 'Hidden target search by sequential optimization', Rapport # 2004/61, PRISM-CNRS, 2004.

5

Hosted Roaming Hubs with Virtual GTs

Votes are not what count most; it is the way they are counted.

Joseph Vissarionovitch Djougachvili

5.1 Purpose

In order to allow the hosting of a Roaming Hub in any country and to have the roaming destinations of several networks, it is useful to assign several GTs to the Roaming Hub which become ‘Virtual’ in each one of the corresponding networks. Also, it is simpler to host several Roaming Hubs from different countries in a single place. This Roaming Hub has its own GT, as well as these ‘Virtual GTs’.

But the internal handling of the response to incoming TCAP transactions is very specific and is explained in this chapter.

CgPa is the SCCP Calling Party Address.

CdPa is the SCCP Called Party Address.

In Figure 5.1, the Roaming Hub is physically located in France, but is also logically in Gambia and Singapore with two virtual GTs.

In Gambia and Singapore, a GT address translation must be programmed so that the signals of the two VPLMNs addressing one of the two logical GTs are rerouted to the GT of the physical Hub in France. We will see that the address translation *must use* the ‘prefix method’ [5.2] so that the dialogue can be properly established between the RH and the VPLMN, *in the case of the multi-IMSI* service.

That is the case, in the example, if the mobile is visiting VPLMN#1 with an ‘auxiliary IMSI’ belonging to GSM Gambia.

This address translation *leaves the SCCP Calling Party Address (VPLMN#1) unchanged.*

5.2 TCAP Dialogue Implementation Constraints

5.2.1 TCAP Protocol Reminder

Reference [5.1] gives a brief introduction to TCAP. It is the Transaction protocol used in the SS7 stack and also in many other applications since it can use any other transport protocol.

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

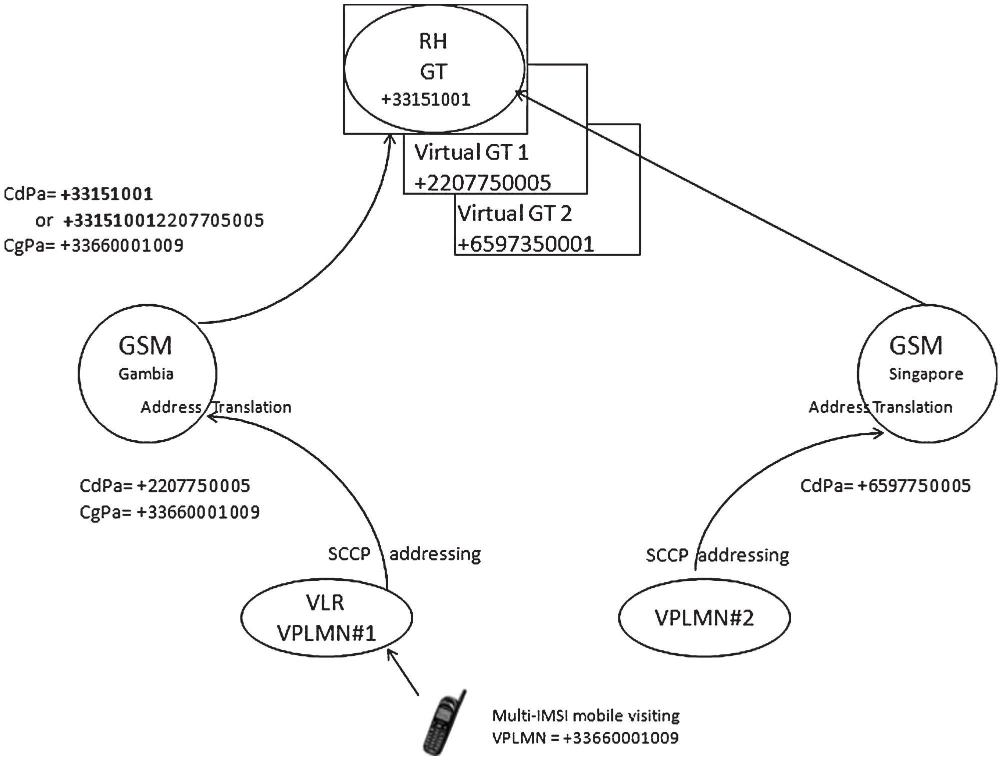


Figure 5.1 Principle of a hosted Roaming Hub with two virtual GTs

There are two types of information carried in TCAP transactions:

- Dialogue: this contains the application context, destination and origin references.
- Component: this contains the MAP or CAMEL messages.

There are three main types of TCAP transactions: BEGIN, CONTINUE and END as well as various ABORT or CANCEL transactions in case of errors.

The four Component types are as follows:

- Invoke: used to initialise a MAP or CAMEL transaction (see Chapter 2 for the complete list).
- Return Result: used to provide the result of the operation with all the parameters if successful.
- Return Error: returns the 'user error' in the case of unsuccessful completion by the distant system (example: unknown subscriber in a HLR).
- Reject: used to carry a system error, such as bad format, no response, etc.

5.2.2 TCAP Dialogue 'Segmentation'

Due to the fixed length limitation of SCCP messages, the session must use several SCCP blocks to perform an exchange. Below, each line corresponds to an SCCP message in either direction. AC means 'Application Context'.

Invoker side *Consumer side*

(a) SEND-ROUTING-INFO-FOR-SM Session

→ BEGIN + dialogue (AC) + component (SRI for SM)

SMSC HLR

← END + dialogue (AC) + component (SRI for SM ack)

(b) UPDATE-LOCATION

(1) → BEGIN + dialogue (AC) + component (Update Location)

VLR (2) ← CONTINUE + dialogue (AC) + component (1st INSERT) HLR

(3) → CONTINUE

(4) ← CONTINUE + component (2nd INSERT)

(5) → CONTINUE

(6) ← END + component (Update Location ack)

(c) SMS-MO (Long SMS)

This is the case of an SMS of 155 characters. The dialogue and component cannot be held in a single SCCP message, so the sending MSC will send a BEGIN with the dialogue but without the component, then send the component in a separate SCCP message using a CONTINUE (3).

(1) → BEGIN + dialogue (AC)

MSC (2) ← CONTINUE + dialogue (AC) SMSC

(3) → CONTINUE + component (FWD-SM-MO)

(4) ← END + component

(d) INITIAL DP

This is the main CAMEL message which is sent by the VMSC to the subscriber SCP when a prepaid customer initiates a call. It is a TCAP session with many messages, not all of which are all shown in the example below.

(1) → BEGIN + dialogue (AC) + component (IDP)

MSC/SSF (2)←CONTINUE+dialogue(AC)+component(Request Report BCSM Event) SCP

…

(3) → CONTINUE + component (Event report BCSM = answer)

(4) → CONTINUE + component (Event Report BCSM = disconnect)

(5) ← END + component (Release call)

TCAP protocol is such that, in any session, the *second SCCP message, and the others,* sent by the ‘invoker side’ is sent to the SCCP Called Party *received in the previous CONTINUE* from the ‘consumer side’ (HLR in example (b), SMSC in (c)), that is with the SCCP message (2) in example (b) and (c). So if BEGIN (1) is to +2207705005 Called SCCP (the Roaming Hub virtual GT) and the CONTINUE (2) is received from Calling Party +33151001, the CONTINUE (3) will be sent to +33151001, not the same Called Party as the BEGIN (1); *it will fail in general* because the *VPLMN does not necessarily* have roaming with the physical GT +33151001 of the Roaming Hub, only with the virtual GT +2207705005.

So the responding consumer side *must return* in the Calling Party Address of the CONTINUE, ((2) in example (b) and (c)), the *virtual GT that has been used by the invoker* in the BEGIN Called Party Address (a virtual GT).

But this Called Party Address was modified by the translation process (in Gambia or Singapore) and is not the GT of the Gambia Virtual Hub any more: it is the GT of the physical Roaming Hub in France.

Which GT address translation method will work for all cases, (virtual visitor or outbound subscriber virtual roaming)?

So that the Roaming Hub may determine the GT of the virtual Roaming Hub used and force it into the Calling Party GT, it sends the CONTINUE.

Note: this is a frequent problem with the sending of segmented, long SMSs when the receiving MSC does not have a proper TCAP setup.

Here another similar failure case is explained, but this concerns the CdPa PC, not the GT.

It is a long SMS case (> 120 characters) in MAP ≥ V2 (most frequent). The session must be 'segmented' because sending the TCAP dialogue and the component in a single SCCP block would be longer than the total maximum value (272 characters).

Invoker side *Consumer side*

FORWARD-SM-MT Session

→ BEGIN + dialogue (AC) + No component **sent to local GMSC**
SMSC MSC
← CONTINUE + dialogue (AC) in an SCCP message **whose Cg Pa includes the MSC PC** (it should not!)
→ CONTINUE + component (FORWARD-SM-MT) **sent to distant MSC PC (not to the local GMSC!)**
Message is lost because SMSC cannot route to this PC in a distant network.

This problem appears rather frequently with the incorrect setup of Siemens MSCs; they set their PC in the SCCP CgPa of the messages that they return when they receive a BEGIN. In order to cope with it, in general, the SCCP layer of the SMSC should have a function (not standard) *which takes out any PC in a SCCP CgPa.*

5.2.3 Different Methods for GT Address Translation in Roaming Hub Partners

This concerns the address translation method used by GSM Gambia or GSM Singapore in Figure 5.1.

5.2.3.1 First Method: Straight Address Translation to Real GT Roaming Hub

In Gambia and in Singapore we make a translation:

+220 775 0005 → +33151001
+659 735 0001 → +33151001

The called Party received by the RH is the same in both cases, and the SCCP Calling Party in the OPEN RSP is +33151001. So the FWD-SMS-MO would be sent to +33151001 which VPLMN#1 and VPLMN#2 do not necessarily have roaming with: therefore it would fail.

5.2.3.2 Use of the 'Prefix' Method (Hub Indicator HI)

Another 'prefix' method [5.2], later called the 'Hub Indicator' in [5.3], is to change the Called Party Address so the SCCP message is routed to the physical Roaming Hub, but such that the Called Party Address contains the Virtual GT address as an extension, so that it can be extracted by the Signalling End Point.

It is thus necessary to use this ‘Hub Indicator’ (HI = +33151001) method for the address translator.

+220 775 0005 → +33151001 2207750005
+659 735 0001 → +33151001 6597350001

(SCCP accepts an address of 22 digits).

The Roaming Hub then takes out its own HI from any received Called Party Address.

5.2.3.3 Comparison of the Two Methods

Assume the message from VPLMN#1 in Figure 5.1 is a long SMS-MO sent by a multi-IMSI roamer of Sierra Leone visiting France, which is then segmented as in (2) of example (c) of Section 5.2.2 and arrives at the physical RH. Only the dialogue of TCAP BEGIN is received, without any component as shown in Table 5.1.

There is nothing in the BEGIN received to tell which subscriber it is (no IMSI, no MSISDN).

So, the response CONTINUE sent by the Roaming Hub will be as shown in Table 5.2.

For the particular MAP message UPDATE_LOCATION, it would be possible to recover the Called Party Address from the IMSI. The case of a long, segmented SMS-MO sent by an outbound virtual roamer is the most general case, and the BEGIN may not have any component with parameters allowing the identification of which network the mobile belongs to.

So, the ‘prefix’ method for the Roaming Hub is mandatory for the multi-IMSI case.

5.2.3.4 Capabilities Required with the TCAP Programming Interface

The software must be capable of changing the Calling Party Address in the SCCP CONTINUE after it has received a BEGIN. Exercises 11.1 and 11.2 in Chapter 11 show the traces of a correct implementation. In Chapter 3, with multiple Point Codes in the Roaming Hub, we saw that it was also necessary to change the Point Code in the Calling Party Address so that it corresponds to the Roaming Hub Point Code concerned.

Table 5.1 Straight address translation to Real GT Roaming Hub

	1st Method	2nd Method ‘prefix’
Calling Party Address	+3366001009	+33660010009
Called Party Address	**+33151001**	**+33151001**2207750005

Table 5.2 Use of the Prefix Method (Hub Indicator HI)

	1st Method	2nd Method ‘prefix’
FWD-SM-MO sent from +3366001009	**To: +33151001** (fail: there is no roaming of +3366001009 with +33151001)	To: +220750005 OK

References and Further Reading

[5.1] Henry-Labordère, A. and Jonack, V., 'SMS and MMS interworking in mobile networks', Chapters 1 and 2, Artech Publishing House, 2004.

[5.2] Henry-Labordère, A., 'Système de reroutage optimal de messages courts d'un centre de messages vers un autre avec traduction globale d'adresse', Brevet FR 02 09 667.

[5.3] GSMA OC IRHG Doc 5_007: 'Technical Architecture Alternatives for Open Connectivity Hubbing Model'.

6

Location-based Services and Virtual Roaming

– Quels sont ces gens dont nous étudierons les déplacements ?
– A leur désignation C120, C88, A37 ce sont visiblement des agents secrets dont on veut controler les allées et venues. Du reste, je n'en sais pas beaucoup plus que vous là-dessus. On m'a recommandé le secret sous peine de haute trahison.

– Who are these people whose movements we will study?
– Their names, C120, C88 and A37, clearly suggest that they are secret agents whose comings and goings must be controlled. In fact, I do not know any more about them than you do. I was told the secret subject to the penalty for high treason.

'La parcelle Z', Jacques Spitz, 1942, J. Vigneau, editor

Jacques Spitz (a French engineer from Ecole Polytechnique and a science fiction writer) was telling the story of a somewhat jealous inventor who wanted to follow the movements of his young wife. He extracted a living cell of the 'target' and inserted it between two glass plates in a biological liquid. The 'Z cell' then followed her wanderings remotely with the help of science fiction explanations. Nowadays, the 'Z cell' is the handset carried by three billion mobile customers worldwide. The story does not finish well; his wife was not unfaithful at all (she was visiting her old mother and not her lover) but jealousy kills her in the end.

There are now more useful applications (LBS) for the times when a mobile customer needs to use their location for information. In the case of virtual roaming, the HPLMN may wish to provide its outbound subscribers with their usual LBS. They can be MO-LR (initiated by the mobile, for example to obtain its own location and pass it to a GMLC (Gateway Mobile Location Centre), or MT-LR (initiated by the network) where the request is initiated by the GMLC. Ideally the service should be used for 2G subscribers with legacy handsets (no GPS) to have a wide commercial availability.

6.1 Traces Show How an SMLC Really Works

This book is certainly not the first to explain A-GPS and other methods, but it is unique in giving traces which really explain 'how it works' to engineers who develop SMLCs or want to assess the capabilities of a product. It becomes easier to understand how an SMLC knows whether a handset is GPS-equipped

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

or if an alternative method, such as E-OTD or ‘Measurement Reports’ should be used. The fast and accurate mathematical algorithm applicable to ‘circle intersections’ (TA + Measurements method) and also ‘hyperbola intersections’ (E-OTD method) is given as a reference, [5.1] Chapter 13, with execution traces if one wants to reuse it.

It also makes clear that a Roaming Hub can provide a centralized LBS service for customers with the prerequisite setup in the VPLMNs.

The problem of being able to obtain one’s own outbound subscriber location in a VPLMN has only two solutions:

(1) ‘Spyware measurements’ in the handset; they include two methods:
   - **Java applets in the handset itself:** this method is used by web-based servers, those of the HPLMN itself or those from a 3rd party such as the ‘Google MAP’ service (one connects to their site and obtains a MAP centred at the estimated location).
   - **SIM Tool Kits in the SIM card:** the ‘spyware in the SIM card’. It is reserved for the HPLMN which obtains measurements *from the mobile itself* and must have available the map of BTS locations or Cell Ids to compute a location. This is very difficult but Google has obtained this map partially, either from cooperative HPLMNs and/or by survey campaigns. It allows the use of the ‘Extended Cell ID’ method where Timing Advance and Measurements to adjacent BTSs provide a better accuracy than just the cell. A SIM Tool Kit must be installed in the cards; this will also be explained under ‘SIM Tool Kit’ methods.

(2) **Network MAP-based methods for obtaining location:** the VPLMN has an MLC (Mobile Location Centre) and allows its HPLMN partners to access it *through the two specialized MAP services* (MAP Location Service Enquiry package):
   - MO-LR: SUBSCRIBER LOCATION REPORT: the Visited MSC sends the location to the GMLC in the HPLMN.
   - MT-LR: PROVIDE LOCATION INFORMATION: the GMLC in the HPLMN requests the location from the VPLMN MLC.

   Note that even if the MO-LR function exists in the BSSAP protocol to trigger a ‘Perform Location Request’, no common handset has it in a menu. So it is triggered by various means: SMS-MO, data connection and use of a Java applet which reads the GPS position, etc. As it impacts the virtual Roaming Hub, the specifics of these MAP-based methods will be explained.

We will also explain the architecture of a simple SMLC so it can be installed in small VPLMNs and *does not need to have the BSSAP-LE protocol in the MSC or the MAP Location Service Enquiry Package* which are charged for by the NSS vendors. If a Virtual Roaming Hub service exists, and if the VPLMN has an MLC, the Virtual Roaming Hub will be able to allow the HPLMN’s GMLC to access it even if this MAP package is not available. Many layered protocols are used, making the development of an SMLC a very demanding project:

- MAP/TCAP;
- BSSAP-LE/SCCP Connection Oriented (GSM 49.031);
- BSSLAP (GSM 48.071);
- Radio resource LCS Protocol (GSM 44.031).

Some decoding of responses is required, necessitating the use of other protocols to obtain the details.

This chapter is really for the developers of an SMLC; with the traces and the references, it is quite possible to develop your own SMLC software.

6.2 ‘Spyware Measurements’ in the Handset

These can be obtained by:

- spyware (java applet or proprietary OS) in the handset itself;
- spyware in the SIM card.

They can use:

- the GPS position (if available);
- the Cell ID and Measurements to the neighbouring BTS made by the handset.

6.2.1 Spyware in the Handset (Java Applet or Proprietary OS)

This is what is involved when you load the 'Google MAP' application: a java applet or proprietary OS (e.g. Nokia Symbian '.sisx', Microsoft '.cab') is installed in the handset which can access the GPS position, if available, or the measurements as explained below. It is easy for the server to know the type of spyware to load because it gets the model type in the 'HTTP GET' parameters when the handset connects to the server with the HTTP protocol.

When one connects to the 'Google MAP' application, the server can read the above data and estimate a position (if GPS is available, it is quite accurate (20 m)). We will explain the way such servers can use customer traffic to find the Cell ID Map *without* needing to perform a full survey. The companies have performed limited surveys in certain countries and cities and promote this 'legend'; in fact, *the traffic itself and the ergonomics allow a statistically accurate worldwide Map of the cells to be obtained.*

With this 'spyware', whenever a customer is connected to the server, their position can be read and used for any legal purpose.

6.2.2 How a Location Server Can 'Automatically' Learn the Map of the Cells

When the handset is connected to the MAP application server, if it is GPS equipped and in an open space, one gets a map accurately centred at the correct location: it uses the GPS position read by the server in the handset and *also reads the serving Cell ID*! Therefore a worldwide survey is fairly quickly done by the mobile users themselves.

If there is no GPS available, the server can also read the serving Cell ID in the handset and, if it knows the location of the centre of the cell, uses it as an estimate for the centre of the Map that it displays with the accuracy estimate (500 m for example).

If the Cell ID is unknown, but the LAC centre is known (a LAC is a group of BTSs which include tens of Cell IDs and the LAC may cover half a medium city and its surroundings), the server will give a large scale Map. But the customer zooms in when they want to get more accurate information, and this zooming is used by the server to match the unknown Cell ID location with the final zoom position. As more users make searches for the same area, the information can be statistically improved without any demand on the networks concerned! This is a most clever approach (*which can be logically deduced from the tests of their service)* and which is usable only if there is a large number of users whose 'mapping cooperation' is obtained without them being asked explicitly.

No doubt that limited local surveying improves the service and the marketing presentation but it is really not useful.

To add automatic identification of the BTS locations *and their power level*, and to be able to use the networks' measurements, is a huge mathematical problem. This is why, in most cases, these servers only give a 'Cell ID' position (accurate to a few hundred metres in a city) in the absence of usable GPS.

6.2.3 Spyware in the SIM Tool Kit Methods for MT-LR

With this approach, there is no need for a MAP Location Service Enquiry package or BSSAP-LE.

A SIM Tool Kit is installed in the cards. It is triggered by the reception of a particular 'mute' SMS-MT received from the HPLMN. The SIM card must have access to the 'AT-commands' (the service is declared in the SST file of the SIM card), which allow it to obtain the 'Cell Environment description'. Following the same data flow as for an OTA SIM download or upload, the STK will return this 'Cell environment' to the HPLMN and the HPLMN will make the computation if it has the location of the BTS and its cell coverage in the VPLMN.

6.2.4 Syntax of the AT Command Sent by the STK or the Java Applet for the 'Cell Environment'

A standard AT command, or a vendor command for specific handsets, can be used to get the GPS position or the cell environment. We give the details of the cell environment to show there is no difference to what we have in the measurements obtained remotely by the SMLC through the BSC.

6.2.4.1 Syntax (Wavecom Modem GSM)

Table 6.1 shows the AT commands to read the location measurements of a handset.

Command syntax: AT = CCED + <mode> [, <request dump>].

6.2.4.2 Result of Direct Handset-based Measurements with AT Commands

(1) Main cell: MCC, MNC, LAC, CI, Base Station Id Code, BCCH Freq (absolute), RXLEVEL, RXLEVEL Full, RXLEVEL Sub, RxQual, RxQualFull, RxQual Sub, Idle TS.
(2) Neighbour1 to Neighbour6: MCC, MNC, LAC, CI, Base Station Id Code, BCCH Freq (absolute), RXLEVEL.
(3) One Timing Advance (TA) to servicing BTS: indicates distance in units of 1100 m (e.g. **1**).

If the 'measurements to the Neighbour BTSs', which are made locally by the Handset, are compared with the 'TA Response' of the SMLC, one can see that we have the plain cell_ID (e.g. **208,20,0032,0418**) for Neighbour #1

The Neighbour Base Stations can belong to networks other than the VPLMN in which the handset is currently registered!

6.2.4.3 Comparison with Network-based Measurements Made through the BSC

In Section 6.4 we explain the principle of an SMLC using the TA method, which reads the measurements of the handset *from the BSC, which already has them from the previous 'paging'*. We get the

Table 6.1 AT commands to read the location measurements of a handset

Command	Possible responses
AT+CCED = 0,3 (main cell and neighbours 1 to 6): you can see MCC, MNC sequences (here 208,10 (SFR) and 208,20 (Bouygues), 208,01 (Orange))	**208,20,523,62120**, 37,706,24,,,0,,,0 208,20,0032,0418, 37,835,20, 208,01,65533,12418,37,831,12, 208,10,1349,1201, 34,818,13, 208,20,0006,9899, 39,713,9, 208,20,0002,0172, 33,711,12, 208,20,0101,31425, 36,824,10, **1**

'BaseStation Id Code' in the 'Measurement Report' parameter below (for which additional mapping data are required if a HPLMN wants to use them), and may also have the Cell ID ('Neighbour Cell Identity List') in the same way as when the measurements are made by the handset.

(1) Timing Advance
  15
(9) Cell Identity
  208,20,523,62120
(11) Neighbour Cell Identity List
  208.20.0032.0418
  208.01.65533.12418
  etc. (in the same order as for the Measurement Report)
(20) Measurement Report (GSM 44.008)
Serving cell: BA-USED 1 DTX-USED 1 RXLEVEL-FULL-SERVING-CELL 35 MEAS-VALIS 1 RXLEVEL-SUB-SERVING-CELL 36 RXQUAL-FULL-SERVING-CELL 1 RXQUAL-SUB-SERVING-CELL 3 NO-NCELL 3
Neighbour cell# 1 RXLEVEL 26 BSSH-FREQ 31 Base Station Id Code 23
Neighbour cell# 1 RXLEVEL 40 BSSH-FREQ 04 Base Station Id Code 35
Neighbour cell# 2 RXLEVEL 57 BSSH-FREQ 01 Base Station Id Code 24
Neighbour cell# 2 RXLEVEL 56 BSSH-FREQ 10 Base Station Id Code 03
Neighbour cell# 3 RXLEVEL 13 BSSH-FREQ 02 Base Station Id Code 32
Neighbour cell# 3 RXLEVEL 09 BSSH-FREQ 09 Base Station Id Code 12

The data that can be used are exactly the same as when the measurement is made directly from the handset with AT commands.

So the STK method is rather popular because it is simple (if one has a way of getting the cell and BTS map, not only of the partners' network but also the others because the handset obtains measurements to all).

6.2.4.4 Computation of Mobile Location Estimate with TA and Measurement Reports

This method is the most accurate if no GPS or Time Of Arrival (TOA) is used.

By some standard propagation model using the RXLEVELs and the power of the transmitter known for the various BTSs, the RXLEVELs are converted to distances to the BTS. This, to be accurate, requires that the VPLMN provides the full data on its Radio Network. The Timing Advance is readily converted to a distance to the Serving BTS. So the location estimate is the point closest to circles centred on the serving (TA) and the neighbouring BTS (RXLEVEL conversion to distance). This is shown in Figure 6.1.

The SMLC uses the 'Resultant and the Sturm method' [5.1] Chapter 13, which computes the position in the case of 'hyperbolic triangulation'. We use exactly the same method here to minimize the sum of the squares of the distance to the various *circles* centred at the BTS #i with centres X_i, Y_i and radius R_i. The equation of each circle is:

$$P_i(X, Y) = (X - X_i)^2 + (Y - Y_i)^2 - R_i^2$$

A best estimate, if there are several BTS measurements, is to try to find a point close to all the circles (if we have a point X,Y on the circle $P_i(X,Y) = 0$). As all the circles will not intersect exactly, the appropriate functional for the mobile location is to minimize the sum of the squares, so that negative and positive values are equally important for all the P_i. The functional is:

$$\underset{X,Y}{\text{Min}}\ Q(X, Y) = \sum P_i^2(X, Y)$$

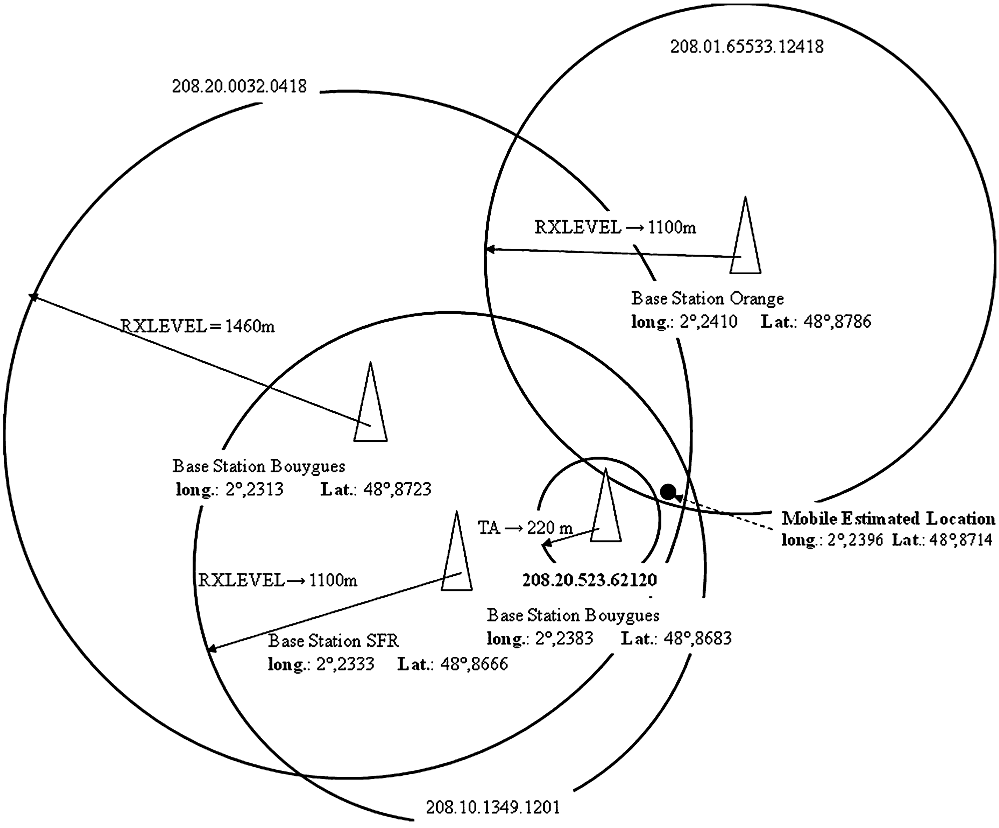


Figure 6.1 Location estimate with handset or network-based measurements; use of TA AND Measurement Reports

This is a non-constraint optimization problem; the minimization of a 4th degree polynomial. We look for the point which minimizes the equation. The results are given in the annex of this chapter and are displayed in Figure 6.1. This is the method we prefer because a greater precision is reached in a given amount of computations, while a brute force Monte Carlo method (randomly taking locations and evaluating the functional) may take a long time, with only a probabilistic value of the uncertainty.

In the case of E-OTD (see Section 6.6), ‘hyperbola intersections’ are used. It is the same optimization problem for each hyperbola (determined by a pair of BTSs, each of the two ‘loci’ of the hyperbola, and a time difference), P_i (X,Y) being a second degree equation with a ‘nonpositive definite’ matrix (it is ‘positive definite’ for an ellipse or a circle). The same algorithm is applied to the minimization of the resulting functional Q(X,Y).

6.2.4.5 Use of Timing Advance (TA) Only

This is a much less accurate method provided by certain SMLC versions (e.g. Alcatel-Lucent) but it is very simple in terms of algorithms. As shown in Figure 6.2, the position is estimated centred along the direction of the serving antenna (defines a 120° sector if the BTS has such directional sectors) at a distance given by the Timing Advance value × 1100 metres.

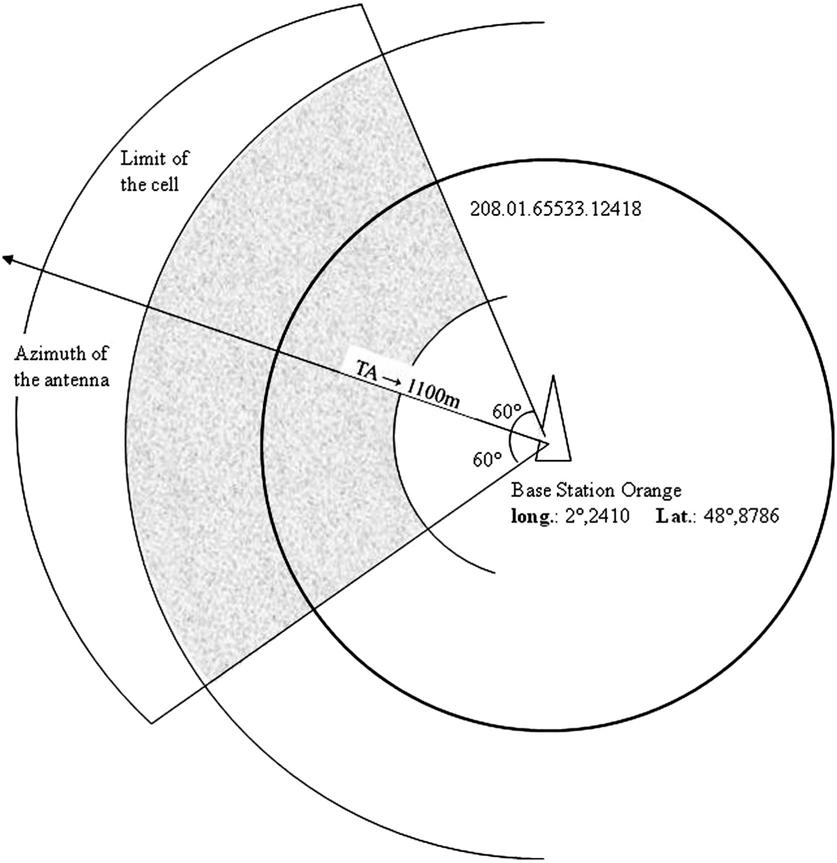


Figure 6.2 Location estimate; use of TA only

The darker area shows the uncertainty, because Timing Advance measurements are ±550 m compared with the accuracy of the previous method which makes use of the 'measurement reports', which give the distance to the *neighbouring* BTS.

6.3 Network MAP-based Location Obtaining Methods: Prerequisites

They assume [6.3] that an SMLC exists which does the location computation; the MAP services simply allow the reading of the result. *It works only if there is an MLC, and if the MSC has the Location Service Enquiry package* (MAP). Also, the BSCs must have the BSSAP-LE stack [6.2].

There are two architectures applicable to GSM networks (handsets are called MS) and UMTS (handsets are called UE, and RNC replaces BSC):

- NSS-based SMLC: the MSCs must have the BSSAP-LE stack and *the MLC could be hosted outside the VPLMN.*
- BSS-based SMLC: there is no need to have BSSAP-LE in the MSCs but the MLC must be in the VPLMN as it will communicate directly with the BSCs.

For a 'Network Initiated location request', a GMLC (Gateway Mobile Location Centre) interrogates the Visited MSC with a MAP PROVIDE SUBSRIBER LOCATION and gets back the 'Geographic Location' in the Acknowledgement.

6.3.1 Location Alerts and Mobile Originating Location Request (MO-LR)

This is for the 'location alert' service: when customers are in the vicinity of a Point of Interest, a Location Request can be sent by the handset.

This is *not important in practice* because few handsets have the function to generate a CM Service Request 'Perform Location Request' from a user menu, but it is included in the standards. So we include it to explain the concept.

The VMSC must have the BSSAP-LE package and the MAP Application Context 'location service enquiry'. It does limit the scope as few virtually visited networks will have it.

The following procedure allows an MS to request either its own location, or location assistance data from the network. Location assistance data may be used subsequently by the MS to compute its own

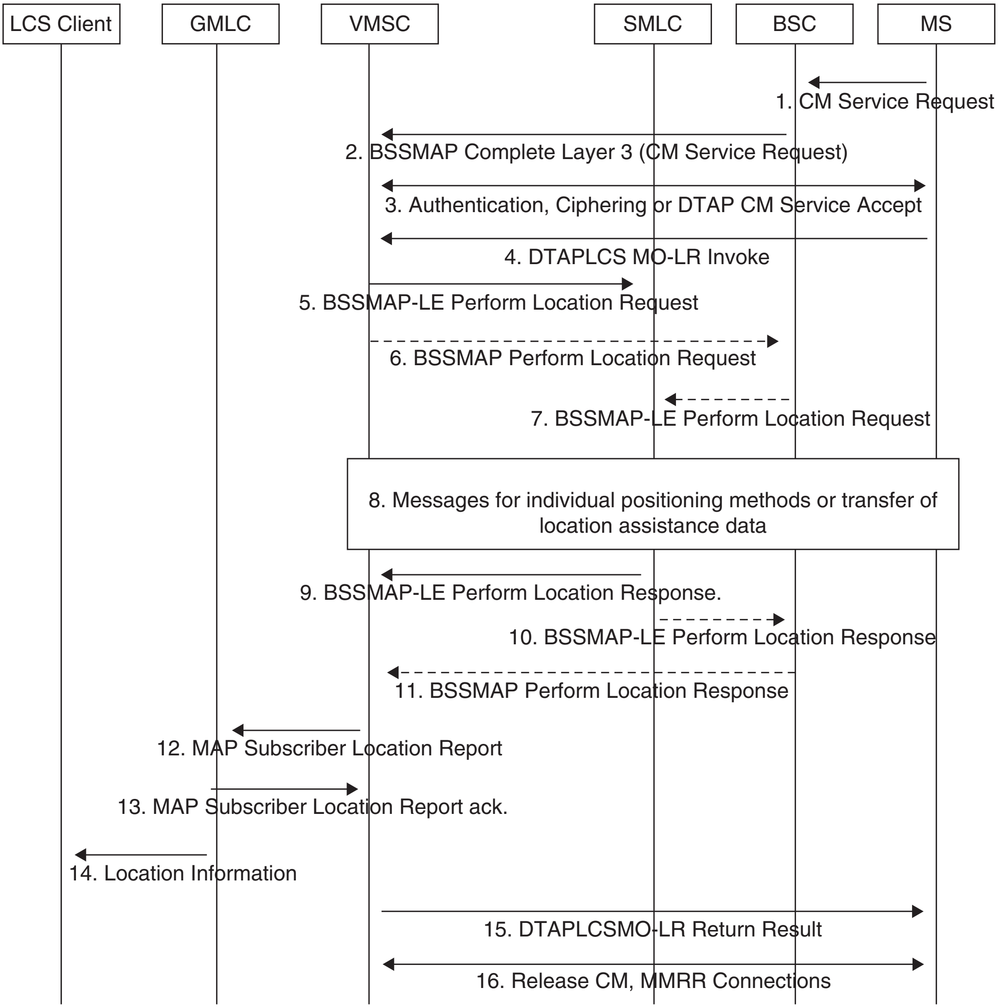

LCS Client
GMLC
VMSC
SMLC
BSC
MS
1. CM Service Request
2. BSSMAP Complete Layer 3 (CM Service Request)
3. Authentication, Ciphering or DTAP CM Service Accept
4. DTAPLCS MO-LR Invoke
5. BSSMAP-LE Perform Location Request
6. BSSMAP Perform Location Request
7. BSSMAP-LE Perform Location Request
8. Messages for individual positioning methods or transfer of location assistance data
9. BSSMAP-LE Perform Location Response.
10. BSSMAP-LE Perform Location Response
11. BSSMAP Perform Location Response
12. MAP Subscriber Location Report
13. MAP Subscriber Location Report ack.
14. Location Information
15. DTAPLCSMO-LR Return Result
16. Release CM, MMRR Connections

Figure 6.3 Obtaining MAP location: LR-MO

location throughout an extended interval using a mobile-based position method. The ciphering key enables the MS to decipher other location assistance data broadcast periodically by the network. The MO-LR, after a location update request, may be used to request ciphering keys or GPS assistance data using the follow-on procedure described in [6.10]. The procedure may also be used to enable an MS to request that its own location be sent to another LCS client.

6.3.1.1 Location Preparation Procedure

(1) The MS requests an SDCCH and sends a DTAP CM service request, indicating a request for call-independent supplementary services, to the BSC, with an SS-code = all MO-LR.

(2) The BSC includes the current Cell ID and TA value within the BSSMAP Complete Layer 3 Information message used to convey the CM service request across the A interface. If the MS is, instead, in dedicated mode, the MS sends a DTAP CM Service Request on the already established SACCH: the VMSC will then already have been supplied with the current Cell ID from either the serving BSC or serving MSC in the case of an established call with MSC-MSC handover.

(3) The VMSC instigates authentication and ciphering if the MS was in idle mode, or returns a DTAP CM Service Accept if the MS was in dedicated mode. If the target MS supports any MS-based or MS-assisted positioning method(s), the MS will provide the BSC and MSC with the positioning method(s) it supports via controlled early classmark sending (see [6.10] and [6.6]).

(4) The MS sends a DTAP LCS MO-LR invoke to the VMSC. If the MS is requesting its own location or that its own location be sent to another LCS client, this message carries LCS QoS information (e.g. accuracy, response time). If the MS is requesting that its location be sent to another LCS client, the message will include the identity of the LCS client and may include the address of the GMLC through which the LCS client should be accessed. If a GMLC address is not included, the VMSC may assign its own GMLC address and may verify that the identified LCS client is supported by this GMLC. If a GMLC address is not available for this case, the VMSC will reject the location request. If the MS is, instead, requesting location assistance data or ciphering keys, the message specifies the type of assistance data or deciphering keys and the positioning method for which the assistance data or deciphering applies. The VMSC verifies in the MS's subscription profile that the MS has permission to request its own location, request that its location be sent to another LCS client or request location assistance data or deciphering keys (whichever applies). If the MS is requesting positioning and has an established call, the VMSC may reject the request for certain nonspeech call types.

(5) The VMSC sends a BSSMAP-LE PERFORM LOCATION request message to the SMLC associated with the MS's current cell location if the SMLC is NSS based (Table 6.2). This message is transported using SCCP connection-oriented signalling inside an SCCP Connection Request message. The BSSMAP-LE message indicates whether a location estimate or location assistance data is requested and includes the MS's location capabilities and current Cell ID. If the MS's location is requested, the message also includes the currently assigned radio channel type (SDCCH, TCH-FR or TCH-HR), the requested QoS and, if available, any location measurement information including the TA value received from the BSC in step (2). If location assistance data is requested instead, the message carries the requested types of location assistance data.

(6) If the SMLC is BSS based, the VMSC instead sends the BSSMAP PERFORM LOCATION message to the serving BSC for the target MS.

(7) In the case of a BSS-based SMLC, the BSC forwards the BSSMAP-LE PERFORM LOCATION request received in step (6) to the SMLC. If the MS's location is requested, the BSC may add additional measurement data to the message to assist with positioning. The message is transported inside an SCCP connection request.

Table 6.2 Content of a BSSAP-LE Perform Location Request received by the SMLC

Information Element	Purpose	Example
Message Type	Code of PERFORM LOCATION REQUEST	43 (code of this operation)
Location Type	Type of location being requested	0 (current location)
Cell Identifier	Current location Cell-ID of the target handset	605.3.1234.5678
Classmark Information Type 3	Tells if handset is GPS equipped or supports E-OTD	See [6.10] MS Classmark 3 Information element and trace in Section 6.4.4.2
LCS Client Type	–	Emergency service
Chosen Channel	Type of Radio channel used by the handset	–
LCS Priority	Priority of the Location Request	–
LCS QoS	Required Quality of Service	Horizontal and vertical accuracy
GPS Assistance Data	If present, this is another way of knowing that the handset is GPS equipped and which assistance data it requires (absolute time, satellite ephemeris, etc.)	The handset asks for Reference Time requested, Identity of the visible satellite to be used, etc.
BSSAP APDU	Additional measurements available (TA may be directly available)	–

6.3.1.2 Positioning Measurement Establishment Procedure

(8) If the MS is requesting its own location, the actions described under step (10) for an MT-LR are performed. If the MS is instead requesting location assistance data, the SMLC transfers this data to the MS as described in subsequent sections. The SMLC determines the exact location assistance data to transfer according to the type of data specified by the MS, the MS location capabilities and the current Cell ID.

6.3.1.3 Location Calculation and Release Procedure

(9) When a location estimate best satisfying the requested QoS has been obtained or when the requested location assistance data has been transferred to the MS, the SMLC returns a BSSMAP-LE Perform Location response to the VMSC if the SMLC is NSS based. This message carries the location estimate or ciphering keys if these were obtained. If a location estimate or deciphering keys were not successfully obtained, or if the requested location assistance data could not be transferred successfully to the MS, a failure cause is included in the Perform Location response.

(10) For a BSS-based SMLC, the BSSMAP-LE Perform Location response is instead returned to the serving BSC.

(11) In the case of a BSS-based SMLC, the BSC forwards the BSSMAP PERFORM LOCATION response received in step (10) to the VMSC.

(12) If the MS requested transfer of its location to another LCS client and a location estimate was successfully obtained, the VMSC will send a MAP Subscriber Location Report to the GMLC obtained in step (4) carrying the MSISDN of the MS, the identity of the LCS client, the event causing the location estimate (MO-LR) and the location estimate and its age.

(13) The GMLC will acknowledge receipt of the location estimate provided that it serves the identified LCS client and the client is accessible.

(14) The GMLC transfers the location information to the LCS client either immediately or upon request from the client.

(15) The VMSC returns a DTAP LCS MO-LR Return Result to the MS, carrying any location estimate requested by the MS, ciphering keys or a confirmation that a location estimate was successfully transferred to the GMLC serving an LCS client.
(16) The VMSC may release the CM, MM and RR connections to the MS, if the MS was previously idle, and the VMSC may record billing information.

6.3.2 Network Initiated Location Request (MT-LR)

The GMLC in the HPLMN is requesting the location.

Figure 6.4 illustrates general network positioning for LCS clients external to the PLMN. In this scenario, it is assumed that the target MS is identified using either an MSISDN or IMSI.

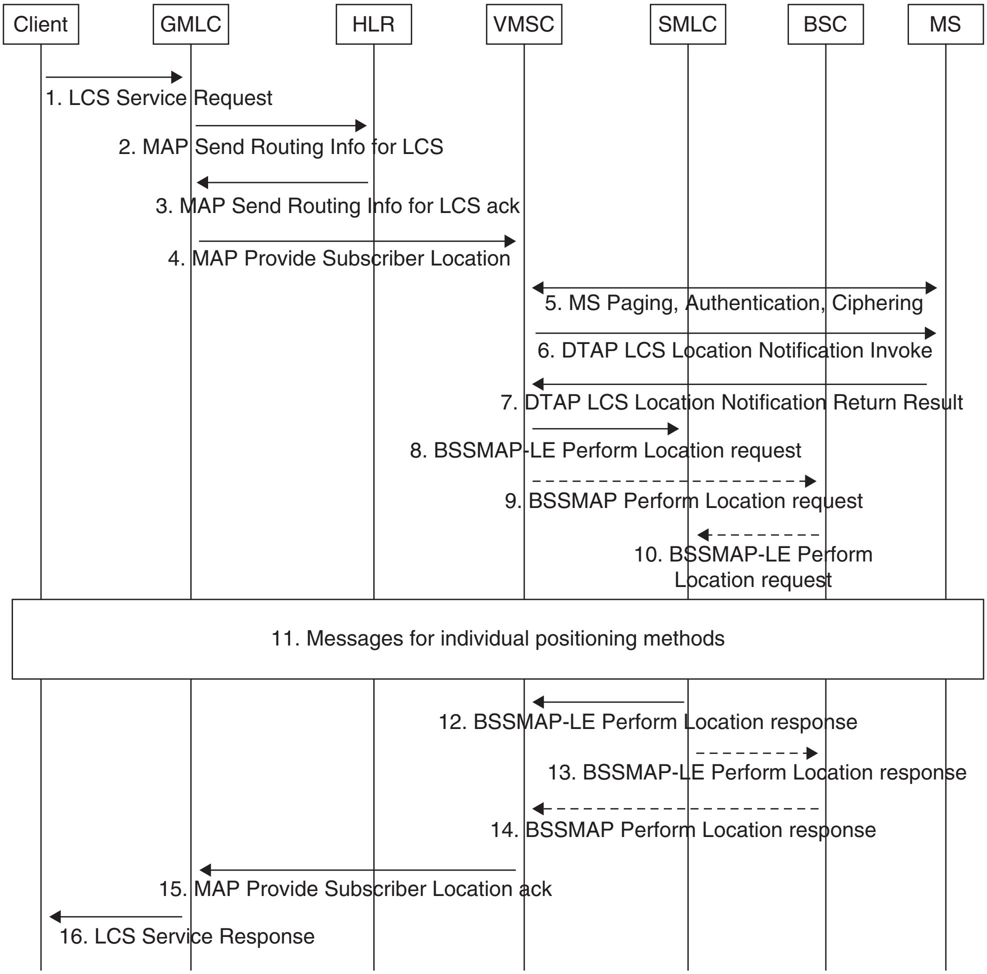

Client
GMLC
HLR
VMSC
SMLC
BSC
MS
1. LCS Service Request
2. MAP Send Routing Info for LCS
3. MAP Send Routing Info for LCS ack
4. MAP Provide Subscriber Location
5. MS Paging, Authentication, Ciphering
6. DTAP LCS Location Notification Invoke
7. DTAP LCS Location Notification Return Result
8. BSSMAP-LE Perform Location request
9. BSSMAP Perform Location request
10. BSSMAP-LE Perform Location request
11. Messages for individual positioning methods
12. BSSMAP-LE Perform Location response
13. BSSMAP-LE Perform Location response
14. BSSMAP Perform Location response
15. MAP Provide Subscriber Location ack
16. LCS Service Response

Figure 6.4 General Network Positioning for an MT-LR

6.3.2.1 Location Preparation Procedure

(1) An external LCS client requests the current location of a target MS from a GMLC. The GMLC verifies the identity of the LCS client and its subscription to the LCS service requested and derives the MSISDN or IMSI of the target MS to be located and the LCS QoS from either subscription data or data supplied by the LCS client. For a call-related location request, the GMLC obtains and authenticates the called party number of the LCS client. If a location is required for more than one MS, or if periodic location is requested, steps (2) to (12) below may be repeated.

(2) If the GMLC already knows both the VMSC location and IMSI for the particular MSISDN (e.g. from a previous location request), this step and step (3) may be skipped. Otherwise, the GMLC sends a MAP_SEND_ROUTING_INFO_FOR_LCS message to the home HLR of the target MS to be located with either the IMSI or MSISDN of this MS.

(3) The HLR verifies that the SCCP calling party address of the GMLC corresponds to a known GSM network element that is authorized to request MS location information. The HLR then returns the current VMSC address and whichever of the IMSI and MSISDN was not provided in step (2) for the particular MS.

(4) The GMLC sends a MAP_PROVIDE_SUBSCRIBER_LOCATION message to the VMSC indicated by the HLR. This message carries the type of location information requested (e.g. current location), the MS subscriber's IMSI, LCS QoS information (e.g. accuracy, response time) and an indication of whether the LCS client has the override capability. For a call-related location request, the message also carries the LCS client's called party number. The message may optionally carry the identity of the LCS client.

(5) If the GMLC is located in another PLMN or another country, the VMSC first authenticates that a location request is allowed from this PLMN or from this country. If not, an error response is returned. If the target MS has an established circuit call other than speech, the location request may be denied and an error response is then returned to the GMLC. If the location request is allowed for a nonspeech circuit call, it will be up to the SMLC to decide, on the basis of the applicable position methods and requested QoS, whether positioning is possible. The VMSC then verifies LCS barring restrictions in the MS user's subscription profile in the VLR. In verifying the barring restrictions, barring of the whole location request is assumed if any part of it is barred or any requisite condition is not satisfied. If LCS is to be barred without notifying the target MS, and an LCS client accessing a GMLC in the same country does not have the override capability, an error response is returned to the GMLC. Otherwise, if the MS is in idle mode, the VLR performs paging, authentication and ciphering. This procedure will provide the MS user's current Cell ID and certain location information that includes the TA value in the BSSMAP Complete layer 3 information used to convey the Paging Response. If the target MS supports any MS-based or MS-assisted positioning method(s), the MS will also provide the BSC and MSC with the positioning method(s) it supports via controlled early classmark sending (see [6.10] and [6.6]). If the MS is, instead, in dedicated mode, the VMSC will already have any early classmark information and will have been supplied with the current Cell ID from either the serving BSC or serving MSC in the case of an established call with MSC-MSC handover.

(6) If the location request comes from a value-added LCS client and the MS subscription profile indicates that the MS must either be notified or notified with privacy verification and the MS supports notification of LCS (according to the MS Classmark 2), a DTAP LCS Location Notification Invoke message is sent to the target MS indicating the type of location request (e.g. current location), the identity of the LCS client and whether privacy verification is required. Optionally, the VMSC may, after sending the DTAP LCS Location Notification Invoke message, continue in parallel the location process, i.e. continue to step (8) without waiting for a DTAP LCS Location Notification Return Result message in step (7).

(7) The target MS notifies the MS user of the location request and, if privacy verification was requested, the target MS indicates to the MS user whether the location request will be allowed or not allowed in the absence of a response and waits for the user to grant or withhold permission. The MS then returns a DTAP LCS Location Notification Return Result to the VMSC indicating, if privacy verification was requested, whether permission is granted or denied. Optionally, the DTAP LCS Location Notification Return Result message can be returned some time after step (6), but before step (15). If the MS user does not respond after a predetermined time period, the VMSC will infer a 'no response' condition. The VMSC will return an error response to the GMLC if privacy verification was requested and either the MS user denies permission or there is no response, with the MS subscription profile indicating barring of the location request in the absence of a response.

(8) The VMSC sends a BSSAP-LE PERFORM LOCATION message to the SMLC associated with the MS's current cell location if the SMLC is 'NSS based'. The BSSMAP-LE message includes the type of location information requested, the MS's location capabilities and currently assigned radio channel type (SDCCH, TCH-FR or TCH-HR), the requested QoS and the current Cell ID and, if available, any location information including the TA value received in step (5).

(9) If the SMLC is BSS based, the VMSC instead sends the BSSMAP PERFORM LOCATION message to the serving BSC for the target MS.

(10) In the case of a BSS-based SMLC, the BSC forwards the BSSMAP-LE PERFORM LOCATION request received in step (9) to the SMLC. The BSC may add additional measurement data to the message to assist with positioning. The message is transported inside an SCCP connection request.

6.3.2.2 Positioning Measurement Establishment Procedure

(11) If the requested location information and the location accuracy within the QoS can be satisfied by the reported Cell ID and, if available, TA value, the SMLC may send a MAP_PERFORM_LOCATION ack immediately. Otherwise, the SMLC determines the positioning method and instigates the particular message sequence for this method, defined in subsequent sections. If the position method returns position measurements, the SMLC uses them to compute a location estimate. If there has been a failure to obtain position measurements, the SMLC may use the current Cell ID and, if available, TA value to derive an approximate location estimate. If an already computed location estimate is returned for an MS-based position method, the SMLC may verify consistency with the current Cell ID and, if available, TA value. If the location estimate so obtained does not satisfy the requested accuracy or the location attempt failed, e.g. due to missing data, and sufficient response time still remains, the SMLC may instigate a further location attempt using the same (e.g. providing more assistance data to MS) or a different position method. If a vertical location coordinate is requested but the SMLC can only obtain horizontal coordinates, these may be returned.

6.3.2.3 Location Calculation and Release Procedure

(12) When location information best satisfying the requested location type and QoS has been obtained, the SMLC returns it to the VMSC in a Perform Location response if the SMLC is NSS based. If a location estimate could not be obtained, the SMLC returns a Perform Location response containing a failure cause and no location estimate.

(13) For a BSS-based SMLC, the location information is instead returned to the serving BSC.

(14) In the case of a BSS-based SMLC, the BSC forwards the BSSMAP PERFORM LOCATION response received in step (13) to the VMSC.

(15) The VMSC returns the location information and its age to the GMLC, if the VMSC has not initiated the Privacy Verification process in step (6). If step (6) has been performed for privacy verification, the VMSC returns the location information only, if it has received a DTAP LCS Location Notification Return Result indicating that permission is granted. If a DTAP LCS Location Notification Return Result message indicating that permission is not granted is received, or there is no response with the MS subscription profile indicating barring of location in the absence of a response, the VMSC will return an error response to the GMLC. If the SMLC did not return a successful location estimate, but the privacy checks in steps (5) to (7) were successfully executed, the VMSC may return the last known location of the target MS if this is known and the LCS client is requesting the current or last known location. The VLR may then release the Mobility Management connection to the MS, if the MS was previously idle, and the VMSC may record billing information.

(16) The GMLC returns the MS location information to the requesting LCS client. If the LCS client requires it, the GMLC may first transform the universal location coordinates provided by the VMSC into some local geographic system. The GMLC may record billing for both the LCS client and inter-network revenue charges from the VMSC’s network.

6.3.3 Changes in the VLR Profile for LBS for Virtual Roaming

The two above cases assume that the visitor is allowed to use the local VPLMN SMLC and the list of authorized GMLCs is in the VLR profile received from the HLR in the HPLMN. But with virtual roaming, the requesting GMLC for an MT-LR must be the GT of the Roaming Hub. The original profile, if there was bilateral roaming and if the VPLMN had granted access to its SMLC, would be:

MSISDN of client: +436643901212 (Mobilkom Austria)
IMSI of client: +232013920029363

```
provisioned SS
  {
    ss-Data :
    {
      ss-Code clir (calling line id restriction)’12’H,
      ss-Status Quiescent-Provisioned-Registered-Active’07’H,
      ss-SubscriptionOption cliRestrictionOption :
temporaryDefaultAllowed
    },
    ss-Data :
    {
      ss-Code clip (calling line id presentation)’11’H,
      ss-Status Quiescent-Provisioned-Registered-Active’07’H,
      ss-SubscriptionOption overrideCategory : overrideDisabled
    },
    ss-Data :
    {
      ss-Code colr (connected line id restriction)’14’H,
      ss-Status Quiescent-Not Provisioned-Not Registered-Not
active’00’H
    },
  ss-Data :
  {
   ss-Code call unrelated(allow location by designated LCS
clients)′B3′H,
   ss-Status Quiescent-Provisioned-Not Registered-Active′05′H
  }
 },
 lcsInformation
 {
  gmlc-List
  {
   ′+436640589′H,
   ′+436640586′H,
   ′+436640586′H,
   ′+436640587′H
  }
 }
 lcsInformation
 {
  lcs-PrivacyExceptionList
  {
   {
    ss-Code ′B3′H, /* SS-Code ‘Call Session Unrelated’ allowing
location by designated external LCC client, (‘C04H would allow all
MO-LR)
    ss-Status ′05′H,
    externalClientList
    {
     {
      clientIdentity
      {
       externalAddress ′+436640001′H
      },
      gmlc-Restriction gmlc-List
     },
     {
      clientIdentity
      {
       externalAddress ′+436640002′H
      },
      gmlc-Restriction gmlc-List
     },
    }
   }
  }
 },
```

As seen in the UPDATE LOCATION procedure, the client Identity and exception GTs are changed to be the Roaming Hub GT.

6.3.4 Explanations of the LCS Parameters in the Mobile Profile to be provisioned in the HLR

6.3.4.1 GMLC List

This contains the GTs of the GMLC which are authorized to send a PROVIDE SUBSCRIBER LOCATION request. In the case of an external hosted GMLC, the GT of the Roaming Hub must be declared in the HLR of any HPLMN for a customer who has the LCS service in this VPLMN.

6.3.4.2 LCS Privacy Exception List

This defines the list of LCS clients that are allowed to locate a target MS, and for each class it provides the ‘SS-Code’. It also defines the E164 addresses (such as +436640002 in the example above) which are allowed to perform MT-LR on this target MS.

6.4 Simple BSS-based SMLC Architecture Using the Mobile TA and Measurements

The simple SMLC described below has the minimum requirements on the NSS. It integrates the GMLC and SMLC functions. To avoid the cost of LMUs, it uses the location computation method of Section 6.2.4.4.

6.4.1 The MAP Location Service Enquiry is Required in the MSC

In order to read the measurements made by the handset, a connection must be established between the MS and the MLC. Paging must be performed if the MS is in idle mode. But the PAGING RESPONSE will always go to the MSC to which the BSC is connected. So, the paging must be performed by the MSC. This is why *the MAP Location Service Enquiry package is mandatory* in all the MSCs as paging is part of this procedure. As seen in Figures 6.4 and 6.5, at the end of the paging the MLC receives a BSSAP-LE Perform Location Request inside an SCCP CP ‘Connection Request’, which has a ‘Connection ID’ that allows measurements to be requested to compute the position.

The only prerequisite is to have BSSAP-LE [6.4] in the BSCs (*not needed in the MSCs* if we use ‘BSS-based SMLC’). Only LR-MT services are offered to the HPLMNs for their virtual visitors, with special charges which bring additional revenues to the VPLMN.

This architecture *does not require there to be an LMU type B (in the BTS) or type A (stand alone).*

6.4.2 Detailed Data Flow

Steps (1) to (9) are *almost the same* as in the standard model for a BSS-based SMSC. But, instead of a SEND ROUTING INFO FOR LCS at step (2), which requires having the HLR configured to have this MAP service (additional cost), we use an ordinary SEND ROUTING INFO FOR SM to have the IMSI. The ‘LCS client ID’ is not required (we use just the IMSI) if the GMLC GT is provisioned as an accepted SMLC in all the MSCs (they control the access in the MAP parameter of the PROVIDE SUBSCRIBER LOCATION (3) and not the individual authorization for a given subscriber): this is possible in particular with Siemens MSCs. If an unauthorized GT is used, the request is denied by the MSC. This simplified method reduces the cost of the necessary software and provisioning work in the HLR.

The Perform Location Request ([6.4]) is then sent by the BSC (9) to the SMLC to start the Position Computation.

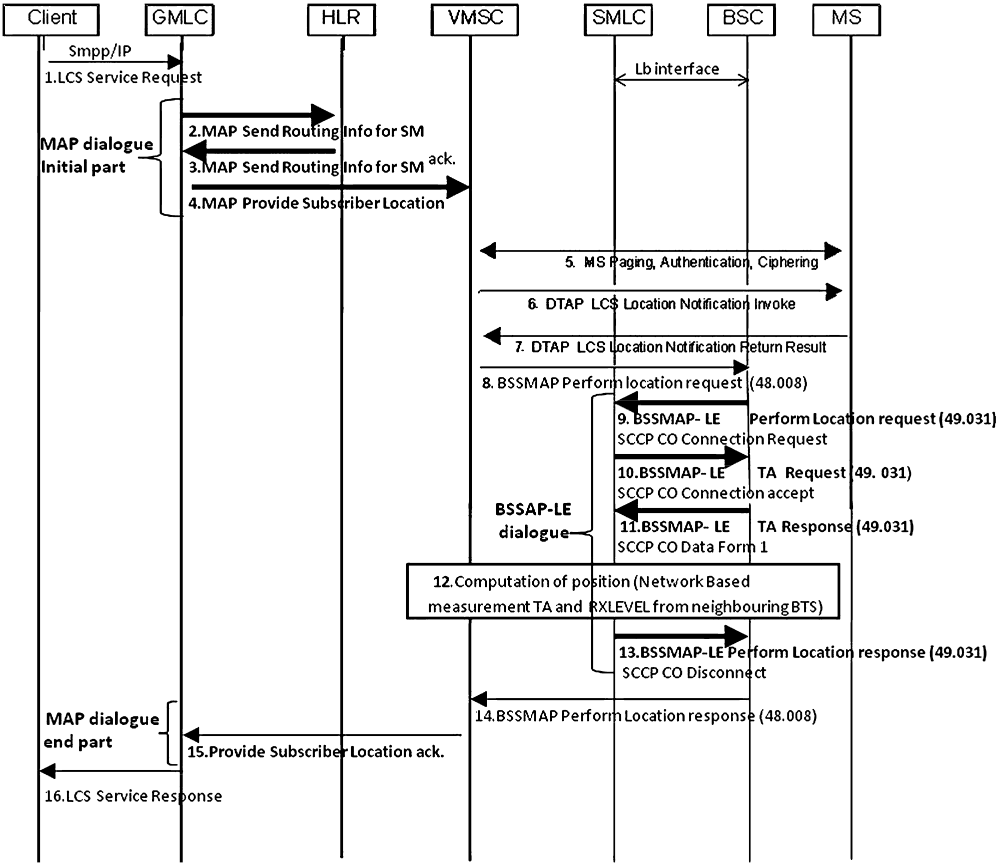

Client
GMLC
HLR
VMSC
SMLC
BSC
MS
Smpp/IP
1.LCS Service Request
Lb interface
MAP dialogue
Initial part
2.MAP Send Routing Info for SM
3.MAP Send Routing Info for SM ack.
4.MAP Provide Subscriber Location
5. MS Paging, Authentication, Ciphering
6. DTAP LCS Location Notification Invoke
7. DTAP LCS Location Notification Return Result
8. BSSMAP Perform location request (48.008)
9. BSSMAP- LE Perform Location request (49.031)
SCCP CO Connection Request
10.BSSMAP- LE TA Request (49. 031)
SCCP CO Connection accept
BSSAP-LE
dialogue
11.BSSMAP- LE TA Response (49.031)
SCCP CO Data Form 1
12.Computation of position (Network Based
measurement TA and RXLEVEL from neighbouring BTS)
13.BSSMAP-LE Perform Location response (49.031)
SCCP CO Disconnect
14.BSSMAP Perform Location response (48.008)
MAP dialogue
end part
15.Provide Subscriber Location ack.
16.LCS Service Response

Figure 6.5 Signalling between an SMLC and Target MS with BSS-based SMLC

(10) The SMLC sends a timing Advance (TA) Request APDU to the mobile on the SCCP connection requested by the BSC.
(11) The TA Response (Timing Advance and measurements) is received (see Section 6.2.4.3).
(12) The computation of position is done with the method of 6.2.4.4.

Steps (13) to (16) are like those in the standard model for a BSS-based SMSC.

6.4.3 NSS-based SMLC Alternative: Possibility of Using an External Hosted SMLC

In the MSCs, it is possible to configure the SMLC with Global Title addressing. In the NSS-based SMLC alternative (the previously recommended 'simple SMLC' architecture used, 'BSS based'), *with the BSSAP-LE stack required in the MSCs,* the initial BSSAP-LE Perform Location Request (8 in Figure 6.4) is sent directly to the SMLC, which could well be hosted even in another country by a Virtual Roaming Hub supplier. The customer VPLMN would simply need to provision the Roaming Hub (with SMLC function) as the MLC of all its MSCs.

6.4.4 Detailed Traces: What Connection Oriented SCCP (SCCP Class 2) is

The most valuable parts of this book are the traces corresponding to the principle above: so here they are as a reference. Connection Oriented SCCP (Class 2) works very much like TCP/IP, which most readers are familiar with.

TCP	**SCCP Connection Oriented**
IP Address origin	Originating Point Code
IP Address destination	Destination Point Code
Socket number	SCCP connection ID

Each SS7 signalling Point Code, when it receives an SCCP CONNECT REQUEST (i.e. Socket opening in TCP), will use the SCCP Connection ID (i.e. Socket Number) to create a back route to the incoming Point Code for all the MSUs (IP packets) of the session. So all packets will be received in the same order and using the same path.

6.4.4.1 MAP Dialogue Initial Part

The MSC will page the MS (assuming it is in idle mode). When the MS answers, it initiates the connection to the BSC then to the MSC. The MSC then sends a BSSAP Perform Location Request *to the BSC*, which opens an SCCP Connection to the SMLC (the Point Code must be configured in each BSC). So the BSC is the initiator of the connection between the MS and the SMLC (through the BSC).

The following is the MAP Dialogue of the GMLC function of the ‘simple SMLC’.

```
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 41
      MAP-OPEN-REQ(1)
        dest_address(Q713)(1)
          L = 013
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3
                 Subsystem Number = VLR(7),
                 Global Title :
                    Translation Type = 0,
                    Numbering Plan = ISDN/Telephony(E164),
                    Encoding Scheme = BCD, odd number of digits,
                    Nature Address Indicator = International number,
                    Address information = 21622001010
        orig_address(Q713)(3)
          L = 011
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = GMLC(9),
                 Global Title :
                    Translation Type = 0,
                    Numbering Plan = ISDN/Telephony(E164),
                    Encoding Scheme = BCD, odd number of digits,
                    Nature Address Indicator = International number,
                    Address information = 21622001049
        MAPorCAP_Application_Context(11)
          L = 009
      Data: (Hex) 060704000001002603
           MAP_location Service Enquiry Package_v3 MAP V3
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   PA_Len = 34
   MAP-PROVIDE-SUBS-LOCATION-REQ(61)
    MAPPN_timeout(45)
      L = 002
      Data: timeout value = 15 sec
    MAPPN_invoke_id(14)
      L = 001
      Data: 1
    MAPPN_imsi(18)
      L = 008
      Data: Address = 605038000008107
    MAPPN_mlc_number(137)
      L = 007
      Data: Ext = No extension
          Ton = International
          Npi = ISDN
          Address = 21622001049
    MAPPN_Location_estimate_Type(144)
      L = 001
      Data: (0):current location
    MAPPN_LCS_Client_internal_id(185)
      L = 001
      Data: (0):broadcast Service
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   PA_Len = 2
   MAP-DELIMITER-REQ(5)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

6.4.4.2 BSSAP-LE Dialogue: between BSC and SMLC

BSSAP-LE dialogue is initiated by the BSC (see (9) in Figure 6.5).

```
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   SCCP_N_CONNECT_IND(5)
    SCPPN_CALLED_ADDR(Q713)
      L = 004
      Data:  Route on SSN, No Global Title included(0x43),
           Signalling Point Code (ITU) = 1-096-2
           Subsystem Number = BSC (BSSAP LE)(250),
    SCPPN_CALLING_ADDR(Q713)
      L = 004
      Data:  Route on SSN, No Global Title included(0x43),
           Signalling Point Code (ITU) = 0-023-7  /* the Point
           Code of the BSC serving the MS
           Subsystem Number = BSC (BSSAP LE)(250),
        SCPPN_USER_DATA
          L = 016
          Data: (Hex) 000E2B44010005080082F35004D2162E
          BSSAP-LE(GSM 49.031) BSSMAP-LE(0)
              L = 014
          Message Type(GSM 49.031): (43):BSSMAP_LE_PERFORM_LOCATION_
REQ
            (68):Location Type
               (0):current location(00)
            (5):Cell Identifier
               (0):The Whole Cell Global Identification(CGI), is
used to identify the cell(00)
               Cell Identification: MCC = 605 MNC = 3 LAC = 1234
               Cell_ID = 5678
       (19):Classmark information Type 3 of the handset (GSM
44.008)
           MS assisted E-OTD supported
           MS assisted GPS supported    /* this handset is GPS
equipped */
           MS based GPS supported
       (75):GPS assistance data requested
Satellite almanac
Reference Time
Reference Location
List of Identity of satellites for which assistance is requested
   - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

BSSAP-LE dialogue SMLC → BSC (see (10) in Figure 6.5)

```
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      SCCP_N_CONNECT_RESP(6)
        SCPPN_USER_DATA
          L = 007
          Data: (Hex) 00052A49020101
          BSSAP-LE(GSM 49.031) BSSMAP-LE(0)
              L = 005
          Message Type(GSM 49.031): (42):BSSMAP_LE_CONNECTION_
ORIENTED_INFORMATION
            (73):APDU
               (1):BSSLAP(details of APDU in GSM 48.071)(01)
               (1):TA(Timing Advance)_REQUEST(01)
   - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

BSSAP-LE dialogue: BSC sends response (see (11) in Figure 6.5)

```
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 37
      SCCP_DATA_IND(9)
        SCPPN_USER_DATA
          L = 030
          Data: (Hex)
001C2A4919010209000001 0F1410E06417DAFAF212345678901213141516
          BSSAP-LE(GSM 49.031) BSSMAP-LE(0)
              L = 028
          Message Type(GSM 49.031): (42):BSSMAP_LE_CONNECTION_
ORIENTED_INFORMATION
             (73):APDU
               (1):BSSLAP(details of APDU in GSM 48.071)(01)
               (2):TA(Timing Advance)_RESPONSE(02)
                  (9):Cell Identity
                       0
                  (1):Timing Advance
                       15
                  (20):Measurement Report(GSM 44.008)
                       (Hex) E06417DAFAF212345678901213141516
                       Serving cell: BA-USED 1 DTX-USED 1 RXLEVEL-
FULL-SERVING-CELL 32 MEASUREMENT-VALID 1 RXsignalLEVEL-SUB-SERVING-
CELL 36 RXsignalQUAL-FULL-SERVING-CELL 1
RXsignalQUAL-SUB-SERVING-CELL 3 NO-NCELL 7
                       Neighbour cell# 1 RXsignalLEVEL 26 BCCH-FREQ
31 BaseStation Idcode 23
                       Neighbour cell# 2 RXsignalLEVEL 36 BCCH-FREQ
04 BaseStation Idcode 35
                       Neighbour cell# 3 RXsignalLEVEL 17 BCCH-FREQ
11 BaseStation Idcode 15
                       Neighbour cell# 4 RXsignalLEVEL 04 BCCH-FREQ
16 BaseStation Idcode 04
                       Neighbour cell# 5 RXsignalLEVEL 33 BCCH-FREQ
06 BaseStation Idcode 10
                       Neighbour cell# 6 RXsignalLEVEL 02 BCCH-FREQ
20 BaseStation Idcode 22
                       Neighbour cell# 7 RXsignalLEVEL 06 BCCH-FREQ
24 BaseStation Idcode 02
        SCPPN_SEGMENTING
          L = 001
          Data: (0):Last data segment
   - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

BSSAP-LE dialogue: the SMLC sends the location to the BSC (see (13) in Figure 6.5)

```
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
       PA_Len = 28
       SCCP_N_DISCONNECT_REQ(16)
        SCPPN_USER_DATA
          L = 024
          Data: (Hex) 00162D4510A23456B412121234567890121314151647O1
00
          BSSAP-LE(GSM 49.031) BSSMAP-LE(0)
              L = 022
          Message Type(GSM 49.031): (45):BSSMAP_LE_PERFORM_LOCATION_
RSP
             (69):Geographic Location
                (Hex) 01032F6922C0C4
                      Position Estimate(3GPP 23.032)
                          Type of Shape Ellipsoid point
                      latitude = 2.2396(degrees)
                      longitude= 48.8714(degrees)
         (71):LCS Cause
            (0):Unspecified(00)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

6.4.4.3 MAP Dialogue End Part between MSC and GMLC

```
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   PA_Len = 16
   MAP-OPEN-CNF(130)
     MAPPN_result(5)
       L = 001
       Data: (0):Accept
     MAPorCAP_Application_Context(11)
       L = 009
       Data: (Hex) 060704000001002603
            MAP_location Service Enquiry Package_v3 MAP V3
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   PA_Len = 12
   MAP-PROVIDE-SUBS-LOCATION-CNF(184)
     MAPPN_invoke_id(14)
       L = 001
       Data: 1
     MAPPN_ellipsis(57)
       L = 002
       Data: Address = 1800
     MAPPN_Geographic Location
       L = 016
       Data:  (Hex) 01032F6922C0C4
                 Position Estimate(3GPP 23.032)
                    Type of Shape Ellipsoid point
                    latitude = 2.2396(degrees)
                    longitude= 48.8714(degrees)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   PA_Len = 2
   MAP-CLOSE-IND(4)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Remember that the same ‘simple SMLC’ equipment provides the two functions GMLC and SMLC in the dialogue.

6.5 Details of a More Accurate Positioning Method: A-GPS

The call flow *from the SMLC* is exactly the same as in Figures 6.3, 6.4 and 6.5; it is just that the positioning method is more precise. This method achieves accuracy only with GPS-equipped handsets with the A-GPS feature (most current GPS handsets have it). When one is indoors, or if the sky is obscured, it takes a very long time to get a GPS location, frequently with total failures. In order to speed up and improve the location computation, the SMLC provides satellite ephemeris and time accuracy on request from the handset. The BSSAP-LE PERFORM LOCATION Request received from the BSC or the MSC contains a field 'GPS Assistance Data', which details the data requested by the handset. At this stage (exactly the same as for the TA positioning method above) there is *a path established between the Handset (MS) and the SMLC using:*

(1) the RR (radio) protocol from the MS to the BSC;
(2) the SCCP connection oriented between the BSC and the SMLC. So the *SMLC can send data to the MS and read the GPS results.*

6.5.1 Signalling Layers between the SMLC and the Handset (Target MS)

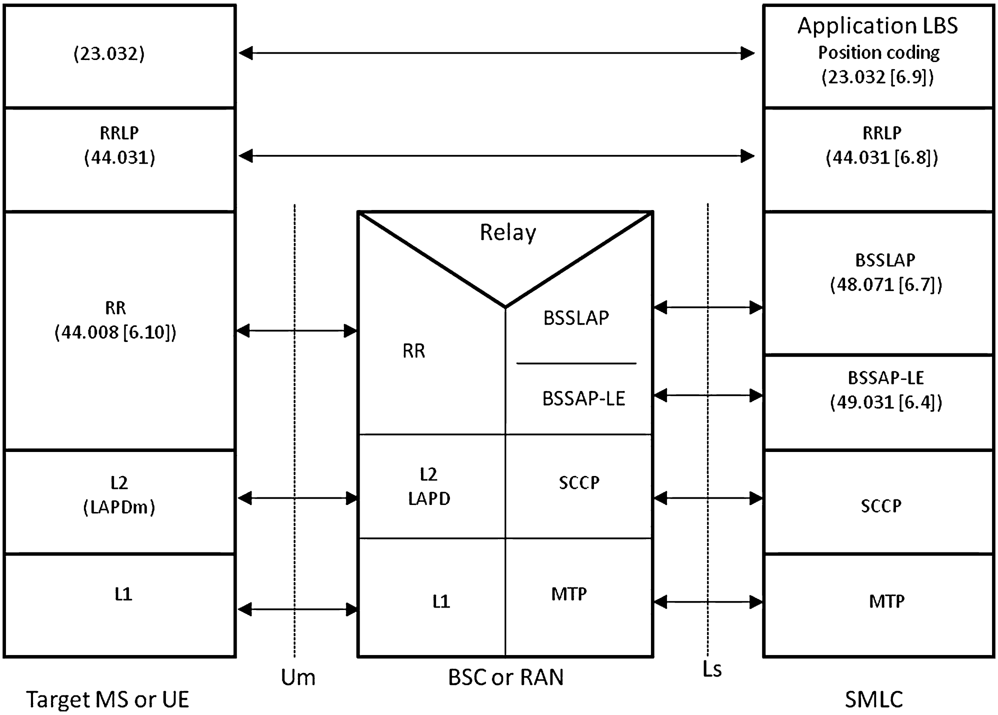


Figure 6.6 Signalling between an SMLC and Target MS (handset) with BSS-based SMLC [6.1]

If, in the PERFORM LOCATION request received from the BSC, the Handset requests GPS Assistance data, the SMLC sends a 'Radio resource LCS Protocol (RRLP)' [6.8] message 'Assistance Data' to the handset via the BSC and the connection (it uses BSSMAP-LE Connected Oriented Information) established by the incoming PERFORM LOCATION Request.

Then the SMLC sends an RRLP message 'Measurement Position request' (44.031) to the handset, packed in a BSSAP APDU (48.071) 'MS POSITION COMMAND', and will receive the result of the location computation performed by the handset. If the QoS is not sufficient, certain SMLCs can perform the computation with their own data received. The trace below explains the details.

As the ‘MS POSITION RESPONSE’ *also returns the same data as the ‘TA Response’* plus the GPS position (in the RRLP Info parameter) computed by the handset (if equipped), this is a general method, which is recommended because if the GPS position is not available, the SMLC can use the TA+ Measurement method of Section 6.4.

The difference in the data path is that to execute a TA_Request, the BSC does not need to interrogate the MS with the RRLP protocol to get the position data, because the TA and Measurement reports returned in the TA_Response are available already from the paging response ((6) and (7) of Figure 6.4) of the MS.

To conclude, if the handset is GPS equipped, the accuracy cannot be better when it works (a few metres). If not, the TA+ Measurement method of 6.2.4.4 provides excellent accuracy for all legacy phones. The two combined methods cover all the market needs.

6.5.2 Trace of BSSAP-LE Dialogue between the SMLC and the Handset

The dialogue is identical to that in 6.4.4.2 and Figure 6.5 with the previous TA (Timing Advance)_ REQUEST positioning method, except that an MS POSITION COMMAND (for GPS), which has different parameters, is sent instead of a TA _REQUEST.

```
BSSAP-LE dialogue SMLC → BSC (see (10) in Figure 6.5)
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
       SCCP_N_CONNECT_RESP(6)
        SCPPN_USER_DATA
          L = 017
          Data: (Hex) 000F2A490C010F19001B06A20101B40002
          BSSAP-LE(GSM 49.031) BSSMAP-LE(0)
              L = 015
          Message Type(GSM 49.031): (42):BSSMAP_LE_CONNECTION_
ORIENTED_INFORMATION
             (73):APDU
               (1):BSSLAP(details of APDU in GSM 48.071)(01)
               (15):MS_POSITION_COMMAND(0F)
                 (25):RRLP Flag
                   (0):positioning command(SMLC → BSC) or final
response(BSC → SMLC)(00)
                 (27):RRLP IE(GSM 44.031)
                       reference number 162
                       Measurement Position request(see GSM 44.031)
                         Position Instruction
                           Method Type = (1):MS Based /* handset
will compute GPS position */
                           Position Method = (1):GPS
                           Measure Response Time = 180
                           Use multiple sets? = (0):multiple sets
are allowed
                           Environment characteristics = (2):mixed
environment
BSSAP-LE dialogue: BSC sends response (see (11) in Figure 6.5)
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
       SCCP_DATA_IND(9)
        SCPPN_USER_DATA
```

```
          L = 028
          Data: (Hex)
001A2A4917010F19001B11A20001456B41212123456789012131415 1
          BSSAP-LE(GSM 49.031) BSSMAP-LE(0)
              L = 026
          Message
Type(GSM 49.031): (42):BSSMAP_LE_CONNECTION_ORIENTED_INFORMATION
             (73):APDU
               (1):BSSLAP(details of APDU in GSM 48.071)(01)
               (15):MS_POSITION_RESPONSE(10)
                 (25):RRLP Flag
                   (0):positioning command(SMLC → BSC) or final
response(BSC → SMLC)(00)
                 (27):RRLP IE(GSM 44.031)
                       (Hex) A20021032F6922C0C44567890121314151
                       reference number 162
                       Measurement Position response (see GSM
44.031)
                          Location Information(3GPP 23.032)
                            Reference Frame (absent)
                            GPS TOW (absent)
                            Fix Type = (0):2D measurement
                            Position Estimate(3GPP 23.032)
                              Type of Shape Ellipsoid point with
uncertainty Ellipse
                              latitude = 2.2396(degrees)
                              longitude= 48.8714(degrees)
                              uncertainty major axis = 69
                              uncertainty minor axis = 103
                              angle of major axis = 137
                          GPS Measurement Information
                          Location Information Error
                 (1):Timing Advance
                       15
                 (20):Measurement Report(GSM 44.008)
                       (Hex) E06417DAFAF21234567890121314151 6
                        Serving cell: BA-USED 1 DTX-USED 1 RXLEVEL-
FULL-SERVING-CELL 32 MEASUREMENT-VALID 1 RXsignalLEVEL-SUB-SERVING-
CELL 36 RXsignalQUAL-FULL-SERVING-CELL 1
RXsignalQUAL-SUB-SERVING-CELL 3 NO-NCELL 7
                       Neighbour cell# 1 RXsignalLEVEL 26 BCCH-FREQ
31 BaseStation Idcode 23
                       Neighbour cell# 2 RXsignalLEVEL 36 BCCH-FREQ
04 BaseStation Idcode 35
                       Neighbour cell# 3 RXsignalLEVEL 17 BCCH-FREQ
11 BaseStation Idcode 15
                       Neighbour cell# 4 RXsignalLEVEL 04 BCCH-FREQ
16 BaseStation Idcode 04
                       Neighbour cell# 5 RXsignalLEVEL 33 BCCH-FREQ
06 BaseStation Idcode 10
```

```
                       Neighbour cell# 6 RXsignalLEVEL 02 BCCH-FREQ
20 BaseStation Idcode 22
                       Neighbour cell# 7 RXsignalLEVEL 06 BCCH-FREQ
24 BaseStation Idcode 02
```

As you can see, the same results as from a TA_Request are obtained; they can be used as a backup if GPS cannot provide an accurate fix.

6.6 The Enhanced Time Difference (E-OTD) Method: Hyperbola Intersections

In the trace in Section 6.4.4.2, we see that the mobile also supports E-OTD, which can be used instead of the TA+Measurement as backup in the absence of GPS. The signalling exchange is exactly as for A-GPS, with the RRLP protocol used to obtain measurements from the handset. The method is more accurate than TA+Measurements, but requires LMUs in a GSM network (the LMU type B which is often included in the BTS is sufficient).

6.6.1 Understanding E-OTD Method in GSM Networks

6.6.1.1 Why the Intersection of Hyperbolas?

The clocks of each BTS are *not synchronized together* in a GSM network (they are synchronized in the UMTS BSS and another method is recommended if GPS is not available): each has a difference RTDi (Real Time Difference) with the clock of a 'reference BTS'. The clock of a handset is also not synchronized with any BTS (call MStd the difference with the same clock reference). So if BTS #i sends a burst message with its time stamp Ti and it is received at MS time T, the 'observed time difference' is:

$$\mathrm{OTDi} = \mathrm{T} - \mathrm{Ti}$$

and the absolute time difference by correcting for the clock differences is:

$$(\mathrm{T} - \mathrm{MStd}) - (\mathrm{Ti} - \mathrm{RTDi}) = \mathrm{OTDi} + \mathrm{RTDi} - \mathrm{MStd}$$

The SMLC knows the RTDi of the various neighbouring BTSs of the target MS and can pass it to the MS for E-OTD position location (MS based) or use it if it makes the position location (MS assist). But the clock difference of the handset MStd *remains unknown accurately* (at the speed of light, 30 metres are 100 nanoseconds, so the method requires accurate time measurements, as an accuracy target of less than 100 m in urban areas was specified by the US government in 1999). For computation purposes by the MS or by the SMLC (E-OTD assist), all we know for each pair of BTS #i and #j sending a burst (not exactly at the same time) is the 'geometric time difference' of the reception of the two burst messages:

$$\mathrm{GTDij} = (\mathrm{OTDi} + \mathrm{RTDi}) - (\mathrm{OTDj} - \mathrm{RTDj})$$

which cancels the term Mstd. The difference in distance is:

$$\mathrm{Dij} = \mathrm{c} \times \mathrm{GTDij}$$

Knowing the position of all the BTSs involved in the position measurement, the handset (the RTDi must be sent before by some means (Assistance data or Cell Broadcast)) or the SMLC can compute the position as the 'intersection of pairs of hyperbolas' having their foci at BTS #i and BTS #j. A hyperbola is the locus of points having a constant distance difference Dij to the two foci i and j.

6.6.1.2 How a 'Burst' of the Neighbouring BTS is Triggered by the Measurement Position Request

The SMLC sends the 'Measurement Position Request' to the MS so that *it waits for burst messages from the environment*. Simultaneously, the BSC simulates the 'forced Handover procedure' by sending a message BSSAP HANDOVER REQUEST [6.6] *to each neighbouring BTS* that contains the IMSI of the MS (this is used in traffic management to create a burst of power to force, in the case of traffic overload, a handset to switch to an other BTS giving a better signal). There will be delays in the transmission over the land network to the BTS, but it does not matter as is explained above.

6.6.1.3 How the Calibration RTDi are Obtained by the SMLC

The 'Reference BTS' is also known as an LMU (Location Management Unit). There are two types: LMU B, which is integrated into a regular BTS, and a stand-alone LMU A, which is basically a mobile handset in a fixed location on top of a light mast. The number of LMUs must be such that any BTS is visible from at least one LMU. The LMU also receives the burst of power from the different neighbours of both the handset and the LMU, and can measure the RTDi for transmission to the SMLC for a refresh of the BTS database. It will be used as E-OTD assistance data for the next position measurement involving these BTSs.

6.6.2 Content of the E-OTD Assistance Data

In order that the handset can compute its position (otherwise the SMLC can do it in 'MS-Assist' mode), the SMLC sends E-OTD assistance data at the beginning of the procedure, either before sending the Measurement Position Request or as additional parameters (see Section 6.6.3), which contain, mainly *for each neighbouring* BTS # i that the SMLC has determined:

- the BTS identity (BSIC is used, not the Cell-ID);
- the Real Time Difference RTDi with respect to a common reference time (this is the BTS clock offset with the 'Reference BTS');
- the distance (North, East, Altitude) of this BTS relative to the 'Reference BTS'.

The handset memorizes these data to be able to perform the E-OTD position computation.

6.6.3 Content of the MS POSITION COMMAND for E-OTD

In the trace in Section 6.5.2, replace the Position Method by E-OTD instead of GPS.

```
                 Measurement Position request (see GSM 44.031)
                    Position Instruction
                      Method Type = (1):MS Based
                      Position Method = (0):E-OTD based /* MS
will make computation */
                      Measure Response Time = 180
                    E-OTD Reference BTS of Assistance Data
```

```
                                  BSIC of Reference BTS
                                  BTS position (23.032) (long, lat)
                                E-OTD Measurement Assistance Data (the
neighbour BTS)
                                  see Section 6.6.2
```

The OTDi are computed by the MS, when it receives the bursts from the neighbouring BTSs asking for a Handover, then the GTDij, knowing the RTDi from the E-OTD Measurement Assistance Data.

In 'MS-based' (meaning that the Mobile Station performs the position computation internally), the 'E-OTD Measurement Assistance Data' allows the handset to compute the position of the neighbouring BTS relative to the 'Reference BTS (or the LMU)' as origin of the local X-Y coordinate system, because the North and East distances of these BTSs are relative to the position of the Reference BTS and the longitude and latitude have been included in the 'E-OTD Reference BTS of Assistance Data' parameter.

As explained in [5.1] Chapter 13, the estimated position is given by the 'intersection of hyperbolas' with the different loci taken as the various pairs of BTSs of the measurement. At least three BTSs are required. The algorithm is the same as in Section 6.2.4.4, whose execution for the 'circle intersection' is given in Section 6.7. The Location Estimate is then returned to the BSC.

If the Method Type is 'MS Assist', the handset does not compute the position and returns the OTDi to the SMLC, which then makes the position calculation.

6.7 Annex: Execution of the Algorithm for Position Computation with the 'Measurement Reports' or E-OTD

The algorithm runs with the data of Figure 6.1 and gives the following listing.

```
Lat 2.2333000 Long 48.8666000 Distance 1100.0000000(m)
Lat 2.2410000 Long 48.8786000 Distance 1100.0000000(m)
Lat 2.2383000 Long 48.8683000 Distance 220.0000000(m)
Lat 2.2313000 Long 48.8723000 Distance 1460.0000000(m)
Number of BTS = 4 Their gravity centre: Xb 2.2359750 Yb 48.8714500
X  -0.452(km) Y  -0.539(km) Distance   1.100(km)
X   0.849(km) Y   0.794(km) Distance   1.100(km)
X   0.393(km) Y  -0.350(km) Distance   0.220(km)
X  -0.790(km) Y   0.094(km) Distance   1.460(km)
```

This algorithm is for finding the best location estimate; see [5.1] Chapter 13.

```
1.1) Obtain the real Xi which are roots of the resultant in X
Coeff a3 : Degree=03: 0.0000000000 X**0
Coeff a2 : Degree=03: 4.0000000000 X**1 -0.0000000000 X**0
Coeff a1 : Degree=03: -0.0000000000 X**1 1.4116573000 X**0
Coeff a0 : Degree=03: 4.0000000000 X**3 -0.0000000000 X**2
1.5609700913 X**1 -1.7170487325 X**0
Coeff b3 : Degree=03: 4.0000000000 X**0
Coeff b2 : Degree=03: -0.0000000000 X**0
Coeff b1 : Degree=03: 4.0000000000 X**2 -0.0000000000 X**1
0.2615579317 X**0
Coeff b0 : Degree=03: -0.0000000000 X**2 1.4116573000 X**1
-0.2765941625 X**0
Display POLYNOMIAL before renormalization
```

```
Degree=18: -0.0000000000 X**7 0.0000000000 X**6 -2472.8517865692
X**5 1542.1779655712 X**4 -1739.3506539816 X**3 1617.7816685975
X**2 -863.1073563089 X**1 325.8572596398 X**0
Display POLYNOMIAL after renormalization
Degree=05: -2472.8517865692 X**5 1542.1779655712 X**4
-1739.3506539816 X**3 1617.7816685975 X**2 -863.1073563089 X**1
325.8572596398 X**0
Sturm’s method to find all the real roots of a real value
coefficient polynomial(AHL 28/9/2008)
Display the polynomial f0 which we compute all the real distinct
roots
Degree=05: -2472.8517865692 X**5 1542.1779655712 X**4
-1739.3506539816 X**3 1617.7816685975 X**2 -863.1073563089 X**1
325.8572596398 X**0
From AHL(‘SMS & MMS interworking..’ 13.7.4.1), the |roots| are ≤
Max of val abs of coeff + 1 = 1740.351
Here is the Quotient Sturm sequence: 6 polynomials computed by
13.7.3.4:
Degree=05: -2472.8517865692 X**5 1542.1779655712 X**4
-1739.3506539816 X**3 1617.7816685975 X**2 -863.1073563089 X**1
325.8572596398 X**0
Degree=04: -12364.2589328460 X**4 6168.7118622849 X**3
-5218.0519619448 X**2 3235.5633371951 X**1 -863.1073563089 X**0
Degree=05: 541.8571771046 X**3 -840.5008317175 X**2 609.7723621109
X**1 -304.3264076243 X**0
Degree=04: 11484.6585053345 X**2 -10932.0953229246 X**1
8170.0385289001 X**0
Degree=05: 84.7889659647 X**1 73.3289580094 X**0
Degree=04: -26214.5067460904 X**0
the PGCD of f0(x) and f’0(x) is: Degree=04: -26214.5067460904 X**0
(if degree of Result 4.00 > 1, there are multiple roots !
w(-Max = -1740.350653982)= 3 w(Max= 1740.350653982)= 2
The number of DISTINCT real roots of f0 is then (w(-Max) - w(Max)
= 1, see 13.7.3.5) computed with accuracy of 0.000000010
with 78 dichotomic searches
root = 0.6195084 f0/Max = 0.0000000
evaluation for X=1 f0/Max = -0.9133176
attention : all the roots of the polynomial DETERMINANT in X may
not give REAL solutions of Y
these real roots Xi of the resultant will allow to have a common
root of f(Y)=0 and g(Y)=0 but NOT NECESSARILY real
search for all Xi, all the real roots of f(Y), then g(Y), select
those which are common and real
1.2) Obtain the real Yi which are roots of the resultant in Y
Coeff a3 : Degree=03: 0.0000000000 X**0
Coeff a2 : Degree=03: 4.0000000000 X**1 -0.0000000000 X**0
Coeff a1 : Degree=03: -0.0000000000 X**1 1.4116573000 X**0
Coeff a0 : Degree=03: 4.0000000000 X**3 -0.0000000000 X**2
0.2615579317 X**1 -0.2765941625 X**0
Coeff b3 : Degree=03: 4.0000000000 X**0
Coeff b2 : Degree=03: -0.0000000000 X**0
Coeff b1 : Degree=03: 4.0000000000 X**2 -0.0000000000 X**1
1.5609700913 X**0
Coeff b0 : Degree=03: -0.0000000000 X**2 1.4116573000 X**1
-1.7170487325 X**0
Dislay POLYNOMIAL before renormalization
Degree=18: -0.0000000000 X**6 -2472.8517865692 X**5 2298.0397759324
X**4 -936.0372338730 X**3 38.5355039238 X**2 -66.7584740348 X**1
-62.1636038668 X**0
Display POLYNOMIAL after renormalization
Degree=05: -2472.8517865692 X**5 2298.0397759324 X**4
-936.0372338730 X**3 38.5355039238 X**2 -66.7584740348 X**1
-62.1636038668 X**0
Sturm's method to find all the real roots of a real value
coefficient polynomial (AHL 28/9/2008)
Display the polynomial f0 which we compute all the real distinct
roots
Degree=05: -2472.8517865692 X**5 2298.0397759324 X**4
-936.0372338730 X**3 38.5355039238 X**2 -66.7584740348 X**1
-62.1636038668 X**0
From AHL('SMS & MMS interworking..' 13.7.4.1), the |roots| are ≤
Max of val abs of coeff + 1 = 2299.040
Here is the Quotient Sturm sequence: 6 polynomials computed by
13.7.3.4:
Degree=05: -2472.8517865692 X**5 2298.0397759324 X**4
-936.0372338730 X**3 38.5355039238 X**2 -66.7584740348 X**1
-62.1636038668 X**0
Degree=04: -12364.2589328460 X**4 9192.1591037295 X**3
-2808.1117016191 X**2 77.0710078476 X**1 -66.7584740348 X**0
Degree=05: 32.7211881391 X**3 81.2626711718 X**2 50.5418725227 X**1
64.6451699606 X**0
Degree=04: 82797.8013604567 X**2 37123.9808950486 X**1
78891.9737380042 X**0
Degree=05: 10.4933311306 X**1 -1.1949969109 X**0
Degree=04: -84193.5160434080 X**0
the PGCD of f0(x) and f'0(x) is: Degree=04: -84193.5160434080 X**0
(if degree of Result 4.00 > 1, there are multiple roots !
w(-Max = -2299.039775932)= 3 w(Max= 2299.039775932)= 2
The number of DISTINCT real roots of f0 is then (w(-Max) - w(Max)
= 1, see 13.7.3.5) computed with accuracy of 0.000000010
with 78 dichotomic searches
root = -0.2825671 f0/Max = -0.0000000
evaluation for X=1 f0/Max = -0.5224946
attention: all the roots of the polynomial DETERMINANT in X may
not give REAL solutions of Y
these real roots Xi of the resultant will allow to have a common
root of f(Y)=0 and g(Y)=0 but NOT NECESSARILY real
search for all Xi, all the real roots of f(Y), then g(Y), select
those which are common and real
2) Evaluate the Sum of the square of distances to all the circles
from the possible combination of optimal solutions X[i] Y[i]
X -0.4518767 Y -0.5388889 Distance 1.1000000
X 0.8488526 Y 0.7944444 Distance 1.1000000
X 0.3927527 Y -0.3500000 Distance 0.2200000
X -0.7897285 Y 0.0944444 Distance 1.4600000
root X# 0 =0.619508380 Y# 0 =-0.282567075 dist**4 = 0.00008881937
3) Display the location and the accuracy
Root X=0 Root Y=0
Localization (centred at gravity centre of the BTS):
X= 0.620(km) Y= -0.283(km) minimum of functional =0.00008881937
Uncertainty (in km) = 0.024
Lat 2.2396 Long 48.8714 Uncertainty 24(m)
```

We obtain the same position as with the GPS positioning. We can conclude that the overall method includes all the accuracy of A-GPS if the handset is GPS equipped, and gives a good accuracy using the backup 'Measurement Report' method.

References and Further Reading

Location Methods

[6.1] ETSI TS 143 059 v8.1.0 (2009-01), 'Digital cellular telecommunications system (Phase 2+), Location Based Services, Functional description Stage 2 of Location services in GERAN', (3GPP TS **43.059** v8.1.0 **Release 8**), *(describes the different standard GSM methods for GSM EDGE networks).*

[6.2] ETSI TS 125 305 v8.1.0 (2009-01), 'Universal Mobile Telecommunications System (UMTS), User Equipment (UE) positioning in Universal Terrestrial Radio Access Network (UTRAN); Stage 2', (3GPP TS **25.305** v8.1.0 **Release 8**), (describes the different standard GSM methods for UMTS networks).

[6.3] ETSI TS 123 271 v8.0.0 (2009-01), 'Digital cellular telecommunications system (Phase 2+), Universal Mobile Telecommunications System (UMTS): LTE; Functional stage 2 description of Location Services (LCS)', (3GPP TS **23.271** v8.0.0 **Release 8**), *(describes the different standard GSM methods for LBS in GSM and UMTS networks, replaces the older specification 03.71).*

Protocol for LBS

[6.4] ETSI TS 149 031 v8.1.0 (2009-01), 'Digital cellular telecommunications system (Phase 2+), Location Based Services, Base Station System Application Part LCS Extension BSSAP-LE', (3GPP TS **49.031** v8.1.0 **Release 8**), *(this is the specification of the BSSAP-LE protocol, with the sub-protocols BSSMAP-LE and DTAP-LE).*

[6.5] ETSI TS 100 589 v8.0.1 (2002-05), 'Digital cellular telecommunications system (Phase 2+), Signalling Transport Mechanism specification for the Base Station System – Mobile Services Switching Centre (BSS-MSC) Interface', (3GPP TS **08.06** version 8.0.1 **Release 1999**), *(this is the specification of the BSSAP protocol, with the sub-protocols BSSAP and DTAP).*

[6.6] ETSI TS 100 590 V8.15.0 (2003-09), 'Digital cellular telecommunications system (Phase 2+); Mobile-services Switching Centre – Base Station system (MSC-BSS) interface; Layer 3 specification', (3GPP TS **08.08** version 8.15.0 **Release 1999**), (gives the detailed formats of the 'measurement reports' and 'Classmark Information' (handset features).

[6.7] ETSI TS 148 071 v8.0.0 (2009-02), 'Digital cellular telecommunications system (Phase 2+), Location Services (LCS); Serving Mobile Location Centre – Base Station system (SMLC-BSS) interface; Layer 3' (3GPP TS **48.071** v8.6.0 **Release 8**), *(protocol which relays to the BSC the encapsulated RRLP data end-to-end between SMLC and handset, replaces the older specification 08.71).*

[6.8] ETSI TS 144 031 v7.6.0 (2007-10), 'Digital cellular telecommunications system (Phase 2+), Location Services (LCS); Mobile station (MS)-Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol

(RRLP)', (3GPP TS **44.031** v7.6.0 **Release 7**), *(end -to end protocol between the SMLC and the MS which carries the GPS assistance data.*

[6.9] ETSI TS 123 032 v8.0.0 (2009-01), 'Digital cellular telecommunications system (Phase 2+), Universal Mobile Telecommunications System (UMTS); LTE; Universal Geographical Area Description (GAD)', (3GPP TS **23.032** v8.0.0 **Release 8**), *(coding of the mobile position, replaces the older specification 03.32).*

[6.10] ETSI TS 144 008 v4.0.0 (2001-03), 'Digital cellular telecommunications system (Phase 2+) Mobile radio interface Layer 3 specification', (3GPP TS **44.008** v4.0.0 **Release 4**).

Books

[6.11] Van Diggelen, Frank, 'A-GPS: Assisted GPS, GNSS, and SBAS', Artech House, 2009.

7

Roaming Costs or Inter-operator Traffic Charge Suppression Systems, and Other Service Improvements

7.1 VMS Anti-tromboning: Large Financial Savings in GSM and UMTS

When an outbound roamer receives a call and does not answer, a new call is made from the visited network *back to* their home VMS (stands for GSM Voice Mail System or UMTS Visio Mail System), then the *two calls are connected* by the VPLMN. An image for this is a paperclip 'trombone'. The costs involved are from two calls, which are:

- HPLMN to VPLMN (international call paid by the HPLMN);
- VPLMN to VMS in the HPLMN (an expensive call charged by the VPLMN to the HPLMN).

For one major French operator, the annual financial costs and lost revenues are more than 10 million USD/year. So it is most important to suppress this 'tromboning' and either keep the savings or share them with the subscriber by applying a smaller charge (there is then *no cost* for the HPLMN). Also, with voice call tromboning, the service may be defective, as in many cases the information carried in the IAM (Initial Address message) of the ISUP coming from the VPLMN in the international network is truncated. It contains only the mandatory header part with the VMS called number, and not:

- the calling party number;
- the original called party number (before call deviation);
- Data or 3G Visio call indication;
- the call reference number.

As a result, VMS will not work properly when one calls someone abroad: the call is 'tromboned' back to the VMS, which must have a prompt to ask the number called, even if it was dialled when the call was made. This is a poor service and most of the time the caller will not proceed further to leave a message.

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

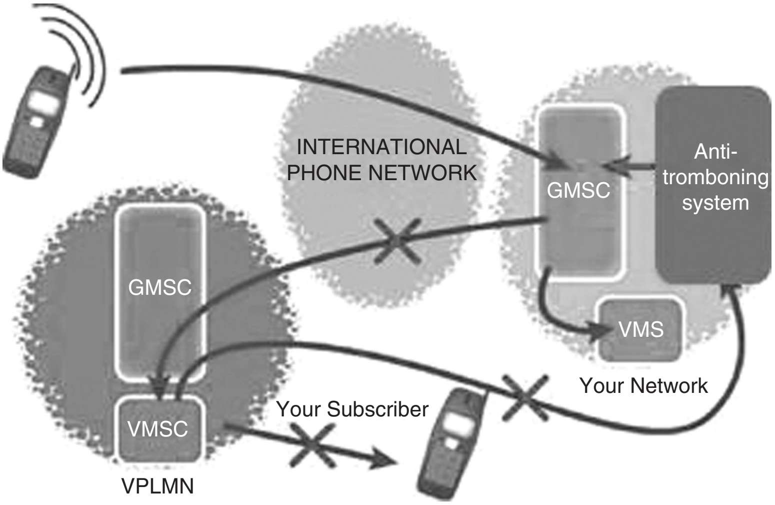


Figure 7.1 Anti-tromboning principle

The purpose of this section is to suppress the costs and guarantee the quality of service. In Figure 7.1 we see a call made to an outbound subscriber of ‘Your Network’ roaming in the VPLMN. The call goes from ‘Your Network’ to the VPLMN and the subscriber does not answer. Without anti-tromboning, another call would be made back to ‘Your Network’. The anti-tromboning effect will be to cancel the two calls (which are barred in Figure 7.1) and replace them by a local call transfer directly to the VMS, as shown by the arrow GMSC → VMS.

7.1.1 ‘Optimal Routing’ (OR) and Other Methods

Section 2.2.14 gave the standard OR principle that can be part of the Roaming Hub, as two of the most effective solutions, detailed below, only use MAP and CAMEL signalling, not ISUP.

But the VPLMN has no interest in doing it, because these automatic calls to the HPLMN partners produce considerable revenue (up to 4 USD/minute).

So the HPLMNs must have a method to suppress the tromboning from their own side. We present three types:

- Active CAMEL logic performed by an IN script in the Service Control Point;
- ISUP and MAP Call Transfer Package based;
- Passive CAMEL monitoring and MAP Call Transfer Package.

The CAMEL-based methods resolve the anti-tromboning provided that the following are in place:

- There is a CAMEL agreement between the HPLMN and the VPLMN. The first method must be developed as a special IN script by the SCP provider.
- Call Forwarding (CF) is activated in the VPLMN for the CAMEL subscribers.

The last two may be provided by other specialized suppliers but they rely on the MAP Call Transfer Package installed in the HPLMN (an option). The second method does not rely on CAMEL roaming but needs to have ‘Original Called Party’ in the ISUP, which limits the scope.

We consider that the third method, 'Passive CAMEL monitoring and MAP Call Transfer Package', is the most simple and effective as most of the voice traffic will be with Roaming Partners that have implemented CAMEL outbound roaming.

7.1.2 Active CAMEL Logic in the Service Control Point

In this case, there is no need for probes and no need to buy the MAP Call Transfer Package. But *all the subscribers must have a 't-CSI' CAMEL profile*, even if they are post-paid, with Call Handling = continue (so that if the SCP sends a CAMEL RELEASE CALL because the subscriber is not prepaid, the call continues). That is, for any incoming call, the SCP is triggered (even for a post-paid subscriber). They must *also have an 'o-CSI'*, so that the SCP is triggered when the foreign VPLMN initiates a back call to the VMS (this is called 'camelization of post-paid subscribers' and is most common in Europe for many reasons).

As shown in Figure 7.2, after interrogating the HLR (2) and (2′), the GMSC gets a 't-CSI' so it will send an Initial DP (3) to the SCP, *which contains the VLR of B* (VLR B was returned by the SEND ROUTING INFO). If it is a foreign VLR, the SCP enters the MSISDN of B or the IMSI of the Called Party contained in the Initial DP into an internal table in order to be able to obtain a matching later if another Initial DP for the same customer B (as an 'Original Called Number') arrives.

The call (4) goes to the VMSC. If B does not answer, as it is CAMEL 'o-CSI', the remote VMSC will send a new Initial DP (5) to the SCP. The SCP recognizes *that it is for IMSI B*, which is an outbound roamer, so it has to perform anti-tromboning. *There are two TCAP CAMEL transactions active at this stage for subscriber B*. To avoid the tromboning, the SCP just has to send a CAMEL CONNECT with the VMS number *within the first transaction*, then a CAMEL RELEASE CALL (7) *in the second transaction*, which will be released (8) without charging the call IAM (4). After the CONNECT, a direct call (6) was made to the VMS.

So it is quite a particular script in the SCP which performs the anti-tromboning as it correlates two TCAP transactions. The implementation must be done by the SCP supplier.

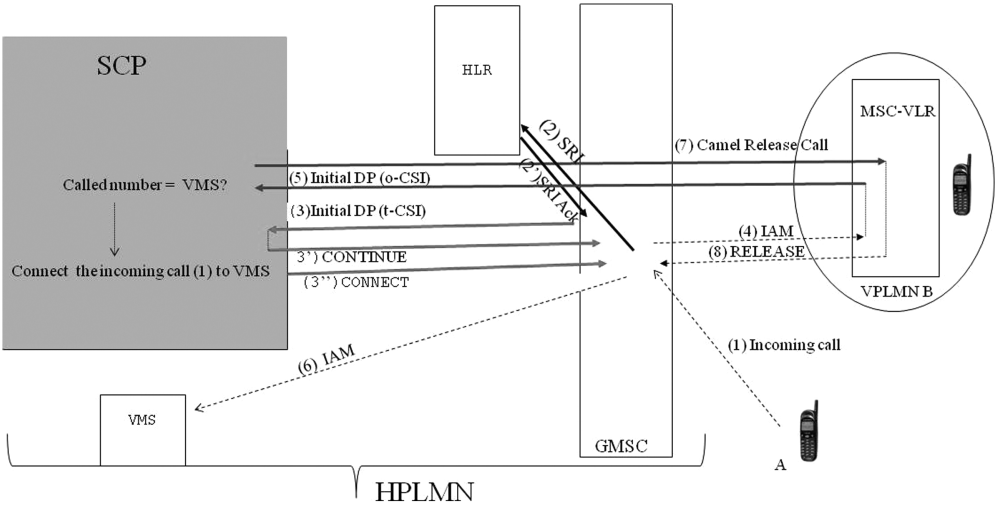


Figure 7.2 Anti-tromboning with active CAMEL logic in the SCP

7.1.3 ISUP and MAP Call Transfer Package

This method uses monitoring of the outgoing international signalling links and can be combined with the Welcome SMS installation. As a prerequisite, the MAP Call Transfer Package, which allows the Optimal Routing (OR) feature, must be installed in the GMSCs and the HLRs. But it will work only if the IAM calls received from the VPLMN through the international network, *when a call is forwarded to VMS*, contain the '*original called party*', which allows the mailbox to be identified. This is a severe limitation.

The MAP Roaming Enquiry Package for *all* the roaming partners will be set to V3 so that the MAP PROVIDE ROAMING NUMBER contains the parameter 'Call Reference', which is necessary to make a RESUME CALL HANDLING to transfer the call locally from A to the VMS. The Call Reference is unique and set by the GMSC to be used for correlation.

Even if the roaming partner does not accept PRN V3, the HLR will repeat using V2 (without the Message Reference and the GMSC Number GT), but from the probing, 'anti-tromboning' knows the Message Reference from the previous attempt.

Figure 7.3 shows the case when the anti-tromboning system is separate from the VMS (it can be integrated). In this case, the 'forward-to-number' in the HLR profile for 'busy', 'no response', and 'not reachable' (all the cases of Call forwarding to VMS) *must have the ISUP number of the anti-tromboning system*, not the VMS, so that the IAM reaches it.

A makes a call to B roaming away. The GMSC sends a SEND ROUTING INFO (2) to the HLR, which sends a PROVIDE ROAMING NUMBER (3) to the VLR *with the 'call reference' if V3 is set*. The IMSI and call reference are monitored and paired by the anti-tromboning system (3″). The Roaming Number is returned (3′) then (2′) to the GMSC, which makes an outgoing call (4) to the VMSC.

If B does not answer, the VMSC will call (5) the 'forward-to-number' in the visitor's profile that is the anti-tromboning system (5′). No call is charged yet because neither (4) nor (5) are answered.

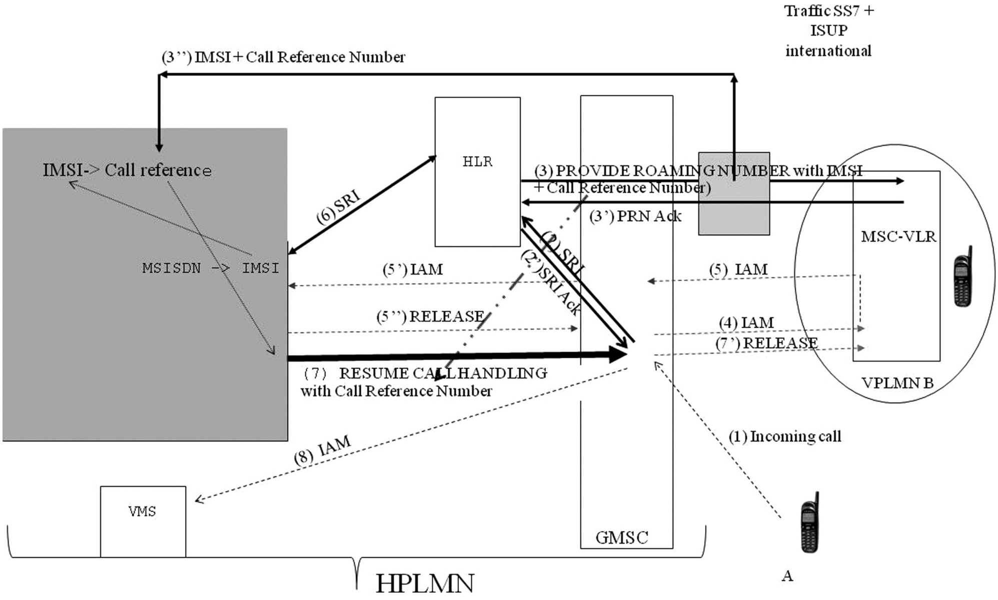


Figure 7.3 Anti-tromboning with ISUP and MAP Call Transfer

We must assume that the international ISUP transmits the ‘original called number’ = MSISDN of B, so that the anti-tromboning can interrogate the HLR (6) to obtain the IMSI. With the IMSI, it can get the call reference, which is the key of the RESUME CALL HANDLING containing the VMS number (from a table with the MSISDN). The call (1) is transferred (8) locally to the VMS and the anti-tromboning system performs a RELEASE (5″), so that neither call (4) or (5) will be charged.

7.1.4 Passive CAMEL Monitoring and MAP Call Transfer Package

This is a combination of the two methods above:

- CAMEL ‘o-CSI’ profile in the HLR for all the subscribers (*but not* t-CSI for the post-paid subscribers) with:
  - probes;
  - MAP Call Transfer Package.

It is *fully passive*, using probes to detect the signals, which allow it to perform anti-tromboning, but it relies, as in 7.1.3, on the MAP Call Transfer Package. Also, if the system fails, the anti-tromboning is simply not performed.

7.1.4.1 MAP Roaming Number Enquiry Package V3 Available

To simplify the initial explanations, we will assume that PROVIDE ROAMING NUMBER works in MAP V3 from the HPLMN to the VPLMN. Then we will explain the method for making it work in versions ≤ MAP V2 if required.

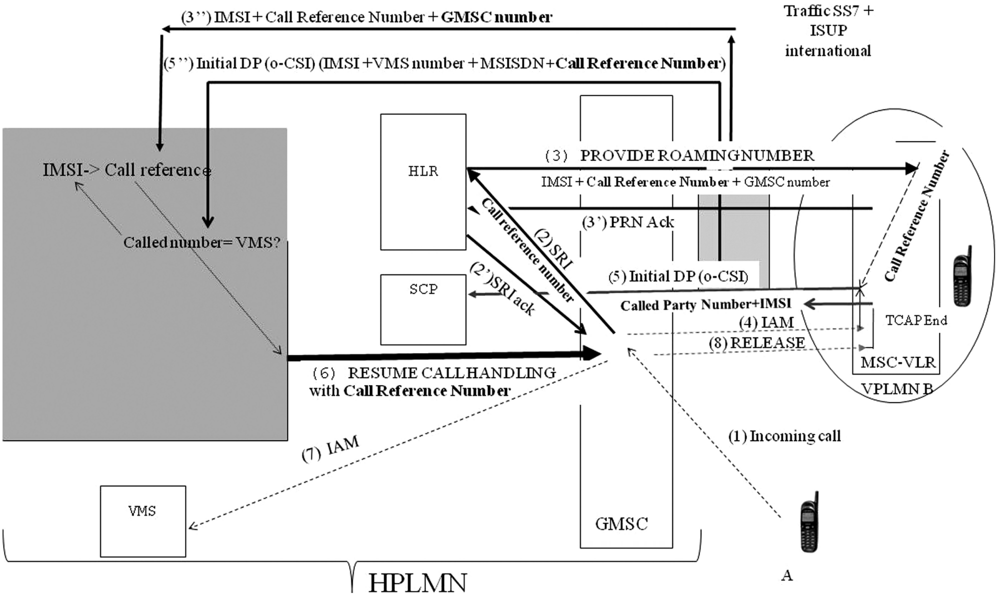

(3'') IMSI + Call Reference Number + GMSC number
Traffic SS7 + ISUP international
(5'') Initial DP (o-CSI) (IMSI +VMS number + MSISDN+Call Reference Number)
IMSI-> Call reference
Called number= VMS?
HLR
SCP
(3) PROVIDE ROAMING NUMBER
IMSI + Call Reference Number + GMSC number
(3') PRN Ack
(2) SRI
Call reference number
(2') SRI ack
(5) Initial DP (o-CSI)
Called Party Number+IMSI
(4) IAM
(8) RELEASE
Call Reference Number
TCAP End
MSC-VLR
VPLMN B
(6) RESUME CALL HANDLING with Call Reference Number
(7) IAM
(1) Incoming call
VMS
GMSC
HPLMN
A

Figure 7.4 Anti-tromboning with Passive CAMEL monitoring and MAP Call Transfer

As this is the best method, we will explain it step by step so that developers and operation staff can have a complete understanding of it:

(1) Assume a call (1) is made by A to B, who is roaming and is CAMELed with ‘o-csi’ (this is the ‘trigger’ for outgoing calls) even if they are post-paid.
(2) A SEND ROUTING INFO (2) (including a Call Reference Number assigned cyclically by the GMSC if MAP V3 is installed), and the GMSC number GT is then sent from the GMSC to the HLR.
(3) The HLR sends a PROVIDE ROAMING NUMBER (3) to the foreign VMSC which contains this same Call Reference number and the same GMSC number GT (if MAP V3 is used between HPLMN and VPLMN), otherwise there is no Call Reference Number and GMSC number.

Action #1 of the Anti-tromboning System in the HPLMN

As above, the three parameters **IMSI + Call reference Number + GMSC number GT** are monitored (3″) by the anti-tromboning system and recorded temporarily for about 30 sec.

(4) Then the GMSC sends a voice call (4) to the subscriber B ‘Roaming number’ received in the Ack of the PROVIDE ROAMING NUMBER (3′). This is a number belonging to the range of the VPLMN.
If B does not answer, the VMSC will want to make an ISUP call to the **‘forwarded-to number’** (the VMS number in general) in its VLR customer profile.
(5) But B is assumed to have a CAMEL profile ‘o-csi’, so the VMSC sends a CAMEL InitialDP (5) to the SCP to check the credit and charge the call from VPLMN to HPLMN.

Action #2 of the Anti-tromboning System in the HPLMN

(6) This received *CAMEL InitialDP is read (5″)* by the anti-tromboning and if the CAMEL parameter **‘Called Party Number’** *is present* (in a usual call it is empty, it is the ‘Called Party *Before Call Deviation* Number’ which is filled), *it shows that it is a conditional call forwarding with ‘tromboning’*. Whether the call to the outbound roaming subscriber is forwarded conditionally to the VMS or to a personal number, it will then work in all cases. *We do not need to bother about the particular value of ‘Called Party Number’ or to provision anything about the VMS number(s).*

The anti-tromboning system makes use of the **IMSI** from *the InitialDP* as a key to get the required parameter from the PROVIDE ROAMING NUMBER record.

$$\text{IMSI} \rightarrow \text{GMSC Number GT}$$

(The system works in a large network with several GMSCs.)

Note that this record will have the same Call Reference Number as in the Initial DP because MAP V3 was used (the VMSC uses the Call Reference Number if received in the PROVIDE ROAMING NUMBER to set that in the Initial DP). But we use the IMSI as a key in order to find a record, even if MAP V2 had been used in fall-back. No Call Reference Number is present, as explained in the next section, so that the system also works if the VMSC accepts only MAP V2 PROVIDE ROAMING NUMBER.

Then it sends a MAP RESUME CALL HANDLING (6) to the GMSC GT concerned (we had the GMSC number from the PROVIDE ROAMING NUMBER parameter), with the following MAP parameters:

- **Call Reference Number** from CAMEL (identifies the incoming call (1));
- **Called Party Number** (from the InitialDP = the VMS number);
- **GMSC number GT** from the PRN (this is a required parameter).

(7) The GMSC will transfer the call (1) to the VMS *without any international cost* and with full mailbox identification *with a new call (Initial Address Message (IAM)) (7).*
(8) How does it terminate? The GMSC will make an ISUP RELEASE (8) to terminate the voice call (4) as a consequence of the call transfer, and the VMSC will send a CAMEL ‘Release Call’ in a ‘TCAP END’ to close the transaction (5) containing the InitialDP.

If B makes an ordinary call, there is an Initial DP also from the VPLMN to the SCP, but the anti-tromboning logic will not do anything because the CAMEL parameter ‘Called Party Number’ is absent. If the subscriber is post-paid, the SCP will send CAP RELEASE CALL, but as the Call Handling has been set at ‘Continue Call’, the call will normally proceed and be charged by the normal roaming billing.

So this passive solution is quite simple and elegant, working for large networks with several GMSCs, provided that the HPLMN has the MAP Call Transfer Package and MAP V3 for the MAP Roaming Number enquiry package between HPLMN and VPLMN. Also, it does not require any special provisioning for the customers, not even a table of their VMS numbers (if there are several). The provisioning is done when the conditional call forwarding number is provided in the HLR or by the subscribers themselves with their handset.

7.1.4.2 How It Works for the Case PROVIDE ROAMING NUMBER is ≤ MAP V2

The HPLMN will still declare the VPLMN in V3. So first PROVIDE ROAMING NUMBER #1 is sent in V3, which allows it to probe the IMSI, the Call Reference Number and the GMSC number. It will be rejected by the VPLMN and the HPLMN *will repeat this in V2* (PRN #2 without the Call Reference Number and GMSC number), *but the previously probed Call Reference number is still valid for the GMSC call transfer*, and it was recorded in the anti-tromboning database. However, the Call Reference Number in the Initial DP (5) will not correlate with it, because the PRN #2 which is accepted by the VPLMN does not include one.

The incoming Initial DP (5) is read and if the CAMEL ‘Called Party Number’ is present, we extract the IMSI to perform the direct call transfer.

When we access the temporary database, we will find two PROVIDE ROAMING NUMBER records for this IMSI (the first corresponding to V3, the second to the V2 fall-back).

We use record #1, which has the **Call Reference Number** and the **GMSC number GT**, to send the RESUME CALL HANDLING to the GMSC concerned with the:

- **Call Reference Number** from PRN #1 (identifies the incoming call (1));
- **Called Party Number** (from the Initial DP = the VMS number);
- **GMSC number GT** from PRN #1(this is a required parameter).

In summary, with this anti-tromboning system it is possible to:

- allow full VMS services: deposit + retrieval for outbound subscribers even in the case when the International voice ISUP network does not transmit the Calling Party number or the Original Called Party number (frequent case);
- suppress all tromboning costs.

7.1.4.3 For the Developers: All the Trace Details

If you develop an anti-tromboning system, here are the details of the recommended method.

The number of the CAMEL outbound roamer of Armenia (+374) (roaming in Lebanon (+961) is +37494987654. It has VMS supplied (forward-to-number = +37493297130) and the no-reply Conditional Forwarding condition at 10 sec.

We make a call to this number from +33140123456 in France (+33):

(1) Anti-tromboning monitors the international SS7 and then after 10 sec receives:
   - *** InitialDP indication ***;
   - CallReferenceNumber=1584B40001;
   - IMSI=+**283052000345678**;
   - called Party BCD Number: **absent**, (BCD means Before Call Deviation);

– called Party Number = **present** +37493297130, (that shows that the call is redirected);
– calling Party Number = +33140123456, (calling party from France);
– original Called Party ID = +37494987654 (the called number of Armenia);
– redirection Information: **no reply**;
– redirecting Party ID = +37494987654 (also the called number of Armenia).
It is recognized as Call Forwarding because the 'calledPartyNumber' is **present** in the InitialDP.

(2) Anti-tromboning makes a request in this case to the PRN temporary database using the **IMSI** as a key. The example is the well-known SQL database request: SELECT * FROM 'ProvideRoaming Number' WHERE 'IMSI' like **'+283052000345678**' AND 'CallReference' not like '0'.

(3) The record returned by the database is:
– IMSI = **+283052000345678**, VMSC = +961360023 (this is Lebanon), GMSC = +37493297100, CallRef = *1584B40001*.
(The same CallRef is obtained: it matches that in the InitialDP. It also provides the required GMSC number GT to which we send the RESUME CALL HANDLING).

(4) Anti-tromboning *sends* (it is active then) to GMSC = +37493297100:
– *** MAP RESUME CALL HANDLING request ***;
– IMSI = **+283052000345678**;
– CallReference = *1584B40001*;
– Forwarding Options = **no reply**;
– Forwarded-to-Number = +37493297130.

As you can see, the 'redirection Information' = **noreply** from the Initial DP is sent back in the RESUME CALL HANDLING parameter 'Forwarding Options', so that the IAM ISUP message (7) of Figure 7.4 will also have it. If the VMS has different prompt messages when the called subscriber does not reply ('your correspondent has not answered' or 'your correspondent is busy'), it plays the appropriate prompt.

(5) The GMSC returns a MAP RESUME CALL HANDLING confirmation to Anti-tromboning, indicating that the call transfer to VMS has been successful.
(6) Then the VMSC (Lebanon) sends a CAMEL RELEASE (8) to the SCP (Armenia) which Anti-tromboning monitors and shows that the tromboning attempt has been successfully cancelled.

7.2 Call Back and Local Calls Optimization

We want to suppress (or reduce) the charges from the roaming partners when an outbound subscriber is making a call. The most striking example will be an outbound subscriber A making a call to a number B in the same VPLMN. Two principles will be used to suppress the charge or reduce it:

- Replace the outbound call by a 'call back' (a call A → B could be charged at 4 USD/minute while a call HPLMN → VPLMN in general costs much less as it is paid by the HPLMN at prices carefully negotiated with its supplier).
- Replace the call A → HPLMN B → VPLMN B by a local call A → B.

7.2.1 Classical Call

In Figure 7.5, the HPLMN of A will be charged by the VPLMN for a long distance (1) call to HPLMN B, which has to charge its subscriber B for the call (2) to the VPLMN.

7.2.2 Call Back: Ergonomics Improvement with a SIM Tool Kit

Call back, in particular the use of USSD, has been a favourite since 2000. When A wants to call any number, they perform a 'USSD call':

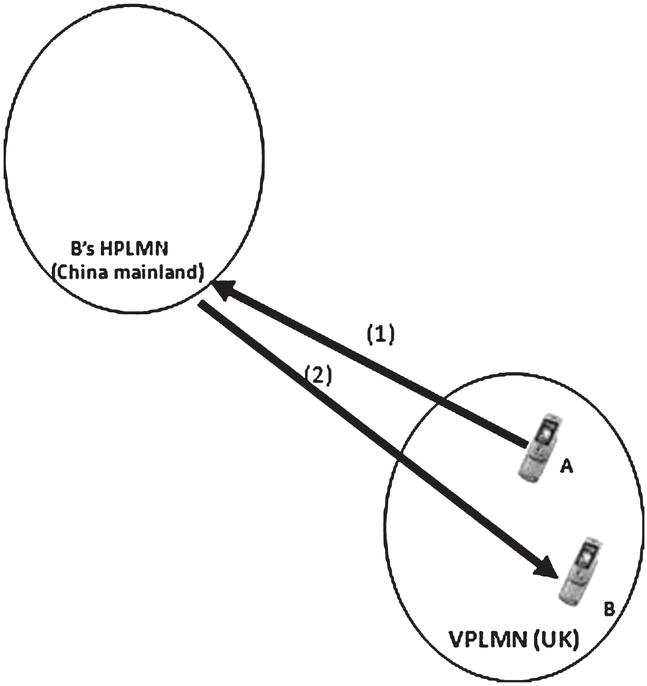


Figure 7.5 Classical outgoing call while roaming

- 222*Number of B# (if 222 is the Call Back service number);
- then press the Call button of the handset.

A PROCESS USSD REQUEST (such as (1)) is sent from VPLMN to the HPLMN HLR then to a Call Back platform. This gets the roaming number of B (3), and performs two calls: a call back (3) to A and a call (4) to the roaming number of B.

The ergonomics are poor (the address book cannot be used) and USSD is often not available in the VPLMN for roamers, in particular, to avoid this procedure which loses revenues for the VPLMN.

This is much improved if HPLMN A installs a SIM Tool Kit in the SIM cards, as shown in Figure 7.6. With 'SIM Card Call Control' (see Chapter 9), the call control is transferred to the SIM card when *a number is dialled normally*. The STK can then send a message (1), USSD, SMS-MO (it can be rejected without charging) or some other MAP message [2.1], which is always opened in the VPLMN.

The rest is the same as previously; there is still call back but the ergonomics are almost those of a normal call. And B does not pay to receive the call.

7.2.3 Call Back: Ergonomics Improvement with a CAMEL Platform

Another approach to Call Back, to give transparent call dialling ergonomics, *is to set all the outbound subscribers as CAMEL whether they are post-paid or prepaid.* When a call is made, an INITIAL DP (1) is send from the VPLMN to the 'proxy' HPLMN in the VPLMN, as shown in Figure 7.7.

The 'SCP Proxy' gets the A-number in the Calling Party Number of the INITIAL DP as well as the B-Number. The Call Back procedure is the same. And in order that A is charged if it is post-paid, the SCP will behave as an SSF with 'o-CSI' to the real SCP. The price can be better for A while the

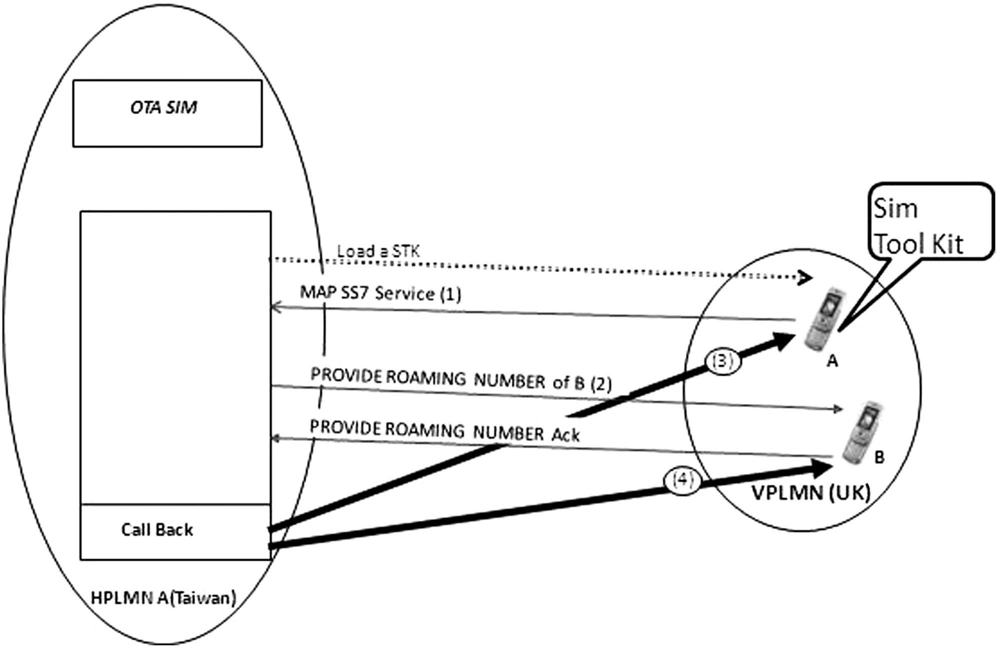


Figure 7.6 Call Back with SIM Tool Kit

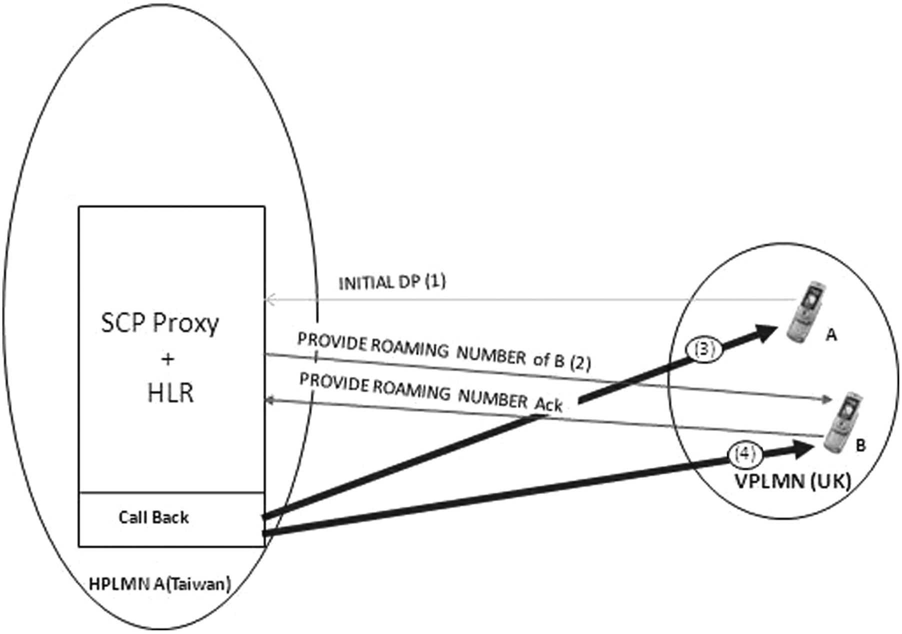


Figure 7.7 Call Back with forced 'CAMEL'

HPLMN also increases the margin. This is possible because the Inter Operator Tariff (IOT) charge from VPLMN to HPLMN A has been suppressed. This is less general than the previous solution which did not require a CAMEL agreement between HPLMN A and the VPLMN. However, it is more efficient, because it can be extended to a 'Local Roaming Number system'.

7.2.4 Implementing Call Back: Use an IVR or Simply CAMEL?

Most current call back systems use a clumsy IVR triggered by some USSD platform to make the two calls to A and B. In Chapter 1, you have the list of CAMEL primitives and there is *'Initiate Call Attempt (ICA)' (Phase 4)*. It was specified for 'wake-up calls': the SCP has the wake-up times of the subscribers and makes the call with a voice message (no IVR involved, of course).

With the 'SCP proxy' method, as the system has the CAMEL ICA service, it can directly use the existing MSC-SSF (provided it has the SSF part of ICA) to make the calls without any additional equipment.

7.2.5 Fully Transparent Ergonomics: Local Roaming Number System

The Call Back procedure is not really transparent (no ring-back tone), even if the Call dialling can be made transparent. Assume we use the CAMEL method. If the Call Back system finds that B (from the Called Party Number in the Initial DP (1)) is in the same VPLMN as A, a local call will always be cheaper.

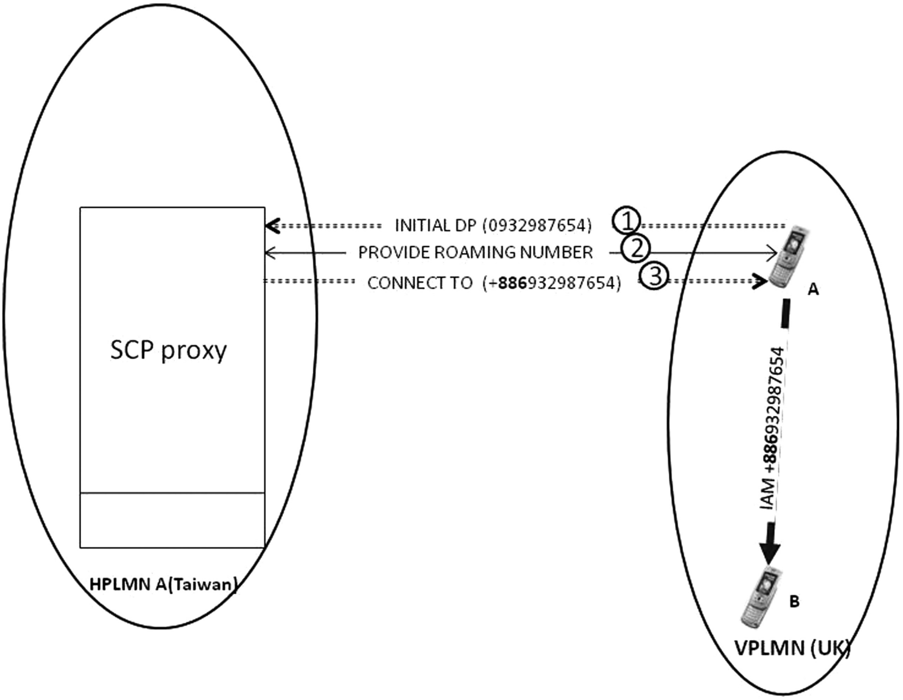


Figure 7.8 Local Roaming Number: A of Taiwan, roaming in the UK, makes a local call to B in the UK

Figure 7.8 shows a Local Roaming Number.

The system will query the Roaming Number of B (2).

Then the SCP proxy makes a CAMEL CONNECT (3) (to the Roaming Number of B): the call is completely normal with ring-back tone. In fact, it provides the same transparency as if the VPLMN had installed Optimal Routing. The best solution is a CAMEL-based system with a combined Call Back and Local Roaming System. With a very detailed table of all the IOTs, it can take the cheapest.

The same service, including Local Call, could be done with a SIM Tool Kit, but ordering, having and deploying an STK solution will take about six months, while the CAMEL-based solution is immediate.

7.3 Dialled Number Correction with CAMEL

Another elegant application of 'forced CAMEL' for post-paid outbound subscribers is dialled number correction. If the Taiwanese subscriber is in the UK and dials a national home number B 0932987654 from their address book, it will fail in the visited network because the number is not in international format. A method and agreement exists where the VPLMN creates a specific number table for certain roaming partners in the MSCs, such that based on the Calling Party number (e.g. **+886**935123456) it will perform:

- 0932987654 → **+886**932987654.

But this method requires a special feature in all the VPLMNs. A better method, because it is under the control of the HPLMN, is to use the 'forced CAMEL', as shown in Figure 7.9.

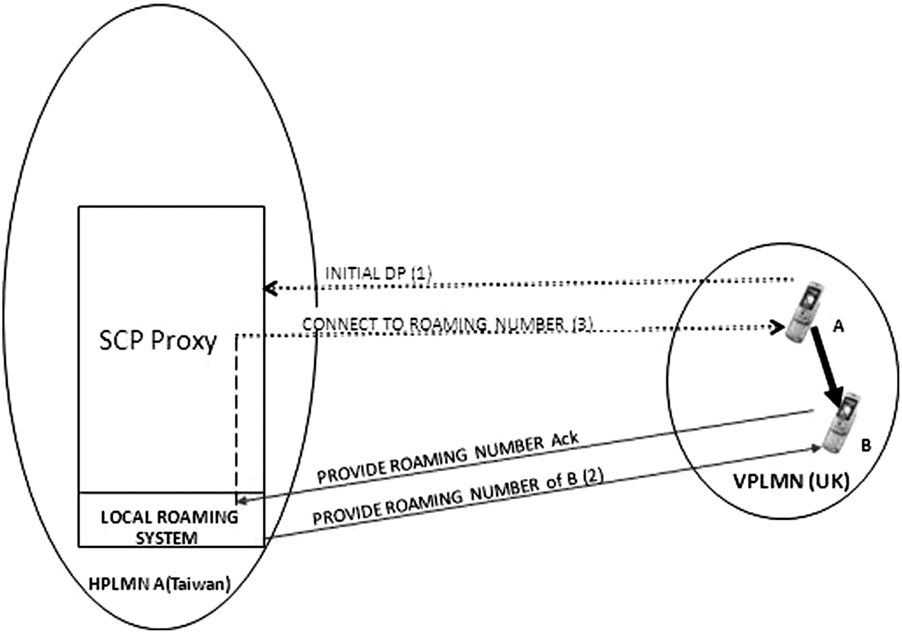

SCP Proxy
LOCAL ROAMING SYSTEM
HPLMN A(Taiwan)
INITIAL DP (1)
CONNECT TO ROAMING NUMBER (3)
PROVIDE ROAMING NUMBER Ack
PROVIDE ROAMING NUMBER of B (2)
A
B
VPLMN (UK)

Figure 7.9 Dialled number correction with CAMEL

The Initial DP has 0932987654 as ‘Calling Party Number before call deviation’. In the HPLMN SCP, it is easy because it is one of the subscribers to make the above transformation (any national destination number). And the ‘trick’ is to send a CAMEL CONNECT to +886932987654 instead of a standard CAMEL CONTINUE (0932987654 would be dialled by the VMSC and would fail).

As a result, one should not be surprised when CAMEL traces are analysed to see that many SCPs use CONNECT instead of CONTINUE systematically. If, in addition, the Roaming Number of B is used instead of the MSISDN, the Local ‘Roaming Number System’ is implemented. If there is a group travelling in the same country, this provides large savings which can be allocated by the HPLMN to reduce charges for its customers as well as increase its margin. The tendency to have a ‘proxy SCP’ for roaming optimization is strong and the service can easily be added in a Roaming Hub as it includes only SS7 signalling.

References and Further Reading

[7.1] Henry-Labordère, A., ‘Système Optimisant le Renvoi Tardif d’Appels vers une messagerie vocale de mobile (SORTA)’, Patent FR 05 51804.

8

SIM Cards ‘Over The Air’ Provisioning

May you be in heaven, half an hour before the devil knows you are dead.

Irish toast

8.1 Principles of SIM OTA Using SMS: Download and Upload

Remote updating of the SIM is relevant to virtual roaming for:

- adding or modifying a SIM Tool Kit, such as one used for the Virtual Roaming bi-IMSI (outbound subscribers);
- modifying the network preference list to optimize the cost of roaming;
- backing up the address book.

8.1.1 Applications and Different OTA Methods: for Handsets and for SIM Cards

OTA means ‘Over the Air’, in other words remote action by a Service Centre, part of the Virtual Roaming equipment, on a remote handset or the SIM card in the handset (these are distinct objects).

Handset
This is more ‘application oriented’ and is used for:

- downloading a WAP profile so that the phone becomes GPRS enabled;
- downloading a game (‘Java Applet’), etc.

This is used, for example, to provision the GPRS access parameters of a handset (‘OTA GPRS’), and is the subject of the next chapter.

SIM Card
This is more ‘Telecom oriented’ and is covered here. It is used to:

(1) ‘download’ (meaning from your SMSC to the SIM card) for functions such as:
   – updating the SMSC parameters (or a particular file in the SIM);

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

- restoring the personal Address Book after a SIM card change;
- loading a ‘Java card’ application (a ‘SIM Tool Kit’), which may create a new menu for your applications or perform special ways of making a call (automatic ‘call back’ for example).

(2) ‘upload’(reading the SIM card into your SMSC) to perform functions such as:
- remote backup service for the personal Address Book in the SIM etc.

There are three ways of updating or reading a SIM card:

(1) Locally, with a ‘card reader’ into which the SIM is inserted and which is connected to a USB interface of a PC with the proper software. It requires the customer to come to one of your offices.

(2) With ‘Cell Broadcasting’. This does not concern us, as we want to be able to perform any OTA on the SIM cards, even visiting another network, and also few networks have general coverage Cell Broadcast installed.

(3) With SMS. The big advantages are:
- coverage in any network visited by your handsets;
- very high security with the personal SIM card OTA keys that you hold (128 bit key); only you can download or upload the SIM card;
- secured ‘Proof of Receipt’ to be sure that the end-to-end action has been performed for the identified customer, allowing the handling of sophisticated transactions such as payment by handsets with secure customer authentication;
- ‘upload’ possibility (reading of the SIM card), which is sometimes not known and is important. For example, reading the ‘SIM Service Table’ allows the checking of which services are allocated to the customer.

An integrated OTA server handles SMS OTA only and does so in a particularly efficient manner *due to the integration of the OTA process into the SMSC*. It allows *a very high speed* to be achieved even for the large files which may need to be loaded.

There is a Web Interface to OTA a particular customer, and also a ‘bulk facility’ which allows it to quickly OTA a large number of customers. The ‘bulk facility’ is very much like the HALYS ‘bulk SMS’ that you are used to handling.

8.1.2 The SMS SIM OTA: How it Works for Download and Upload

In Figure 8.1 we see three cases.

On the left, Figure 8.1 shows the ‘download’ of a file from the SMSC to the SIM. It sends an SMS with one or more FORWARD SHORT MESSAGE MT (SMS-MT Mobile Terminated) to the handset, which sends it to the SIM card and Acknowledges the result. The handset sends it to the SIM card and sends back the FORWARD SHORT MESSAGE MT Acknowledgment with OK or not OK.

The SMSs sent to the SIM card contain the commands to write to the SIM card as well as the data to be written.

8.1.2.1 PoR by SMS-MO ‘SUBMIT’

The middle part of Figure 8.1 shows the ‘upload case’. Commands to read a file of the SIM card are sent, as well as an indication that the result should be sent by the handset to the SMSC as an ordinary SMS-MO (as sent by a normal customer). An interesting feature is that the ‘Return Path’ is set automatically! The handset sends the SMS-MO with the data t*o the originating SMSC even if it is not the usual SMSC setup in the SIM card*. One can understand why it is like this in the GSM design: there can be several SMSCs and the OTA upload should always arrive at the sending SMSC. This method is quite general and works with any handset.

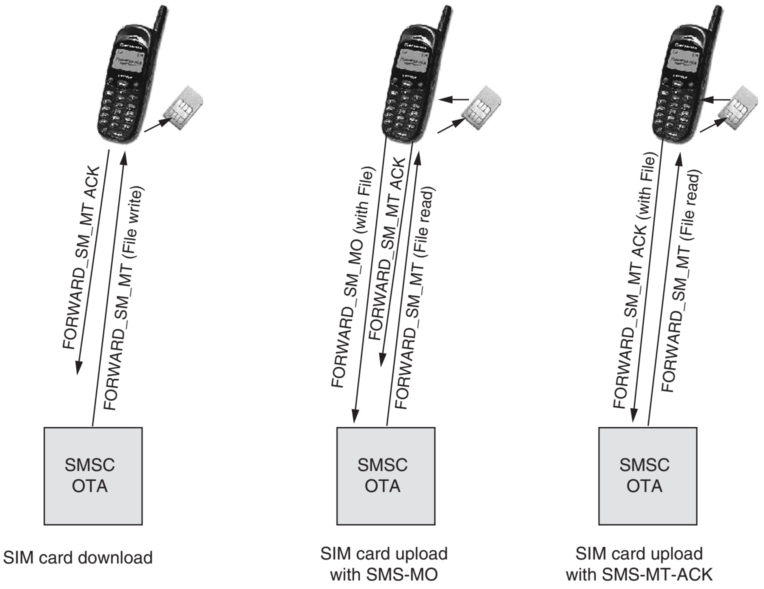

FORWARD_SM_MT ACK
FORWARD_SM_MT (File write)
SMSC
OTA
SIM card download
FORWARD_SM_MO (with File)
FORWARD_SM_MT ACK
FORWARD_SM_MT (File read)
SMSC
OTA
SIM card upload
with SMS-MO
FORWARD_SM_MT ACK (with File)
FORWARD_SM_MT (File read)
SMSC
OTA
SIM card upload
with SMS-MT-ACK

Figure 8.1 Upload and download of SIM cards

8.1.2.2 PoR by SMS-MT Ack 'DELIVER REPORT'

On the right of Figure 8.1 is shown another method for 'upload', where it is specified that the result of the reading should be received in the SMS-MT Acknowledgment (a parameter containing an SMS of type 'DELIVER REPORT'), as specified in the command sent to the SIM card. It looks simpler, but not all handsets properly implement the standard. This parameter is included if the MAP version of the Short Message Relay Package V3 is supported in the VMSC.

To use the standard vocabulary, the small arrow from the handset to the SIM is 'Local Data Download' and from the SIM to the handset 'Local Data Upload'.

8.1.2.3 OTA with a Chain of Hubs

Figure 8.2 further illustrates the case of OTA SIM through a chain of SMSCs with the 'Roaming Hub (SMSeXchange)' capability in the middle. If an 'origin SMSC' has asked for a PoR for the download, it will be able to receive the PoR, because the PoR will go to the 'Final SMSC' used in this download and not to the 'Home SMSC B' in the handset.

To use the standard vocabulary, the small arrow from the handset to the SIM is 'Local Data Download' and from the SIM to the handset 'Local Data Upload'.

Not all SIM cards have the OTA 3.48 capability. If you request a PoR (Proof of Receipt), you should always receive it (including error reject) if it has OTA 3.48. The PoR is a very important feature as it is generated 'end-to-end' by the SIM card and cannot be faked.

8.1.3 Checking the Result of a SIM Download with the Handset

After a successful upload (from the PoR) with an address book, you may be surprised that the entries do not appear in the handset directory! This is because the list of entries in the handset (not the SIM card) *is updated only when the phone is switched on*:

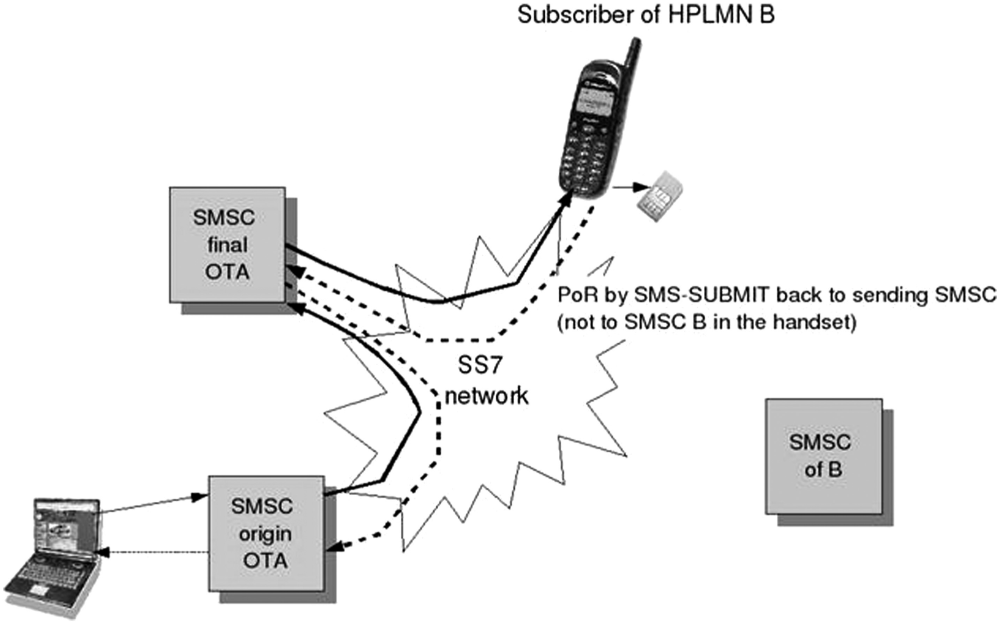


Figure 8.2 OTA involving an SMSeXchange

- You immediately see the entries which have been modified.
- But *you will only see the new entries after switching Off then On*.

8.1.4 Uploading Large SIM Files with Concatenated SMS: Single PoR

An integrated OTA SIM server can upload large SIM files very efficiently (Address Book with 100 entries for example). For further details see the detailed example 8.3.2.2 for this type of payload: there is only one Secured Data Command Header and only one set of SELECT commands in the SIM directory for the Abbreviated Dialling Number file.

There will be only *one PoR* (Proof of Receipt) (for example the reception of an SMS-MO if the PoR by SMS-SUBMIT was selected) for *the sequence of many concatenated SMSs*. This single PoR is received by the sending SMSC and is stored for matching with the sent payload. It contains the number of GSM 11.11 commands successfully executed.

8.1.5 Security in OTA

There are personal data on an operator's SIM cards. So with their card manufacturer they will select a 'Minimum Security Level' for the files of the SIM card, which is defined in the standard GSM 11.11 with their individual security level for READ or UPDATE.

(When using a local card reader, you can get access to the SIM card by sending a command with the 'PIN Code'.)

This security method *does not apply to OTA*, and the local security GSM 11.11 commands such as VERIFY CHV (Verify 'Pin Code') do not apply to OTA, only to a local card reader.

The security is ensured by either a Digital Signature or a Ciphering Checksum, eventually with full ciphering based on individual (secret) keys for each SIM card. Without them, no one can read or update the SIM card by OTA.

The security is based on:

- a method (the 'Minimum Security Level') which is factory programmed in the SIM and not readable or modifiable, either with a card reader or by OTA;
- a signature authentication key KID, configured individually for each SIM by the manufacturer and not readable; all OTA systems apply at least this 'signature' security, which leaves the data clear;
- a key KIc for optional ciphering of a payload, configured individually for each SIM by the manufacturer and not readable.

These keys are not readable by OTA or by a local card reader. The KiC and KID can be modified only with:

- knowledge of their current value;
- a special modification key KIK.

The basic algorithm for a signature (with KID) or for ciphering is the well-known DES (one 56-bit key padded to 64) or 3DES 'outer CBC' (cipher block chaining) with two 56-bit keys padded to 64, known as K_1 and K_2.

Note: How does 3DES outer CBC work?

The principle uses the standard well-known DES, which works with a key padded to 64 bits, three times.

Let **M** be the Message to be encrypted by the 3DES outer CBC algorithm.

Let **K1** be the first 64 bits of the KID, and **K2** the last 64 bits of the KID.

The Encrypted Message E(M) by 3DES outer CBC is:

$$\mathbf{E(M) = E_{K1}(D_{K2}(E_{K1}(M)))}$$

Where:

- E_K is the DES encrypt with the key K;
- D_K is the DES decrypt with the key K.

And the 'Cryptographic Checksum' is the last eight bytes of E(M).

Cipher block chaining means that data are coded in blocks of 64 bits, but because the result of a block also depends on the previous one, the algorithm for a block takes as initialization the result of the last one.

8.1.6 SIM Download/Upload: Different Type of Applications

8.1.6.1 On Request General SIM Downloads

- SMSC parameters.
- Forbidden HPLMNs (when a new national competitor appears).

8.1.6.2 Regular (2–3 months) General SIM Downloads

- Preferred HPLMNs (to optimize the 'Steering of Roaming' in the most efficient and legal way).

8.1.6.3 Real-time Individual SIM Uploads (Read the Content of the Handset)

- Change in handset and IMEI (needs SIM Tool Kit): stolen handset detection.
- Network Measurements (QoS and detailed location computation) (needs SIM Tool Kit).
- Address Book on request backup (standard SIM).

8.1.7 Integrated vs External OTA SIM Servers

8.1.7.1 Downloaded File Size and Performance Issue When Using OTA by SMS-PP

SIM cards used to be 16 Kb (rarely with OTA 3.48) and are now 32, 64 and 128 Kb (necessary for the largest SIM Tool Kits) with current developments (2007) at up to 1 Gb. If you consider a large SIM Tool Kit (12 Kb), whenever there is a change, it must be entirely downloaded and installed in the SIM card. As the useful data size of a ‘concatenated SMS’ is about 130 bytes, that will make 12 × 1000/130 = 93 SMSs for each SIM card. Although 140 bytes (maximum) are available for each binary SMS, there is a Header which must be created to ‘concatenate’ the long SMS so it can be handled as a whole. So the useful data is about 130 bytes.

So if these 93 SMSs are sent with a standard SMS procedure, it uses a lot of radio resources (one new paging for each SMS) and time (about 10 sec for each SMS in the best case when the OTA server is sending a new one as soon as the previous one is acknowledged).

8.1.7.2 External OTA SIM Servers from Card Vendors

All card vendors sell their OTA SIM platform on a ‘one off’ or often on a service basis. They rely on the SMSC of the mobile operator for the transmission of SMSs to the SIM cards and are mostly connected to the SMSC using the SMPP standard protocol. In the example of a 12 Kb file, the best that can be achieved is 93 × 10 = 930 sec (¼ hour) to download the whole file. And if there is a radio coverage problem during the sequence, this is a lot greater because of the retries.

So it makes the downloading of large SIM Tool Kits rather impractical, and the card vendors often propose replacing the card (at a cost) for a software update in the SIM Tool Kit.

8.1.7.3 Integrated (with SMSC) OTA SIM Servers

With an OTA SIM server integrated with the SMSC, the 12 Kb file is simply transferred to the SMSC (using FTP for example) with the phone number and the security key. Then the ciphering (if requested), the computation of the secured signature, the segmentation and the coding of the header are done by the SMSC. Why is it a lot more efficient and faster?

It is because the SMSC can use the very efficient SMS-MT delivery provided by the V3 version of the MAP protocol, since it can send the first SMS of the sequence (initial paging) with the parameter ‘More Message to Send’, then all the following SMSs (*the network does not perform any more radio ‘paging’*). Because there is no ‘paging’, the SMS-MT delivery takes 1–2 sec instead of 6–10 sec and it does not waste radio resources.

But the possibility of using a different procedure SMS-MT for the different SMSs *is not available in the SMPP protocol* for an ‘external OTA SIM server’! There is just ‘sm_submit’ in the protocol, which makes an HLR interrogation, then a radio paging sends the SMS, 93 times in the example.

So the OTA SIM server integrated with the SMSC will be a lot more efficient; only using radio paging and about 100 sec (less than 2 minutes) on average instead of ¼ hour for the same 12 Kb SIM Tool Kit file.

8.1.8 Bi-IMSI SIM Tool Kits for Virtual Roaming

This STK is very useful as an automatic IMSI selection can be done automatically without manipulating two SIM cards. The principle is:

- When the handset is turned on for the first time, the STK takes control and tries to register using the 'nominal IMSI', trying the various networks which are providing local coverage. The UL takes about 10 sec if successful. The handset tries all the networks in sequence.
- If it has failed with all the networks, it tries to register using the 'auxiliary' IMSI.

If there are many networks covering the area, a successful first registration in a new country can take more than 2 minutes.

In order to speed up another 'Update Location', the STK should have application files in the SIM card to record the last network it had registered in (this is the standard EFloci file for Location Information with the last four networks the handset was registered in) and also which IMSI it had used. There are good and poor STKs, so when a vendor is selected, care must be taken to test the above points to provide customer satisfaction.

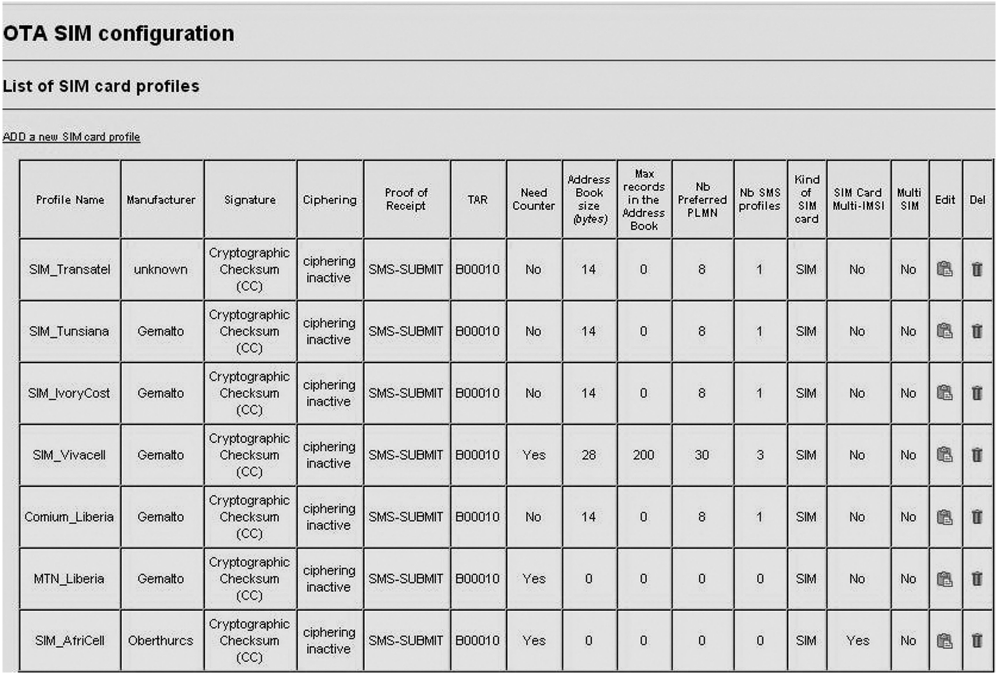
8.2 OTA SIM Provisioning Interface Examples

The SMSC with an OTA SIM module allows it to have an OTA provisioning interface to describe the profile of the SIM cards and the individual keys of the SIM cards which are necessary.

8.2.1 SIM Card Profiles

The OTA SIM server associated with the Roaming Hub service must have a menu showing all the SIM profiles already configured with their different parameters.

Several SIM cards can belong to the same profile and the profile parameters are applied for all the SIMs.



OTA SIM configuration

List of SIM card profiles

ADD a new SIM card profile

Profile Name	Manufacturer	Signature	Ciphering	Proof of Receipt	TAR	Need Counter	Address Book size *(bytes)*	Max records in the Address Book	Nb Preferred PLMN	Nb SMS profiles	Kind of SIM card	SIM Card Multi-IMSI	Multi SIM	Edit	Del
SIM_Transatel	unknown	Cryptographic Checksum (CC)	ciphering inactive	SMS-SUBMIT	B00010	No	14	0	8	1	SIM	No	No	📋	🗑
SIM_Tunsiana	Gemalto	Cryptographic Checksum (CC)	ciphering inactive	SMS-SUBMIT	B00010	No	14	0	8	1	SIM	No	No	📋	🗑
SIM_IvoryCost	Gemalto	Cryptographic Checksum (CC)	ciphering inactive	SMS-SUBMIT	B00010	No	14	0	8	1	SIM	No	No	📋	🗑
SIM_Vivacell	Gemalto	Cryptographic Checksum (CC)	ciphering inactive	SMS-SUBMIT	B00010	Yes	28	200	30	3	SIM	No	No	📋	🗑
Comium_Liberia	Gemalto	Cryptographic Checksum (CC)	ciphering inactive	SMS-SUBMIT	B00010	No	14	0	8	1	SIM	No	No	📋	🗑
MTN_Liberia	Gemalto	Cryptographic Checksum (CC)	ciphering inactive	SMS-SUBMIT	B00010	Yes	0	0	0	0	SIM	No	No	📋	🗑
SIM_AfriCell	Oberthurcs	Cryptographic Checksum (CC)	ciphering inactive	SMS-SUBMIT	B00010	Yes	0	0	0	0	SIM	Yes	No	📋	🗑

Figure 8.3 Example of SIM profiles configured

Explanation of the Different Parameters

The parameters shown in Figure 8.3 are as follows:

- **Profile Name:** is the profile name for the same kind of SIM card.
- **Manufacturer:** is the manufacturer name for these SIM cards.
- **Signature:** is the kind of algorithm to sign the commands OTA 23.048 sent to the SIM card.
- **Ciphering:** indicates if you want to cipher your commands (increase the security level).
- **Proof of Receipt:** when you send a command you can specify if you want to be sure that the end-to-end action has been performed for the identified customer, and whether PoR is by SMS-MO SUBMIT or SMS-MT ack DELIVER REPORT.
- **TAR (Toolkit Application Reference):** represents the value of Remote File Manager TAR (between B00000 and B000FF).
- **Address book capacity:** indicates the number of records you can have in the SIM address book.
- **Preferred PLMN capacity:** indicates the number of PLMN you can configure into the SIM. The file containing the preferred PLMN is very useful in the case where one of your subscribers is near a border. Imagine that the power of the BTS of the foreign operator is bigger than yours; your subscriber will be located on the foreign network even if they are in their own country. So if in the preferred PLMN file your network is in the top position and if the power of your BTS is sufficient, your subscribers will never roam.
- **Need Counter:** indicates if the SIM cards need a counter. Indeed, some SIM cards need to have a counter value in the OTA 23.048 commands in order to be accepted. For each command accepted, the counted value is incremented.
- **BI-IMSI:** indicates if the SIM cards can contain a dual IMSI.
- **Kind of SIM:** indicates if it is a SIM [8.1] or USIM (UMTS) [8.4] card; there are more files with USIM.

8.2.2 Customer Information

A file having the SIM card profile and the keys for all the individual subscribers must be created. Frequently, a Mobile Network uses several profiles corresponding to different batches of SIM cards.

The length of KiK, KiD and KiC is either 8 bytes or 16 bytes; it depends on the SIM. Those with 8 bytes use DES and those with 16 bytes use 3DES.

Note: If you want to search all the SIM cards, put ‘%’ in the MSISDN or IMSI field. If you want to search all the French SIM cards, just put in ‘+33%’.

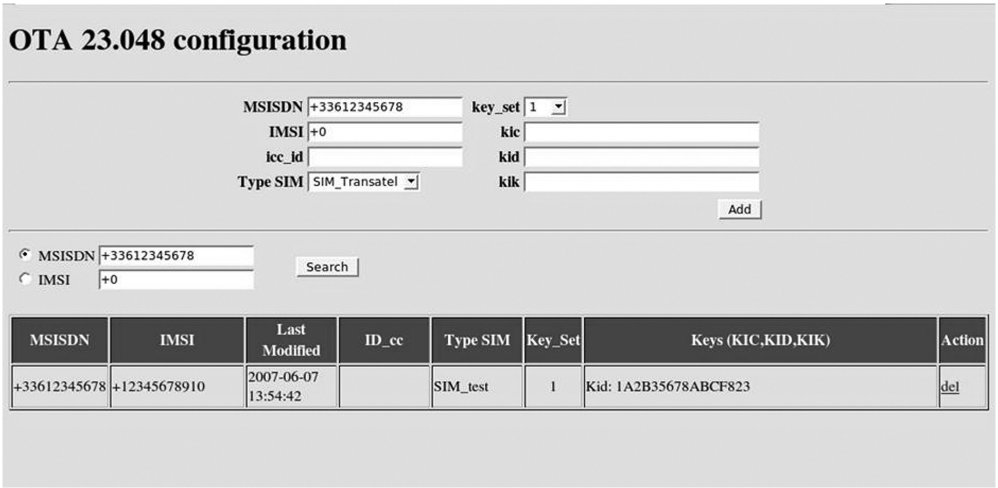
Figure 8.4 shows a search for customer information.

8.2.3 Read/Update a SIM Card

8.2.3.1 Read a SIM Card

This tool, as shown in Figure 8.5, allows the main parameters of a SIM card to be read like the list of preferred PLMN, the SMS parameters like SMSC commercial, Validity period etc. In order to use this tool, you must request a PoR by SUBMIT or DELIVER REPORT because all the answers are sent in the PoR.

Example: If you want to know what Service Provider is configured in the SIM, Figure 8.6 shows a fully detailed trace of the PoR.



OTA 23.048 configuration

MSISDN +33612345678 key_set 1
IMSI +0 kic
icc_id kid
Type SIM SIM_Transatel kik

● MSISDN +33612345678
○ IMSI +0

MSISDN	IMSI	Last Modified	ID_cc	Type SIM	Key_Set	Keys (KIC,KID,KIK)	Action
+33612345678	+12345678910	2007-06-07 13:54:42		SIM_test	1	Kid: 1A2B35678ABCF823	del

Figure 8.4 Customer information: search a particular SIM card

8.2.3.2 Update a SIM Card

This tool, as shown in Figure 8.7, allows the updating of a particular SIM card, like the list of preferred PLMN.

8.3 Coding the Binary Payload to Download (Write) and Upload (Read) Files of the SIM Card (Access with Remote File Manager)

There are very accurate specifications ([8.1], [8.2], [8.3], [8.4]) but these have few detailed examples, so that they are rather difficult to study to a level of detail which allows one to create payloads or develop OTA software.

8.3.1 Different Types of File in the SIM Card

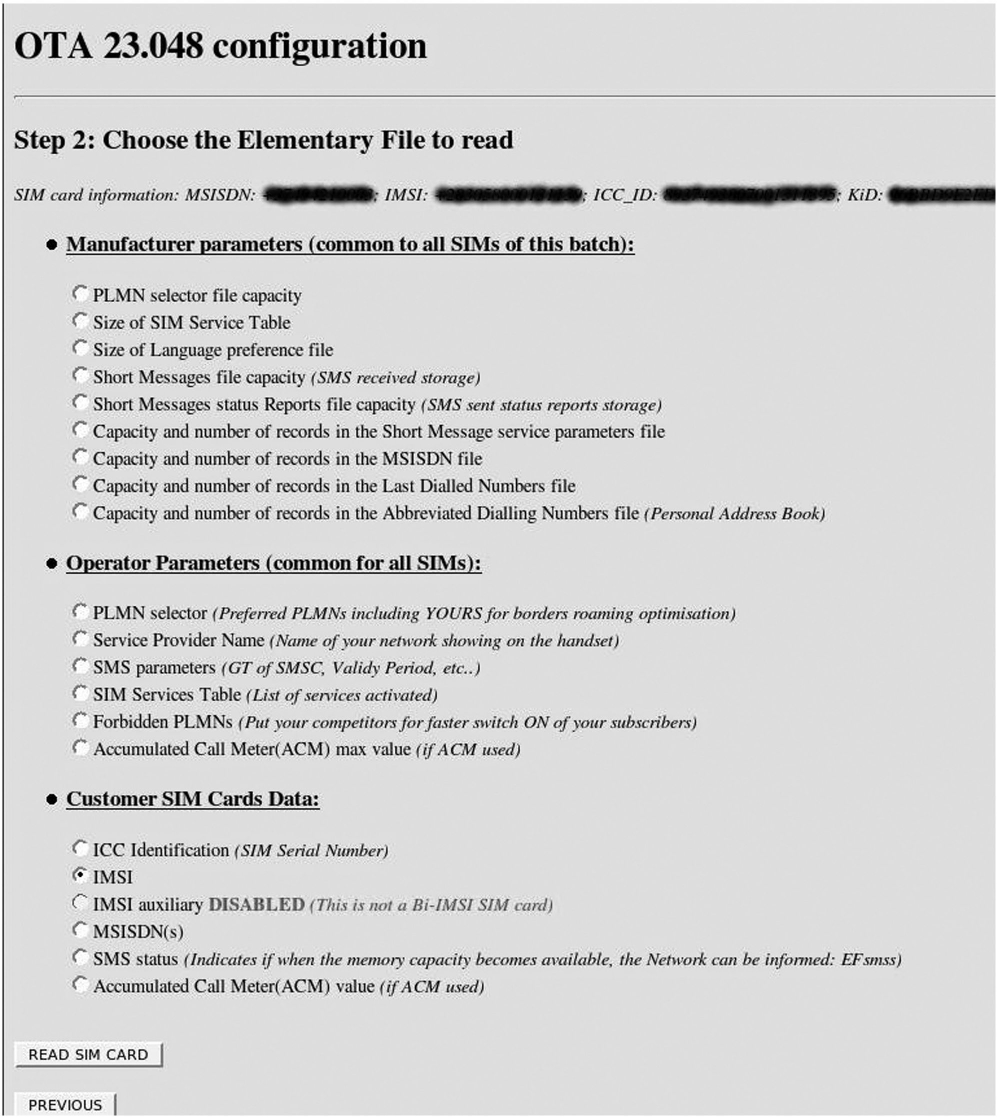
The specifications [8.1] GSM 11.11 and [8.4] for USIM define three types of file:

(1) ‘Transparent’ (only one record): use READ BINARY and UPDATE BINARY (example: Service Provider Name (SPN)).
(2) ‘Linear fixed’ (up to many records): use READ RECORD and UPDATE RECORD (example: Abbreviated Dialling Numbers (ADN)).
(3) ‘Cyclic’: use READ RECORD and UPDATE RECORD (example Last Dialled Numbers (LDN)).

They are organized in a standard directory structure for SIM cards [8.1] or USIM cards [8.4] (3G).

8.3.2 File Download Examples Using the Remote File Manager

All these scripts send GSM 11.11 commands to the ‘Remote File Manager’ (TAR = B00010).



OTA 23.048 configuration

Step 2: Choose the Elementary File to read

SIM card information: MSISDN: [redacted]; IMSI: [redacted]; ICC_ID: [redacted]; KiD: [redacted]

- **Manufacturer parameters (common to all SIMs of this batch):**

  ○ PLMN selector file capacity
  ○ Size of SIM Service Table
  ○ Size of Language preference file
  ○ Short Messages file capacity *(SMS received storage)*
  ○ Short Messages status Reports file capacity *(SMS sent status reports storage)*
  ○ Capacity and number of records in the Short Message service parameters file
  ○ Capacity and number of records in the MSISDN file
  ○ Capacity and number of records in the Last Dialled Numbers file
  ○ Capacity and number of records in the Abbreviated Dialling Numbers file *(Personal Address Book)*

- **Operator Parameters (common for all SIMs):**

  ○ PLMN selector *(Preferred PLMNs including YOURS for borders roaming optimisation)*
  ○ Service Provider Name *(Name of your network showing on the handset)*
  ○ SMS parameters *(GT of SMSC, Validy Period, etc..)*
  ○ SIM Services Table *(List of services activated)*
  ○ Forbidden PLMNs *(Put your competitors for faster switch ON of your subscribers)*
  ○ Accumulated Call Meter(ACM) max value *(if ACM used)*

- **Customer SIM Cards Data:**

  ○ ICC Identification *(SIM Serial Number)*
  ● IMSI
  ○ IMSI auxiliary **DISABLED** *(This is not a Bi-IMSI SIM card)*
  ○ MSISDN(s)
  ○ SMS status *(Indicates if when the memory capacity becomes available, the Network can be informed: EFsmss)*
  ○ Accumulated Call Meter(ACM) value *(if ACM used)*

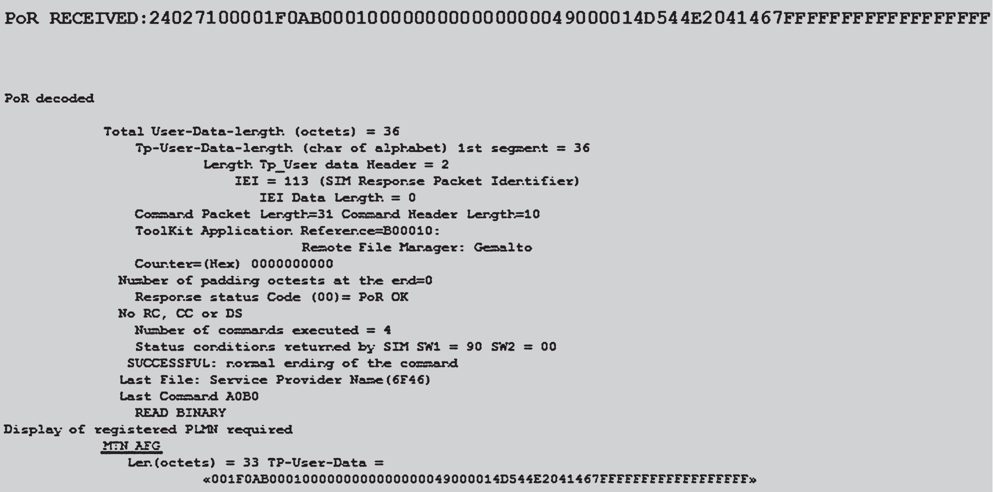
Figure 8.5 Read SIM card interface

8.3.2.1 Example of Service Provider Name (SPN) Download (‘Transparent File’)

The Service Provider Name (SPN) is the main network name which displays on the handset or alternatively the name of the Visited Network, if different.

As the file is a ‘transparent’ type (there is only one record), the writing is done with the UPDATE BINARY GSM 11.11 command.

Table 8.1 shows the script to update the Service Provider Name.



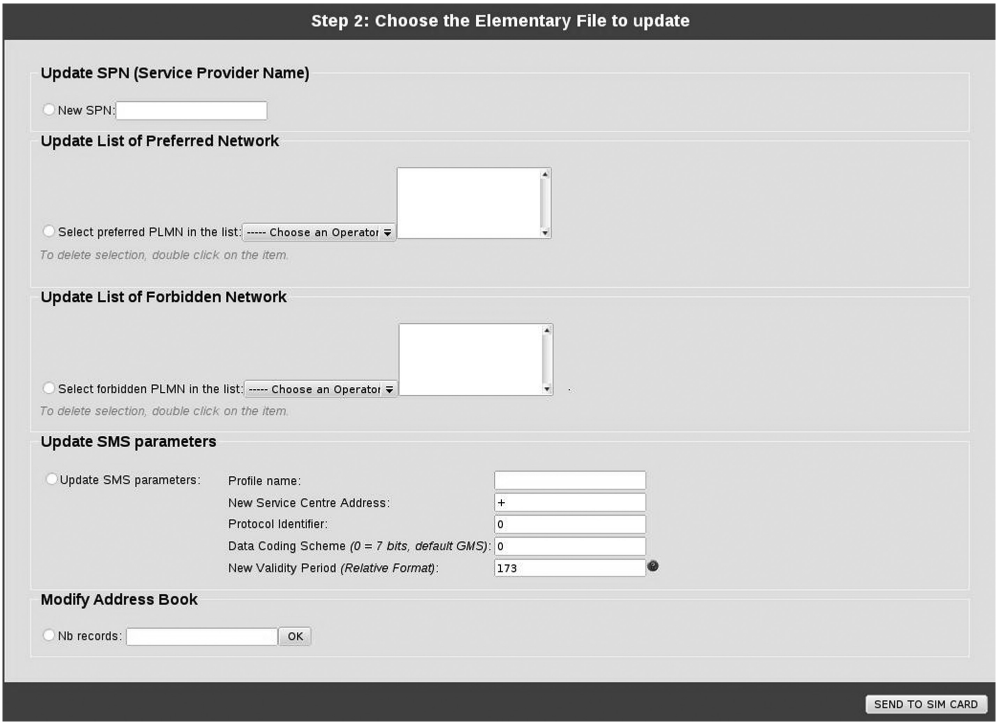
```
PoR RECEIVED:24027100001F0AB000100000000000000000049000014D544E2041467FFFFFFFFFFFFFFFFFFF



PoR decoded

            Total User-Data-length (octets) = 36
                Tp-User-Data-length (char of alphabet) 1st segment = 36
                        Length Tp_User data Header = 2
                            IEI = 113 (SIM Response Packet Identifier)
                               IEI Data Length = 0
                Command Packet Length=31 Command Header Length=10
                ToolKit Application Reference=B00010:
                                    Remote File Manager: Gemalto
                Counter=(Hex) 0000000000
              Number of padding octests at the end=0
                Response status Code (00)= PoR OK
              No RC, CC or DS
                Number of commands executed = 4
                Status conditions returned by SIM SW1 = 90 SW2 = 00
               SUCCESSFUL: normal ending of the command
              Last File: Service Provider Name(6F46)
              Last Command A0B0
                READ BINARY
Display of registered PLMN required
            MTN AFG
               Len(octets) = 33 TP-User-Data =
                        «001F0AB000100000000000000000049000014D544E2041467FFFFFFFFFFFFFFFFFFF»
```

Figure 8.6 Proof of Receipt (PoR) decoding



Step 2: Choose the Elementary File to update

Update SPN (Service Provider Name)

○ New SPN:

Update List of Preferred Network

○ Select preferred PLMN in the list: ----- Choose an Operator

To delete selection, double click on the item.

Update List of Forbidden Network

○ Select forbidden PLMN in the list: ----- Choose an Operator

To delete selection, double click on the item.

Update SMS parameters

○ Update SMS parameters:

Profile name:	
New Service Centre Address:	+
Protocol Identifier:	0
Data Coding Scheme *(0 = 7 bits, default GMS)*:	0
New Validity Period *(Relative Format)*:	173

Modify Address Book

○ Nb records:

Figure 8.7 Update SIM or USIM card interface

Table 8.1 Script to update the Service Provider Name

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0 A4 00 00 02 6F 46	SELECT 6F46 (Service Provider Name)
A0 D6 00 00 11	UPDATE BINARY length = 17
01 A_1 A_2… A_N FF .. FF	Service Provider Name record (total 17 bytes)

Example: Set ‘Exec Telecom’ as SPN (the Home Network name which displays on the handset).

This is what you write in Hex in the ‘text part’ of the bulk SMS file, by putting together these four commands and the ‘record’ containing the name you want to display. You have to enter it in Hexadecimal.

```
A0A40000023F00A0A40000027F20A0A40000026F46A0D60000110145786563546 56C
                                                          E x e c T E L
65636F6DFFFFFFFFFF
E C O M
```

Note: For a full display, most handsets will handle a maximum of 11 characters (such as in ExecTelecom). You must also add ‘FF’ at the end, so that there is always a total of 16 Hex characters after the 11 of the UPDATE BINARY command and the first byte of the record which must be 01.

8.3.2.2 Example of ‘Address Book’ (Abbreviated Dialling Number) and Download (‘Linear Fixed’ File)

You can download some entries of the Address Book (name and telephone numbers) to the SIM card. The SMSC will optimize the download time of any file by:

- automatically packing several entries per SMS;
- automatically creating the sequence of ‘concatenated SMS’;
- using the optimized MAP V2+ procedure to suppress the ‘paging’ time between each SMS.

Therefore, downloading big files to the SIM becomes practical.

It avoids the costly change of SIM cards (as some card manufacturers do for any change) when there are SIM Tool Kit changes, or asking the customer to come to your shop where there is a rather expensive SIM provisioning system provided by the card manufacturer, with a SIM card reader/writer for the update.

As the file is ‘linear fixed’ (there can be several records), the writing is done with the UPDATE RECORD GSM 11.11 command. We use here the mode ‘absolute mode’ to write record #8. But we could use the mode ‘next record’ to write the next one available.

Table 8.2 shows the script to update the Address Book.

Note 1: Some card manufacturers such as Gemalto only handle 30-byte ADN records. To be compatible with them, use 30 when the specification [8.1] allows for a variable length to save space.

Note 2: Coding of the ADN record:

NAME = MAMA

A1 A2 .. AN FF.. FF = 4D 41 4D 41 FF FF FF FF FF FF FF FF FF FF FF FF in Hex padded with ′FF′ to complete 16 bytes for the Name

Table 8.2 Script to update the Address Book

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 10	SELECT 7F10 (Directory TELECOM)
A0 A4 00 00 02 6F 3A	SELECT 6F3A (Abbreviated Dialling Numbers)
A0 DC 08 04 1E	UPDATE RECORD #8, absolute, length = 30
A_1 A_2… A_N FF .. FF B_1 B_2 .. B_M FF .. FF	Name (16 bytes) padded with ‘FF’ and Telephone number (14 bytes) padded with ‘FF’

Telephone number = +33140432125 (a little tricky to code!)
B1 B2 .. BN FF .. FF = 07 91 33 41 40 23 21 F5 FF FF FF FF FF FF
07 = number of useful bytes which follow
91 = Npi ISDN, Ton = International (corresponds to the ‘+’ in the number)
33 41 40 23 21 F5 = the number with the ‘quartets’ inverted and ‘F’ for the last quartet because there is an odd number of digits
FF FF FF FF FF FF are the 6 padding ‘FF’ to complete 14 bytes for the number

This is what you write in Hex in the ‘text part’ of the *bulk SMS file*, by putting together these four commands and the ‘record’ containing the Address Book entry #8 you want to add or modify:

```
A0A40000023F00A0A40000027F10A0A40000026F3AA0DC08041E4D414D41FFFFFFFF
FFFFFFFFFFFFFFFF07913341402321F5FFFFFFFFFFFF
```

M A M A

33140432125

8.3.2.3 Example of SMS Parameters Download (‘Linear Fixed’ File)

It may be very useful to have the tool to change the SMS parameters in the SIM, such as:

- changing the SMSC address;
- setting UCS2 (Russian, Arabic) when the customer does not know how to do it;
- correcting a wrong Validity period.

Table 8.3 shows the script of commands (the Gemalto card used has, for this file, a record length of 28 hex).

As the file is ‘linear fixed’ (there can be several records), the writing is done with the UPDATE RECORD GSM 11.11 command). We use the mode ‘next record’, which sets the pointer to write the first record after the file SELECT.

The explanation of the example in Table 8.4 is as follows:

- Alpha Identifier of this profile: Vivacell;
- Parameter Indicator = **E1** which means:
  - bit 1 Destination Address: present;
  - bit 2 Service Centre Address;
  - bit 3 TP-Protocol Identifier: not present;
  - bit 4 TP-Data Coding Scheme: not present (default);
  - bit 5 Validity Period;
  - bit 6-8 Reserved (not used): set to 1.

Table 8.3 Script to update the SMS parameters

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 10	SELECT 7F10 (Directory TELECOM)
A0 A4 00 00 02 6F 42	SELECT 6F42 (SMS parameters)
A0 DC 00 02 28	UPDATE RECORD, next record, length = 40
56 69 76 61 63 65 6C 6C FF FF FF FF	SMS parameter record ‘Vivacell’
E1	
FF FF FF FF FF FF FF FF FF FF FF FF	
07 91 73 94 23 79 33 F3 FF FF FF FF	GT = +37493297333
00 00 AD	

Table 8.4 Details of the SMS parameter file

Bytes	Description	M/O	Length
1 to Y	Alpha-Identifier of this profile	O	Y bytes
Y+1	Parameter Indicators	M	1 byte
Y+2 to Y+13	TP-Destination Address (Default)	M	12 bytes
Y+14 to Y+25	TS-Service Centre Address	M	12 bytes
Y+26	TP-Protocol Identifier	M	1 byte
Y+27	TP-Data Coding Scheme	M	1 byte
Y+28	TP-Validity Period	M	1 byte

- Destination Address (default destination number of a SMS-MO): Nothing (FF …);
- SMSC Address: +37493297333;
- PID = 0: Standard;
- DCS (Coding scheme) = 00: 7 bits (‘text’ the default GSM);
- Validity Period VP (in ‘*relative time*’ format) = 173 (AD hex) and as such:
  - VP = 0 to 143 (VP + 1) × 5 min;
  - 144 to 167 12 hours + (VP – 143) × 30 min;
  - 168 to 192 (VP – 166) × 1 day;
  - 197 to 255 (VP – 192) × 1 week;
  - so here it is: 173 – 166 = 7 days.

Note: You can create several SMS profiles in a SIM card, identified with different ‘Alpha Identifiers’. As you have set the ‘Alpha Identifier’, *it will be displayed by the handset*. When you look at the ‘Message Parameters’ menu, you see ‘Vivacell’ as the title instead of a vague default name.

When you look at the very detailed traces, they also show the following.

```
UPDATE RECORD(DC)Rec No: 0 mode: next record(2) length: 40
          Alpha Identifier of SMSC profile: Vivacell
          Parameter Indicator E1
             Default Destination Address present
             SMSC Address not present
```

```
              PID not present
              DCS not present
              VP not present
           Default Destination Address:
           SMSC Address:
               Ext = No extension
               Ton = International
               Npi = ISDN
               Address = 37493297333
           Protocol IDentifier 00
           Data Coding Scheme 00
           Validity(Relative) Period = 7 day(s)
```

8.3.3 *Example of a SIM File 'Upload' (Remote Reading by the SMSC) Using the Remote File Manager*

8.3.3.1 Reading the Serial Number ('Transparent File')

Table 8.5 shows the script of commands for OTA 'upload' (reading) of the Serial Number of a SIM.

The Response will be sent by the SIM card (through the handset) to the sending SMSC in either the Confirmation (or ack) of the SMS-MT (if you have selected PoR = SMS_DELIVER_REPORT) or in an SMS-MO (PoR = SMS_SUBMIT, that is SPI2 = 21).

For example, in main.log, if you have selected PoR = SMS_SUBMIT, you receive OK (**00**), *in the sending SMSC.*

```
4 38513 +33660000067 +37493297311 +37493297333 +33608123456
+32485222829 0 70407001929400 34 0 0 1 0 0 0 4 1D02710000180AB0001
000000000000000039000982330000503006520F0
```

And the serial number read remotely is **982330000503006520F0**, which read in clear (quartet inversion) is 893203005030056020. The T0 response ***9000*** indicates it is OK.

8.3.3.2 Reading the Location Information ('Transparent File')

As shown in Table 8.6, the SMSC receives the PoR in an SMS-MO (SUBMIT) OK (**00**).

```
4 33367 +33660000067 +37493297311 +37493297333 +33608123456
+32485222829 0 70407011124100 34 0 0 1 0 0 0 4
1E02710000190AB0001000000000000000049000B8000CB602F80200C03C00
```

And the Location Information is (see GSM 11.11):

Table 8.5 Script to read the Identification Circuit Code (ICC) of the SIM code

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 2F E2	SELECT 2FE2 (ICC Identification)
A0 B0 00 00 0A	READ BINARY, length = 10

Table 8.6 Script to read the Location Information

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0 A4 00 00 02 6F 7E	SELECT 6F7E (Location Identification)
A0 B0 00 00 0B	READ BINARY, length = 11

Table 8.7 Script to read the SMS parameters

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 10	SELECT 7F10 (Directory TELECOM)
A0 A4 00 00 02 6F 42	SELECT 6F42 (SMS parameters)
A0 B2 00 02 28	READ RECORD, next record, length = 40 SMS parameter record as detailed in 8.3.3.3

TMSI B8000CB6
LAI 02F80200C0, that is 208 20 ***192***, Bouygues (France)
MCC = 208, MNC = 20, LAC = ***192*** (00C0h) (Paris area)
TMSI time 3C
Location Update status 00

8.3.3.3 Reading the SMS Parameters (‘Linear Fixed File’)

As the file is ‘linear fixed’ (there can be several records), the reading is done with READ RECORD (GSM 11.11 command). We use the mode ‘next record’, which sets the pointer to the read the first record after the file SELECT. As shown in Table 8.7, it is very similar to the previous example of writing the same file, except that no new parameters are provided.

The result of the reading in Hexadecimal is as follows.

```
56 69 76 61 63 65 6C 6C FF FF FF FF  Alpha Identifier of this
profile 'Vivacell'
E1   Parameter Indicator(tells which fields exist)
FF FF FF FF FF FF FF FF FF FF FF FF TP-Destination Address
(default)
07 91 73  94 23  79 33  F3 FF FF FF FF Service Centre Address
(padded with FF):
    +37493297333
00   Protocol Identifier(PID)
00   Data Coding Scheme(DCS)(00 = 7 bits default GSM)
AD   Validity Period(VP) in 'Relative Format'
```

For the coding of these fields see the ‘upload case’ example of the SMSC parameters (from GSM 23.040).

Table 8.8 Script to read the SIM Service Table

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 10	SELECT 7F10 (Directory TELECOM)
A0 A4 00 00 02 6F 38	SELECT 6F38 (SIM Service Table)
A0 B0 00 00 0A	READ BINARY, length = 10 Parameter record as detailed below

8.3.3.4 Reading the SIM Service Table ('Transparent File')

The result of the Reading shown in Table 8.8 in hexadecimal is:

FF 3F FF 0F 3F 00 3C 03 00 0C
which corresponds to these services (a Comium Liberia SIM card):
CHV1 disable function
Abbreviated Dialling Number (ADN)
Fixed Dialling Numbers (FDN)
Short Message Storage (SMS)
Advice of Charge (AoC)
Capability Configuration Parameters (CCP)
PLMN selector
NO RFU
MSISDN
Extension 1
Extension 2
SMS Parameters
Last Number Dialled
Cell Broadcast Message Identifier
NO Group Identifier Level 1
NO Group Identifier Level 2
Service Provider Name (SPN)
Service Dialling Number (SDN)
Extension 3
NO RFU
NO VGCS Group Identifier List (EFvgcs and EFvgcss)
NO VBS Group Identifier (EFvbs and EFvbss)
NO enhanced Multi-Level Precedence and Pre-emption Service
NO Automatic Answer for eMLPP
NO Data download via SMS-Cell Broadcast
Data download via SMS-PointToPoint
Menu selection
NO Call Control
Proactive SIM
NO Cell Broadcast Message Identifier Range
NO Barred Dialling Numbers (BDN)
NO Extension 4

```
NO De-personalization Control Keys
NO Cooperative Network List
NO Short Message Status Report
NO Network’s indication of alerting in the MS
NO Mobile Originated SMS control by SIM
GPRS
NO Image (IMG)
NO SoLSA (Support of Local Service Area)
NO USSD string data object supported in Call Control
NO RUN AT COMMAND command
NO PLMN Selector List with Access Technology
NO OPLMN Selector List with Access Technology
NO HPLMN with Access Technology
NO CPBCCH Information
NO Investigation Scan
NO Extended Capability Configuration Parameters
NO MExE (this is for Certificate Management)
```

8.3.3.5 Reading the Phase Identification File (‘Transparent File’)

Like above, we see the following in the trace for the Command:

```
SELECT(A4)Master File(MF)(3F00)
SELECT(A4)Directory File(DFgsm)(7F20)
SELECT(A4)Phase identification(6FAE)
READ BINARY(B0)offset: 0 length 1 data
```

and for the Response:

```
........
Response Status Code(00) = PoR OK
   No RC, CC or DS
   Number of commands executed = 4
   Status conditions returned by SIM SW1 = 90 SW2 = 00
   SUCCESSFUL: normal ending of the command
   Last File Phase identification(6FAE)
   Last Command B0
   READ BINARY
   Phase 2 and PROFILE DOWNLOAD
.......
```

So, this is a Phase 2+ SIM card.

8.3.3.6 More Complicated: OTA Reading and Updating the PLMN Selector Table (‘Transparent File’ Variable Length) for the ‘Steering of Roaming’

Another method is used to manage the roaming preferences of outbound subscribers, the so-called ‘Steering of Roaming’. It consists of probing the UPDATE LOCATION messages arriving at a HPLMN and selectively rejecting them. The method explained in this section is much better.

This SIM file is used for the ‘Steering of Roaming’ and contains the preferred MCC-MNC codes set by an operator for their outbound subscribers. This is so that their phone does not automatically select one of their major competitors in this country that is a roaming partner (they want the traffic of their inbound visitors), unless there is no other coverage. For example, Orange France sets for the UK:

234 33	Orange UK
234 30	T-Mobile UK
.....	

They do not have 234 15 Vodafone UK in the list of 80 preferred networks that they set in their SIM cards, so whenever Orange UK has coverage, they will be selected by the handset of their outbound subscribers in the UK, then T-Mobile UK and others (Vodafone UK, O2 UK) but only if there is no other choice.

This method has existed since the beginning of roaming (1994), but with OTA (spreading since 2000 [8.2]) it is easy for Orange France to dynamically change the order of preference remotely, say every month. And with this method, there is, most often, *no attempt at all to register in the not-preferred network* and no complaints from them because of useless SS7 traffic, including international SS7. This useless traffic is easily monitored and would create justified complaints and difficulties for roaming commercial relations as well as ‘counter attacks’.

This is why other ‘Steering of Roaming’ ‘makeshift solutions’ which use a platform in the Home Network to refuse SS7 registration attempts (‘UPDATE LOCATION’) have rapidly gained strong opposition. It is easy to understand why, as this useless traffic also creates additional SS7 international charges, as well as pointless usage of the radio bandwidth of the ‘visited-rejected’ roaming partner.

In addition, with most handsets, a rejected registration attempt *adds the rejected network into the SIM card’s ‘Forbidden PLMN list’*! So if a roamer, when they arrive at an airport, is ‘steered’ to a new network with possibly better prices, but a limited coverage including the airport, *they will be locked by this SIM card setting from the possibility of roaming in the main network which has coverage elsewhere*. They can no longer use their handset on the networks which have been rejected by the ‘Steering of Roaming’.

This is because the registration logic of a handset is:

- detect the networks covering the area;
- use the last network it was registered into if available (this is written in the Location Info file of the SIM);
- skip the forbidden networks of the Forbidden PLMN file;
- select the preferred PLMN available in the order of the Preferred PLMN file.

To show this, if you are able to change the ‘Preferred Network’ list of your handset, turn it on and off, and you remain with the previous network if you use ‘automatic mode’.

Steering of Roaming Based on the SIM Card’s Updatable Preferred Networks Settings

The ‘steering of roaming’ by OTA of the PLMN selector file is simple, efficient and ideal if you have the OTA system. It has been practised for years by the major mobile operators.

To force the switch to a Preferred Network, *the OTA system must erase the Location Info file of the SIM card.*

Reading the Preferred PLMN file is more complicated because you do not know the length (240 bytes for Orange France, 24 for Base Belgium, etc.) and because it set by the card manufacturer, it may be difficult to find *what the exact value is* later. So the SMSC must go through two phases:

- Get the length of the file with a GSM 11.11 GET_RESPONSE.
- Read the file PLMN selector with the length which has been obtained.

8.3.3.7 Get the Length of the File

As shown in Table 8.9, the SMSC receives the PR in an SMS-MO (SUBMIT) OK (**00**):

....
Response Status Code (00) = PR OK
No RC, CC or DS
Number of commands executed = 4
Status conditions returned by SIM SW1 = 90 SW2 = 00
SUCCESSFUL: normal ending of the command
Last File PLMN selector (6F30)
Last Command C0
GET RESPONSE: Requested record length = ***18*** (hex)
....

The length is ***18*** in hexadecimal, that is 24 bytes, which the SMSC send uses now in a READ BINARY.

8.3.3.8 Read the PLMN Selector File

As shown in Table 8.10, the SMSC receives the PoR in an SMS-MO (SUBMIT) OK **(00**):

....
Response Status Code (**00**) = PoR OK
No RC, CC or DS
Number of commands executed = 4

Table 8.9 Script to get the length of a file from the SIM card

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0 A4 00 00 02 6F 30	SELECT 6F30 (PLMN selector File)
A0 C0 00 00 0F	GET RESPONSE, length = 15 (always)

Table 8.10 Script to read the PLMN Selector file

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0**C** A4 00 00 02 6F 30	SELECT 6F30 (PLMN selector File)
A0 B0 00 00 ***18***	READ BINARY, length = 24

```
Status conditions returned by SIM SW1 = 90 SW2 = 00
SUCCESSFUL: normal ending of the command
Last File PLMN selector (6F30)
Last Command B0
READ BINARY
```

In this example, the Base card +32485222829 had a PLMN selector empty (all FF). Let us set some preferences.

8.3.3.9 Update the PLMN Selector File to Set the Preferred PLMN

For the command shown in Table 8.11, if we look at the super-detailed traces of OTA, we see the seven good friends that we have added as preferences (this card allowed only eight, but when you order the SIM cards, ask for 80).

```
......
SELECT(A4)Master File(MF)(3F00)
SELECT(A4)Directory File(DFgsm)(7F20)
SELECT(A4)PLMN selector(6F30)
UPDATE BINARY(D6)offset: 0 length 24 data:
                MCC-MNC = 285 05 K Telecom (Vivacell) Armenia
                MCC-MNC = 285 04 Karabakh Telecom
                MCC-MNC = 274 04 Viking (Iceland)
                MCC-MNC = 623 02 Telecel Centrafrique
                MCC-MNC = 619 04 Comium Sierra-Leone
                MCC-MNC = 618 04 Comium Liberia
                MCC-MNC = 412 40 MTN Afghanistan
```

In the trace, you see the status given by the protocol, called ‘T0’ in GSM 11.11, of the ‘download’ in the PoR that you have requested to be received by an SMS-MO.

```
........
Response Status Code (00) = PoR OK
No RC, CC or DS
Number of commands executed = 4
Status conditions returned by SIM SW1 = 90 SW2 = 00
SUCCESSFUL: normal ending of the command
......
```

Now, whenever the Base (Belgium) subscriber roams in these countries, it will always select these

Table 8.11 Script to update the PLMN Selector file

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0 A4 00 00 02 6F 30	SELECT 6F30 (PLMN selector File)
A0 D6 00 00 ***18***	UPDATE BINARY, length = 24
82F55082F54072F44026F32016F94016F84014F204FFFFFF	Record with 7 MCC-MNC (last is FFFFFF)

networks automatically whenever they have coverage. And it will not create incorrect traffic that our other roaming partners in these countries would complain about, jeopardizing our commercial relations.

What if you had set an incorrect length (such as F0 hex = 240, like Orange France, not supported by the Base card)?

In the PoR you would get:

```
......
Response Status Code (00) = PoR OK
No RC, CC or DS
Number of commands executed = 3 (shows that the last one was incorrect)
Status conditions returned by SIM SW1 = 67 SW2 = 00
Incorrect parameter P3 (P3 is the length in GSM 11.11)
Last File Forbidden PLMN (6F7B)
Last Command D6
......
```

8.3.3.10 You Want to be Sure? Read the Updated PLMN Selector File Now

You use the same commands as in 8.3.3.8, and this time in the trace you see:

```
.........
Response Status Code (00) = PoR OK
                No RC, CC or DS
                Status conditions returned by SIM SW1 = 90 SW2 = 00
                SUCCESSFUL: normal ending of the command
                Last File PLMN selector (6F30)
                Last Command B0
                READ BINARY
                MCC-MNC = 285 05
                MCC-MNC = 285 04
                MCC-MNC = 274 04
                MCC-MNC = 623 02
                MCC-MNC = 619 04
                MCC-MNC = 618 04
                MCC-MNC = 412 40
```

now with all the seven MCC-MNC of your preferred HPLMNs!
Simple?

8.3.3.11 Improving the Efficiency of the Registration of Your Subscribers While in Your HPLMN: Avoid Scanning Your Competitors by Setting the Forbidden PLMN File

When one of your subscribers’ handsets turns on in your country, it scans the different networks, even your competitors (they get rejected, of course) and it may take more than ½ a minute before they scan your network and register successfully.

To *avoid this waste of time and radio resources*, the efficient way is to enter the identity MCC-MNC of your national competitors in the ‘black list’ of Forbidden PLMNs (up to four networks, because it was designed at a time when no one was considering that there could be more GSMs in the same area).

In the traces for the command in Table 8.12, you see for the UPDATE command:

Table 8.12 Script to update the Forbidden PLMN file

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0**C** A4 00 00 02 6F 7B	SELECT 6F7B (Forbidden PLMN File)
A0 D6 00 00 ***0C***	UPDATE BINARY, length = 12
02F60102F610FFFFFFFFFFFF	Record with 2 MCC-MNC (last 2 are FFFFFF)

SELECT(A4)Master File(MF)(3F00)
SELECT(A4)Directory File(DFgsm)(7F20)
SELECT(A4)Forbidden PLMNs(6F7B)
UPDATE BINARY(D6)offset: 0 length 12 data:
MCC-MNC = 206 10 Orange Mobistar
MCC-MNC = 206 01 Proximus Belgacom

And in the PoR in the received SMS-MO:

Response Status Code (00) = PoR OK
No RC, CC or DS
Status conditions returned by SIM SW1 = 90 SW2 = 00
SUCCESSFUL: normal ending of the command
Last File Forbidden PLMNs(6F7B)
Last Command D6

So now the Base subscriber will not scan the competitors and will directly register more quickly in the Base (Belgium) HPLMN.

8.3.3.12 Changing the 'Auxiliary IMSI' of a Dual IMSI Virtual Roaming SIM Tool Kit

Card vendors provide the 'dual IMSI' SIM Tool Kit which allows the handset to select an 'Auxiliary IMSI' (which has roaming) when the main IMSI does not have roaming. This application is flexible and the 'Auxiliary IMSI' can be OTA changed, as in a standard structure SIM file, with a proprietary Gemalto name, which is 8F07, as shown in Table 8.13.

Table 8.13 Script to update the Auxiliary IMSI file (bi-IMSI virtual roaming)

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0A4 00 00 02 8F 07	SELECT 8F07 (Second IMSI File)
A0 D6 00 00 ***09***	UPDATE BINARY, length = 9
0816F8402143658709	Record with new IMSI 618 04 1234567890 (same format as main IMSI file 6F07)

Table 8.14 Script to read the SIM Tool Kit usage of the memory

Applet Management Command GSM 03.48	Description
80 CA FF 20 05	GET DATA Card Resources, length = 5

8.4 Coding the Binary Payload to Download (Write) and Upload (Read) Data of the SIM Card (Access with Applet File Manager)

8.4.1 Data Upload (Reading)

This will use the Applet Management Commands described in GSM 03.48, not the Remote File Manager as previously. And the TAR used is **000000**.

8.4.2 Reading the SIM Card Resources

Table 8.14 shows the Applet Management Command.

```
.......
Toolkit Application Reference=000000:
                  Applet File Manager(2G)
                  Counter=(Hex) 0000000000
                  Number of padding bytes at the end=0
                  RC, CC or DS = (Hex) BF778D1A8BCE4551
                  GET DATA(CA) P1: FF length 5:
                  P2(20) = Card resources used and available
.....
```

And the result shows the memory EEPROM used in the SIM and ***seven*** applets installed:

```
Response Status Code (00) = PoR OK
                  No RC, CC or DS
                  Number of commands executed = 1
                  Status conditions returned by SIM SW1 = 90 SW2 = 00
                  SUCCESSFUL: normal ending of the command
                  Last Command 80CAFF20
                  Card resources: Free EEPROM 5B3Ch Number of installed Applets 7
```

8.5 Coding a Binary Payload Which Triggers the Execution of a Remote SIM Tool Kit (Using the Applet File Manager)

Previously, with the Remote File Manager of the SIM card, we have been able to download and upload *standard files of the SIM*. Now we want the SMSC to be able to *remotely interrogate* our subscribers and *get useful information from the handset* such as:

- IMEI (Automatic Device Management);
- Location Information (for Location Based Services) etc.

These are not stored in SIM standard files, but are stored or updated in the ‘handset’ (such as the IMEI).

It is possible to program some applications in ‘Java card language’ which reside permanently in the SIM. How to do this, and load and install them in the SIM card is not discussed here. These applications can send the ‘Proactive SIM commands’ (described in GSM 11.14) to the handset according to a programmed logic. These applications are grouped in ‘Personal Toolkit Application References’, which are assigned when the program is ‘installed’ in the SIM card. A particular application within this group is referred to by an ‘Item identifier’.

For example, the SMSC could trigger the execution of ‘Item 10’ of the ‘Personal Toolkit ***B00018***’ (for example reading the IMEI and sending the result in an SMS to the SMSC) and the trace would be as below.

```
Toolkit Application Reference=B00018:
                 Personal Applet File Manager
              Counter=(Hex) 0000000000
              Number of padding bytes at the end=0
              RC,CC or DS = (Hex) B0F32DE01E555FE9
       ENVELOPE(C2)length 11 data GSM 11.14:
          D3098202838190010A9500
          BER_TLV(D3) Menu Selection tag length 9
           Device Identity tag(82) length 2
            Source     device(83): (131):Network
            Destination device(81): (129):SIM card
           Item identifier tag(90) length 1
            Identifier of item chosen = 0A
           Help request tag(95) length 0
```

As shown in Table 8.15, the ENVELOPE GSM 11.11 allows the ‘Menu Selection’ GSM 11.14 command to be passed to the SIM.

To execute the IMEI interrogation, the SIM Tool Kit will execute some ‘Proactive SIM commands’ such as ‘PROVIDE LOCAL INFORMATION (IMEI)’ then ‘SEND SHORT MESSAGE’.

The SMSC can only pass an ENVELOPE (Menu Selection) which refers to a function in the SIM Tool Kit. *It is not possible for the SMSC to ask directly for the execution of a sequence of GSM 11.14 commands, without referring to the SIM Tool Kit which sends them.*

8.6 More Details on OTA Formats

8.6.1 Detailed Analyser: See the Cryptographic Checksum

As you know, the SMSC has a very detailed integrated MAP protocol analyser which can be activated. Look at the full details that it provides, with the fully decoded trace of a SIM download SMS-MT.

Table 8.15 Script to read the IMEI using a SIM Tool Kit in the SIM card

Command GSM 11.11	Description
A0 C2 00 00 0B	ENVELOPE, length = 11 then
Command GSM 11.14	–
D3 09	Menu Selection, length = 9
82 02 83 81	Device Identity, length = 2
90 01 0A	Item identifier = 10 (0Ah)
95 00	Help Request

The Payload for a card (Base in Belgium) +32485222829 is:

A0A40000023F00A0A40000027F10A0A40000026F3AA0DC02041E48414C5953FFFFFF FFFFFFFFFFFFFFFF07913341402321F5FFFFFFFFFFFF
(this is an entry in the Address Book)

The security parameter selected is ***02010015B00010*** (SPI2 = ***01*** so that a PoR is requested in all cases by SMS-DELIVER-REPORT) and it is a Gemalto card (the TAR for the Remote File Manager is ***B00010***). No ciphering (so that the payload is ′in clear′).

The KID security algorithm selected is (***15***): 3DES_outer_CBC with 2 different keys. The KID is then 16 bytes (8 + 8). For this card, the Key # **1** and it is:

C49FBDD5EB38C0F77195BD6126D4BEB3
with Security = ′Cryptographic Checksum(CC)′

The resulting CC (8 bytes) of the Header and the Payload computed by the OTA software is:

7F2B4E4FA0E8DC21 that you see in *italic* in the trace

You may use this example to check that your OTA is well configured. If you change a single bit in the payload or the Header the CC is entirely different.

```
---------  HDR ---------  [ Sat Apr  7 08:59:17 2007 ]
  MAPE-E Instance = 0
  MAPE-E Type = MAP_MSG_SRV_REQ (0000C7E0)
  MAPE-E Dialog_ID = 299
  MAPE-E Src = 1D
  MAPE-E Dst = 15
  MAPE-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
  - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
     PA_Len = 154
     MAP-FORWARD-SHORT-MESSAGE-REQ(Version 2)(3)
       MAPPN_timeout(45)
         L = 002
         Data: timeout value = 45sec
       MAPPN_invoke_id(14)
         L = 001
         Data: 1
       MAPPN_sm_rp_da(23)
         L = 019
         Data: TA_IMSI
              Ext = No extension
              Ton = International
              Npi = ISDN
              Address = 206205001005602
       MAPPN_sm_rp_oa(24)
         L = 009
         Data: TA_SC_ADR
              Ext = No extension
              Ton = International
              Npi = ISDN
              Address = 37493297333
       MAPPN_sm_rp_ui(25)
       L = 111
       Data: Message Type = SMS_DELIVER(SMS-MT)
           TP_RP = No request for reply path
           TP_UDHI= Header in TP-User-Data
           TP_SRI = A status report will not be returned to the SME
           TP_VPF = TP_VP field not present
           TP_MMS = No more messages are waiting for the MS in
this SC
           Originating mobile address            =
             Type of number = International
             Numbering Plan = ISDN
             Address = 33612345678
           TP-Protocol-Identifier =  7F (SIM Data upload or
download)
           TP-Data-Coding-Scheme = F6
             Message Class = Class 2(SIM Card)
             Alphabet = 8bit(image/sound/download)
           TP_Service_Centre_Time_Stamp = 07.04.07 10:59:15 08
           TP-User-Data-length = 83
             Length TP_User Data Header = 2
              IEI = 112 (SIM Command Packet Identifier)
               IEI Data Length = 0
           Command Packet Length=78 Command Header Length=21
           Security Parameter Indicator:
            SPI1(02):
             Cryptographic Checksum(CC)
             No Ciphering
             No Counter available
            SPI2(01):
             PoR to be sent to Sending Entity
             No Security applied to PoR
             PoR not ciphered
             PoR by SMS-DELIVER-REPORT
           KIc(00)
             Algorithm known implicitly by both entities
             DES in CBC mode
             Keyset number(KIc-KID-KIK) used 0
           KID(15)
             DES
             Triple DES 2 different keys
             Keyset number(KIc-KID-KIK) used 1
           Toolkit Application Reference=B00010:
                  Remote File Manager: Gemalto
           Counter=(Hex) 0000000000
           Number of padding bytes at the end=0
           RC,CC or DS = (Hex) 7F2B4E4FA0E8DC21
      SELECT(A4)Master File(MF)(3F00)
      SELECT(A4)Directory File(DFtelecom)(7F10)
      SELECT(A4)Abbreviated dialling numbers(6F3A)
      UPDATE RECORD(DC)Rec No: 2 mode: absolute/current record(4)
```

```
length: 30
           Alpha Identifier: HALYS
           Number: Ext = No extension
              Ton = International
              Npi = ISDN
              Address = 33140432125
              TP-User-Data =
’004E1502010015B000100000000000007F2B4E4FA0E8DC21A0
A40000023F00A0A40000027F10A0A40000026F3AA0DC02041E48414C5953FFFFFFFF
FFFFFFFFFFFFFF07913341402321F5FFFFFFFFFFFF’
   - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
   −−−−−−−− HDR −−−−−−−−−− [ Sat Apr  7 08:59:17 2007 ]
   MAPE-E Instance = 0
   MAPE-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   MAPE-E Dialog_ID = 299
   MAPE-E Src = 1D
   MAPE-E Dst = 15
   MAPE-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt =
0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
   −−−−−−−− HDR −−−−−−−−  [ Sat Apr  7 08:59:26 2007 ]
   MAPE-R Instance = 0
   MAPE-R Type = MAP_MSG_DLG_IND (000087E3)
   MAPE-R Dialog_ID = 299
   MAPE-R Src = 15
   MAPE-R Dst = 1D
   MAPE-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt =
0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 16
      MAP-OPEN-CNF(130)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001001902
                MAP_ShortMsgMTRelayPackage_v2v3 MAP V2
   - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    −−−−−−−− HDR −−−−−−−−  [ Sat Apr  7 08:59:26 2007 ]
   MAPE-R Instance = 0
   MAPE-R Type = MAP_MSG_SRV_IND (000087E1)
   MAPE-R Dialog_ID = 299
   MAPE-R Src = 15
   MAPE-R Dst = 1D
   MAPE-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
```

```
        PA_Len = 49
        MAP-FORWARD-SHORT-MESSAGE-CNF(Version 2)(132)
          MAPPN_invoke_id(14)
            L = 001
            Data: 1
    - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Note 1: The **bold** text part is the 'payload' that you have entered (see examples).

The *italic* part is the 'Cryptographic Checksum' (3DES outer CBC algorithm) computed automatically by the SMSC with the payload and the 'OTA key' KID specific to each SIM. *If a single bit is changed, it is entirely different*. So the security is very high (KID is 128 bits).

The *italic* text part is the beginning of the 'Secured Data Packet' GSM 03.48 formatted by the SMSC.

The rest of the SMS is formatted by the SMSC also.

8.6.2 Details of Optional Ciphering

Ciphering prevents the payload from being understandable and improves the security.

Assume we get this TP-PDU SMS with a ciphered payload. We want to have the payload in clear and verify the signature.

/* TP-UDL(47h) and TP-UD complete */
47 E4 0A 98 33 11 11 11 11 7F 16 07 02 29 17 01 15 04
35 02 70 00 **00 30 15 06 01 24 24 B0 00 10** /* CPL CHI CHL SPI KIc KID TAR */
C8 AB 21 F2 7F 0C 68 67 28 AB 8D 83 60 D6 34 A7 5B E5 48 3C FB
7A F6 7C 58 B8 5C 13 B0 F9 FE 5C D0 64 83 E5 AF 21 57 78 /* CNTR PCNTR RC/CC/DS and Secured Data ciphered */

Take the ciphered Data in *italic* (which you cannot interpret) that is CNTR-PCTNR-RC/CC/DS-SecuredData:

```
C8 AB 21 F2 7F 0C 68 67 28 AB 8D 83 60 D6 34 A7 5B E5 48 3C FB
7A F6 7C 58 B8 5C 13 B0 F9 FE 5C D0 64 83 E5 AF 21 57 78
```

decoded by the ciphering key:

```
KIc:  30 42 30 42 30 44 30 44 30 45 30 45 30 46 30 46   /* (3DES CBC)*/
```

it gives:

00 00 00 00 00 05 ***21 FD 15 D4 91 A6 36 6F*** **A0 A4 00 00 02 3F 00**
A0 A4 00 00 02 7F 10 A0 A4 00 00 02 6F 3A 00 00 00 00 00

The deciphered RC/CC/DS shows in ***bold italic***. It has been computed from:

00 30 15 06 01 24 24 B0 00 10 *00 00 00 00 00 05* **A0 A4 00 00 02**
3F 00 A0 A4 00 00 02 7F 10 A0 A4 00 00 02 6F 3A ***00 00 00 00 00***

The PCNTR Padding Counter is 5 and corresponds to the last five '***00***' after …6F 3A (so as to give a total of 40 bytes, a multiple of 8).

These '00' *have been added in the Computation* of the RC/CC/DS, *because of ciphering to give a number of bytes 'to be ciphered', which is a multiple of 8*.

To check, if we take the above 40 bytes coded by:

```
KID: 01 23 45 67 89 AB CD EF 10 02 76 FE DC BA 01 23 /* (3DES CBC) */
```

it gives for the CC:

```
55 1D B5 35 2D 61 87 CA 89 84 A5 77 E0 D0 D1 37 84 18 05 79 36
5A 85 1B C1 35 A6 AD 7A A9 BF CC EF 8F 5C AE F2 04 91 FA 21 FD
15 D4 91 A6 36 6F (we find the CC).
```

If there is *no ciphering, there is no need for padding* and then PCNTR = 0 in the computation of the CC/RC/DS.

8.7 Details for the Upload of a Big SIM Address Book (Multiple Entries) Using Concatenated SMS

In this example we load an address book with three entries in a SIM card:

MOMO: +33140432125
MAMA: +33140432126
MAMY: +33140432127

And we request a ‘not ciphered’ Proof of Receipt (PoR) by the SUBMIT method to indicate that the upload was done successfully.

Table 8.16 shows the script to update the Address Book for multiple entries.

This address book is sent in two concatenated SMSs.

First SMS

```
Data: Message Type = SMS_DELIVER(SMS-MT)
                TP_RP = No request for reply path
                TP_UDHI= Header in TP-User-Data
                TP_SRI = A status report will not be returned to
the SME
                TP_VPF = TP_VP field not present
                TP_MMS = More messages are waiting for the MS in
this SC
```

Table 8.16 Script to update the Address Book (multiple entries in one record)

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 10	SELECT 7F10 (Directory TELECOM)
A0 A4 00 00 02 6F 3A	SELECT 6F46 (Abbreviated Dialling Numbers)
A0DC08041E	UPDATE RECORD # 8, absolute, length = 30
4D4F4D4FFFFFFFFFFFFFFFFFFFFFFFFF	Name MOMO
07913341402321F5FFFFFFFFFFFF	Phone number +33140432125
A0DC09041E	UPDATE RECORD # 9, absolute, length = 30
4D414D41FFFFFFFFFFFFFFFFFFFFFFFF	Name MAMA
07913341402321F6FFFFFFFFFFFF	Phone number +33140432126
A0DC0A041E	UPDATE RECORD # 10, absolute, length = 30
4D414D59FFFFFFFFFFFFFFFFFFFFFFFF	Name MAMY
07913341402321F6FFFFFFFFFFFF	Phone number +33140432127

```
               Originating mobile address             =
                 Type of number = International
                 Numbering Plan = ISDN
                 Address = 33899990007
               TP-Protocol-Identifier = 7F (SIM Data upload or
download)
               TP-Data-Coding-Scheme = F6
                 Message Class = Class 2(SIM Card)
                 Alphabet     = 8 bit (image/sound/download)
               TP_Service_Centre_Time_Stamp = 07.05.10 12:06:32 08
               TP-User-Data-length = 140
                 Length TP_User Data Header = 7
                   IEI = 112 (SIM Command Packet Identifier)
                     IEI Data Length = 0
                   IEI = 0 (Concatenated SMS 8-bit reference
number)
                     IEI Data Length = 3
                      (Hex) 040201
                       Reference Number 4
                       Number of sm 2
                       Sequence Number 1
               Command Packet Length=148 Command Header Length=21
               Security Parameter Indicator:
                SPI1(02):
                 Cryptographic Checksum(CC)
                 No Ciphering
                 No Counter available
                SPI2(21):
                 Por to be sent to Sending Entity
                 No Security applied to PoR
                 PoR not ciphered
                 PoR by SUBMIT
               KIc(00)
                 Algorithm known implicitly by both entities
                 DES in CBC mode
                 Keyset number(KIc-KID-KIK) used 0
               KID(15)
                 DES
                 Triple DES 2 different keys
                 Keyset number(KIc-KID-KIK) used 1
               Toolkit Application Reference=B00010:
                         Remote File Manager: Gemalto
               Counter=(Hex) 0000000000
               Number of padding bytes at the end=0
               RC, CC or DS = (Hex) 23476C7A96139383
          1)    SELECT(A4)Master File(MF)(3F00)
          2)    SELECT(A4)Directory File(DFtelecom)(7F10)
          3)    SELECT(A4)Abbreviated dialling numbers(6F3A)
          4)    UPDATE RECORD(DC)Rec No: 8 mode: absolute/current
record(4) length: 30
```

```
           Alpha Identifier: MOMO
           Number: Ext = No extension
              Ton = International
              Npi = ISDN
              Address = 33140432125
         5)   UPDATE RECORD(DC)Rec No: 9 mode: absolute/current
record(4) length: 30
           Alpha Identifier: MAMA
           Number: Ext = No extension
              Ton = International
              Npi = ISDN
              Address = 33140432126
          6)  UPDATE RECORD(DC)Rec No: 10 mode: absolute/current
record(4) length: 30
           Alpha Identifier: MAMY
           .....
              TP-User-Data =
’00941502210015B00010000000000000023476C7A96139383A0
A40000023F00A0A40000027F10A0A40000026F3AA0DC08041E4D4F4D4FFFFFFFFFFF
FFFFFFFFFFFFFF07913341402321F5FFFFFFFFFFFFA0DC09041E4D414D41FFFFFFFF
FFFFFFFFFFFFFFFF07913341402321F6FFFFFFFFFFFFA0DC0A041E4D414D59FFFFFF
FFFFFFFFFF’
```

As you can see there are *six* GSM 11.11 commands in the payload.

Second SMS

```
TP-User-Data-length = 26
               Length TP_User Data Header = 7
                 IEI = 112 (SIM Command Packet Identifier)
                   IEI Data Length = 0
                 IEI = 0 (Concatenated SMS 8-bit reference
number)
                   IEI Data Length = 3
                    (Hex) 040202
                    Reference Number 4
                    Number of sm 2
                    Sequence Number 2
                     SIM download, No display of concatenated SMS
number 2
              TP-User-Data =
                ’FFFFFFFF07913341402321F7FFFFFFFFFFFF’
PoR:
MAPPN_sm_rp_ui(25)
         L = 033
         Data: Message Type = SMS_SUBMIT(SMS-MO)
              TP_RP  = No request for reply path
              TP_UDHI= Header in TP-User-Data
              TP_SRR = Status Report not requested
              TP_VPF = TP_VP relative format
              TP_RD  = Accept SMS with same TP_MR
```

```
            TP_Message reference = 116
            Destination mobile address           =
              Type of number = International
              Numbering Plan = ISDN
              Address = 33899990007
            TP-Protocol-Identifier =  00 (No Interworking: SME-to-
SME protocol)
            TP-Data-Coding-Scheme = 04
              Message Class = Default (Handset MEmory)
              Alphabet = 8 bit (image/sound/download)
            Validity(Relative) Period = 7 day(s)
            TP-User-Data-length = 19
              Length TP_Use r Data Header = 2
                IEI = 113 (SIM Response Packet Identifier)
                 IEI Data Length = 0
            Command Packet Length=14 Command Header Length=10
            Toolkit Application Reference=B00010:
                    Remote File Manager: Gemalto
            Counter=(Hex) 0000000000
            Number of padding bytes at the end=0
            Response Status Code(00)= PoR OK
            No RC, CC or DS
            Number of commands executed = 6
            Status conditions returned by SIM SW1 = 90 SW2 = 00
             SUCCESSFUL: normal ending of the command
            Last File Abbreviated dialling numbers(6F3A)
            Last Command A0DC
            TP-User-Data =
              '000E0AB0001000000000000000069000'
       MAPPN_sm_rp_da(23)
        L = 009
        Data: TA_SC_ADR
            Ext = No extension
            Ton = International
            Npi = ISDN
            Address = xxxxxxxxxx
       MAPPN_sm_rp_oa(24)
        L = 017
        Data: TA_SC_ADR
            Ext = No extension
            Ton = International
            Npi = ISDN
            Address = 32485222829
```

As you can see, the PoR gives the number of GSM 11.11 commands which were correctly executed, that is *six* (all correct).

8.8 Security Keys, how to use the Card Vendor Provided Data

On the SIM card, most data are write-protected by a security key. The security can be:

Table 8.17 Card manufacturer file providing the security key KID

GSM No	ICCID/IMSI/KAPPLI1/ADM1
604872	892310560400029920 618046000029920 227C3AA6FECAB362 2604CB42
604873	892310560400029921 618046000029921 D40FB064FBCA24D1 39C5506E

- ciphering (with the KiC key);
- a signature (with the KID key) used to compute the 8-byte CC/RC/DS which you can see in underlined bold italic in the above example. The files with the minimum security level only necessitate the signature. So only the operator, who has the **KID** key, can update the files in the SIM card.

Table 8.17 shows a card manufacturer file providing the security key KID.

The example below will help to find the key and use it in the data that you get from the SIM card vendor. It is not simple as the vendor does not always state it clearly.

Example 1

Some vendors (such as Gemalto) call KID the OTAC-1 key and also APPLI1.

The ADM1 key has the same role as the KID (OTAC-1) key but for local access with a SIM card reader. You do not use ADM1 for OTA.

Here is an example of a file provided by Gemalto to a Liberia operator (+2315xxxxxx).

The first line is for the MSISDN +2315 **604869**.

The card ICCID (the unique identity) is 892310560400029917 (not used).

The IMSI is 618046000029917.

The **KID** is B3DF04101E3E7555 (*8 bytes only* coded in Hex) → means *it is DES_outer_CBC*.

The ADM1 key is 1429788F (not used).

So the KID is only 8 bytes in this file. This means that it is not ‘3DES_cbc with two keys’ which is used to compute the signature (it needs a full 16-byte key). So it means that ‘DES in CBC mode’ is used which needs only an 8-byte key.

As the OTA server implements 3DES_cbc, you will duplicate the KID key (K2 = K1) to obtain the 16-byte key that you use:

B3DF04101E3E7555B3DF04101E3E7555

Because:

$$\mathbf{E(M) = E_{K1}(D_{K1}(E_{K1}(M))) = E_{K1}}$$

Example 2

Other vendors will give a *16-byte KID*. It means *it is 3DES_outer_CBC*.

Key1=26 48 20 42 BF 3A F6 D7 68 2F FA EC 76 FC 0D C8 **KIc** used for ‘Ciphering’.
Key2=26 48 20 42 BF 3A F6 D7 68 2F FA EC 76 FC 0D C8 **KID** used for ‘Cryptographic Checksum’.
Key3=26 48 20 42 BF 3A F6 D7 68 2F FA EC 76 FC 0D C8 **KIK**.

You should note that for this card: **KIc** = **KID** = **KIK**.

References and Further Reading

[8.1] ‘Digital cellular telecommunications system (Phase 2+), Specification of the SIM-Mobile Equipment (SIM-ME) interface’, ETSI TS 100 977 v8.3.0 (2000–07) (GSM 11.11). Explains the various files, directory structure and file access commands of a SIM card.

[8.2] ‘Digital cellular telecommunications system (Phase 2+), Security Mechanisms for the SIM application toolkit’, ETSI TS 101 181 v8.3.0 (2000–07) (GSM 03.48). Explains the computation and format of the security.

[8.3] ‘Digital cellular telecommunications system (Phase 2+), Specification of the SIM Application Toolkit for the SIM-Mobile Equipment (SIM-ME) interface’, GSM 11.14, v8.3.0 (2000–07). Explains the proactive additional commands used to develop and install SIM Tool Kits.

[8.4] ‘3GPP Technical Specification Group Terminals: Characteristics of the USIM Application’, 3GPP TS 31.102 V6.4.0 (2003–12).

9

Handset 'Over The Air' Provisioning of GPRS Profiles, Automatic Device Management

9.1 The Data Access Path in GSM: Purpose of GPRS Profile Settings

If you browse through the menus of a handset, you will see 'connection' menus allowing you to select a particular data access mode, for example Internet (with fixed monthly charges), MMS (volume dependent) which includes a name (e.g. MMS.VIVACELL.AM, called the APN), a WAP Gateway IP address and a few user-selectable parameters depending on the handset.

9.1.1 Creation of a Data Connection

More detailed data of this 'GPRS profile' are included which are not user selectable with most handsets. The manual setup is laborious and to have a widely used data service, they are either factory set up in the handsets sold by a mobile operator or must be remotely loaded using 'OTA GPRS'.

A connection to a data service by a roaming visitor, such as sending an MMS, has the following steps. It is *always mobile initiated*, even if it is triggered by receiving of a special SMS-MT in the reception of an MMS.

The mobile is turned on in an SGSN-covered area within the GPRS roaming agreement between a VPLMN and HPLMN. An UPDATE LOCATION GPRS procedure is performed between the SGSN and the HLR in the HPLMN and a GPRS profile is loaded (see Chapter 1). It includes the list of authorized APNs *which must match those already set in the handset. If* successful, the mobile is 'GPRS attached', but no data connection path is yet established.

Then the user selects a data service, which uses a particular APN, and the connection is initialized. The SGSN checks that this APN is in the list that it has received from the HLR, and then establishes a connection (a 'PDP context') with its HPLMN GGSN through the GRX and the VPLMN GGSN as shown in Figure 9.1. The VPLMN has interrogated its DNS in order to get the IP address corresponding to the APN. The HPLMN GGSN uses the WAP Gateway IP address in the Create PDP context, and the connection to the service (such as MMS deposit on the MMSC) is made from the HPLMN.

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

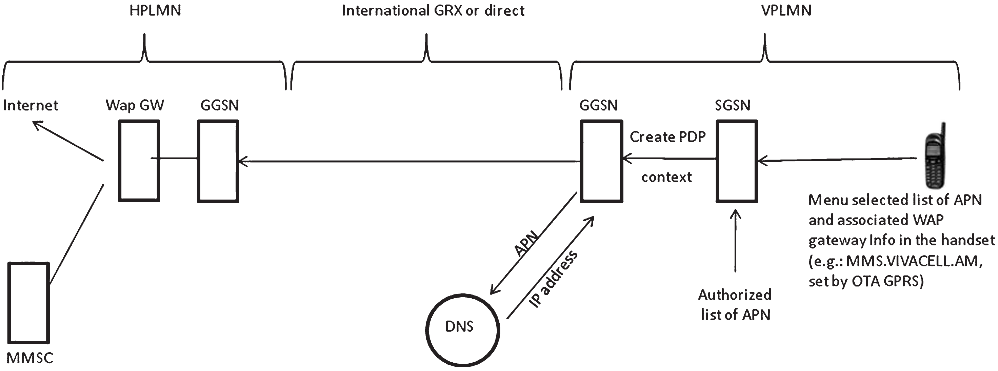

HPLMN
International GRX or direct
VPLMN
Internet
Wap GW
GGSN
GGSN
SGSN
Create PDP
context
Menu selected list of APN and associated WAP gateway Info in the handset (e.g.: MMS.VIVACELL.AM, set by OTA GPRS)
APN
IP address
DNS
Authorized list of APN
MMSC

Figure 9.1 GPRS data connection path

9.1.2 Two Standards for GPRS Profiles: Which One to Set?

The full GPRS profiles for the two different standards, OMA and Nokia-Ericsson, shown in Figure 9.2 show that it is impractical for a user to do the setup manually.

The profiles are coded in WML (an optimized HTML), more precisely in WBXML, where the text tags are replaced by binary tags to reduce the volume. An OTA GPRS server does the coding with the data provided by the HPLMN and sends them using 'concatenated SMS' to the destination handset. The Nokia-Ericsson example will use two SMSs to upload, while OMA uses five, and neither will work with models which are of the other type.

There are various methods to get the model of a handset. But there are more than 13 000 models with hundreds of manufacturers and even Nokia has 'Nokia-Ericsson' types and 'OMA' types. If one has the TAC (model number), is it 'Nokia-Ericsson' or 'OMA'? Some service companies claim to have created 'databases' by trial and error or by studying the 13 000 handset models specifications. We explain the 'stochastic' learning solution [9.1] which creates the correspondence automatically. There are three problems in performing Automatic Device Management:

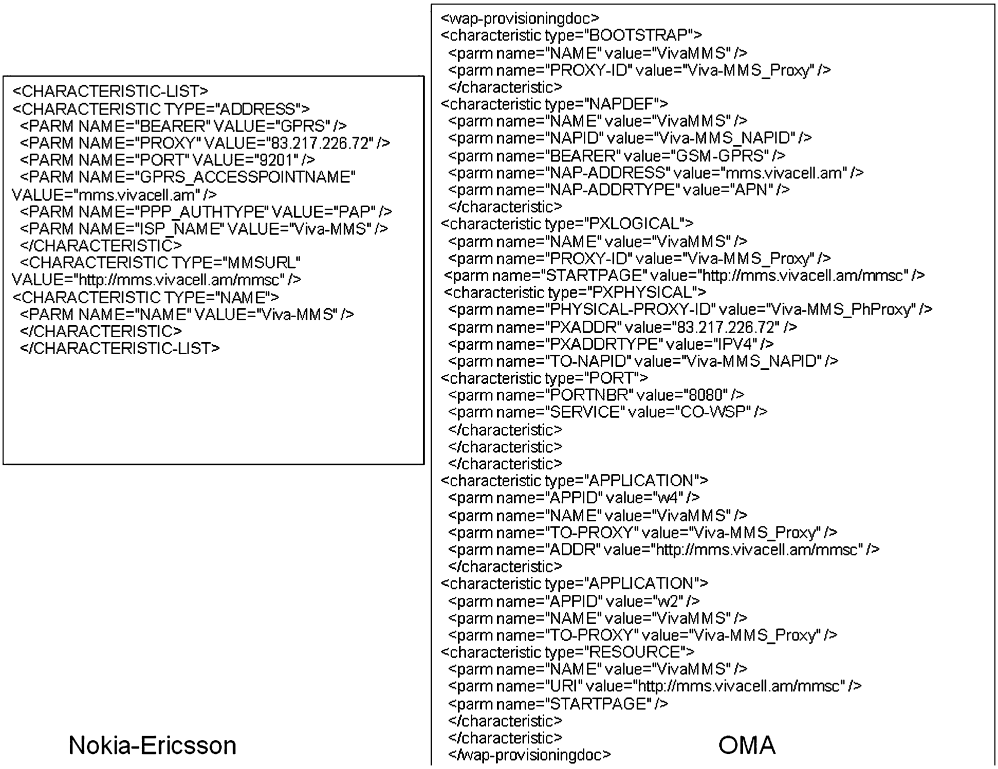
- How is the model type (IMEI) obtained without the customer's intervention, including automatic detection of change?
- Given the IMEI, what is the profile type to be used?
- Once a profile is loaded in a handset, how can it be automatically controlled so that it works?

9.2 Obtaining the IMEI of a Handset for Device Management

They can be separated into three categories:

- static billing files processing;
- automatically using the signalling generated by the mobile;
- on request from the OTA server.

Keep in mind that the VLR has the IMEI of the mobiles, but until recently, the MAP protocols or proprietary extensions did not allow it to be made available to an OTA GPRS server. This subject has been a problem for many VAS vendors that did not know the solution. The provision of a hosted service to manage the handset model database can easily be incorporated into a Roaming Hub.



```
<CHARACTERISTIC-LIST>
<CHARACTERISTIC TYPE="ADDRESS">
  <PARM NAME="BEARER" VALUE="GPRS" />
  <PARM NAME="PROXY" VALUE="83.217.226.72" />
  <PARM NAME="PORT" VALUE="9201" />
  <PARM NAME="GPRS_ACCESSPOINTNAME"
VALUE="mms.vivacell.am" />
  <PARM NAME="PPP_AUTHTYPE" VALUE="PAP" />
  <PARM NAME="ISP_NAME" VALUE="Viva-MMS" />
  </CHARACTERISTIC>
  <CHARACTERISTIC TYPE="MMSURL"
VALUE="http://mms.vivacell.am/mmsc" />
<CHARACTERISTIC TYPE="NAME">
  <PARM NAME="NAME" VALUE="Viva-MMS" />
  </CHARACTERISTIC>
  </CHARACTERISTIC-LIST>
```

```
<wap-provisioningdoc>
<characteristic type="BOOTSTRAP">
  <parm name="NAME" value="VivaMMS" />
  <parm name="PROXY-ID" value="Viva-MMS_Proxy" />
  </characteristic>
<characteristic type="NAPDEF">
  <parm name="NAME" value="VivaMMS" />
  <parm name="NAPID" value="Viva-MMS_NAPID" />
  <parm name="BEARER" value="GSM-GPRS" />
  <parm name="NAP-ADDRESS" value="mms.vivacell.am" />
  <parm name="NAP-ADDRTYPE" value="APN" />
  </characteristic>
<characteristic type="PXLOGICAL">
  <parm name="NAME" value="VivaMMS" />
  <parm name="PROXY-ID" value="Viva-MMS_Proxy" />
 <parm name="STARTPAGE" value="http://mms.vivacell.am/mmsc" />
 <characteristic type="PXPHYSICAL">
  <parm name="PHYSICAL-PROXY-ID" value="Viva-MMS_PhProxy" />
  <parm name="PXADDR" value="83.217.226.72" />
  <parm name="PXADDRTYPE" value="IPV4" />
  <parm name="TO-NAPID" value="Viva-MMS_NAPID" />
<characteristic type="PORT">
  <parm name="PORTNBR" value="8080" />
  <parm name="SERVICE" value="CO-WSP" />
  </characteristic>
  </characteristic>
  </characteristic>
<characteristic type="APPLICATION">
  <parm name="APPID" value="w4" />
  <parm name="NAME" value="VivaMMS" />
  <parm name="TO-PROXY" value="Viva-MMS_Proxy" />
  <parm name="ADDR" value="http://mms.vivacell.am/mmsc" />
  </characteristic>
<characteristic type="APPLICATION">
  <parm name="APPID" value="w2" />
  <parm name="NAME" value="VivaMMS" />
  <parm name="TO-PROXY" value="Viva-MMS_Proxy" />
<characteristic type="RESOURCE">
  <parm name="NAME" value="VivaMMS" />
  <parm name="URI" value="http://mms.vivacell.am/mmsc" />
  <parm name="STARTPAGE" />
  </characteristic>
  </characteristic>
  </wap-provisioningdoc>
```

Nokia-Ericsson
OMA

Figure 9.2 Nokia-Ericsson and OMA profile types

9.2.1 *Static Method: Use of Billing Files*

Most vendors allow the insertion of the IMEI (with the IMSI) into the call and SMS records. By processing these files regularly, it is possible to create the IMSI → IMEI database used in Figure 9.4. This, however, requires organizing the regular processing of batches of billing tickets, and automatic methods are more practical.

9.2.2 *Automatic Detection of Handset Model Using Signalling from Mobile*

See the five methods below, including those specifically designed for ‘device management’, to automatically update the GPRS profiles when a handset model change is detected.

9.2.2.1 SIM Tool Kit

When the handset is powered on (in particular after a change!), the SIM gets the IMEI of the handset, compares it with a file containing the last IMEI and, if it is different, sends an SMS-MO to a Device Management Centre, which would be the Roaming Hub.

9.2.2.2 HLR Alerting the Device Management Centre

This is the same idea, except that the revenue from the sale of the special feature goes to the HLR vendor (e.g. Ericsson) instead of the SIM card vendor. They use an extension in UPDATE LOCATION so that the IMEI is transmitted by the VLR. The HLR has a register to memorize the last IMEI and, if different, sends a MAP ‘ADD IMEI’ (proprietary MAP) to a Device Management Centre. This is quite elegant and avoids SIM Tool Kits for the purpose, but the feature has a price.

9.2.2.3 EIR Checks

The EIR of a customer MNO could be provided by the Roaming Hub, so that it receives all MAP requests concerning checking for stolen handsets.

If the Device Management Centre is integrated with the EIR (checking of stolen phones), it will receive a MAP CHECK IMEI (which contains the IMEI in the parameters) for any UPDATE LOCATION, call or SMS-MO (depending on the MSC-VLR setup). Just setting the CHECK IMEI for an UPDATE LOCATION does not place a load on the network and is sufficient for our Device Management purposes.

However, this method *will only work if the CHECK IMEI contains the IMSI* as a parameter in a proprietary extension of MAP, which is not standard. In the trace example below (Ericsson), the inclusion of the parameter IMSI *is not standard* (only IMEI is included in standard MAP, which does not allow the creation of IMSI ↔ IMEI).

```
TC_INVOKE(Request operation(Last))
TCPPN_LAST_CPT(2)
L = 001
Data: 1
TCPPN_COMPONENT(1)
L = 030
Data: Component type: Invoke(A1)
Invoke ID(2)
L = 001
Data: 137
MAP_ERICSSON_CHECK_IMEI(43)
imei(4)
L = 008
Data: Address = 358358005554070
imsi(193) /* Not standard in MAP */
L = 008
Data: Address = 634051110012544
```

9.2.2.4 Roaming Hub Case: Extraction in the MAP UPDATE LOCATION Messages

In the case of a Roaming Hub, some signalling messages will transit which contain the IMEI or the IMEISV.

When the VPLMN supports ADD (Automatic Device Detection), the UPDATE LOCATION and UPDATE LOCATION GPRS include the IMEISV (that is with the Software Version) of the handset. So the Roaming Hub can create the database IMSI → IMEI for all the handsets which are activated through the service. This IMEISV will be provided by the latest MAP versions or by ‘extension containers’ with certain NSS vendors.

9.2.2.5 Roaming Hub Case with the GPRS Virtual Data Service: Use of GTP

Every time a virtual visitor connects to the Internet or to the MMSC, the GTP Create PDP Context contains the IMEISV and the IMSI.

9.2.2.6 Roaming Hub Case: Use of CAMEL Initial DPs

Recent implementations of Initial DP, Initial DP SMS and Initial DP GPRS, include the IMEI which can be recorded with the IMSI and the Calling Party number, which are also included.

9.2.3 On Request from the OTA Server Method

This *possibility* has been feasible recently due to upgrades of MAP. It is possible to obtain the IMEI with a direct PROVIDE SUBSCRIBER INFO (MAP Version 3) for the target IMSI specifying ‘requested info = IMEI’ or with an ANY TIME INTERROGATION. If the profile type of this TAC is known, the download of the profile can be done. It is the simplest by far.

Figure 9.3 shows how the IMSI ↔ IMEI is obtained for automatic device management.

The ‘forced MMSC connection method’ is the most complicated, but also the most standard, if the network for which we want the IMEIs has GPRS installed. However, the automatic connection will work only if a minimum ‘MMS profile’ exists already! It can be used to get the IMEI of a phone which is already configured, not to obtain it for the first time.

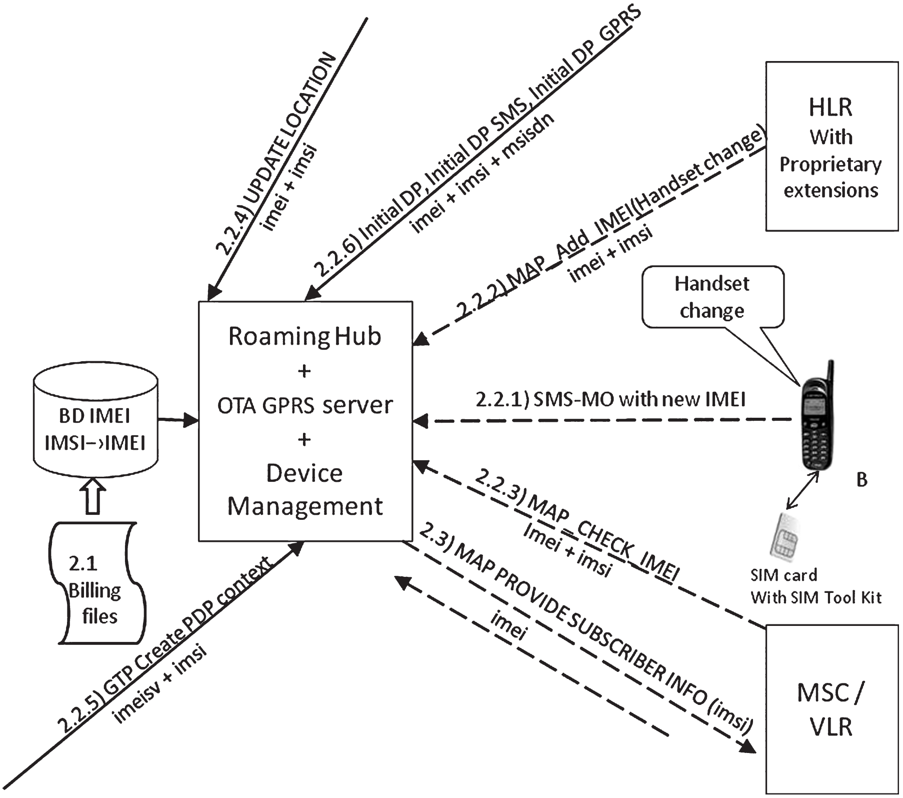


Figure 9.3 Obtaining the IMSI ↔ IMEI for automatic device management

9.3 Method to Remotely Check that a Loaded GPRS Profile Works

Assume that some GPRS profile has been loaded in a handset but you are not sure it works: not sure of the handset model, not sure which type of profile (OMA or Nokia-Ericsson) applies to this model, or not sure that the profile coding was correct. There is one method which allows you to remotely check that the profile works by performing this ‘loop’:

- Send an MMS notification to the handset from the OTA GPRS server.
- If the MMS GPRS profile works, the mobile connects to the OTA server because the URL also tells it is the MMSC containing the MMS.
- If the mobile does not connect within a few seconds, the profile is wrong and another one is loaded and retested automatically by this method until the connection works.

Recall that for MMS delivery, an ‘MMS notification’ packed in an SMS is sent to the destination handset, which contains the URL with the MMSC as domain name, so that the handset establishes (automatically or sometimes with a customer confirmation) a GPRS connection to GET the MMS. The message which is sent to the MMSC contains the IMEISV (the IMEI + the Software Version) or the model type in text.

The method is then to have the OTA server behave as an MMSC, and send an ‘MMS notification’ to its own IP address (http://192.168.1.1/otagprsserver below). The handset will try to retrieve an MMS, *while providing its model type automatically*. Information can be given to the handset in the form of an automatic MMS such as: ‘Congratulations, we have verified that your handset, NokiaN95, is properly configured for the data services’.

9.3.1 Example of MMS Notification Sent by SMS-MT to the Handset to Get its Model Type

This is the ‘text part’ content of the SMS-MT given by a protocol analyser, which is the same as in Figure 9.6 but with:

```
……..
Content Location: http://192.168.1.1/otagprsserver/
```

in order to force the connection to the OTA GPRS server itself and to ‘send’ to the handset a confirmation that its model type is properly configured for GPRS.

9.3.2 Corresponding HTTP GET Sent by the Handset and Providing the Model Type

If the MMS GPRS profile *was correctly set*, the handset will connect (automatically) to http://192.168.1.1/otagprsserver, which is the OTA GPRS server, thus providing confirmation that a previously loaded profile works.

The OTA server receives a HTTP GET request with a display as shown below, where the interesting parts are shown:

```
GET /otagprsserver/   HTTP/1.1
X-ICAP-Version: 1.0
Host: www.halys.fr
Accept: */*, application/vnd.wap.mms-message, application/vnd.wap.sic
Accept-Charset: utf-8
```

```
Accept-Language: en
User-Agent: NokiaN95/30.0.015 Series60/3.1 Profile/MIDP-2.0 Configuration/CLDC-1.1
X-Nokia-MusicShop-Bearer: GPRS/3G
X-Nokia-BEARER: UMTS
X-Nokia-CONNECTION_MODE: TCP
X-Nokia-gateway-id: NWG/4.1/Build79
X-Nokia-ipaddress: 10.186.245.29
```

And the HTTP GET contains the full model type (the 'User-Agent' = Nokia N95) in text (but not the IMEI). In a LINUX system, this trace in found in /var/log/httpd/access_log.

9.4 Architecture of a Classical OTA GPRS Server

9.4.1 Integrated or SMPP-connected GPRS Server

Figure 9.4 shows a GPRS server integrated with an SMSC which allows downloads using concatenated SMS without intermediate paging between each SMS.

For automatic device management, they rely on the existence of an accurate database IMEI (TAC) → Profile Type which, whatever they may claim, no one has in full (>13 000 models).

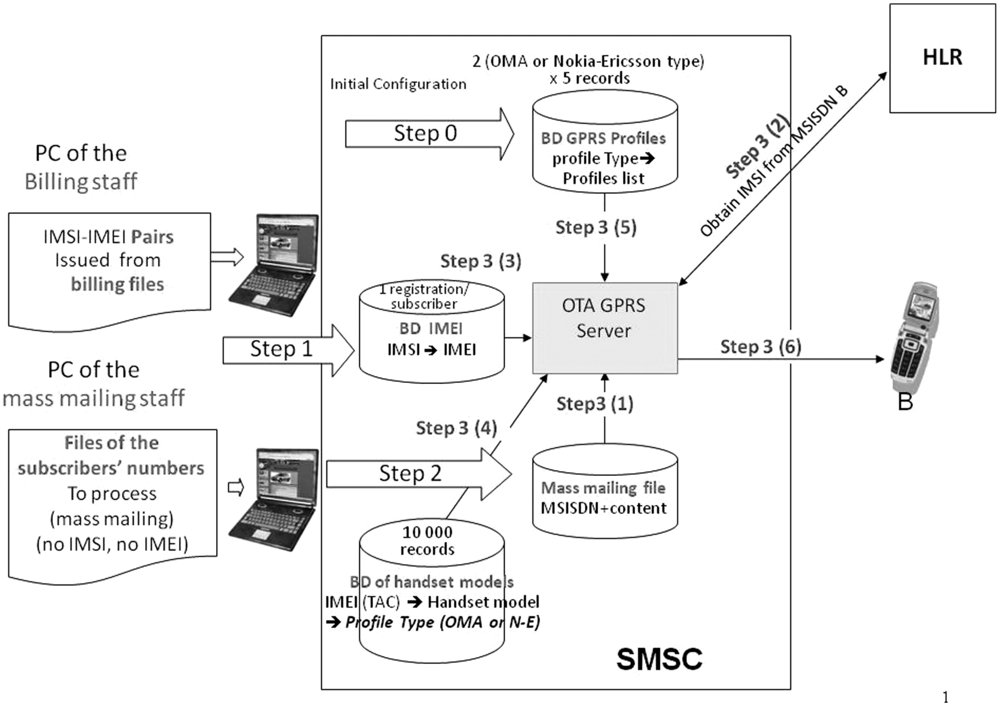


Figure 9.4 Classical OTA GPRS server

By some method they are able to get the IMEI from the MSISDN or the IMSI, and then the Profile Type. And the upload is done with formatted SMSs.

When the OTA GPRS server is connected through SMPP to the server:

- It cannot easily get the IMSI from the MSISDN (it is used below for security NETWORK PIN).
- The loading of concatenated SMSs will need a new paging between each SMS, which creates a lot of radio usage.

9.4.2 Security

It should be impossible to modify the GPRS profiles from any other equipment than the HPLMN.

There are four levels of security defined by the two standards of OTA, and the one selected is set in the GPRS profile:

- *no* security;
- network pin;
- user pin;
- user network pin.

Network Pin: this is the IMSI, and the reception can then be automatic because the customer does not have to enter anything. So this should be used for an automatic device management service. External OTA GPRS servers will have difficulties in obtaining the IMSI list.

User Pin: a four-digit number is agreed between the handset owner and the sender (for example the customer care staff). When the profile is received, the PIN must be entered in the handset to be accepted.

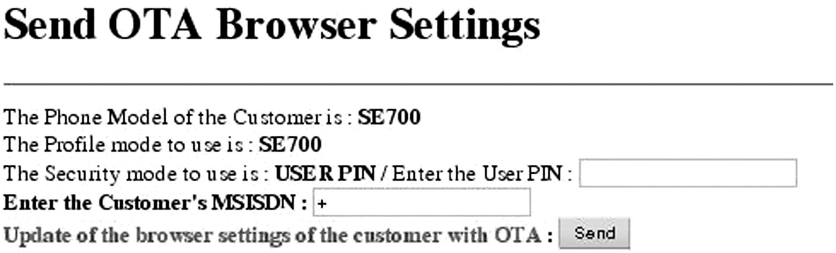
User Network Pin: This is the previous two combined.

Figure 9.5 shows a typical Customer Care interface to send a GPRS profile manually on demand, including the case where the customer is asked to provide their IMEI.

To prevent fraud, the sent profile includes a HMAC function signature, where the data of the profiles are signed by the HMAC standard function using the PIN (either User Pin or Network Pin as selected) as the key, and the signature is included in the profile sent.

9.5 Stochastic Automatic GPRS Profile Type Learning OTA Server

The OTA server is integrated with the main SMSC which forwards the MMS notification SMS sent by an MMSC. This creates a loop which is fundamental in GPRS profile learning. The principle is simple: if a handset is able to send MMS, the GPRS profile is correct. And if it had been guessed (Nokia-Ericsson or OMA), it can be confirmed and the GPRS profile type becomes known for the TAC.



Send OTA Browser Settings

The Phone Model of the Customer is : **SE700**

The Profile mode to use is : **SE700**

The Security mode to use is : **USER PIN** / Enter the User PIN :

Enter the Customer's MSISDN : +

Update of the browser settings of the customer with OTA :

Figure 9.5 Sending browser settings by OTA

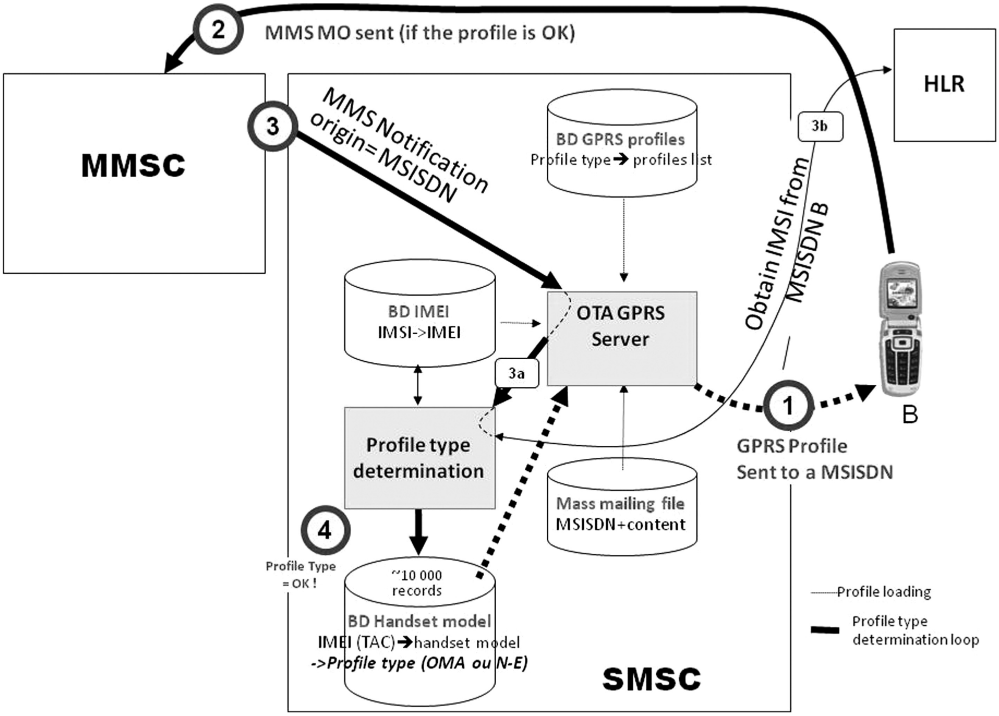


Figure 9.6 Stochastic learning OTA GPRS server

Figure 9.6 shows the following actions. In (1) a GPRS Profile is guessed for the handset. Assume it is correct, and then later it will send an MMS-MO (2) to a destination. The MMSC will ask (3) the SMSC in the OTA GPRS server to send an 'MMS notification' SMS. The SMSC extracts the origin address from the WAP (the 'from' parameter and can confirm (3a and 4) in the database that the last guessed profile is correct.

Little by little, the GPRS profile types of all the handset types become accurately determined.

9.5.1 Extracting the Origin Number from the MMS Notification

The MMSC sends an 'MMS notification' to the receiving party which most often has an Alpha identifier of the MMSC in the SMS origin address, *not the MMS sender number*. For this method, the integrated OTA GPRS server must extract *the origin address* from *the SMS content* which is coded according to [9.3], that is to have WAP decoding software. Figure 9.6 shows this.

```
http://mms.vivacell.am/mmsv/INBOX*A7289CED7DBD5B4BEBS1F05D97A822C0
/*SMS protocol decoding*/
MAPPN_sm_rp_ui(25)
Data: Message Type=SMS-DELIVER (SMS-MT)
……..
TP-Originating-Address
Address= VivaCell          /* Common Origin Address networkname*/
```

```
……..
TP-User-Data –
……            /* WAP protocol decoding to obtain the origin Address*/
MMS Encapsulation protocol and WAPOTA(OMAformat):Browser setting, etc,..
              Transaction ID 01 (Hex)
              PDU type: (6):PUSH
                   Header length 29
              Application type: (190): application/vnd.wap.mms-messag
Message-Type: message-notification
                   Transaction-ID: AqconO19vVtL64HwXZcoIsBvBhBCSTeR
                   MMS-Version: 1.0
                   From: +37493600666      /* Origin Address identifies the MMS sending mobile*/
                   Message Class: Personal
                   Message-Size: 273 bytes
                   Expiry (Relative): 50590848 secs
                   Content Location:
       http://mms.vivacell.am/mmsv/INBOX*A7289CED7DBD5B4BEBS1F05D97A822C0
```

The system will conclude that +37493600666 has been able to send an MMS, *so that its last tried GPRS profile type is correct.* And the IMSI → IMEI correspondence for +37493600666 is used to confirm the whole TAC GPRS profile type.

9.6 Stochastic Convergence

In Section 9.3 we have shown how a check could be done after each GPRS profile download. If this is not included in the OTA procedure, a check is also provided by traffic observation over a few days; this is what we call ‘stochastic convergence’.

As OTA GPRS downloading continues for a certain period (hence the ‘automatic and stochastic’ name of the method), the percentage of unconfirmed TACs will become less than a small threshold. As new models are introduced, the process must go on, but once a GPRS profile type is confirmed, it will stay like this.

9.6.1 Convergence Time

Let N be the average number of GPRS accesses/day/subscriber.

Set the {Probability 0 GPRS access during 1 hour} to:

$(1 - N/24)$

so: {Probability 0 access during 24 hours}:

$(1 - N/24)^{24}$

and during J days:

$(1 - N/24)^{24 \times J}$

and if there are M subscribers with the same model, the Probability that none of the M subscribers with this handset type makes a GPRS access during J days is:

$(1 - N/24)^{24 \times J \times M}$

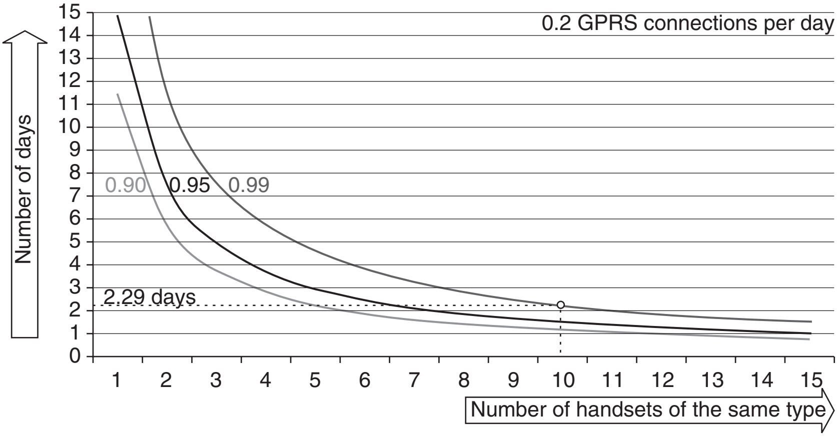


Figure 9.7 Curves of convergence time

In Figure 9.7 we have drawn various curves for J and M for different values 0.90, 0.95, 0.99 of the probability that at least one of the subscribers has made a GPRS access, and for a given N, this is function (J,M):

$(1 - N/24)^{24\times J\times M} = 1 - P$

If one takes N = 0.2 GPRS/day, with P = 0.99 (almost certain) and a population of 10 mobiles of a given type, one finds J = 2.29 days, provided that no GPRS traffic occurred such that the other profile type must be set for a new OTA download. The stopping criteria is that for all the models with a sufficient number of users M, one has P = 0.99 since the last download.

9.7 Best Order to Try an Unknown Handset GPRS Profile Type

To take the general case, we will assume that there are more than two GPRS profile types and want to determine the order when we try an unknown profile type: should we start with the most frequent one?

Let p be the total number of GPRS profile types.

Let $c_1, c_2, \ldots, c_p$ be the cost (in number of SMSs) of an OTA attempt with the GPRS profile #i to the unconfirmed models (total number M). These costs are different because some require more SMSs than others (see Figure 9.2, the OMA profile requires five SMSs and the N-E requires two).

Let $q_1, q_2, \ldots, q_p$ be the a priori probability of these different types (from a market study).

Let j1, j2, … , jp be the sequence of indices such that:

$q_{j1}/c_{j1} > q_{j2}/c_{j2} > \ldots > q_{jp}/c_{jp}$

(quantities q_i/c_i are sorted by decreasing value)

A theorem [9.2] says that the optimal order of the attempts is:

j1, j2, …, jp

which minimizes the mathematical expectation of the *total cost in total number of SMSs* until convergence is reached (this is not the same criteria as *the total number of OTA downloads*).

For example, if there are only two profiles and $q_{oma} = 0.65$ and $q_{ne} = 0.35$, we have:

0.35/2 SMS > 0.65/5 SMS (0.175 > 0.13)

and one must start with the N-E profiles (not intuitive because they are less frequent).

One checks that on average:

$2 + 0.65 \times 5 = 5.25$ SMSs per handset with the policy N-E then OMA
$5 + 0.35 \times 2 = 5.70$ SMSs per handset with the policy OMA then N-E (more)

The full demonstration for $p > 2$ uses linear programming theory with a $p \times p!$ matrix but the demonstration for $p = 2$ is elementary.

Hence, if:

$c_1 + q_2c_2 < c_2 + q_1c_1$, with $q_1 + q_2 = 1$

(policy 1 then 2 better than 2 then 1),

$c_1(1\text{-}q_1) < c_2(1\text{-}q_2)$

that is:

$c_1q_2 < c_2q_1$

which gives:

$q_1/c_1 > q_2/c_2$

as sufficient condition for the order 1 then 2 to give a lower average total number of SMSs.

References and Further Reading

[9.1] Henry-Labordère, A., Manai, W. and Mathian, B., 'Procédé de détermination automatique du profil de personnalisation GPRS d'un mobile', Patent FR 07 58 567.

[9.2] Henry-Labordère, A. and Zerhouni, C. M., '*Décisions bayesiennes avec information incomplète*', METRA, Volume 12, 1972.

[9.3] 'Wireless Application Protocol, WAP-209-MMS Encapsulation Protocol', Version 05 Jan 2002, page 14–15, www.wapforum.org.

10

Current Developments and Directions: GSM-UMTS ↔ VoIP Roaming

Wherever I wander, wherever I rove,
My heart is in the Highlands wherever I go.

Robert Burns (1759–1796)

10.1 Pirate Techniques?

This chapter may be considered to contain 'pirate techniques' if not studied carefully, but these systems exist and have nothing illegal about them. The superficial response of some mobile operators that they will decrease their roaming revenue is also wrong. We will show, on the contrary, that the charging of VoIP calls including Visio is simple (includes prepaid customers) and it is possible to obtain better rates for the user and increased revenue for the operators. Some revenues will be decreased, *not theirs* but those of their roaming partners and they will not know about it directly except by observing their visitors' traffic statistics trend.

The second part, 'attracting and locking visitors' by modifying their SIM or USIM card (UMTS), could be the most controversial. But no more than the so-called 'Steering Of Roaming', which uses the 'partners'' resources as explained in Chapter 8, without bringing them the revenue of the visitors. The commercial offering and the method explained is a possible answer for those who are disadvantaged by the 'SOR'. Many people that have a SIM card reader on their PC will be able to test the method for their own handset; all the background is given in Chapter 8.

The last part is IMS, a rather new concept, for which we present a brief overview. Nothing is controversial except the date of a large deployment when many resources are devoted to 4G LTE.

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3

10.2 Seamless 'Free Roaming'? GSM-UMTS with SS7 ↔ VoIP Gateways

10.2.1 Business Case and Usable Terminals for VoIP ↔ GSM Service

Only dishonest (or ignorant) authors will attempt to deny Robert Burns was the real originator of the idea: 'home is where the heart is', which is the basis of the seamless SS7 ↔ VoIP roaming method of this chapter.

A number of solutions have recently appeared that allow a roamer to have the same services and rates as at home, whether by using a PC, or with a Wimax or Wifi dual mode handset. These services are offered commercially by certain mobile operators and also work at home using the Wi-Fi personal base station for Internet access. Several manufacturers (Nokia, Samsung, etc.) propose 'mixed mode' handset GSM + Wi-Fi using the UMA standard between the handset and a Gateway when Wi-Fi is used.

But many recent handsets integrate a SIP softphone directly, which is sometimes locked because with some fixed-charge monthly data subscriptions, it would be possible to make 'free calls'.

The cost of data roaming is very high, and no economy can be achieved by making phone calls (SIP or UMA) over a mobile data connection while roaming. So the practical case will be to use a fixed line or Wi-Fi connection while roaming, at a marginal cost when a traveller is at their hotel and rents the Internet connection chiefly to access their email.

10.2.2 System Architecture GSM and UMTS Using an SS7-VoIP Gateway

- An SS7-VoIP Gateway in the HPLMN of the GSM operator (for cost-efficiency reasons).
- A terminal which can be a PC with a USB key where the SIM or USIM card is inserted, a UMA standard GSM-Wi-Fi handset or a GSM handset with a SIP softphone integrated.

For a PC, it is most convenient that the softphone software is on the USB key so that no initial loading is necessary. This means that in an Internet-equipped aircraft, the USB key to make voice calls can be distributed by the stewards and the service used immediately.

The user takes their SIM or USIM card from their handset and inserts it in a slot of a special USB key that contains a card reader. Then the USB key is plugged into the PC, which will automatically start the software on the key, which has a configuration file containing the IP address of the SS7-VoIP gateway. The first software executed is the 'client relay authentication' of Figure 10.1, which will verify that the SIM card is really authenticated in the HLR:

- It reads the IMSI of the card.
- It sends it (1) by IP to the address of the SS7-VoIP gateway, which will behave as an MSC/VLR for the authentication, executing the A3 standard GSM algorithm.
- The IMSI is used to prepare a SEND AUTHENTICATION (3) to the HLR, which knows the secret Ki key of this IMSI and returns (4) a random number RAND and a key computed from Ki and RAND: SRES = Ki (RAND).
- Over the Internet, the SS7-VoIP gateway sends (5) only the RAND to the PC. The PC sends the RAND to the SIM card and a RUN GSM command.
- As a result, the SIM card (which if legal has the same Ki key as in the HLR) returns (6) an SREScalc to the PC: SREScalc = Ki (RAND).
- The PC sends it by Internet (7) and (8) to the SS7-VoIP gateway, which compares SRES and SREScalc. If they are the same, it is a real card of the HPLMN and the session establishment proceeds.
- An UPDATE LOCATION (9) using the IMSI is performed by the SS7-VoiP gateway (as a normal MSC-VLR). The HLR returns the MSISDN of the subscriber, which will be used as the Calling Line Identity for Calls and SMSs that they perform. *At this stage the subscriber in China is registered normally in a home MSC/VLR* (the SS7-VoIP gateway).

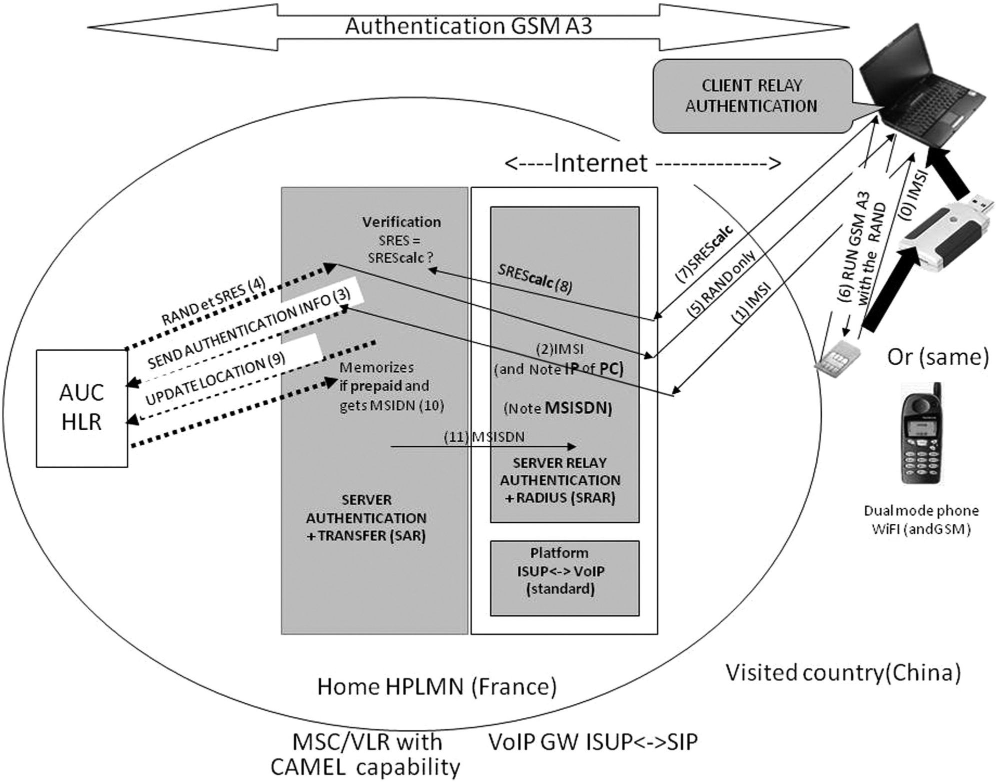

Authentication GSM A3
CLIENT RELAY AUTHENTICATION
<----Internet ------------->
Verification
SRES = SREScalc ?
RAND et SRES (4)
SEND AUTHENTICATION INFO (3)
UPDATE LOCATION (9)
AUC
HLR
Memorizes if prepaid and gets MSIDN (10)
SREScalc (8)
(2)IMSI
(and Note IP of PC)
(Note MSISDN)
(11) MSISDN
SERVER RELAY AUTHENTICATION +RADIUS (SRAR)
SERVER AUTHENTICATION +TRANSFER (SAR)
Platform ISUP<-> VoIP (standard)
(7)SREScalc
(5) RAND only
(1) IMSI
(6) RUN GSM A3 with the RAND
(0) IMSI
Or (same)
Dual mode phone WiFI (andGSM)
Home HPLMN (France)
Visited country(China)
MSC/VLR with CAMEL capability
VoIP GW ISUP<->SIP

Figure 10.1 Registration of user for GSM ↔ VoIP seamless roaming

When the user replaces the SIM card in the handset, the HLR will CANCEL LOCATION of the SS7-VoIP gateway and the handset can be reused normally. To provide an address book, the softphone reads the Address Book of the SIM card so that all these contacts are directly usable.

In [10.1] there is also an alternative registration method for systems which would not be hosted by a HPLMN but by a nonmobile operator commercial party which has access to the SS7 network and to the roaming agreements of a mobile operator. They set their own SS7-VoIP gateway in a given country and force an unconditional call transfer using SS7 (using the MAP ‘Supplementary Services’ of Chapter 1 and the IMSI that is read by the softphone).

Another implementation is to provide an individual box, which is a combination of an ‘air interfaced GSM modem’ on one side and an Internet service access on the other, for each roamer. When they remotely connect the PC, the home ‘GSM modem’ registers in the HPLMN: they are still at home for all applicable rates. It is clever, but as it necessitates a number of boxes for each roamer, it is unsuitable to offer the service generally.

10.2.3 Receiving Calls or SMS

Figure 10.2 shows a call (1) made to the user in China (a French number), which arrives on the Home Network GMSC:

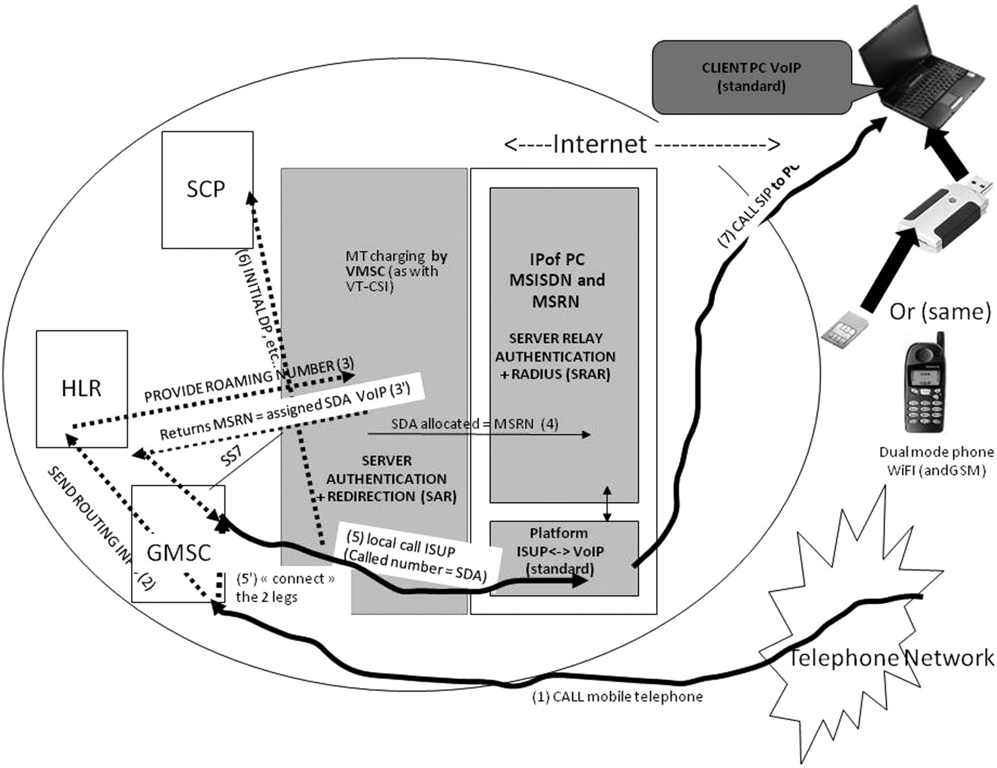

CLIENT PC VoIP (standard)
<----Internet ------------->
SCP
(6) INITIAL DP, etc..
MT charging by VMSC (as with VT-CSI)
IPof PC MSISDN and MSRN
SERVER RELAY AUTHENTICATION +RADIUS (SRAR)
(7) CALL SIP to PC
Or (same)
HLR
PROVIDE ROAMING NUMBER (3)
Returns MSRN = assigned SDA VoIP (3')
SS7
SDA allocated = MSRN (4)
SERVER AUTHENTICATION + REDIRECTION (SAR)
Dual mode phone WiFI (andGSM)
SEND ROUTING INF
(2)
GMSC
(5') « connect » the 2 legs
(5) local call ISUP (Called number = SDA)
Platform ISUP<-> VoIP (standard)
Telephone Network
(1) CALL mobile telephone

Figure 10.2 Receiving a call and CAMEL charging (prepaid) of MT call to outbound subscriber

- This sends SEND ROUTING INFO (2) to the HLR.
- The HLR knows that the customer is registered in the SS7-VoIP gateway (MSC/VLR) and sends the PROVIDE ROAMING NUMBER to the gateway with the IMSI of the called party (3).
- The gateway has a range of roaming numbers (MSRN) allocated, as a normal MSC/VLR, and returns an available one (3′) while keeping the correspondence IMSI ↔ MSRN.
- The GMSC makes an ISUP local call to this MSRN (the ‘B’ number in the call), and the call terminates to the VoIP gateway (5).
- The IMSI can be deduced from the MSRN, and the IP address of the PC found from the IMSI ↔ IP correspondence created at the registration phase. A SIP call (7) is also made to the PC, which rings.
- If B is prepaid, the SCP is interrogated for credit with an INITIAL DP (6).

For the reception of SMS-MT by the subscriber in China, it is the same principle:

- The Home SMSC will interrogate the HLR and the FORWARD SHORT MESSAGE MT will be sent to the Visited MSC, i.e. the SS7-VoIP gateway.
- The SS7-VoIP gateway will send it to the PC using the MESSAGE PDU of the SIP protocol.

10.2.4 Making Calls or Sending SMS

In Figure 10.3, the softphone in the USB key is able to read the address book of the SIM card, so calls are easy. The SIP protocol allows a call (1) to be made to the SS7-VoIP Gateway:

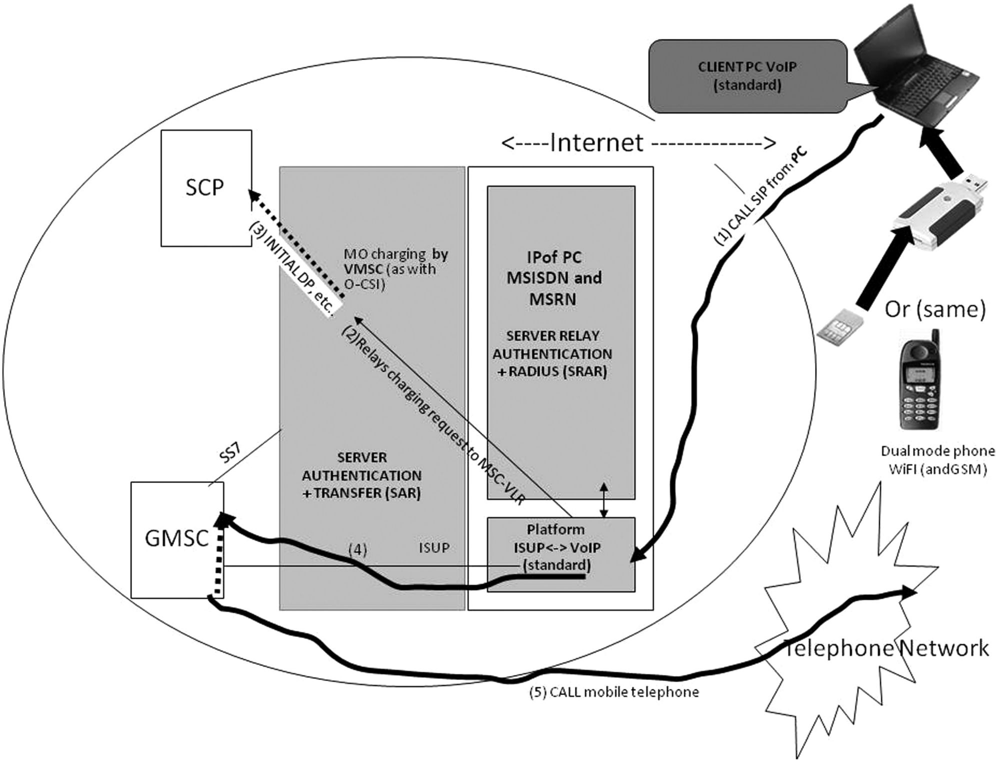

CLIENT PC VoIP (standard)
<----Internet ------------>
SCP
(3) INITIAL DP, etc.
MO charging by VMSC (as with O-CSI)
IPof PC MSISDN and MSRN
SERVER RELAY AUTHENTICATION + RADIUS (SRAR)
(1) CALL SIP from PC
Or (same)
(2)Relays charging request to MSC-VLR
SS7
SERVER AUTHENTICATION + TRANSFER (SAR)
Dual mode phone WiFI (and GSM)
GMSC
(4)
ISUP
Platform ISUP<-> VoIP (standard)
Telephone Network
(5) CALL mobile telephone

Figure 10.3 Outbound subscriber makes a call to PSTN and CAMEL charging (prepaid) of MO call

- The MSISDN of the calling party is available from the registration step.
- The SS7-VoIP Gateway has a SIP presence server to know which subscribers are connected.
- The calls to connected users are directly executed with SIP.
- If they are not connected, the SIP → ISUP conversion is made and the call uses the PSTN. But the CLI is automatically set and the receiving party *will see the mobile phone number* of the user.

10.2.5 Charging VoIP Calls Based on Location: Use of IP Address Resolution

Charging for prepaid customers (using VoIP does not mean that the HPLMN wants the service to be free) is accomplished by the CAMEL protocol in the Gateway, which makes an Initial DP to the SCP. For the HPLMN, the visited MSC/VLR is always the Gateway. How is it possible to have tariffs depending on the location of the user?

A simple way is to use the IP address of the caller in the SIP ‘Invite’ message (the ‘call’), which has the IP or proxy address (hotel) of the user. Unless the content is modified on the Internet, it allows the use of the Access Provider registers (APNIC for Europe, etc.) to obtain the name of the address provider and their country (example: www.afnic.fr/outils/whois).

If you enter 89.31.156.34, you get:

```
information related to ‘89.31.156.0 - 89.31.156.255’
   inetnum:    89.31.156.0 - 89.31.156.255
```

netname: COSMOFON
country: MK (Macedonia)

A Macedonia VoIP rate could be applied for calls made or received for this customer.

While always setting the unique GT of the SS7-VoIP Gateway as 'VMSC GT', a specific internal table of different 'Cell Ids' for each country of the user would allow different rates to be used as most SCPs can have 'Cell Id' specific rates. To avoid confusion with existing Cell Id rates, a specific coding such as '999.99.0.Country Code' could be used. As 999 is not an existing 'MobileCountryCode', this location code for Internet access will not be confused with other mobile network locations, and also the last field used for the coding of the Country Code has a range (0, 65535) which is more than enough to code all the countries.

For post-paid customers, MOC (Mobile Originated Calls) and MTC (Mobile Terminated Calls) tickets with the Cell ID are created for billing.

What is the best rate for the GSM-UMTS ↔ VoIP so that both the HPLMN and their customers benefit? Table 10.1 gives the logic and the possible strategies.

If the rates in bold are used, the customer has a reduction of 50%, the margin per call is the same, but the customer will call more so the revenue of the HPLMN will increase (VPLMN gets nothing).

In Chapter 7, where the 'VMS anti-tromboning' suppresses all these costs for the VPLMN, a similar pricing strategy for the reception of messages while roaming could apply: the costs from the international carrier or from the roaming partners are suppressed and can be shared with the customer.

10.2.6 Visio Calls SIP ↔ UMTS

These systems apply directly when the Visio function of the SIP phone is used. Between two users connected to the SS7-VoIP gateway, there is no need for conversion; SIP handles the session negotiation for the Visio calls. Commercially it is very interesting; the user may be in a country where there is no UMTS and they are still able to make Visio calls to their colleagues using their PC!

The softphone displays the list of connected users so it is immediately possible to know if a SIP-SIP Visio call is possible.

If the SS7-VoIP Gateway has a SIP ↔ H324-M (the standard for 3G Visio call) capability, it is possible to receive and make a Visio call from the PC to any UMTS phone.

10.3 Attracting the Visitors and Forcing Them to Roam Immediately in a Given VPLMN

10.3.1 Offering the GSM-UMTS ↔ VoIP to Lock Visitors into One's Network

In a given country A, there are four mobile operators and one is a subsidiary B of a large group which uses 'Steering of Roaming'. So the visitors of the various subsidiaries are directed to B when they visit

Table 10.1 Business rates: improved charging rates with VoIP roaming

Direction of call	HPLMN to Roamer inVPLMN	Roamer inVPLMN to HPLMN
Cost for HPLMN: normal GSM call	0.20 USD/min	0.80 USD/min (IOT)
Charged to customer (margin 100%): normal GSM call	0.40 USD/min	1.60 USD/min
Cost for HPLMN: VoIP roaming	No charge (VoIP call)	No charge (the VPLMN is not used)
Charged to customer: VoIP roaming	**0.20** to 0.40 USD	**0.80** to 1.60 USD

A. What can another operator C, which was a good previous roaming partner of A before this, do to fight back?

One approach is that the 'USB key softphone' of Section 10.2 is promoted by C and distributed at the hotels with the Internet temporary connection that most travellers request. There is an SS7-VoIP Gateway in C and the softphone's software is set to address it. The travellers have a given credit, controlled by CAMEL in C, and advantageous rates for local calls and calls to other countries including theirs, while still being able to receive the calls to their mobile number when they stay at the hotel and use their PC.

When they insert the USB key (with their SIM card), the 'softphone' promoted by C can read and *write* their SIM or USIM card because *they had to enter their 'PIN code'* to perform the registration procedure! And in the softphone there is a 'preferred PLMN list' which, no surprise, has C at the top and, if naughty, a 'forbidden PLMN list' which has B, the competitor, and these new files are written to the card. The existing 'Preferred PLMN list' may be read and smartly updated also (that is C and their friends at the top, by deleting some networks if space needs to be found). The user need not be aware of this.

As explained in Chapter 8, setting the 'preferred PLMN list' is not enough. The logic in the handset monitors the Network Codes broadcast by the coverage of the radio signal received, then first considers *the last network* (which is B most likely) (provided there is coverage) before searching with the Preferred PLMN list.

C wants *to force* the switch to its network immediately after the SIM card is back in the handset. Otherwise, even with the updated file, it would still register on B. To achieve this, the 'softphone' must erase the two files of the SIM card which contain the 'identification of the last network': the 'Location Information File' for GSM-UMTS in circuit mode and 'GPRS Location Information File' for GPRS (GSM and UMTS).

To completely avoid an initial network search, instead of erasing the softphone, write a Location Information of C with the MCC-MNC (any LAC will do).

If the softphone does it, the user registers immediately in C without a long network search when they insert the card back in the handset, and C will perform an excellent service for this traveller.

10.3.2 Erasing the SIM Card Localization Information (Last LAC)

This file concerns the GSM services (circuit mode) such as voice, and SMS (circuit mode). The script to erase the Localization Information is shown in Table 10.2.

One gets the information saying that the last network is MCC = 283, MNC = 5 (VivaCell Armenia). Even if the preferred PLMN was set to a competitor, when the handset is turned off/on it will remain on this network unless this file is erased with FFFF.

TMSI 5800B897
LAI MCC = 283 MNC = 5 LAC = 1011
TMSI time 0
Location Update status 0

Table 10.2 Script to erase the Localization Information of the SIM card

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0**C** A4 00 00 02 6F 30	SELECT 6F7E (Location Information File)
A0 B0 00 00 **0B**	READ BINARY, length = 11

Table 10.3 Script to erase the GPRS Localization Information of the SIM card

Command GSM 11.11	Description
A0 A4 00 00 02 3F 00	SELECT 3F00 (Master File)
A0 A4 00 00 02 7F 20	SELECT 7F20 (Directory GSM)
A0**C** A4 00 00 02 6F 53	SELECT 6F53 (GPRS Location Information File)
A0 B0 00 00 **0E**	READ BINARY, length = 14

10.3.3 Erasing the SIM Card GPRS Localization Information (Last RAC)

This is for the GPRS services (which include SMS sending and receiving in GPRS mode). The script to erase the GPRS Localization Information is shown in Table 10.3.

With this command one reads:

```
P-TMSI D51DDC10
P-TMSI signature value 096C32
RAI MCC = 283 MNC = 5 LAC = 1011
RAC = 111
Routing Area Update status 0
```

Note that in this example, the LAC is the same for GSM and GPRS and that the GPRS location has the RAC (Remote Area Code) in addition.

If OTA of Chapter 8 is used to attempt to erase these files, frequently they are not updatable and the decoding of the response gives this:

```
<ResponseStatusCode>(00): PoR OK</ResponseStatusCode>
<Crypto>No RC,CC or DS</Crypto>
<NumberOfCommandsExecuted>4</NumberOfCommandsExecuted>
<StatusConditionsReturnedBySIM>
<SW1>98</SW1>
<SW2>04</SW2>
</StatusConditionsReturnedBySIM>
<Info>access condition not fulfilled (with Gemalto: means file not made OTAble!)</Info>
<LastFile>Location information (6F7E)</LastFile>
<LastCommand>A0D6</LastCommand>
```

10.4 IMS, the all IP Network Architecture

IP Multimedia System (IMS) is a standardized architecture for Next Generation Networks (NGNs) with all IP equipment: SIGTRAN for signalling and SIP for VoIP replacing ISUP for telecom operators (fixed or mobile). It allows the provision of multimedia services. In the mobile case, the main higher-level protocols, MAP and CAP as well as TCAP, are based on the existing 3GPP standard.

The existing systems (packet and circuit switching) are supported as well as newer or existing services offered on the Internet. They can be used as well in roaming cases. A multimedia session can be between two IMS users, between an IMS and a fixed web access, or between two fixed web accesses. So IMS is intended to provide a convergence between the Internet users and the mobile users.

10.4.1 Origin of IMS

An industrial forum called 3G.IP proposed IMS in 1999 and the standardization task has been taken on by 3GPP within a group handling UMTS (3G) specifications. The first version was 5 (2G → 3G) with the addition of SIP for call control. Compatibility with previous GSM (2G) and GPRS (2.5G) was also included. The various phases are as follows:

- The Pre-IMS (or 'Early IMS') allows the implementation of IMS in networks which do not include 'full IMS'.
- To handle the CDMA 2000 case, another group, 3GPP2, has added compatibility with CDMA 2000 to IMS 3GPP.
- IMS version 6 adds interoperability with WLAN.
- IMS version 7 adds interworking with fixed networks.

Figure 10.4 illustrates the network architecture in versions 5, 6 and 7.

10.4.2 Principles Claimed for IMS

- **Access independent**: IMS works with any network: fixed, mobile or wireless, including packet-switching functions such as GPRS, UMTS, CDMA 2000, WLAN, WiMAX, DSL, cable, etc. Legacy systems such as GSM are supported through gateways.
- **Mobility of users and terminals**: the mobile network provides terminal mobility and IMS provides user mobility through SIP.
- **Extension of IP services**: IMS should offer VoIP, 'Push to talk' on Cellular networks, multiplayer games, videoconferences, instant messaging, community services and content sharing.

10.4.3 Fixed/Mobile Convergence

IMS was initially designed for mobile networks, but in version 7 fixed networks are also supported, with the acronym FMC (Fixed/Mobile convergence). The idea is that the user has a single telephone and number, and a single address book and answering machine, whether they are at home or away, with transparent routing of the calls between fixed and mobile.

10.4.4 IMS vs UMA (Unlicensed Mobile Access)

A simpler approach than changing the network is to adapt the IP terminal (fixed PC), or a mobile with GPRS or a data connection, to use existing protocols to communicate with the radio network (in the case of mobile users). This is what is used in commercial offerings such as combined GSM-Wi-Fi handsets allowing the use of the Wi-Fi connection with the home base station, while having the same GSM number to make or receive calls: the handset using Wi-Fi behaves as a GSM phone.

UMA uses the standard layers of the GSM standard between the handset and the network for call establishment, *not SIP*. UMA uses CM/MM (corresponding to TCAP in the fixed network) / RR (corresponding to BSSAP in the fixed network) LAPDm (corresponding to SCCP in the fixed network). Only the physical layer is replaced by IP once a connection is established. UMA allows the use of the main existing network equipment with a software evolution.

10.5 Making a 4G 'IP Call' to a Mobile

Using 4G will require establishing an IP connection 'Network Initiated'. This will allow the use of the large band network for Visio calls with much better quality that the circuit mode H324-M

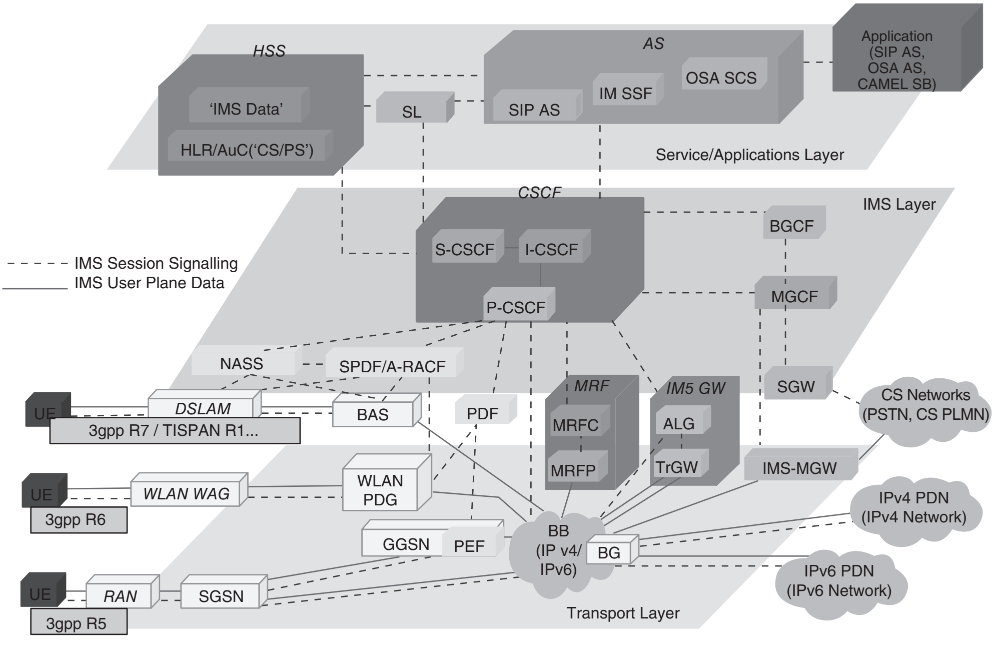


Figure 10.4 IMS versions 5, 6 and 7 architecture

of the present UMTS. In fact, the standards have long prepared for this and all the procedures exist for:

- interrogating the HLR to get the IP address of the visited Node;
- sending a request to 'Activate a PDP context' to this Node.

There are two ways to call a mobile using IP:

(1) The equivalent of a classical voice call. The mobile is not connected to the GGSN (the IP Gateway).
(2) The mobile is permanently connected through a GGSN to a 'presence server'. This is how emails are received immediately.

10.5.1 Paging through the GTP Protocol

This case is resource consuming and for IMS, GPRS or UMTS it is interesting to see the existing solutions available to make a 'call' to the mobile, using IP at the network initiation.

As shown in Figure 10.5:

- A MAP SEND ROUTING INFO FOR GPRS (2) is sent by the GGSN which has received a VoIP call request to the MS.
- The HLR returns (Ack of (2)) the SGSN IP address which it has from the UPDATE LOCATION GPRS.
- The GGSN sends a Notification Request (GTP protocol) (3) to the visited SGSN which confirms (Response of 3).

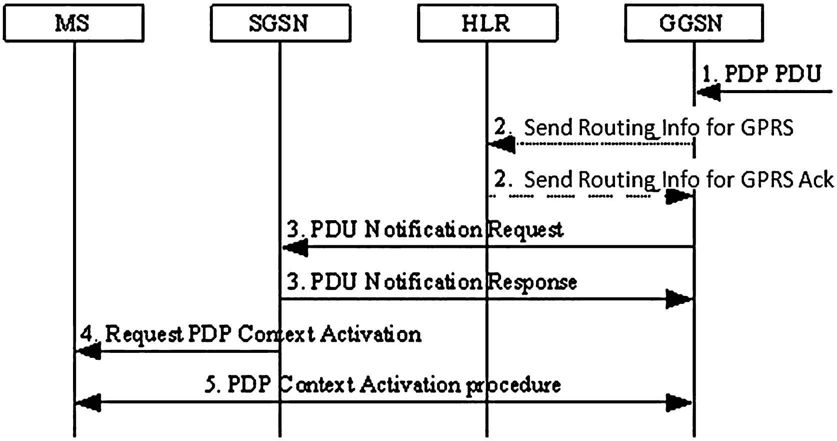

MS
SGSN
HLR
GGSN
1. PDP PDU
2. Send Routing Info for GPRS
2. Send Routing Info for GPRS Ack
3. PDU Notification Request
3. PDU Notification Response
4. Request PDP Context Activation
5. PDP Context Activation procedure

Figure 10.5 PDP Context establishment network initiated

- Then the SGSN sends a ‘Request PDP Activation’ (a paging GPRS) to the MS (4).
- And it is the MS which initiates the PDP Context activation procedure (5).

10.5.2 Paging for Data Service Connection through the MAP Protocol

This method is directly usable with GPRS or UMTS networks. It is similar to the procedure to ‘send MMS’.

An ‘MMS notification’ SMS is sent to the called party that contains a specific URL to connect to the presence server.

References and Further Reading

[10.1] Henry-Labordère, A., ‘Système de Terminaisons d’appels vers des numéros de mobiles par IP sans coopération du réseau de mobiles’, Patent FR 07 301 546 3, European patent application.

11

Worked-out Examples

11.1 Examples of Chapter 1

11.1.1 Example 1: SMSeXchange Behaviour

This is the case of a Virtual visitor (UK) visiting a VPLMN (Sierra Leone). An SMS-MT is sent to this visitor by a Sierra Leone subscriber of this VPLMN. The VPLMN has not set the Roaming Hub (located in Gambia) as its SMSeXchange (as it should): it does not have roaming with the UK network and uses a ‘third party’ SMSeXchange.

Figures 11.1 and 11.2 show a ticket with an SMS-MT received and relayed successfully by the Roaming Hub, which has as Calling Party GT the ‘third party’ SMSeXchange.

Question:

- Draw the path and explain the situation. Draw the path if the Roaming Hub was (correctly) used as the SMSeXchange of Sierra Leone. What is the improvement?

11.1.2 Example 2: Mobile Subscriber Purge

The purpose of the exercise is to get familiar with traces at MAP protocol level (specified in TS 29.002), and to review some of the procedures of Chapter 1.

Question: the two occurrences of SEND ROUTING INFO FOR SM for the same number 37493212345 do not give the same result (they are spaced by one week) and this user left their phone at home (with a charge).

What are the differences in the response?

What happened?

```
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
  PA_Len = 41
  MAP-OPEN-REQ(1)
   dest_address(Q713)(1)
    L = 013
```

Virtual Roaming Systems For GSM, GPRS and UMTS: Open Connectivity in Practice Arnaud Henry-Labordère

Field Name	Value	Note
Type ticket	SMS_DELIVER	
Msg type	FWD_SM_MT	
Error code		
Msg Ref	OGA_20090115_124611_242445	
Timestamp	20090115_124816_742928	*Jan 15 2009 at 12:48:16 (742928 μs)*
Calling Party (SCCP)	+2207750005	*E164 address*
Called Party (SCCP)	+23277100952	*E164 address*
orig Ref (TCAP)		
dest Ref (TCAP)		
MAP version	2	
Origin Address	+23277928009	
Destination Address		
HPLMN (CC) orig	3384141	*France*
HPLMN (MGT) orig	8	*Nilcom*
VPLMN (CC) orig	3384141	*France*
VPLMN (MGT) orig	8	*Nilcom*
HPLMN (CC) dest	44	*UK*
HPLMN (MGT) dest	7761	*Cable & Wireless Guernsey*
VPLMN (CC) dest	232	*Sierra Leone*
VPLMN (MGT) dest	77	*Africell (Sierra Leone)*
IMSI	234550440017074	
IMSI auxiliary		
MSC Number	+23277100952	
SGSN number		
Name		
Coding	0	
UDHI	0	
text length	1	
Message number	0	
Number of messages	0	
Destination port	0	

Figure 11.1 Ticket sample #1

```
Data:  Route on GT, Global Title included(0x13),
       Signalling Point Code (ITU) = 1-096-3 (2819)
       Subsystem Number = HLR(6),
       Global Title :
          Translation Type = 0,
```

Field Name	Value	Note
Type ticket	SMS_SUBMIT	
Msg type	FWD_SM_MT	
Error code		
Msg Ref	OGA_20090115_124611_242440	
Timestamp	20090115_124816_742973	*Jan 15 2009 at 12:48:16 (742928 μs)*
Calling Party (SCCP)	+3384141	*E164 address*
Called Party (SCCP)	+2207750005	*E164 address*
orig Ref (TCAP)		
dest Ref (TCAP)		
MAP version	2	
Origin Address	+23277928009	
Destination Address		
HPLMN (CC) orig	3384141	*France*
HPLMN (MGT) orig	8	*Nilcom*
VPLMN (CC) orig	3384141	*France*
VPLMN (MGT) orig	8	*Nilcom*
HPLMN (CC) dest	44	*UK*
HPLMN (MGT) dest	7761	*Cable & Wireless Guernsey*
VPLMN (CC) dest	232	*Sierra Leone*
VPLMN (MGT) dest	77	*Africell (Sierra Leone)*
IMSI	234550440017074	
IMSI auxiliary		
MSC Number	+23277100952	
SGSN number		
Name		
Coding	0	
UDHI	0	

Figure 11.2 Ticket sample #2

```
                Numbering Plan = ISDN/Telephony(E164),
                Encoding Scheme = BCD, odd number of digits,
                Nature Address Indicator = International number,
                Address information = 37493212345
        orig_address(Q713)(3)
          L = 011
          Data:  Route on GT, Global Title included(0x12),
                No SPC in address
                Subsystem Number = MSC(8),
                Global Title :
                  Translation Type = 0,
                  Numbering Plan = ISDN/Telephony(E164),
                  Encoding Scheme = BCD, odd number of digits,
                  Nature Address Indicator = International number,
                  Address information = 23675500010
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001001403
                MAP_ShortMsgGatewayPackage_v1_or_v2 MAP V3
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 32
      MAP-SEND-ROUTING-INFO-FOR-SM-REQ(1)
        MAPPN_timeout(45)
          L = 002
          Data: timeout value = 10 sec
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_msisdn(15)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 37493212345
        MAPPN_sm_rp_pri(16)
          L = 001
          Data: (1):High Priority
        MAPPN_sc_addr(17)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 23675500010
        MAPPN_GPRS_Support_Indicator(118)
          L = 000
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
----------------- HDR ---------------- [ Thu Jan 29 18:10:22 2009
(281291 us) ]
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 16
      MAP-OPEN-CNF(130)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        MAPorCAP_Application_Context(11)
```

```
         L = 009
         Data: (Hex) 060704000001001403
              MAP_ShortMsgGatewayPackage_v1_or_v2 MAP V3
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 33
      MAP-SEND-ROUTING-INFO-FOR-SM-CNF(130)
        MAPPN_invoke_id(14)
         L = 001
         Data: 1
        MAPPN_imsi(18)
         L = 008
         Data: Address = 283058000469205
        MAPPN_msc_num(19)
         L = 007
         Data: Ext = No extension
               Ton = International
               Npi = ISDN
               Address = 37493297106
        MAPPN_sgsn_number(82)
         L = 007
         Data: Ext = No extension
               Ton = International
               Npi = ISDN
               Address = 37493297400
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
      MAP-CLOSE-IND(4)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
# ROUTER # <= MTU_SEND_ROUTING_INFO_FOR_SM_CNF :
              16 154 0 0 0 0 +0 +283058000469205 +37493297106
+37493297400 0 -1
# ROUTER # => MTU_MS_PURGE_REQ
              247 156 +33899990007 +0 E374938000469205 +0 0 3 0
2819 +283058000469205 22 3 +37493297106 +0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 43
      MAP-OPEN-REQ(1)
        dest_address(Q713)(1)
         L = 015
         Data:  Route on GT, Global Title included(0x13),
                Signalling Point Code (ITU) = 1-096-3 ( 2819)
                Subsystem Number = HLR(6),
                Global Title :
                  Translation Type = 0,
                  Numbering Plan = ISDN/Mobile(E214),
                  Encoding Scheme = BCD, odd number of digits,
                  Nature Address Indicator = International number,
                  Address information = 374938000469205
        orig_address(Q713)(3)
         L = 011
```

```
       Data:  Route on GT, Global Title included(0x12),
              No SPC in address
              Subsystem Number = VLR(7),
              Global Title :
                Translation Type = 0,
                Numbering Plan = ISDN/Telephony(E164),
                Encoding Scheme = BCD, odd number of digits,
                Nature Address Indicator = International number,
                Address information = 23675500010
     MAPorCAP_Application_Context(11)
       L = 009
       Data: (Hex) 060704000001001B03
              MAP_MS Purging Package_v3 MAP V3
- - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   PA_Len = 28
   MAP-PURGE-MS-REQ(57)
     MAPPN_timeout(45)
       L = 002
       Data: timeout value = 22 sec
     MAPPN_invoke_id(14)
       L = 001
       Data: 1
     MAPPN_imsi(18)
       L = 008
       Data: Address = 283058000469205
     MAPPN_vlr_number(55)
       L = 007
       Data: Ext = No extension
             Ton = International
             Npi = ISDN
             Address = 37493297106
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   PA_Len = 2
   MAP-DELIMITER-REQ(5)
- - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   PA_Len = 16
   MAP-OPEN-CNF(130)
     MAPPN_result(5)
       L = 001
       Data: (0):Accept
     MAPorCAP_Application_Context(11)
       L = 009
       Data: (Hex) 060704000001001B03
              MAP_MS Purging Package_v3 MAP V3
- - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
- - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
   MAP-PURGE-MS-CNF(180)
     MAPPN_invoke_id(14)
```

```
          L = 001
          Data: 1
        MAPPN_freeze_tmsi(156)
          L = 000
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
# ROUTER # <=  MTU_MS_PURGE_CNF :
               249 156 0 0 0 0 +0 1 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      MAP-CLOSE-IND(4)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
# ROUTER # =>  MTU_SEND_ROUTING_INFO_FOR_SM_REQ
            12 157 +33899990007 +0 +37493210002 +0
f47414063e18947e93a0 0 0 2819 +37493210002 +33899990007 10 3 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      MAP-OPEN-REQ(1)
        dest_address(Q713)(1)
          L = 013
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3 ( 2819)
                 Subsystem Number = HLR(6),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Encoding Scheme = BCD, odd number of digits,
                   Nature Address Indicator = International number,
                   Address information = 37493212345
        orig_address(Q713)(3)
          L = 011
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = MSC(8),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Encoding Scheme = BCD, odd number of digits,
                   Nature Address Indicator = International number,
                   Address information = 23675500010
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001001403
                 MAP_ShortMsgGatewayPackage_v1_or_v2 MAP V3
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 32
      MAP-SEND-ROUTING-INFO-FOR-SM-REQ(1)
        MAPPN_timeout(45)
          L = 002
          Data: timeout value = 10 sec
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_msisdn(15)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 37493212345
        MAPPN_sm_rp_pri(16)
          L = 001
          Data: (1):High Priority
        MAPPN_sc_addr(17)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 23675500010
        MAPPN_GPRS_Support_Indicator(118)
          L = 000
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      MAP-OPEN-CNF(130)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 0607040000010014003
                MAP_ShortMsgGatewayPackage_v1_or_v2 MAP V3
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Jan 29 18:12:01 2009
(502169 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 157
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 26
      MAP-SEND-ROUTING-INFO-FOR-SM-CNF(130)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_imsi(18)
          L = 008
          Data: Address = 283058000469205
        GPRS_Node_Indicator(123)
```

```
          L = 000
        MAPPN_sgsn_number(82)  /* The MSC GT is erased */
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 37493297400
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      MAP-CLOSE-IND(4)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
# ROUTER # <=  MTU_SEND_ROUTING_INFO_FOR_SM_CNF :
            16 157 0 0 0 0 +0 +283058000469205 +0 +37493297400 0 -1
```

11.1.3 Example 3: Change of Password

This concerns a Supplementary Service procedure.

Questions:

(1) Which field is included in the identification of the requesting subscriber?
(2) Is it mono or bi-IMSI virtual roaming?
(3) How many password attempts were made by the subscriber?
(4) What is the correct password?

```
----------------- HDR ---------------- [ Tue Feb  3 18:53:38 2009
(016766 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 68
      MAP-OPEN-IND(2)
        dest_address(Q713)(1)
          L = 018
          Data:  Route on SSN, Global Title included(0x53),
                 Signalling Point Code (ITU) = 4-019-5 ( 8349)
                 Subsystem Number = HLR(6),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Encoding Scheme = BCD, odd number of digits,
                   Nature Address Indicator = International number,
                   Address information = 3389999000722077500005
        dest_ref(GT E164 final or IMSI)(2)
          L = 009
          Data: Ext = No extension
```

```
                Ton = International
                Npi = land mobile E212
                Address = 607020100330008
        orig_address(Q713)(3)
          L = 013
          Data:  Route on GT, Global Title included(0x13),
                Signalling Point Code (ITU) = 1-096-3 ( 2819)
                Subsystem Number = VLR(7),
                Global Title :
                  Translation Type = 0,
                  Numbering Plan = ISDN/Telephony(E164),
                  Encoding Scheme = BCD, odd number of digits,
                  Nature Address Indicator = International number,
                  Address information = 33660001009
        orig_ref(4)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 33660001009
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001001202
                MAP_NetworkFunctionalSsPackage_v1 or v2 MAP V2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:38 2009
(016916 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 8
      MAP-REGISTER-PASSWORD-IND(92)
        MAPPN_invoke_id(14)
          L = 001
          Data: 25
        MAPPN_ss_code(218)
          L = 001
          Data: (144):all barring SS
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:38 2009
(017002 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_REGISTER_PASSWORD_IND:
              159 32833 +33660001009 +607020100330008
+33899900072207750005 +33660001009 0 2 2819 8349 +0 144 0
----------------- HDR ---------------- [ Tue Feb  3 18:53:38 2009
(017038 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
----------------- HDR ---------------- [ Tue Feb  3 18:53:38 2009
(025135 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU-REGISTER-PASSWORD-REQ
              158 19 +2207750005 I619050100330008 E232770100330008
+2207750005 f474142a488894961500 2 0 2819 +2207750005 28 2 144 0
------------------ HDR --------------- [ Tue Feb  3 18:53:38 2009
(025196 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 61
      MAP-OPEN-REQ(1)
        dest_address(Q713)(1)
          L = 015
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3 ( 2819)
                 Subsystem Number = HLR(6),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Mobile(E214),
                   Encoding Scheme = BCD, odd number of digits,
                   Nature Address Indicator = International number,
                   Address information = 232770100330008
        dest_ref(GT E164 final or IMSI)(2)
```

```
          L = 009
          Data: Ext = No extension
                Ton = International
                Npi = land mobile E212
                Address = 619050100330008
        orig_address(Q713)(3)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = VLR(7),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Encoding Scheme = BCD, even number of digits,
                   Nature Address Indicator = International number,
                   Address information = 2207750005
        orig_ref(4)
          L = 006
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 2207750005
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001001202
                 MAP_NetworkFunctionalSsPackage_v1 or v2 MAP V2
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:38 2009
(025342 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 20
      MAP-REGISTER-PASSWORD-REQ(91)
        MAPPN_timeout(45)
          L = 002
          Data: timeout value =  28 sec
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_ss_code(218)
          L = 001
          Data: (144):all barring SS
        MAPPN_ellipsis(57)
          L = 006
          Data: Address = 192207750005
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:38 2009
(025442 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:39 2009
(616789 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 16
      MAP-OPEN-CNF(130)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001001202
                MAP_NetworkFunctionalSsPackage_v1 or v2 MAP V2
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------- HDR --------------- [ Tue Feb  3 18:53:39 2009
(616890 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-IND(90)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_linked_id(44)
          L = 001
          Data: (Hex) 01
        MAPPN_guidance_info(282)
```

```
          L = 001
          Data: (0):Enter PassWord
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:39 2009
(616979 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_GET_PASSWORD_IND:
               155 19 +0 1 0 1
------------------ HDR ---------------- [ Tue Feb  3 18:53:39 2009
(617015 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
# ROUTER # <=  MTU_GET_PASSWORD_IND:
               155 19 +0 1 0 1
----------------- HDR ----------------- [ Tue Feb  3 18:53:39 2009
(620920 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU-GET-PASSWORD-REQ
               154 32833 +2207750005 1 0 0
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------- HDR --------------- [ Tue Feb  3 18:53:39 2009
(621066 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 32833
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 11
      MAP-GET-PASSWORD-REQ(89)
        MAPPN_invoke_id(14)
```

```
          L = 001
          Data: 1
        MAPPN_guidance_info(282)
          L = 001
          Data: (0):Enter PassWord
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:39 2009
(621147 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 32833
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
----------------- HDR ----------------- [ Tue Feb  3 18:53:41 2009
(116810 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-CNF(212)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_current_password(283)
          L = 004
          Data: (Hex) 31323334
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:41 2009
(116904 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_GET_PASSWORD_CNF :
               156 32833 0 0 0 0 +0 1 31323334
------------------ HDR ---------------- [ Tue Feb  3 18:53:41 2009
(116945 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:41 2009
(124943 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU-GET-PASSWORD-RSP
               157 19 0 0 0 0 +0 1 31323334
------------------ HDR ---------------- [ Tue Feb  3 18:53:41 2009
(124995 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-RSP(211)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_current_password(283)
          L = 004
          Data: (Hex) 31323334
   - - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:41 2009
(125066 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Feb  3 18:53:42 2009
(616823 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-IND(90)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
        MAPPN_linked_id(44)
          L = 001
          Data: (Hex) 01
        MAPPN_guidance_info(282)
          L = 001
          Data: (1):Enter New PassWord
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
---------------- HDR ------------------ [ Tue Feb  3 18:53:42 2009
(616933 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_GET_PASSWORD_IND:
              155 19 +0 2 1 1
------------------ HDR ---------------- [ Tue Feb  3 18:53:42 2009
(616975 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
# ROUTER # <=  MTU_GET_PASSWORD_IND:
              155 19 +0 2 1 1
------------------ HDR ---------------- [ Tue Feb  3 18:53:42 2009
(620825 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU-GET-PASSWORD-REQ
               154 32833 +2207750005 2 1 0
------------------ HDR ---------------- [ Tue Feb  3 18:53:42 2009
(620873 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 32833
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 11
      MAP-GET-PASSWORD-REQ(89)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
        MAPPN_guidance_info(282)
          L = 001
          Data: (1):Enter New PassWord
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:42 2009
(620941 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 32833
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:44 2009
(116839 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-CNF(212)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
        MAPPN_current_password(283)
```

```
          L = 004
          Data: (Hex) 30303030
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:44 2009
(116932 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_GET_PASSWORD_CNF :
               156 32833 0 0 0 0 +0 2 30303030
------------------ HDR ---------------- [ Tue Feb  3 18:53:44 2009
(117004 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:44 2009
(124833 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU-GET-PASSWORD-RSP
               157 19 0 0 0 0 +0 2 30303030
------------------ HDR ---------------- [ Tue Feb  3 18:53:44 2009
(124875 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-RSP(211)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
        MAPPN_current_password(283)
```

```
          L = 004
          Data: (Hex) 30303030
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:44 2009
(124944 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAPE-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:45 2009
(616865 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-IND(90)
        MAPPN_invoke_id(14)
          L = 001
          Data: 3
        MAPPN_linked_id(44)
          L = 001
          Data: (Hex) 01
        MAPPN_guidance_info(282)
          L = 001
          Data: (2):Enter New PassWord Again
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:45 2009
(616972 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_GET_PASSWORD_IND:
               155 19 +0 3 2 1
------------------ HDR ---------------- [ Tue Feb  3 18:53:45 2009
(617012 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
# ROUTER # <=  MTU_GET_PASSWORD_IND:
              155 19 +0 3 2 1
------------------ HDR ---------------- [ Tue Feb  3 18:53:45 2009
(624864 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU-GET-PASSWORD-REQ
              154 32833 +2207750005 3 2 0
------------------ HDR ---------------- [ Tue Feb  3 18:53:45 2009
(624925 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 32833
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 11
      MAP-GET-PASSWORD-REQ(89)
        MAPPN_invoke_id(14)
          L = 001
          Data: 3
        MAPPN_guidance_info(282)
          L = 001
          Data: (2):Enter New PassWord Again
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:45 2009
(624994 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 32833
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Feb  3 18:53:47 2009
(252926 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-CNF(212)
        MAPPN_invoke_id(14)
          L = 001
          Data: 3
        MAPPN_current_password(283)
          L = 004
          Data: (Hex) 30303030
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:47 2009
(253021 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_GET_PASSWORD_CNF :
               156 32833 0 0 0 0 +0 3 30303030
------------------ HDR ---------------- [ Tue Feb  3 18:53:47 2009
(253059 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 32833
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:47 2009
(261028 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU-GET-PASSWORD-RSP
               157 19 0 0 0 0 +0 3 30303030
```

```
------------------ HDR ---------------- [ Tue Feb  3 18:53:47 2009
(261075 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 14
      MAP-GET-PASSWORD-RSP(211)
        MAPPN_invoke_id(14)
          L = 001
          Data: 3
        MAPPN_current_password(283)
          L = 004
          Data: (Hex) 30303030
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:47 2009
(261147 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 19
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:48 2009
(816915 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 14
      MAP-REGISTER-PASSWORD-CNF(214)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_new_password(284)
          L = 004
          Data: (Hex) 30303030
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Feb  3 18:53:48 2009
(817013 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_REGISTER_PASSWORD_CNF :
               160 19 0 0 0 0 +0 1 30303030
------------------ HDR ---------------- [ Tue Feb  3 18:53:48 2009
(817050 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 19
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-CLOSE-IND(4)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Feb  3 18:53:48 2009
(825044 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU-REGISTER-PASSWORD-RSP
               161 32833 0 0 0 0 +2207750005 0 30303030
------------------ HDR ---------------- [ Tue Feb  3 18:53:48 2009
(825088 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 32833
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-REGISTER-PASSWORD-RSP(213)
        MAPPN_invoke_id(14)
          L = 001
          Data: 25
        MAPPN_new_password(284)
          L = 004
          Data: (Hex) 30303030
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Feb  3 18:53:48 2009
(825157 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 32833
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      MAP-CLOSE-REQ(3)
        MAPPN_release_method(7)
          L = 001
          Data: (0):Normal Release
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - -
```

11.2 Examples of Chapter 3: Roaming Hub with Several Point Codes

Answer the following questions after analysing the trace of the ‘intermediate layer’:

(1) What PC exists within this Roaming Hub, and what is the unique SCCP stack PC?
(2) What is the type of the Point Codes?

```
MUX_mtp3_m3ua_transfer_ind: type=0x8f01 src=0xef dst=0x31
status=0x00 len=0x0018, 83 5f 1f d0 37 09 00 03 05 09 02 42 01 04
43 40 1f 01 05 03 06 5f 1f 01
MTP3orM3UA Layer: SI=3(SCCP) SSF=8(NI=2(NAT),priority=0) DPC=8031
OPC=8000 SLS=3
|00001001 |SCCP Message Type                   |9
|----0001 |Protocol Class                      |Class 0
|1000---- |Message Handling                    |Return message on
                                                error (48)
|00000011 |Pointer to parameter Called Party   |3
|00000011 |Pointer to parameter Calling Party  |5
|00000011 |Pointer to parameter Data           |9
|Called address parameter | 0242
|00001011 |Parameter Length                    |2
|-------0 |Point Code Indicator                |PC absent
|------1- |Subsystem No. Indicator             |SSN present
|--0000-- |Global Title Indicator              |GT not included
|-1------ |Routing Indicator                   |Route on PC + SSN
|0------- |For national use                    |0
|xxxxxxxx |Subsystem number                    |1
|Calling address parameter | 0443401f
|10011111 |Parameter length                    |4
|-------1 |Point Code Indicator                |PC included
|------1- |Subsystem No. Indicator             |SSN present
|--0000-- |Global Title Indicator              |GT not included
|-1------ |Routing Indicator                   |Route on PC + SSN
```

```
|0-------  |For national use                    |0
|xxxxxxxx  |Calling Party SPC                   |8000
|xxxxxxxx  |Subsystem number                    |1
|Data parameter
|10011111  |Parameter length                    |5
|00000011  |Tag                                 | SST
|10011111  |Affected SSN                        |6
|xxxxxxxx  |Affected SPC                        |8031
/* Transfer to PC unique 8349 */
INFO ++ MTP-DECODE-IND: Message Type 9  PTR(s)[3 5 9 0]
MUX_mtp3_m3ua_transfer_ind: type=0x8f01 src=0xef dst=0x31
status=0x00 len=0x0018, 83 9d 20 d0 37 09 00 03 05 09 02 42 01 04
43 40 1f 01 05 03 06 9d 20 01
MTP3orM3UA Layer: SI=3(SCCP) SSF=8(NI=2(NAT),priority=0) DPC=8349
OPC=8000 SLS=3
|00001001  |SCCP Message Type                   |9
|----0001  |Protocol Class                      |Class 0
|1000----  |Message Handling                    |Return message on
                                                 error (48)
|00000011  |Pointer to parameter Called Party   |3
|00000011  |Pointer to parameter Calling Party  |5
|00000011  |Pointer to parameter Data           |9
|Called address parameter | 0242
|00001011  |Parameter Length                    |2
|-------0  |Point Code Indicator                |PC absent
|------1-  |Subsystem No. Indicator             |SSN present
|--0000--  |Global Title Indicator              |GT not included
|-1------  |Routing Indicator                   |Route on PC + SSN
|0-------  |For national use                    |0
|xxxxxxxx  |Subsystem number                    |1
|Calling address parameter | 0443401f
|10011111  |Parameter length                    |4
|-------1  |Point Code Indicator                |PC included
|------1-  |Subsystem No. Indicator             |SSN present
|--0000--  |Global Title Indicator              |GT not included
|-1------  |Routing Indicator                   |Route on PC + SSN
|0-------  |For national use                    |0
|xxxxxxxx  |Calling Party SPC                   |8000
|xxxxxxxx  |Subsystem number                    |1
|Data parameter
|10011111  |Parameter length                    |5
|00000011  |Tag                                 | SST
|10011111  |Affected SSN                        |6
|xxxxxxxx  |Affected SPC                        |8349
/* other SST to PC 8032 */
MUX_mtp3_m3ua_transfer_ind: type=0x8f01 src=0xef dst=0x31
status=0x00 len=0x0018, 83 5f 1f d0 37 09 00 03 05 09 02 42 01 04
43 40 1f 01 05 03 06 60 1f 01
MTP3orM3UA Layer: SI=3(SCCP) SSF=8(NI=2(NAT),priority=0) DPC=8032
OPC=8000 SLS=3
```

```
|00001001 |SCCP Message Type                    |9
|----0001 |Protocol Class                       |Class 0
|1000---- |Message Handling                     |Return message on
                                                 error (48)
|00000011 |Pointer to parameter Called Party   |3
|00000011 |Pointer to parameter Calling Party  |5
|00000011 |Pointer to parameter Data           |9
|Called address parameter | 0242
|00001011 |Parameter Length                     |2
|-------0 |Point Code Indicator                 |PC absent
|------1- |Subsystem No. Indicator              |SSN present
|--0000-- |Global Title Indicator               |GT not included
|-1------ |Routing Indicator                    |Route on PC + SSN
|0------- |For national use                     |0
|xxxxxxxx |Subsystem number                     |1
|Calling address parameter | 0443401f
|10011111 |Parameter length                     |4
|-------1 |Point Code Indicator                 |PC included
|------1- |Subsystem No. Indicator              |SSN present
|--0000-- |Global Title Indicator               |GT not included
|-1------ |Routing Indicator                    |Route on PC + SSN
|0------- |For national use                     |0
|xxxxxxxx |Calling Party SPC                    |8000
|xxxxxxxx |Subsystem number                     |1
|Data parameter
|10011111 |Parameter length                     |5
|00000011 |Tag                                  | SST
|10011111 |Affected SSN                         |6
|xxxxxxxx |Affected SPC                         |8032
/* translated to PC 8349 unique */
INFO ++ MTP-DECODE-IND: Message Type 9  PTR(s)[3 5 9 0]
MUX_mtp3_m3ua_transfer_ind: type=0x8f01 src=0xef dst=0x31
status=0x00 len=0x0018, 83 9d 20 d0 37 09 00 03 05 09 02 42 01 04
43 40 1f 01 05 03 06 9d 20 01
MTP3orM3UA Layer: SI=3(SCCP) SSF=8(NI=2(NAT),priority=0) DPC=8349
OPC=8000 SLS=3
|00001001 |SCCP Message Type                    |9
|----0001 |Protocol Class                       |Class 0
|1000---- |Message Handling                     |Return message on
                                                 error (48)
|00000011 |Pointer to parameter Called Party   |3
|00000011 |Pointer to parameter Calling Party  |5
|00000011 |Pointer to parameter Data           |9
|Called address parameter | 0242
|00001011 |Parameter Length                     |2
|-------0 |Point Code Indicator                 |PC absent
|------1- |Subsystem No. Indicator              |SSN present
|--0000-- |Global Title Indicator               |GT not included
|-1------ |Routing Indicator                    |Route on PC + SSN
|0------- |For national use                     |0
```

```
|xxxxxxxx |Subsystem number                    |1
|Calling address parameter | 0443401f
|10011111 |Parameter length                    |4
|-------1 |Point Code Indicator                |PC included
|------1- |Subsystem No. Indicator             |SSN present
|--0000-- |Global Title Indicator              |GT not included
|-1------ |Routing Indicator                   |Route on PC + SSN
|0------- |For national use                    |0
|xxxxxxxx |Calling Party SPC                   |8000
|xxxxxxxx |Subsystem number                    |1
|Data parameter
|10011111 |Parameter length                    |5
|00000011 |Tag                                 | SST
|10011111 |Affected SSN                        |6
|xxxxxxxx |Affected SPC                        |8349
/* SSA is answered to PC 8000 */
MUX_mtp3_m3ua_transfer_ind: type=0xcf00 src=0xef dst=0x31
status=0x00 len=0x0018, 83 40 1f 9d 30 09 00 03 05 09 02 42 01 04
43 40 1f 01 05 01 06 9d 20 01
MTP3orM3UA Layer: SI=3(SCCP) SSF=8(NI=2(NAT),priority=0) DPC=8000
OPC=8349 SLS=3
|00001001 |SCCP Message Type                   |9
|----0001 |Protocol Class                      |Class 0
|1000---- |Message Handling                    |Return message on
                                                error (48)
|00000011 |Pointer to parameter Called Party   |3
|00000011 |Pointer to parameter Calling Party  |5
|00000011 |Pointer to parameter Data           |9
|Called address parameter | 0242
|00001011 |Parameter Length                    |2
|-------0 |Point Code Indicator                |PC absent
|------1- |Subsystem No. Indicator             |SSN present
|--0000-- |Global Title Indicator              |GT not included
|-1------ |Routing Indicator                   |Route on PC + SSN
|0------- |For national use                    |0
|xxxxxxxx |Subsystem number                    |1
|Calling address parameter | 0443401f
|10011111 |Parameter length                    |4
|-------1 |Point Code Indicator                |PC included
|------1- |Subsystem No. Indicator             |SSN present
|--0000-- |Global Title Indicator              |GT not included
|-1------ |Routing Indicator                   |Route on PC + SSN
|0------- |For national use                    |0
|xxxxxxxx |Calling Party SPC                   |8000
|xxxxxxxx |Subsystem number                    |1
|Data parameter
|10011111 |Parameter length                    |5
|00000001 |Tag                                 | SSA
|10011111 |Affected SSN                        |6
|xxxxxxxx |Affected SPC                        |8349
```

```
/* translated as if it was answer from 8031 */
INFO ++ MTP-DECODE-IND: Message Type 9  PTR(s)[3 5]
affected PC 8349 new PC 8031
SUPPRESSION  PC present in CgPa
MUX_mtp3_m3ua_transfer_ind: type=0xcf00 src=0xef dst=0x31
status=0x00 len=0x0016, 83 40 df d7 37 09 00 03 05 07 02 42 01 02
42 01 05 01 06 5f 1f 01
MTP3orM3UA Layer: SI=3(SCCP) SSF=8(NI=2(NAT),priority=0) DPC=8000
OPC=8031 SLS=3
|00001001 |SCCP Message Type                  |9
|----0001 |Protocol Class                     |Class 0
|1000---- |Message Handling                   |Return message on
                                               error (48)
|00000011 |Pointer to parameter Called Party  |3
|00000011 |Pointer to parameter Calling Party |5
|00000011 |Pointer to parameter Data          |7
|Called address parameter | 0242
|00001011 |Parameter Length                   |2
|-------0 |Point Code Indicator               |PC absent
|------1- |Subsystem No. Indicator            |SSN present
|--0000-- |Global Title Indicator             |GT not included
|-1------ |Routing Indicator                  |Route on PC + SSN
|0------- |For national use                   |0
|xxxxxxxx |Subsystem number                   |1
|Calling address parameter | 0242
|10011111 |Parameter length                   |2
|-------0 |Point Code Indicator               |PC absent
|------1- |Subsystem No. Indicator            |SSN present
|--0000-- |Global Title Indicator             |GT not included
|-1------ |Routing Indicator                  |Route on PC + SSN
|0------- |For national use                   |0
|xxxxxxxx |Subsystem number                   |1
|Data parameter
|10011111 |Parameter length                   |5
|00000001 |Tag                                | SSA
|10011111 |Affected SSN                       |6
|xxxxxxxx |Affected SPC                       |8031
/* 2nd SSA answered */
MUX_mtp3_m3ua_transfer_ind: type=0xcf00 src=0xef dst=0x31
status=0x00 len=0x0018, 83 40 1f 9d 30 09 00 03 05 09 02 42 01 04
43 40 1f 01 05 01 06 9d 20 01
MTP3orM3UA Layer: SI=3(SCCP) SSF=8(NI=2(NAT),priority=0) DPC=8000
OPC=8349 SLS=3
|00001001 |SCCP Message Type                  |9
|----0001 |Protocol Class                     |Class 0
|1000---- |Message Handling                   |Return message on
                                               error (48)
|00000011 |Pointer to parameter Called Party  |3
|00000011 |Pointer to parameter Calling Party |5
|00000011 |Pointer to parameter Data          |9
```

```
|Called address parameter | 0242
|00001011 |Parameter Length                   |2
|-------0 |Point Code Indicator               |PC absent
|------1- |Subsystem No. Indicator            |SSN present
|--0000-- |Global Title Indicator             |GT not included
|-1------ |Routing Indicator                  |Route on PC + SSN
|0------- |For national use                   |0
|xxxxxxxx |Subsystem number                   |1
|Calling address parameter | 0443401f
|10011111 |Parameter length                   |4
|-------1 |Point Code Indicator               |PC included
|------1- |Subsystem No. Indicator            |SSN present
|--0000-- |Global Title Indicator             |GT not included
|-1------ |Routing Indicator                  |Route on PC + SSN
|0------- |For national use                   |0
|xxxxxxxx |Calling Party SPC                  |8000
|xxxxxxxx |Subsystem number                   |1
|Data parameter
|10011111 |Parameter length                   |5
|00000001 |Tag                                | SSA
|10011111 |Affected SSN                       |6
|xxxxxxxx |Affected SPC                       |8349
/* translated as if coming from 8032 */
INFO ++ MTP-DECODE-IND: Message Type 9  PTR(s)[3 5]
affected PC 8349 new PC 8032
SUPPRESSION  PC present in CgPa
MUX_mtp3_m3ua_transfer_ind: type=0xcf00 src=0xef dst=0x31
status=0x00 len=0x0016, 83 40 1f d8 37 09 00 03 05 07 02 42 01 02
42 01 05 01 06 60 1f 01
MTP3orM3UA Layer: SI=3(SCCP) SSF=8(NI=2(NAT),priority=0) DPC=8000
OPC=8032 SLS=3
|00001001 |SCCP Message Type                  |9
|----0001 |Protocol Class                     |Class 0
|1000---- |Message Handling                   |Return message on
                                               error (48)
|00000011 |Pointer to parameter Called Party  |3
|00000011 |Pointer to parameter Calling Party |5
|00000011 |Pointer to parameter Data          |7
|Called address parameter | 0242
|00001011 |Parameter Length                   |2
|-------0 |Point Code Indicator               |PC absent
|------1- |Subsystem No. Indicator            |SSN present
|--0000-- |Global Title Indicator             |GT not included
|-1------ |Routing Indicator                  |Route on PC + SSN
|0------- |For national use                   |0
|xxxxxxxx |Subsystem number                   |1
|Calling address parameter | 0242
|10011111 |Parameter length                   |2
|-------0 |Point Code Indicator               |PC absent
|------1- |Subsystem No. Indicator            |SSN present
```

```
|--0000-- |Global Title Indicator                |GT not included
|-1------ |Routing Indicator                     |Route on PC + SSN
|0------- |For national use                      |0
|xxxxxxxx |Subsystem number                      |1
|Data parameter
|10011111 |Parameter length                      |5
|00000001 |Tag                                   | SSA
|10011111 |Affected SSN                          |6
|xxxxxxxx |Affected SPC                          |8032
```

11.3 Examples of Chapter 4

11.3.1 Example 1: Update Location – Post-paid Subscriber

Answer the following questions:

(1) Is it a Virtual visitor case or a multi-IMSI outbound subscriber?
(2) What shows it is a post-paid subscriber?
(3) What is the sequence of invoke-id in the INSERT SUBSCRIBER DATA in the incoming side and in the outgoing side?
(4) Why must the invoke-ids be different, and what would happen if they were the same?
(5) Is it possible for a HLR to send all the INSERT SUBSCRIBER DATA in parallel?

```
-------------------- HDR -------------- [ Tue Oct 28 15:23:21 2008
(342878 us) ]
    MAPE-R Instance = 0
    SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
    SS7E-R Dialog_ID = 33125
    SS7E-R Src  = 15
    SS7E-R Dst  = 1D
    SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
    - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
        PA_Len = 43
        MAP-OPEN-IND(2)
          dest_address(Q713)(1)
            L = 013
            Data:  Route on SSN, Global Title included(0x53),
                   Signalling Point Code (ITU) = 4-019-5 ( 8349)
                   Subsystem Number = HLR(6),
                   Global Title :
                     Translation Type = 0,
                     Numbering Plan = ISDN/Telephony(E164),
                     Nature Address Indicator = International number,
                     Address information = 33151001220775005
          orig_address(Q713)(3)
            L = 013
            Data:  Route on GT, Global Title included(0x13),
                   Signalling Point Code (ITU) = 1-096-3 ( 2819)
                   Subsystem Number = VLR(7),
                Global Title :
                  Translation Type = 0,
                  Numbering Plan = ISDN/Telephony(E164),
                  Nature Address Indicator = International number,
                  Address information = 33660001009
        MAPorCAPMAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001000103
                MAP_LocationUpdatingPackage MAP V3
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(343033 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 33
      MAP-UPDATE-LOCATION-IND(40)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_imsi(18)
          L = 008
          Data: Address = 607029900068192
        MAPPN_msc_num(19)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 33660001009
        MAPPN_vlr_number(55)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 33660001009
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(343141 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *
Nxt = 0
```

```
# ROUTER # <= MTU_UPDATE_LOCATION_IND:
            83 33125 +33660001009 +0 +33899990007 +0 0 3
+607029900068192 +33660001009 +33660001009 +0 00
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(343180 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *
Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAPE-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(350873 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # => MTU_UPDATE_LOCATION_REQ
               82 6 +2207750005 +0 E232770100330008 +0
f4741495027094c0c450 3 2819 +619050100330008 28 3 +2207750005
+2207750005 +0 00
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(350936 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 42
      MAP-OPEN-REQ(1)
        dest_address(Q713)(1)
          L = 015
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3 ( 2819)
                 Subsystem Number = HLR(6),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Mobile(E214),
                   Nature Address Indicator = International number,
                   Address information = 232770100330008
      orig_address(Q713)(3)
        L = 010
        Data: Route on GT, Global Title included(0x12),
              No SPC in address
              Subsystem Number = VLR(7),
              Global Title :
                Translation Type = 0,
                Numbering Plan = ISDN/Telephony(E164),
                Nature Address Indicator = International number,
                Address information = 2207750005
      MAPorCAP_Application_Context(11)
        L = 009
        Data: (Hex) 060704000001000103
              MAP_LocationUpdatingPackage MAP V3
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
        (Hex) 272D021C000E0101120816090501300300F81306912270570050
370691227057005000
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(351073 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
     PA_Len = 35
     MAP-UPDATE-LOCATION-REQ(39)
      MAPPN_timeout(45)
        L = 002
        Data: timeout value =  28 sec
      MAPPN_invoke_id(14)
        L = 001
        Data: 1
      MAPPN_imsi(18)
        L = 008
        Data: Address = 619050100330008
      MAPPN_msc_num(19)
        L = 006
        Data: Ext = No extension
              Ton = International
              Npi = ISDN
              Address = 2207750005
      MAPPN_vlr_number(55)
        L = 006
        Data: Ext = No extension
              Ton = International
              Npi = ISDN
              Address = 2207750005
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(351180 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043179 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 16
      MAP-OPEN-CNF(130)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001000103
                MAP_LocationUpdatingPackage MAP V3
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
 ------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043284 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 113
      MAP-INS-SUBS-DATA-IND(44)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_msisdn(15)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
```

```
               Address = 23277928255
        MAPPN_subscriber_data_comp(99)
         L = 097
         Data: (Hex)
82010A830100A6090401110401210401122A74EA30904011184010581010 1A3060401
12840100A30B0401418401053003830110A3060401428401 05A306040151840105A0
0D040121300830068301108401 04A00D0401293008300683011084 0104
          Tag ASN1 skipped in subscriber profile decoding(82) m = 1
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(83) m = 1
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(A6) m = 9
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(A7) m =
78 EOC = 0
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
----------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(043495 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INS_SUBS_DATA_IND:
              91 6 1 +23277928255 +0 +0 +0 +0 +0
82010A830100A6090401110401210401122A74EA309040111840105810101A3060401
12840100A30B0401418401053003830110A306040142840105A306040151840105A0
0D0401213008300683011084 0104A00D04012930083006830110840104
----------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(043556 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
# ROUTER # <=  MTU_INS_SUBS_DATA_IND:
            91 6 1 +23277928255 +0 +0 +0 +0 +0
82010A830100A6090401110401210401122A74EA309040111840105810101A306040
112840100A30B0401418401053003830110A306040142840105A306040151840105
A00D04012130083006830110840104A00D04012930083006830110840104
----------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(043606 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 108
      MAP-INS-SUBS-DATA-IND(44)
       MAPPN_invoke_id(14)
         L = 001
         Data: 2
       MAPPN_subscriber_data_comp(99)
         L = 101
         Data: (Hex)
A763A00D04012A3008300683011084 0104A00D04012B30083006830110840104A115
040192301030068301108401043006830120840104A1150401933010300683011084
01043006830120840104A115040194301030068301108401043006830120840104
         Tag ASN1 skipped in subscriber profile decoding(A7) m =
99 EOC = 0
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
---------------- HDR -------------- [ Tue Oct 28 15:23:23 2008
(043761 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INS_SUBS_DATA_IND:
             91 6 2 +23277928255 +0 +0 +0 +0 +0
A763A00D04012A30083006830110840104A00D04012B30083006830110840104A115
040192301030068301108401043006830120840104A1150401933010300683011084
01043006830120840104A115040194301030068301108401043006830120840104
---------------- HDR -------------- [ Tue Oct 28 15:23:23 2008
(043799 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
# ROUTER # <=  MTU_INS_SUBS_DATA_IND:
             91 6 2 +23277928255 +0 +0 +0 +0 +0
A763A00D04012A30083006830110840104A00D04012B30083006830110840104A
1150401923010300683011084010430068301208401 04A11504019330103006 83
011084010430068301208401 04A115040194301030068301108401043006830120
840104
```

```
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(051621 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_INS_SUBS_DATA_REQ
               90 33125 1 +23277928255 +0 +2207750005 +0 +0 +0
82010A830100A6090401110401210401 22A74EA309040111840105810101A3060401
12840100A30B0401418401053003830110A3060401428401 05A306040151840105A
00D04012130083006830110840104A00D040129300830068301108401 04
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(051692 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 28
      MAP-OPEN-RSP(129)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        orig_address(Q713)(3)
          L = 010
          Data: Route on GT, Global Title included(0x12),
                No SPC in address
                Subsystem Number = HLR(6),
                Global Title :
                  Translation Type = 0,
                  Numbering Plan = ISDN/Telephony(E164),
                  Nature Address Indicator = International number,
                  Address information = 2207750005
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001000103
                MAP_LocationUpdatingPackage MAP V3
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(051799 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 113
      MAP-INS-SUBS-DATA-REQ(43)
        MAPPN_invoke_id(14)
         L = 001
         Data: 1
        MAPPN_msisdn(15)
         L = 007
         Data: Ext = No extension
               Ton = International
               Npi = ISDN
               Address = 23277928255
        MAPPN_subscriber_data_comp(99)
         L = 097
         Data: (Hex)
82010A830100A6090401110401210401 22A74EA3090401118401058101 01A3060401
12840100A30B0401418401053003830110A3060401428401 05A306040151840105A0
0D04012130083006830110840104A00D040129300830068301108 40104
          Tag ASN1 skipped in subscriber profile decoding(82) m = 1
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(83) m = 1
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(A6) m = 9
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(A7) m =
78 EOC = 0
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
---------------- HDR ---------------- [ Tue Oct 28 15:23:23 2008
(051930 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
---------------- HDR ---------------- [ Tue Oct 28 15:23:23 2008
(051976 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # => MTU_INS_SUBS_DATA_REQ
              90 33125 2 +23277928255 +0 +2207750005 +0 +0 +0
```

```
A763A00D04012A300830068301108401O4A00D04012B30083006830110840104A11
5040192301030068301108401043006830120840104A1150401933010300683011O8
40104300683012084O104A11504019430103006830110840104300683012084O104
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(052038 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 117
      MAP-INS-SUBS-DATA-REQ(43)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
        MAPPN_msisdn(15)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 23277928255
        MAPPN_subscriber_data_comp(99)
          L = 101
          Data: (Hex)
A763A00D04012A300830068301108401O4A00D04012B30083006830110840104A115
040192301030068301108401043006830120840104A115040193301030068301108 4
0104300683012084O104A11504019430103006830110840104300683012084O104
           Tag ASN1 skipped in subscriber profile decoding(A7) m =
99 EOC = 0
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(052164 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943244 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      MAP-INS-SUBS-DATA-CNF(166)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943333 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INS_SUBS_DATA_CNF :
               92 33125 0 0 0 0 1
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943375 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943421 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      MAP-INS-SUBS-DATA-CNF(166)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943485 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <= MTU_INS_SUBS_DATA_CNF :
              92 33125 0 0 0 0 2
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943545 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951230 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # => MTU_INS_SUBS_DATA_RSP
              93 6 0 0 0 0 1
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951283 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 19
      MAP-OPEN-RSP(129)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        orig_address(Q713)(3)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = SSN not known(0),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                  Nature Address Indicator = International number,
                  Address information = 2207750005
        MAPorCAP_Application_Context(11)
          L = 000
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951371 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      MAP-INS-SUBS-DATA-RSP(165)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951433 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951482 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_INS_SUBS_DATA_RSP
               93 6 0 0 0 0 2
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951540 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 5
      MAP-INS-SUBS-DATA-RSP(165)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951615 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(443364 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 14
      MAP-UPDATE-LOCATION-CNF(162)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_hlr_number(81)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 23277180950
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(443463 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_UPDATE_LOCATION_CNF :
               84 6 0 0 0 0 +0 +23277180950 +23277928255 +0
+23277928255 +0|0|-1|0 +0|0|-1|0 +0|0|-1|0
```

```
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(443503 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-CLOSE-IND(4)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(447571 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_UPDATE_LOCATION_RSP
               85 33125 0 0 0 0 +2207750005 +2207750005
+607029900068192 +23277928255
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(447616 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 13
      MAP-UPDATE-LOCATION-RSP(161)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_hlr_number(81)
          L = 006
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 2207750005
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(447689 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 5
      MAP-CLOSE-REQ(3)
        MAPPN_release_method(7)
          L = 001
          Data: (0):Normal Release
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

11.3.2 Example 2: SMS-MO

Answer the following questions:

(1) Which of the two routing methods is used?
(2) Which Service Centre is the SMS-MO sent to?

```
------------------- HDR -------------- [ Tue Oct 28 15:23:21 2008
(342878 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 43
      MAP-OPEN-IND(2)
        dest_address(Q713)(1)
          L = 013
          Data:  Route on SSN, Global Title included(0x53),
                 Signalling Point Code (ITU) = 4-019-5 ( 8349)
                 Subsystem Number = HLR(6),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 33151001220775005
        orig_address(Q713)(3)
          L = 013
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3 ( 2819)
                 Subsystem Number = VLR(7),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 33660001009
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001000103
                MAP_LocationUpdatingPackage MAP V3
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(343033 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 33
      MAP-UPDATE-LOCATION-IND(40)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_imsi(18)
          L = 008
          Data: Address = 607029900068192
        MAPPN_msc_num(19)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 33660001009
        MAPPN_vlr_number(55)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 33660001009
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(343141 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_UPDATE_LOCATION_IND:
              83 33125 +33660001009 +0 +33151001220775005 +0 0 3
+607029900068192 +33660001009 +33660001009 +0 00
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(343180 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(350873 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_UPDATE_LOCATION_REQ
               82 6 +2207750005 +0 E232770100330008 +0
f4741495027094c0c450 3 2819 +619050100330008 28 3 +2207750005
+2207750005 +0 00
------------------ HDR ---------------- [ Tue Oct 28 15:23:21 2008
(350936 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 42
      MAP-OPEN-REQ(1)
        dest_address(Q713)(1)
          L = 015
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3 ( 2819)
                 Subsystem Number = HLR(6),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Mobile(E214),
                   Nature Address Indicator = International number,
                   Address information = 232770100330008
        orig_address(Q713)(3)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = VLR(7),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                 Address information = 2207750005
         MAPorCAP_Application_Context(11)
           L = 009
           Data: (Hex) 060704000001000103
                 MAP_LocationUpdatingPackage MAP V3
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
SERVTYPE 82 overall_length 77 MAX_ONE_SEGMENT 205 map_version 3
seg_msg 0
          (Hex) 272D021C000E0101120816090501300300F81306912270570050
370691227057005000
-------------- HDR ------------- [ Tue Oct 28 15:23:21 2008
(351073 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 35
      MAP-UPDATE-LOCATION-REQ(39)
         MAPPN_timeout(45)
           L = 002
           Data: timeout value =  28 sec
         MAPPN_invoke_id(14)
           L = 001
           Data: 1
         MAPPN_imsi(18)
           L = 008
           Data: Address = 619050100330008
         MAPPN_msc_num(19)
           L = 006
           Data: Ext  = No extension
                 Ton  = International
                 Npi  = ISDN
                 Address = 2207750005
         MAPPN_vlr_number(55)
           L = 006
           Data: Ext  = No extension
                 Ton  = International
                 Npi  = ISDN
                 Address = 2207750005
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
-------------- HDR ------------- [ Tue Oct 28 15:23:21 2008
(351180 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043179 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 16
      MAP-OPEN-CNF(130)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001000103
                 MAP_LocationUpdatingPackage MAP V3
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043284 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 113
      MAP-INS-SUBS-DATA-IND(44)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_msisdn(15)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 23277928255
        MAPPN_subscriber_data_comp(99)
          L = 097
          Data: (Hex)
82010A830100A609040111040121040122A74EA309040111840105810101A3060401
12840100A30B0401418401053003830110A306040142840105A306040151840105A0
0D04012130083006830110840104A00D04012930083006830110840104
```

```
          Tag ASN1 skipped in subscriber profile decoding(82) m = 1
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(83) m = 1
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(A6) m = 9
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(A7) m =
78 EOC = 0
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043495 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INS_SUBS_DATA_IND:
              91 6 1 +23277928255 +0 +0 +0 +0 +0
82010A830100A609040111040121040122A74EA309040111840105810101A3060401
12840100A30B0401418401053003830110A306040142840105A306040151840105A0
0D04012130083006830110840104A00D04012930083006830110840104
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043556 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
# ROUTER # <=  MTU_INS_SUBS_DATA_IND:
              91 6 1 +23277928255 +0 +0 +0 +0 +0
82010A830100A609040111040121040122A74EA309040111840105810101A3060401
12840100A30B0401418401053003830110A306040142840105A306040151840105A0
0D04012130083006830110840104A00D04012930083006830110840104
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043606 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 108
      MAP-INS-SUBS-DATA-IND(44)
```

```
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
        MAPPN_subscriber_data_comp(99)
          L = 101
          Data: (Hex)
A763A00D04012A30083006830110840104A00D04012B30083006830110840104A115
040192301030068301108401043006830120840104A1150401933010300683011084
01043006830120840104A115040194301030068301108401043006830120840104
           Tag ASN1 skipped in subscriber profile decoding(A7) m =
99 EOC = 0
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043761 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INS_SUBS_DATA_IND:
               91 6 2 +23277928255 +0 +0 +0 +0 +0
A763A00D04012A30083006830110840104A00D04012B30083006830110840104A115
040192301030068301108401043006830120840104A1150401933010300683011084
01043006830120840104A115040194301030068301108401043006830120840104
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(043799 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
# ROUTER # <=  MTU_INS_SUBS_DATA_IND:
            91 6 2 +23277928255 +0 +0 +0 +0 +0
A763A00D04012A30083006830110840104A00D04012B30083006830110840104A115
040192301030068301108401043006830120840104A1150401933010300683011084
01043006830120840104A115040194301030068301108401043006830120840104
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(051621 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
```

```
# ROUTER # =>  MTU_INS_SUBS_DATA_REQ
               90 33125 1 +23277928255 +0 +2207750005 +0 +0 +0
82010A830100A6090401110401210401 22A74EA309040111840105810101A3060401
12840100A30B0401418401053003830110A306040142840105A306040151840105A
00D04012130083006830110840104A00D040129300830068301108401 04
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(051692 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 28
      MAP-OPEN-RSP(129)
        MAPPN_result(5)
          L = 001
          Data: (0):Accept
        orig_address(Q713)(3)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = HLR(6),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 2207750005
        MAPorCAP_Application_Context(11)
          L = 009
          Data: (Hex) 060704000001000103
                 MAP_LocationUpdatingPackage MAP V3
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(051799 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 113
      MAP-INS-SUBS-DATA-REQ(43)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_msisdn(15)
          L = 007
```

```
         Data: Ext = No extension
               Ton = International
               Npi = ISDN
               Address = 23277928255
        MAPPN_subscriber_data_comp(99)
         L = 097
         Data: (Hex)
82010A830100A6090401110401210401 22A74EA30904011184010581010 1A3060401
12840100A30B040141840105300383 0110A30604014284010 5A3060401518401 05A0
0D04012130083006830110840104A00D04012930083006830110840104
          Tag ASN1 skipped in subscriber profile decoding(82) m = 1
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(83) m = 1
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(A6) m = 9
EOC = 0
          Tag ASN1 skipped in subscriber profile decoding(A7) m =
78 EOC = 0
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - -
----------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(051930 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - -
----------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(051976 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # => MTU_INS_SUBS_DATA_REQ
              90 33125 2 +23277928255 +0 +2207750005 +0 +0 +0
A763A00D04012A3008300683011084 0104A00D04012B3008300683011084 0104A115
0401923010300683011084010430068301208401 04A1150401933010300683011084
0104300683012084 0104A115040194301030068301108401043006830120840104
----------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(052038 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 117
      MAP-INS-SUBS-DATA-REQ(43)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
        MAPPN_msisdn(15)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 23277928255
        MAPPN_subscriber_data_comp(99)
          L = 101
          Data: (Hex)
A763A00D04012A3008300683011084010 4A00D04012B300830068301108401 04A115
0401923010300683011084010430068301208401 04A11504019330103006830110 84
0104300683012084010 4A11504019430103006830110840104300683012084010 4
           Tag ASN1 skipped in subscriber profile decoding(A7) m =
99 EOC = 0
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(052164 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943244 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      MAP-INS-SUBS-DATA-CNF(166)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943333 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INS_SUBS_DATA_CNF :
               92 33125 0 0 0 0 1
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943375 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943421 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      MAP-INS-SUBS-DATA-CNF(166)
        MAPPN_invoke_id(14)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943485 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INS_SUBS_DATA_CNF :
               92 33125 0 0 0 0 2
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(943545 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 33125
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-IND(6)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951230 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_INS_SUBS_DATA_RSP
               93 6 0 0 0 0 1
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951283 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 19
      MAP-OPEN-RSP(129)
        MAPPN_result(5)
          L = 001
          Data:  (0):Accept
        orig_address(Q713)(3)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = SSN not known(0),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 2207750005
        MAPorCAP_Application_Context(11)
          L = 000
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:23 2008
(951371 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      MAP-INS-SUBS-DATA-RSP(165)
       MAPPN_invoke_id(14)
         L = 001
         Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
---------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(951433 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
---------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(951482 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_INS_SUBS_DATA_RSP
              93 6 0 0 0 0 2
---------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(951540 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      MAP-INS-SUBS-DATA-RSP(165)
       MAPPN_invoke_id(14)
         L = 001
         Data: 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
---------------- HDR --------------- [ Tue Oct 28 15:23:23 2008
(951615 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 6
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-DELIMITER-REQ(5)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(443364 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_SRV_IND (000087E1)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 14
      MAP-UPDATE-LOCATION-CNF(162)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_hlr_number(81)
          L = 007
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 23277180950
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(443463 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 1D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <= MTU_UPDATE_LOCATION_CNF :
               84 6 0 0 0 0 +0 +23277180950 +23277928255 +0
+23277928255 +0|0|-1|0 +0|0|-1|0 +0|0|-1|0
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(443503 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = MAP_MSG_DLG_IND (000087E3)
   SS7E-R Dialog_ID = 6
   SS7E-R Src  = 15
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 2
      MAP-CLOSE-IND(4)
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(447571 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 1D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0
*Nxt = 0
# ROUTER # => MTU_UPDATE_LOCATION_RSP
               85 33125 0 0 0 0 +2207750005 +2207750005
+607029900068192 +33151001
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(447616 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_SRV_REQ (0000C7E0)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 13
      MAP-UPDATE-LOCATION-RSP(161)
        MAPPN_invoke_id(14)
          L = 001
          Data: 1
        MAPPN_hlr_number(81)
          L = 006
          Data: Ext = No extension
                Ton = International
                Npi = ISDN
                Address = 331510012207750005
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Oct 28 15:23:25 2008
(447689 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = MAP_MSG_DLG_REQ (0000C7E2)
   SS7E-E Dialog_ID = 33125
   SS7E-E Src  = 1D
   SS7E-E Dst  = 15
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 5
      MAP-CLOSE-REQ(3)
        MAPPN_release_method(7)
          L = 001
          Data: (0):Normal Release
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

11.3.3 Example 3: CAMEL Subscriber Call

This exercise concerns CAMEL for outbound subscribers with two IMSIs.

Answer the following questions:

(1) What are the Nominal IMSI and the Auxiliary IMSI?
(2) How long did the call last?
(3) Which side has disconnected (calling A number or called B number)?
(4) What is the Transformation done on the Called Party Address received by the Roaming Hub? What is the virtual GT used?
(5) What would happen if this transformation was not done? Would the RH still receive the EVENT-REPORT-BCSM?

```
------------------ HDR --------------- [ Thu Oct 30 19:09:14 2008
(654601 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 34205
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 48
      TC_BEGIN
        TCPPN_CPT_PRESENT(12)
         L = 001
         Data: 1
        TCPPN_DEST_ADDRESS(7)
         L = 013
         Data:  Route on SSN, Global Title included(0x53),
                Signalling Point Code (ITU) = 4-019-5 ( 8349)
                Subsystem Number = CAP(146),
                Global Title :
                  Translation Type = 0,
                  Numbering Plan = ISDN/Telephony(E164),
                  Nature Address Indicator = International number,
                  Address information = 331510012207705005
        TCPPN_ORIG_ADDRESS(8)
         L = 013
         Data:  Route on GT, Global Title included(0x13),
                Signalling Point Code (ITU) = 1-096-3 ( 2819)
                Subsystem Number = CAP(146),
                Global Title :
                  Translation Type = 0,
                  Numbering Plan = ISDN/Telephony(E164),
                  Nature Address Indicator = International number,
                  Address information = 33689001610 /* VPLMN#1 =
SFR */
        TCPPN_APPL_CONTEXT(13)
         L = 011
```

```
          Data: (Hex) A1090607040000001003201
                CAP_gsm_ssf_to_gsm_scf_Package Version 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:14 2008
(654885 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 34205
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0
*Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 134
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 127
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 0
        CAP-INITIAL-DP(0)
          CAPTag_Service Key(128)
            L = 001
            Data: 110
          CAPTag_calling_Party_Number(Q763)(131)
            L = 008
            Data: Nature of Address = International number
                  odd number of address signals
                  Screening Indicator = network provided
                  Presentation Indicator = presentation restricted
                  Numbering plan Indicator = ISDN/Telephony(E164)
                  Number incomplete Indicator = complete (calling)
or routing allowed (called)
                  Address signals = 23277928254
          CAPTag_Calling Partys Category(133)
            L = 001
            Data: (10):Ordinary Calling Subscriber
          CAPTag Location Number(138)
            L = 007
            Data: (Hex) 83971657100500
          CAPTag_Bearer Capability(187)
            L = 005
            Data: (Hex) 80038090A3
          CAPTag_Event_Type_BCSM(156)
            L = 001
```

```
           Data: (2):CollectedInfo
         CAPTag_imsi(50)
           L = 008
           Data: Address = 607029900068193
         CAPTag_Location Information(52)
           L = 023
           Data: (Hex) 0201008107913386091016F0A309800702F8100300D3EE
            CAPTag_Age of Location Information(2)
              L = 001
              Data: 0
            VLR_number(129)
              L = 007
              Data: Ext = No extension
                    Ton = International
                    Npi = ISDN
                    Address = 33689001610
            Cell ID(163)
              L = 009
              Data: MCC = 208 MNC = 1 LAC = 768
               Cell_ID = 54254
         CAPTag_Ext Teleservice code(53)
           L = 003
           Data: (17):telephony
         CAPTag_Call_Reference_Number(54)
           L = 005
           Data: (Hex) 53799D490C
         CAPTag_MSC Address(55)
           L = 007
           Data: Ext = No extension
                 Ton = International
                 Npi = ISDN
                 Address = 33689001610
         CAPTag_Called Party(BEFORE Call Deviation) Number(56)
           L = 007
           Data: Ext = No extension
                 Ton = International
                 Npi = ISDN
                 Address = 33140432125
         CAPTag_Time_and_TimeZone(57)
           L = 008
           Data: 2008.10.30 19:09:13 04
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:14 2008
(655249 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INITIAL_DP_IND:
               62 34205 +33689001610 +0 +331510012207705005 +0 0 2
110 +33140432125 +23277928254 2 +607029900068193 +33689001610
+33689001610 0280010391903140 10 -1 17 80038090A3 0 208.1.768.54254
53799D490C +0 +0 +0 +0 +0
----------------- HDR ---------------- [ Thu Oct 30 19:09:14 2008
(658595 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_INITIAL_DP_REQ
               54 2 +2207750005 +0 +23277180955 +0
f47414a48f90941200a0 2 2819 110 +33140432125 +23277928254 2
+619050100330007 +33689001610 +33689001610 0280010381904100 10
65535 17 80038090A3 0 208.1.768.54254 +0 +0 +0 +0 +0 +0
----------------- HDR ---------------- [ Thu Oct 30 19:09:14 2008
(658734 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 2
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 130
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 117
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 128
        CAP-INITIAL-DP(0)
          CAPTag_Service Key(128)
            L = 001
            Data: 110
          CAPTag_calling_Party_Number(Q763)(131)
            L = 008
            Data: Nature of Address = International number
                  odd number of address signals
                  Screening Indicator = network provided
                  Presentation Indicator = presentation allowed
                  Numbering plan Indicator = ISDN/Telephony(E164)
                  Number incomplete Indicator = complete (calling)
or routing allowed (called)
                 Address signals = 23277928254
          CAPTag_Calling Partys Category(133)
            L = 001
            Data: (10):Ordinary Calling Subscriber
          CAPTag IP(Intelligent Peripheral) Capabilities(136)
            L = 001
            Data: (7):IP Routing Address supported-Voice Back
supported-Speech recognition  supported
          CAPTag High layer compatibility(151)
            L = 002
            Data: (Hex) 9180
          CAPTag_Bearer Capability(187)
            L = 005
            Data: (Hex) 80038090A3
          CAPTag_Event_Type_BCSM(156)
            L = 001
            Data: (2):CollectedInfo
          CAPTag_imsi(50)
            L = 008
            Data: Address = 619050100330007
          CAPTag_Location Information(52)
            L = 023
            Data: (Hex) 0201008107913386091016F0A309800702F8100300D3EE
             CAPTag_Age of Location Information(2)
              L = 001
              Data: 0
             VLR_number(129)
              L = 007
              Data: Ext = No extension
                    Ton = International
                    Npi = ISDN
                    Address = 33689001610
             Cell ID(163)
              L = 009
              Data: MCC = 208 MNC = 1 LAC = 768
               Cell_ID = 54254
          CAPTag_Ext Teleservice code(53)
            L = 003
            Data: (17):telephony
          CAPTag_MSC Address(55)
            L = 007
            Data: Ext = No extension
                  Ton = International
               Npi = ISDN
               Address = 33689001610
          CAPTag_Called Party(BEFORE Call Deviation) Number(56)
           L = 007
           Data: Ext = No extension
                 Ton = International
                 Npi = ISDN
                 Address = 33140432125
          CAPTag_Time_and_TimeZone(57)
           L = 008
           Data: 2008.10.30 18:09:14 00
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:14 2008
(659084 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 2
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 45
      TC_BEGIN
        TCPPN_QOS(6)
          L = 001
          Data: 2
        TCPPN_DEST_ADDRESS(7)
          L = 013
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3 ( 2819)
                 Subsystem Number = CAP(146),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 23277180955 /* SCP of
Africell SL */
        TCPPN_ORIG_ADDRESS(8)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = CAP(146),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 2207750005
        TCPPN_APPL_CONTEXT(13)
          L = 011
          Data: (Hex) A109060704000001003201
                CAP_gsm_ssf_to_gsm_scf_Package Version 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(754743 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 2
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 18
      TC_CONTINUE
       TCPPN_CPT_PRESENT(12)
        L = 001
        Data: 1
       TCPPN_APPL_CONTEXT(13)
        L = 011
        Data: (Hex) A1090607040000001003201
              CAP_gsm_ssf_to_gsm_scf_Package Version 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(754849 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 2
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0
*Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 115
      TC_INVOKE(Request operation(Last))
       TCPPN_LAST_CPT(2)
        L = 001
        Data: 0
       TCPPN_COMPONENT(1)
        L = 108
        Data: Component type: Invoke(A1)
        Invoke ID(2)
        L = 001
        Data: 1
       CAP-REQUEST-REPORT-BCSM-EVENT(23)
        CAPTag_List of BCSM_event(160)
         L = 096
         Data: (Hex)
300B800104810100A203800102300B800105810101A2038001023010800106810100
A203800102BE0381013C300B800107810101A203800102300B800109810100A20380
0101300B800109810100A203800102300B80010A810101A203800101
           EventTypeBCSM(128)
            L = 001
            Data: (4):routeSelectFailure
```

```
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (5):oCalledPartyBusy
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call)
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (6):oNoAnswer
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
              DpspecificCriteria(190)
              L = 003
              Data: (Hex) BE0381013C
            EventTypeBCSM(128)
              L = 001
              Data: (7):oAnswer(Called party Answers)
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call)
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (9):oDisconnect(either Calling or Called party
disconnects)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (1):calling party
            EventTypeBCSM(128)
              L = 001
              Data: (9):oDisconnect(either Calling or Called party
disconnects)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (10):oAbandon(Calling party Abandons before
Answer)
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call)
              Sending Side LegID(162)
              L = 003
              Data: (1):calling party
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
----------------- HDR ---------------- [ Thu Oct 30 19:09:16 2008
(755310 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_REQUEST_REPORT_BCSM_EVENT_IND:
               218 2 +0
A060300B800104810100A203800102300B800105810101A2038001023010800106810
100A203800102BE0381013C300B800107810101A203800102300B800109810100A20
3800101300B800109810100A203800102300B80010A810101A203800101
----------------- HDR ---------------- [ Thu Oct 30 19:09:16 2008
(755348 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 2
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 29
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 022
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 2
        CAP-CONNECT(20)
          CAPTag_destination Routing Address(Q763)(160)
            L = 010
            Data: Nature of Address = International number
                  odd number of address signals
                  Screening Indicator = reserved
                  Presentation Indicator = presentation allowed
                  Numbering plan Indicator = ISDN/Telephony(E164)
                  Number incomplete Indicator = complete (calling)
or routing allowed (called)
                  Address signals = 23277190181  /* the RH will
change the CONNECT destination */
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(755468 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_CONNECT_IND:
               228 2 +23277190181 +0 0 +0 +0 0
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(762732 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_REQUEST_REPORT_BCSM_EVENT_REQ
               217 34205 +2207750005
A060300B800104810100A203800102300B800105810101A2038001023010800106
810100A203800102BE0381013C300B800107810101A203800102300B800109810100
A203800101300B800109810100A203800102300B80010A810101A203800101
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(762838 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 34205
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 121
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
         L = 001
         Data: 1
        TCPPN_TIMEOUT(4)
         L = 002
         Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
         L = 108
         Data: Component type: Invoke(A1)
         Invoke ID(2)
         L = 001
         Data: 0
        CAP-REQUEST-REPORT-BCSM-EVENT(23)
         CAPTag_List of BCSM_event(160)
          L = 096
          Data: (Hex)
300B800104810100A203800102300B800105810101A2038001023010800106810100
A203800102BE0381013C300B800107810101A203800102300B800109810100A20380
0101300B800109810100A203800102300B80010A810101A203800101
           EventTypeBCSM(128)
             L = 001
             Data: (4):routeSelectFailure
             MonitorMode(129)
             L = 001
             Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
             Sending Side LegID(162)
             L = 003
             Data: (2):called party
           EventTypeBCSM(128)
             L = 001
             Data: (5):oCalledPartyBusy
             MonitorMode(129)
             L = 001
             Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call)
             Sending Side LegID(162)
             L = 003
             Data: (2):called party
           EventTypeBCSM(128)
             L = 001
             Data: (6):oNoAnswer
             MonitorMode(129)
             L = 001
             Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
```

```
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
              DpspecificCriteria(190)
              L = 003
              Data: (Hex) BE0381013C
            EventTypeBCSM(128)
              L = 001
              Data: (7):oAnswer(Called party Answers)
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call)
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (9):oDisconnect(either Calling or Called party
disconnects)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (1):calling party
            EventTypeBCSM(128)
              L = 001
              Data: (9):oDisconnect(either Calling or Called party
disconnects)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (10):oAbandon(Calling party Abandons before
Answer)
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call)
              Sending Side LegID(162)
              L = 003
              Data: (1):calling party
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(763284 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 34205
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 31
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
        TCPPN_ORIG_ADDRESS(8)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                No SPC in address
                Subsystem Number = CAP(146),
                Global Title :
                  Translation Type = 0,
                  Numbering Plan = ISDN/Telephony(E164),
                  Nature Address Indicator = International number,
                  Address information = 2207750005 /* sets Calling
Party Address to Virtual GT of Roaming Hub */
        TCPPN_APPL_CONTEXT(13)
          L = 011
          Data: (Hex) A109060704000001003201
                CAP_gsm_ssf_to_gsm_scf_Package Version 2
   - - - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(763376 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # => MTU_CONNECT_REQ
               227 34205 +33140432125 +0 0 +0 +0 0
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(763438 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 34205
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 35
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 022
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 1
        CAP-CONNECT(20)
          CAPTag_destination Routing Address(Q763)(160)
            L = 010
            Data: Nature of Address = International number
                  odd number of address signals
                  Screening Indicator = network provided
                  Presentation Indicator = presentation allowed
                  Numbering plan Indicator = ISDN/Telephony(E164)
                  Number incomplete Indicator = complete (calling)
or routing allowed (called)
                  Address signals = 33140432125
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:16 2008
(763570 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 34205
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 6
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:25 2008
(855488 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 34205
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      TC_CONTINUE
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:25 2008
(855579 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 34205
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 30
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 023
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 1
        CAP-EVENT-REPORT-BCSM(24)
          CAPTag_Event_Type_BCSM(128)
            L = 001
            Data: (7):oAnswer(Called party Answers)
          CAPTag_Receiving Side LegID(163)
            L = 003
            Data: (2):called party
          CAPTag_Misc_Call_Info(164)
            L = 003
            Data: (Hex) 800101
             Message Type(128)
              L = 001
              Data: (1):notification
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:25 2008
(855732 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <= MTU_EVENT_REPORT_BCSM_IND:
                220 34205 7 2 1
```

```
------------------ HDR ---------------- [ Thu Oct 30 19:09:25 2008
(859474 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_EVENT_REPORT_BCSM_REQ
               219 2 7 2 1
------------------ HDR ---------------- [ Thu Oct 30 19:09:25 2008
(859540 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 2
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 36
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 023
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 129
        CAP-EVENT-REPORT-BCSM(24)
          CAPTag_Event_Type_BCSM(128)
            L = 001
            Data: (7):oAnswer(Called party Answers)
          CAPTag_Receiving Side LegID(163)
            L = 003
            Data: (2):called party
          CAPTag_Misc_Call_Info(164)
            L = 003
            Data: (Hex) 800101
             Message Type(128)
               L = 001
               Data: (1):notification
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:25 2008
(859733 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 2
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 6
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:37 2008
(256380 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 34205
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      TC_CONTINUE
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:37 2008
(256467 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 34205
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 38
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 031
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 2
        CAP-EVENT-REPORT-BCSM(24)
          CAPTag_Event_Type_BCSM(128)
            L = 001
```

```
           Data: (9):oDisconnect(either Calling or Called party
disconnects)
          CAPTag_event_Specific_Information_BCSM(162)
           L = 006
           Data: (Hex) A70480028090
             Location of Cause:(80)
              (0):user(U)
             Cause value:(90)
              (16):Normal call clearing
          CAPTag_Receiving Side LegID(163)
           L = 003
           Data: (2):called party
          CAPTag_Misc_Call_Info(164)
           L = 003
           Data: (Hex) 800100
            Message Type(128)
              L = 001
              Data: (0):request
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:37 2008
(256675 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_EVENT_REPORT_BCSM_IND:
               220 34205 9 2 0
------------------ HDR ---------------- [ Thu Oct 30 19:09:37 2008
(264380 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_EVENT_REPORT_BCSM_REQ
               219 2 9 2 0
------------------ HDR ---------------- [ Thu Oct 30 19:09:37 2008
(264452 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 2
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 44
      TC_INVOKE(Request operation(Last))
```

```
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value = 1800 sec
        TCPPN_COMPONENT(1)
          L = 031
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 130
        CAP-EVENT-REPORT-BCSM(24)
          CAPTag_Event_Type_BCSM(128)
            L = 001
            Data: (9):oDisconnect(either Calling or Called party
disconnects)
          CAPTag_event_Specific_Information_BCSM(162)
            L = 006
            Data: (Hex) A70480028490
              Location of Cause:(84)
               (4):public network serving the remote user(RLN)
              Cause value:(90)
               (16):Normal call clearing
          CAPTag_Receiving Side LegID(163)
            L = 003
            Data: (2):called party
          CAPTag_Misc_Call_Info(164)
            L = 003
            Data: (Hex) 800100
             Message Type(128)
               L = 001
               Data: (0):request
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:37 2008
(264650 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 2
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0
*Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 6
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Thu Oct 30 19:09:38 2008
(968369 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 2
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      TC_END /* the SCP (consumer side) END the TCAP transaction */
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:38 2008
(968479 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 2
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 19
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 012
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 3
        CAP-RELEASE-CALL(22)
          CAP_TAG_Cause(4)
            L = 002
            Data: (Hex) 8490
              Location of Cause:(84)
               (4):public network serving the remote user(RLN)
              Cause value:(90)
               (16):Normal call clearing
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:38 2008
(968606 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_CAP_RELEASE_CALL_IND:
               55 2 8490 16 4
------------------ HDR ---------------- [ Thu Oct 30 19:09:38 2008
(972397 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_RELEASE_CALL_REQ
               63 34205 8490 4
------------------ HDR ---------------- [ Thu Oct 30 19:09:38 2008
(972467 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 34205
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 27
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 012
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 2
        CAP-RELEASE-CALL(22)
          CAP_TAG_Cause(4)
            L = 002
            Data: (Hex) 8490
              Location of Cause:(84)
               (4):public network serving the remote user(RLN)
              Cause value:(90)
               (16):Normal call clearing
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Thu Oct 30 19:09:38 2008
(972607 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
```

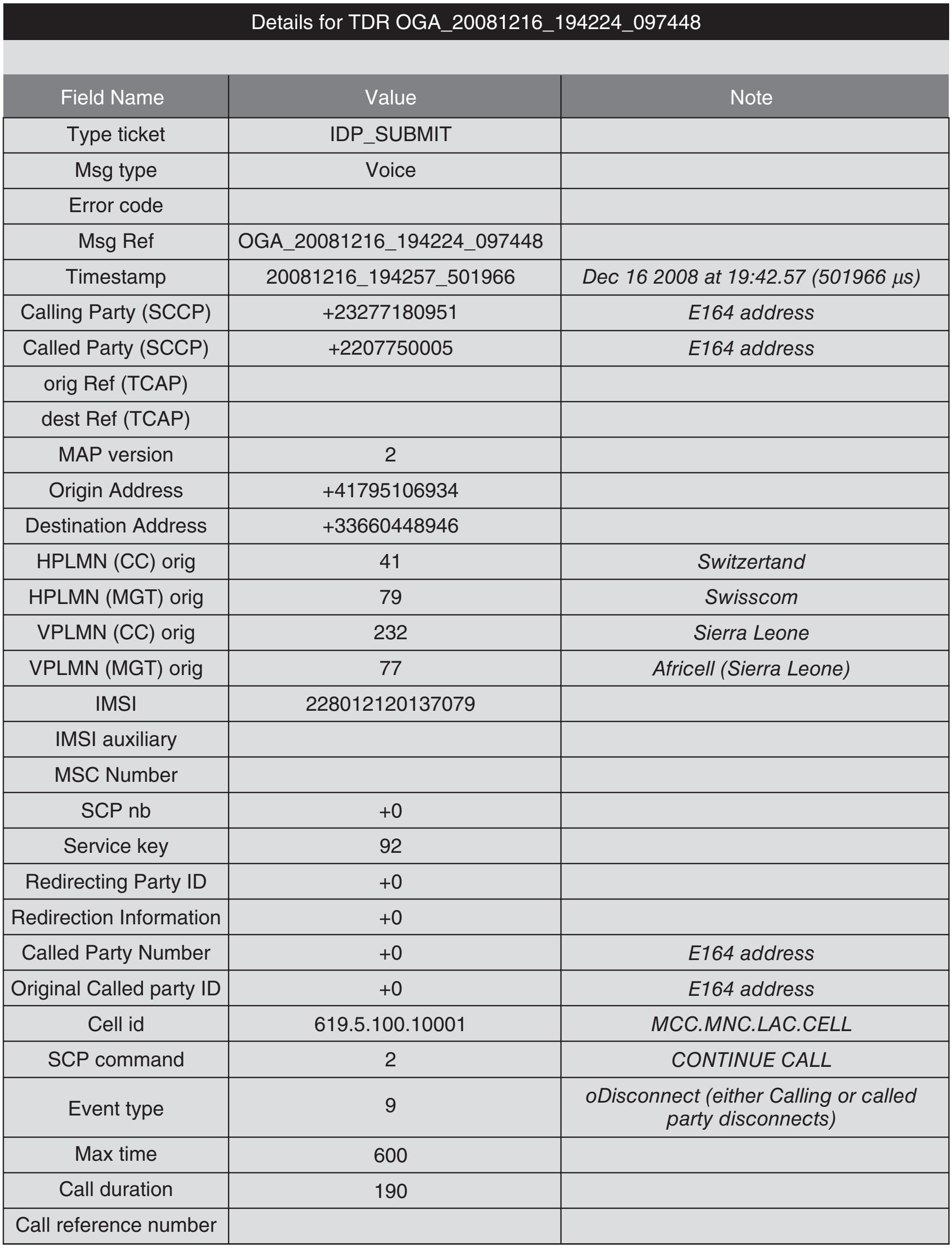
```
    SS7E-E Dialog_ID = 34205
    SS7E-E Src  = 3D
    SS7E-E Dst  = 14
    SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
    - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
        PA_Len = 6
        TC_END              /* the RH END the TCAP IDP transaction
initiated by VMSC */
          TCPPN_QOS(6)
            L = 001
            Data: 2
    - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

11.3.4 Example 4: CAMEL Call with Number Correction Service

Answer the following questions concerning a CAMEL Mobile Originated Call using the trace in Figure 11.3:

(1) Is it a single IMSI or multi-IMSI service?
(2) Why is a CONNECT used? What would happen if the SCP was sending a CONTINUE?
(3) Which side has released the call?
(4) How can the Roaming Hub know how to route the Initial DP to the HPLMN SCP?
(5) You see a ticket for a prepaid voice call (proprietary of a Roaming Hub implementation). How can they get the 'call duration'?

```
-------------------- HDR -------------- [ Tue Dec 16 20:42:24 2008
(096787 us) ]
    MAPE-R Instance = 0
    SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
    SS7E-R Dialog_ID = 33369
    SS7E-R Src  = 14
    SS7E-R Dst  = 3D
    SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
    - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
        PA_Len = 53
        TC_BEGIN
          TCPPN_CPT_PRESENT(12)
            L = 001
            Data: 1
          TCPPN_DEST_ADDRESS(7)
            L = 018
            Data:  Route on SSN, Global Title included(0x53),
                   Signalling Point Code (ITU) = 4-019-5 ( 8349)
                   Subsystem Number = CAP(146),
                   Global Title :
                     Translation Type = 0,
                     Numbering Plan = ISDN/Telephony(E164),
                     Nature Address Indicator = International number,
```



Details for TDR OGA_20081216_194224_097448

Field Name	Value	Note
Type ticket	IDP_SUBMIT	
Msg type	Voice	
Error code		
Msg Ref	OGA_20081216_194224_097448	
Timestamp	20081216_194257_501966	*Dec 16 2008 at 19:42.57 (501966 µs)*
Calling Party (SCCP)	+23277180951	*E164 address*
Called Party (SCCP)	+2207750005	*E164 address*
orig Ref (TCAP)		
dest Ref (TCAP)		
MAP version	2	
Origin Address	+41795106934	
Destination Address	+33660448946	
HPLMN (CC) orig	41	*Switzertand*
HPLMN (MGT) orig	79	*Swisscom*
VPLMN (CC) orig	232	*Sierra Leone*
VPLMN (MGT) orig	77	*Africell (Sierra Leone)*
IMSI	228012120137079	
IMSI auxiliary		
MSC Number		
SCP nb	+0	
Service key	92	
Redirecting Party ID	+0	
Redirection Information	+0	
Called Party Number	+0	*E164 address*
Original Called party ID	+0	*E164 address*
Cell id	619.5.100.10001	*MCC.MNC.LAC.CELL*
SCP command	2	*CONTINUE CALL*
Event type	9	*oDisconnect (either Calling or called party disconnects)*
Max time	600	
Call duration	190	
Call reference number		

Figure 11.3 Ticket for a CAMEL INITIAL DP

```
                  Address information = 338999900072207750005
        TCPPN_ORIG_ADDRESS(8)
          L = 013
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3 ( 2819)
                 Subsystem Number = CAP(146),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 23277180951
        TCPPN_APPL_CONTEXT(13)
          L = 011
          Data: (Hex) A109060704000001003201
                CAP_gsm_ssf_to_gsm_scf_Package Version 2
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - - -
 ac 1
Reception TC BEGIN envoie TC_CONTINUE Msg_Ref_NumberOPEN 0 map_v 1
Nbcptpresent 1
----------------- HDR --------------- [ Tue Dec 16 20:42:24 2008
(096945 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 33369
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 129
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 122
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 1
        CAP-INITIAL-DP(0)
          CAPTag_Service Key(128)
            L = 001
            Data: 92
          CAPTag_calling_Party_Number(Q763)(131)
            L = 008
            Data: Nature of Address = International number
                  odd number of address signals
                  Screening Indicator = network provided
                  Presentation Indicator = presentation allowed
                  Numbering plan Indicator = ISDN/Telephony(E164)
                Number incomplete Indicator = complete (calling)
or routing allowed (called)
                Address signals = 41795106934
         CAPTag_Calling Partys Category(133)
           L = 001
           Data: (10):Ordinary Calling Subscriber
         CAPTag High layer compatibility(151)
           L = 002
           Data: (Hex) 9181
         CAPTag_Bearer Capability(187)
           L = 005
           Data: (Hex) 80038090A3
         CAPTag_Event_Type_BCSM(156)
           L = 001
           Data: (2):CollectedInfo
         CAPTag_imsi(50)
           L = 008
           Data: Address = 228012120137079
         CAPTag_Location Information(52)
           L = 023
           Data: (Hex) 0201008107913272170859F2A3098007
16F95000642711
           CAPTag_Age of Location Information(2)
             L = 001
             Data: 0
           VLR_number(129)
             L = 007
             Data: Ext = No extension
                   Ton = International
                   Npi = ISDN
              Address = 23277180952
           Cell ID(163)
             L = 009
             Data: MCC = 619 MNC = 5 LAC = 100
                   Cell_ID = 10001
         CAPTag_Ext Teleservice code(53)
           L = 003
           Data: (17):telephony
         CAPTag_Call_Reference_Number(54)
           L = 005
           Data: (Hex) D6B11288AD
         CAPTag_MSC Address(55)
           L = 007
           Data: Ext = No extension
                 Ton = International
                 Npi = ISDN
                 Address = 23277180952
         CAPTag_Called Party(BEFORE Call Deviation) Number(56)
           L = 007
           Data: Ext = No extension
```

```
                  Ton = International
                  Npi = ISDN
                  Address = 33660448946
          CAPTag_Time_and_TimeZone(57)
            L = 008
            Data: 2008.12.16 19:46:58 00
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:24 2008
(097286 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_INITIAL_DP_IND:
               62 33369 1 +23277180951 +0 +3389999000722077500005 +0
0 2 2819 8349 92 +33660448946 +41795106934 2 +228012120137079
+23277180952 +23277180952 0280216191648500 10 -1 17 80038090A3 0
619.5.100.10001 D6B11288AD +0 +0 +0 +0 +0
------------------ HDR ---------------- [ Tue Dec 16 20:42:24 2008
(100812 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_INITIAL_DP_REQ
               54 670 1 +2207750005 +0 +41794998954 +0
f474140a4084948ac710 2 0 2819 92 +33660448946 +41795106934 2
+228012120137079 +2207750005 +2207750005 0280216191244200 10 65535
17 80038090A3 0 619.5.100.10001 +0 +0 +0 +0 +0 +0
------------------ HDR ---------------- [ Tue Dec 16 20:42:24 2008
(100923 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 670
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 128
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 115
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 128
        CAP-INITIAL-DP(0)
          CAPTag_Service Key(128)
            L = 001
            Data: 92
          CAPTag_calling_Party_Number(Q763)(131)
            L = 008
            Data: Nature of Address = International number
                  odd number of address signals
                  Screening Indicator = network provided
                  Presentation Indicator = presentation allowed
                  Numbering plan Indicator = ISDN/Telephony(E164)
                  Number incomplete Indicator = complete (calling)
or routing allowed (called)
                  Address signals = 41795106934
          CAPTag_Calling Partys Category(133)
            L = 001
            Data: (10):Ordinary Calling Subscriber
          CAPTag IP(Intelligent Peripheral) Capabilities(136)
            L = 001
            Data: (7):IP Routing Address supported-Voice Back
supported-Speech recognition  supported
          CAPTag High layer compatibility(151)
            L = 002
            Data: (Hex) 9180
          CAPTag_Bearer Capability(187)
            L = 005
            Data: (Hex) 80038090A3
          CAPTag_Event_Type_BCSM(156)
            L = 001
            Data: (2):CollectedInfo
          CAPTag_imsi(50)
            L = 008
            Data: Address = 228012120137079
          CAPTag_Location Information(52)
            L = 022
            Data: (Hex) 0201008106912270570050A309800716F95000642711
             CAPTag_Age of Location Information(2)
               L = 001
               Data: 0
             VLR_number(129)
               L = 006
               Data: Ext = No extension
                     Ton = International
                     Npi = ISDN
```

```
                    Address = 2207750005
            Cell ID(163)
              L = 009
              Data: MCC = 619 MNC = 5 LAC = 100
                    Cell_ID = 10001
          CAPTag_Ext Teleservice code(53)
            L = 003
            Data: (17):telephony
          CAPTag_MSC Address(55)
            L = 006
            Data: Ext = No extension
                  Ton = International
                  Npi = ISDN
                  Address = 2207750005
          CAPTag_Called Party(BEFORE Call Deviation) Number(56)
            L = 007
            Data: Ext = No extension
                  Ton = International
                  Npi = ISDN
                  Address = 33660448946
          CAPTag_Time_and_TimeZone(57)
            L = 008
            Data: 2008.12.16 19:42:24 00
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:24 2008
(101275 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 670
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 45
      TC_BEGIN
        TCPPN_QOS(6)
          L = 001
          Data: 2
        TCPPN_DEST_ADDRESS(7)
          L = 013
          Data:  Route on GT, Global Title included(0x13),
                 Signalling Point Code (ITU) = 1-096-3 ( 2819)
                 Subsystem Number = CAP(146),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 41794998954
        TCPPN_ORIG_ADDRESS(8)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = CAP(146),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
                   Address information = 220775000
        TCPPN_APPL_CONTEXT(13)
          L = 011
          Data: (Hex) A109060704000001003201
                CAP_gsm_ssf_to_gsm_scf_Package Version 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(396813 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 18
      TC_CONTINUE
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
        TCPPN_APPL_CONTEXT(13)
          L = 011
          Data: (Hex) A109060704000001003201
                CAP_gsm_ssf_to_gsm_scf_Package Version 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
 ac 1
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(396944 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 32
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 025
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 2
        CAP-REQUEST-REPORT-BCSM-EVENT(23)
          CAPTag_List of BCSM_event(160)
            L = 013
            Data: (Hex) 300B80010A810101A203800101
             EventTypeBCSM(128)
              L = 001
              Data: (10):oAbandon(Calling party Abandons before
Answer)
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (1):calling party
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(397094 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_REQUEST_REPORT_BCSM_EVENT_IND:
               218 670 1 +0 A00D300B80010A810101A203800101
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(397131 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      TC_CONTINUE
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(397187 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
```

```
    SS7E-R Dst  = 3D
    SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
    - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
        PA_Len = 84
        TC_INVOKE(Request operation(Last))
          TCPPN_LAST_CPT(2)
            L = 001
            Data: 0
          TCPPN_COMPONENT(1)
            L = 077
            Data: Component type: Invoke(A1)
            Invoke ID(2)
            L = 001
            Data: 3
          CAP-REQUEST-REPORT-BCSM-EVENT(23)
            CAPTag_List of BCSM_event(160)
              L = 065
              Data: (Hex)
300B800104810101A203800102300B800107810100A203800102300B800105810101
A203800102300B800109810100A203800101300B800109810100A203800102
               EventTypeBCSM(128)
                 L = 001
                 Data: (4):routeSelectFailure
                 MonitorMode(129)
                 L = 001
                 Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call
                 Sending Side LegID(162)
                 L = 003
                 Data: (2):called party
               EventTypeBCSM(128)
                 L = 001
                 Data: (7):oAnswer(Called party Answers)
                 MonitorMode(129)
                 L = 001
                 Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
                 Sending Side LegID(162)
                 L = 003
                 Data: (2):called party
               EventTypeBCSM(128)
                 L = 001
                 Data: (5):oCalledPartyBusy
                 MonitorMode(129)
                 L = 001
                 Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call
                 Sending Side LegID(162)
                 L = 003
                 Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (9):oDisconnect(either Calling or Called party
disconnects)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (1):calling party
            EventTypeBCSM(128)
              L = 001
              Data: (9):oDisconnect(either Calling or Called party
disconnects)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(397505 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_REQUEST_REPORT_BCSM_EVENT_IND:
               218 670 0 +0
A041300B800104810101A203800102300B800107810100A203800102300B80010581
0101A203800102300B800109810100A203800101300B800109810100A203800102
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(397541 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 29
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
```

```
         L = 022
         Data: Component type: Invoke(A1)
         Invoke ID(2)
         L = 001
         Data: 4
       CAP-CONNECT(20)
         CAPTag_destination Routing Address(Q763)(160)
           L = 010
           Data: Nature of Address = International number
                 odd number of address signals
                 Screening Indicator = reserved
                 Presentation Indicator = presentation allowed
                 Numbering plan Indicator = ISDN/Telephony(E164)
                 Number incomplete Indicator = complete (calling)
or routing allowed (called)
                 Address signals = 33660448946
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(397647 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <= MTU_CONNECT_IND:
             228 670 1 +33660448946 +0 0 +0 +0 0
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(400811 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # => MTU_REQUEST_REPORT_BCSM_EVENT_REQ
             217 33369 1 +2207750005
A00D300B80010A810101A203800101
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(400885 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 33369
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 38
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
```

```
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value = 1800 sec
        TCPPN_COMPONENT(1)
          L = 025
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 1
        CAP-REQUEST-REPORT-BCSM-EVENT(23)
          CAPTag_List of BCSM_event(160)
            L = 013
            Data: (Hex) 300B80010A810101A203800101
             EventTypeBCSM(128)
              L = 001
              Data: (10):oAbandon(Calling party Abandons before
Answer)
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (1):calling party
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(401077 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 33369
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 31
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
        TCPPN_ORIG_ADDRESS(8)
          L = 010
          Data:  Route on GT, Global Title included(0x12),
                 No SPC in address
                 Subsystem Number = CAP(146),
                 Global Title :
                   Translation Type = 0,
                   Numbering Plan = ISDN/Telephony(E164),
                   Nature Address Indicator = International number,
           Address information = 220775000
     TCPPN_APPL_CONTEXT(13)
      L = 011
      Data: (Hex) A1090607040000001003201
          CAP_gsm_ssf_to_gsm_scf_Package Version 2
  - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(401171 us) ]
  MAPE-R Instance = 0
  SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
  SS7E-R Dialog_ID = 0
  SS7E-R Src  = 01
  SS7E-R Dst  = 3D
  SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_REQUEST_REPORT_BCSM_EVENT_REQ
217 33360 0 +2207750005
A041300B800104810101A203800102300B800107810100A203800102300B80010581
0101A203800102300B800109810100A203800101300B800109810100A203800102
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(401249 us) ]
  MAPE-E Instance = 0
  SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
  SS7E-E Dialog_ID = 33369
  SS7E-E Src  = 3D
  SS7E-E Dst  = 14
  SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
  - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
    PA_Len = 90
    TC_INVOKE(Request operation(Last))
     TCPPN_CLASS(3)
      L = 001
      Data: 1
     TCPPN_TIMEOUT(4)
      L = 002
      Data: timeout value =  1800 sec
     TCPPN_COMPONENT(1)
      L = 077
      Data: Component type: Invoke(A1)
      Invoke ID(2)
      L = 001
      Data: 2
     CAP-REQUEST-REPORT-BCSM-EVENT(23)
      CAPTag_List of BCSM_event(160)
       L = 065
       Data: (Hex)
300B800104810101A203800102300B800107810100A203800102300B800105810101
A203800102300B800109810100A203800101300B800109810100A203800102
        EventTypeBCSM(128)
         L = 001
         Data: (4):routeSelectFailure
```

```
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (7):oAnswer(Called party Answers)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (5):oCalledPartyBusy
              MonitorMode(129)
              L = 001
              Data: (1):Notify(SCF) And Continue: DO NOT WAIT
instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
            EventTypeBCSM(128)
              L = 001
              Data: (9):oDisconnect(either Calling or Called party
disconnects)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (1):calling party
            EventTypeBCSM(128)
              L = 001
              Data: (9):oDisconnect(either Calling or Called party
disconnects)
              MonitorMode(129)
              L = 001
              Data: (0):Interrupt(Hold call processing): Request
and WAIT instructions from SCF to continue call
              Sending Side LegID(162)
              L = 003
              Data: (2):called party
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(401564 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_CONNECT_REQ
              227 33369 1 +33660448946 +0 0 +0 +0 0
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(401621 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 33369
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 35
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 022
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 3
        CAP-CONNECT(20)
          CAPTag_destination Routing Address(Q763)(160)
            L = 010
            Data: Nature of Address = International number
                  odd number of address signals
                  Screening Indicator = reserved
                  Presentation Indicator = presentation allowed
                  Numbering plan Indicator = ISDN/Telephony(E164)
                  Number incomplete Indicator = complete (calling)
or routing allowed (called)
                  Address signals = 33660448946
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:25 2008
(401759 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 33369
```

```
  SS7E-E Src  = 3D
  SS7E-E Dst  = 14
  SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
  - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
    PA_Len = 6
    TC_CONTINUE
     TCPPN_QOS(6)
      L = 001
      Data: 2
  - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:37 2008
(496975 us) ]
  MAPE-R Instance = 0
  SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
  SS7E-R Dialog_ID = 33369
  SS7E-R Src  = 14
  SS7E-R Dst  = 3D
  SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
  - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
    PA_Len = 5
    TC_CONTINUE
     TCPPN_CPT_PRESENT(12)
      L = 001
      Data: 1
  - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:37 2008
(497065 us) ]
  MAPE-R Instance = 0
  SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
  SS7E-R Dialog_ID = 33369
  SS7E-R Src  = 14
  SS7E-R Dst  = 3D
  SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
  - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
    PA_Len = 29
    TC_INVOKE(Request operation(Last))
     TCPPN_LAST_CPT(2)
      L = 001
      Data: 1
     TCPPN_COMPONENT(1)
      L = 022
      Data: Component type: Invoke(A1)
      Invoke ID(2)
      L = 001
      Data: 2
     CAP-EVENT-REPORT-BCSM(24)
      CAPTag_Event_Type_BCSM(128)
       L = 001
       Data: (7):oAnswer(Called party Answers)
      CAPTag_event_Specific_Information_BCSM(162)
```

```
            L = 002
            Data: (Hex) A500
          CAPTag_Receiving Side LegID(163)
            L = 003
            Data: (2):called party
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:37 2008
(497199 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_EVENT_REPORT_BCSM_IND:
               220 33369 1 7 2 0
------------------ HDR ---------------- [ Tue Dec 16 20:42:37 2008
(504971 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_EVENT_REPORT_BCSM_REQ
               219 670 1 7 2 0
------------------ HDR ---------------- [ Tue Dec 16 20:42:37 2008
(505041 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 670
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 36
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 023
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 129
        CAP-EVENT-REPORT-BCSM(24)
```

```
          CAPTag_Event_Type_BCSM(128)
            L = 001
            Data: (7):oAnswer(Called party Answers)
          CAPTag_Receiving Side LegID(163)
            L = 003
            Data: (2):called party
          CAPTag_Misc_Call_Info(164)
            L = 003
            Data: (Hex) 800100
             Message Type(128)
               L = 001
               Data: (0):request
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:37 2008
(505235 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 670
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 6
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(797160 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      TC_CONTINUE
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(797249 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 30
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 0
        TCPPN_COMPONENT(1)
          L = 023
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 5
        CAP-APPLY-CHARGING(35)
          (Hex) A00480020258
          Max Call Period Duration(128)
            L = 002
            Data: duration 60.0 seconds
          CAPTag Party To Charge: Sending Side Leg ID(162)
            L = 003
            Data: (1):calling party
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(797381 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_APPLY_CHARGING_IND:
               56 670 0 1 0 600 17
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(797418 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0
*Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 15
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 008
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 6
        CAP-CONTINUE(31)
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(797503 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_CONTINUE_CALL_IND:
               222 670 1
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(801176 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_APPLY_CHARGING_REQ
               64 33369 0 1 0 600 17
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(801264 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 33369
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 41
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 028
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 4
        CAP-APPLY-CHARGING(35)
          (Hex) A00980020258A103010111
          Max Call Period Duration(128)
            L = 002
            Data: duration 60.0 seconds
          Tone(161)
            L = 003
            Data: (Hex) 010111
          CAPTag Party To Charge: Sending Side Leg ID(162)
            L = 003
            Data: (1):calling party
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(801412 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_CONTINUE_CALL_REQ
               221 33369 1
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(801469 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 33369
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 23
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 008
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 5
        CAP-CONTINUE(31)
   - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:38 2008
(801579 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 33369
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 6
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:56 2008
(397610 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 33369
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 5
      TC_CONTINUE
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:56 2008
(397735 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 33369
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 33
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 0
        TCPPN_COMPONENT(1)
          L = 026
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 3
        CAP-APPLY-CHARGING-REPORT(36)
          CAPTag Party To Charge: Receiving Side Leg ID(129)
            L = 001
            Data: (1):calling party
          Call duration (No Tariff switch)(128)
            L = 002
            Data: duration 19.0 seconds
          CAPTAG_callActive(130)
           L = 001
           Data: (Hex) 00
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
----------------- HDR ---------------- [ Tue Dec 16 20:42:56 2008
(397868 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_APPLY_CHARGING_REPORT_IND:
               65 33369 0 1 0 190 0
----------------- HDR ---------------- [ Tue Dec 16 20:42:56 2008
(397905 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 33369
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 33
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 026
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 4
        CAP-EVENT-REPORT-BCSM(24)
          CAPTag_Event_Type_BCSM(128)
           L = 001
           Data: (9):oDisconnect(either Calling or Called party
disconnects)
          CAPTag_event_Specific_Information_BCSM(162)
           L = 006
           Data: (Hex) A70480028090
             Location of Cause:(80)
              (0):user(U)
             Cause value:(90)
              (16):Normal call clearing
          CAPTag_Receiving Side LegID(163)
           L = 003
           Data: (1):calling party
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Dec 16 20:42:56 2008
(398052 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_EVENT_REPORT_BCSM_IND:
               220 33369 1 9 1 0
------------------ HDR ---------------- [ Tue Dec 16 20:42:56 2008
(405615 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_APPLY_CHARGING_REPORT_REQ
               57 670 0 1 0 190 0
------------------ HDR ---------------- [ Tue Dec 16 20:42:56 2008
(405687 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 670
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 41
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 026
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 130
        CAP-APPLY-CHARGING-REPORT(36)
          CAPTag Party To Charge: Receiving Side Leg ID(129)
            L = 001
            Data: (1):calling party
          Call duration (No Tariff switch)(128)
            L = 002
            Data: duration 19.0 seconds
          CAPTAG_callActive(130)
            L = 001
            Data: (Hex) 00
   - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:56 2008
(405841 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_EVENT_REPORT_BCSM_REQ
               219 670 1 9 1 0
------------------ HDR ---------------- [ Tue Dec 16 20:42:56 2008
(405899 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 670
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - - -
      PA_Len = 44
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 031
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 131
        CAP-EVENT-REPORT-BCSM(24)
          CAPTag_Event_Type_BCSM(128)
            L = 001
            Data: (9):oDisconnect(either Calling or Called party
disconnects)
          CAPTag_event_Specific_Information_BCSM(162)
            L = 006
            Data: (Hex) A70480028490
              Location of Cause:(84)
               (4):public network serving the remote user(RLN)
              Cause value:(90)
               (16):Normal call clearing
          CAPTag_Receiving Side LegID(163)
```

```
           L = 003
           Data: (1):calling party
          CAPTag_Misc_Call_Info(164)
           L = 003
           Data: (Hex) 800100
            Message Type(128)
              L = 001
              Data: (0):request
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:56 2008
(406086 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 670
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 6
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:57 2008
(497647 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      TC_CONTINUE
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:57 2008
(497733 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 670
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 19
      TC_INVOKE(Request operation(Last))
```

```
        TCPPN_LAST_CPT(2)
         L = 001
         Data: 1
        TCPPN_COMPONENT(1)
         L = 012
         Data: Component type: Invoke(A1)
         Invoke ID(2)
         L = 001
         Data: 7
        CAP-RELEASE-CALL(22)
         CAP_TAG_Cause(4)
           L = 002
           Data: (Hex) 8090
             Location of Cause:(80)
              (0):user(U)
             Cause value:(90)
              (16):Normal call clearing
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:57 2008
(497876 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = ROUTER_MSG_SRV_REQ (00001235)
   SS7E-E Dialog_ID = 0
   SS7E-E Src  = 3D
   SS7E-E Dst  = 01
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # <=  MTU_CAP_RELEASE_CALL_IND:
               55 670 1 +0 8090 16 3
------------------ HDR ---------------- [ Tue Dec 16 20:42:57 2008
(505650 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = ROUTER_MSG_SRV_IND (00001234)
   SS7E-R Dialog_ID = 0
   SS7E-R Src  = 01
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
# ROUTER # =>  MTU_RELEASE_CALL_REQ
               63 33369 1 +2207750005 8090 3
------------------ HDR ---------------- [ Tue Dec 16 20:42:57 2008
(505718 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_CPT_REQ (0000C781)
   SS7E-E Dialog_ID = 33369
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 27
      TC_INVOKE(Request operation(Last))
        TCPPN_CLASS(3)
```

```
          L = 001
          Data: 1
        TCPPN_TIMEOUT(4)
          L = 002
          Data: timeout value =  1800 sec
        TCPPN_COMPONENT(1)
          L = 012
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 6
        CAP-RELEASE-CALL(22)
          CAP_TAG_Cause(4)
            L = 002
            Data: (Hex) 8090
              Location of Cause:(80)
               (0):user(U)
              Cause value:(90)
               (16):Normal call clearing
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:42:57 2008
(505862 us) ]
   MAPE-E Instance = 0
   SS7E-E Type = TCAP_MSG_DLG_REQ (0000C783)
   SS7E-E Dialog_ID = 33369
   SS7E-E Src  = 3D
   SS7E-E Dst  = 14
   SS7E-E Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 6
      TC_CONTINUE
        TCPPN_QOS(6)
          L = 001
          Data: 2
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
------------------ HDR ---------------- [ Tue Dec 16 20:45:42 2008
(129842 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_DLG_IND (00008784)
   SS7E-R Dialog_ID = 577
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 5
      TC_END
        TCPPN_CPT_PRESENT(12)
          L = 001
          Data: 1
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

```
------------------ HDR ---------------- [ Tue Dec 16 20:45:42 2008
(129939 us) ]
   MAPE-R Instance = 0
   SS7E-R Type = TCAP_MSG_CPT_IND (00008782)
   SS7E-R Dialog_ID = 577
   SS7E-R Src  = 14
   SS7E-R Dst  = 3D
   SS7E-R Rsp_req = 0  Class = 0  Status = 0  Err_info = 0  *Nxt = 0
   - - - - Super Detailed SS7 Analyser (C)HALYS - - - - - - -
      PA_Len = 19
      TC_INVOKE(Request operation(Last))
        TCPPN_LAST_CPT(2)
          L = 001
          Data: 1
        TCPPN_COMPONENT(1)
          L = 012
          Data: Component type: Invoke(A1)
          Invoke ID(2)
          L = 001
          Data: 5
        CAP-RELEASE-CALL(22)
          CAP_TAG_Cause(4)
            L = 002
            Data: (Hex) 809F
              Location of Cause:(80)
               (0):user(U)
              Cause value:(9F)
               (31):Normal, unspecified
   - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - -
```

Index

© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-68262-3