Internet Protocol based Mobile Radio Access Network Architecture for Remote Service Areas

HAMID SHAHZAD
and
NISHANT JAIN

KTH Information and
Communication Technology

Master of Science Thesis
Stockholm, Sweden 2007

COS/CCS 2007-24

Internet Protocol based Mobile Radio Access Network Architecture for Remote Service Areas

Hamid Shahzad
hshahzad@kth.se

&

Nishant Jain
nishnat@kth.se

September 27, 2007

Masters of Science thesis performed at SeaNet AB,
Stockholm, Sweden

Examiner:	Professor Gerald Q. Maguire Jr.
Academic Supervisor:	Professor Gerald Q. Maguire Jr.
Industry Supervisor:	Robby De Candido, SeaNet AB

School of Information and Communication Technology (ICT)

Kungliga Tekniska Högskolan (KTH), Stockholm, Sweden

Abstract

When it comes to their Radio Access Network (RAN) infrastructure, no two Mobile Operators, serving remote service areas, are alike. Despite situations and technologies being diverse, a well designed optimized RAN solution must adapt itself to the existing networking technologies, both with regard to legacy core networks and modern telecommunication networks in order to produce the best network which is possible subject to many constraints. There is a misconception in technical circles that an optimized internet protocol (IP) enabled RAN architecture is more theoretical than practical. On the contrary, the aforesaid is highly dependent on the technology used. Packet optimized IP- GSM Radio Access Network (GRAN) architecture is proposed in this thesis, it uses Internet Protocol (IP) rather than proprietary protocols for communication between Base Transceiver Stations (BTS), Base Station Controllers (BSC), and the Network Switching Subsystem (NSS). This architecture must deliver carrier-grade mobility, scalability, and reliability; while being optimized for efficient roaming, routing and backhauling from remote service areas. In a geographic arena that spans across the globe, classical circuit-switched networks are not cost efficient due to their integrated call control (signaling) and switching architecture. A solution to this may be soft-switching which separates the call control (Media Gateway Controller (MGC)) and switching (Media Gateway (MG)) into separate nodes. This methodology would fundamentally change the way circuit-switched services, such as traditional voice telephony, are handled. For a service provider this enables a much more efficient network, because it allows optimized equipment location for voice termination into other carrier networks. Co-location of media gateways with satellite ground stations enables local termination to the public switched telephone network (PSTN), thus off-loading a great deal of the traffic from the backhaul transmission network of the mobile operator. This thesis adopts soft-switching as part of the call routing processes. The thesis considers the problem of transporting voice and signaling from-to the remote service areas, efficient routing and backhaul to the location of most suitable operator's point of presence. The thesis explores an alternative which uses a packet switched backbone (e.g. IP based) to transport the media as close (geographically) to the dialed party as possible before terminating it at the PSTN network, thus achieving optimal routing of voice and signaling. Considering the aforesaid, the thesis describes a detailed network architecture and an operational system prototype for maritime GSM network deployment, as a befitting and challenging example of remote service area.

Keywords and acronyms: IP backbones, radio access networks, call routing, All-IP networks

Sammanfattning

När det gäller deras Radio access nät, finns det inte två Mobiloperatörer, som betjänar avlägsna områden, som är lika. Trots olika omständigheter och teknologier, ett väl designat optimerat RAN måste anpassa sig till den existerande nätverks teknologin, både med avseende på äldre befintlig teknologi och på moderna telekomnät, för att kunna skapa bästa möjliga nätverk givet många begränsningar. Det är en missuppfattning i tekniska kretsar att en optimerad IP anpassad RAN arkitektur är mer teoretisk än praktisk. Å andra sidan så är det ovan sagda väldigt beroende på vilken teknologi som har använts. En paket optimerad IP-GSM Radio Access Nätverks (IP-GRAN) arkitektur är föreslagen i denna masters uppsats, den baseras på Internet Protokollet (IP) snarare än något egenutvecklat proprietärt protokol för komunikation mellan Basstation (BTS), Basstationscontroller (BSC), och nätets switchade subsystem (NSS). Denna arkitektur måste leverera carrier-grade (operatörs klassad) mobilitet, skalbarhet och tillgänglighet och samtidigt vara optimerat för effektiv roaming, routing och anslutning från avlägsna områden. På ett geografiskt område som sträcker sig runt hela jordklotet är inte klassiska kretskopplade nätverk kostnadseffektiva beroende på deras integrerade signallerings och samtals arkitektur. En bättre arkitektur kan vara en sk "softswitch" lösning som separerar samtalet i en (Media Gateway Controller (MGC)) och signaleringen (Media Gateway (MG)) i separata noder. Denna metod skulle på ett fundamentalt vis ändra det sätt på vilket traditionella kretskopplade tjänster som traditionell telefoni hanteras. För en tjänsteleverantör möjliggör detta ett mycket effektivare nätverk då det möjliggör optimerad utplacering av utrustning för terminering av rösttrafik in i andra operatörers nät. Samlokalisering av media gateways (MG:s) med jordstationer för satellitkommunikation möjliggör lokal anslutning till det allmänna telenätet (PSTN), vilket kraftigt minskar den trafik som behöver transporteras genom operatörens stomnät. Denna mastersuppsats behandlar "softswitching" som en del av metoden att växla och transportera samtalstrafik. Uppsatsen behandlar problemet med att skicka samtalstrafik och signalering från avlägsna områden, effektiv routing och transport av trafiken till den operatör som har den närmaste(alt. mest optimala) anslutningspunkten. Uppsatsen undersöker ett alternativ som använder ett paketförmedlat (IP baserat) transportsätt för att transportera trafiken geografiskt sett så nära den uppringda parten som möjligt innan den termineras i det allmänna telenätet (PSTN) varvid man uppnår optimal växling (alt. routing) av rösttrafik och signalering. I beaktande av ovanstående beskriver uppsatsen en detaljerad nätverksarkitektur och en funktionsduglig systemprototyp för ett maritimt GSM nät som ett utmanande exempel på ett avlägset beläget nät.

Nyckelord och förkortningar: IP baserat, radio access nätverks, optimal växling, All-IP nätverks

Acknowledgements

First and foremost, we would like to record our sincerest gratitude to our academic supervisor, Professor Gerald Q. Maguire Jr., for his supervision, advice, and guidance from the very early stage of this thesis work as well as giving us extraordinary experiences throughout the work. Above all and the most needed, he provided us unflinching encouragement and support in various ways with his patience and knowledge whilst allowing us the room to work in our own way. His truly scientist intuition has made him as a constant oasis of ideas and passions in communication technologies, which exceptionally inspire and enrich our growth as a student, a researcher and a professional we want to be. We are indebted to him more than he knows. One simply could not wish for a better or supportive supervisor.

We gratefully acknowledge Robby De Candido, our industrial supervisor and Director of Operations at SeaNet AB, for his advice, supervision, and crucial contribution, which made him a backbone of this project and so to this thesis. His involvement with his originality has triggered and nourished our intellectual maturity that we will benefit from, for a long time to come. Robby, we are grateful in every possible way and hope to keep up our collaboration in the future.

We thank IP.Access Ltd. (UK), Zynetix Ltd. (UK) and Vodafone (Malta), technology partners and operations partner respectively, of SeaNet; for their esteemed cooperation in running simulations, collecting traces and results and also for the permission to include copyrighted material as part of our thesis. We worked with a great number of people from the aforesaid organizations whose contribution in assorted ways to the research and the making of the thesis deserved special mention. It is a pleasure to convey our gratitude to them all in our humble acknowledgment.

Many thanks go in particular to Jonas Lundhagen, Director of GSM Business Unit, and Mikael Reichel, CEO at SeaNet. We are much indebted to Jonas for his valuable advice in technology related discussions, supervision during system simulations and furthermore, using his precious time to read this thesis and gave his critical comments about it. We have also benefited by advice and guidance from Mike who also always kindly grants us his time even for answering some of our unintelligent questions concerning management issues and also for awarding us the thesis completion stipendium, thus providing us with the financial means to complete this project.

We convey special acknowledgement to Inga Hedenström, Head of Administration at SeaNet, for her indispensable help dealing with travel funds, administration and bureaucratic matters during the progress of our thesis work at SeaNet.

I would also acknowledge Magnus Lundmark and Jeppe Gade, our colleagues at SeaNet, for their advice and their willingness to share their bright thoughts with us, which were very fruitful for shaping up our ideas and research.

And finally, thanks to our family, and numerous friends who endured this long process with us, always offering support and love. We would like to thank everybody who was important to the successful realization of thesis, as well as expressing our apology that we could not mention personally one by one.

Contents

List of figures .... **VIII**
List of tables .... **X**
List of acronyms and abbreviations .... **XI**

1 Introduction **1**
1.1 Problem Statement 3
1.2 Proposed Solution 3
2 GSM System Architecture **5**
2.1 Overview 5
2.2 System Architecture 6
2.2.1 Radio Network- Base Station Subsystem (BSS) 6
2.2.2 Mobile Switching Network (MSN) 8
2.3 Mobility and Switching 11
2.3.1 Location Update 11
2.3.2 Call Routing 13
2.3.3 MSRN Assignment and Routing 17
2.3.4 Call Establishment 17
2.3.4.1 Mobile Orginating Call Setup 17
2.3.4.2 Mobile Terminated Call Setup 19
3 Underlying Technology **22**
3.1 OSI Reference Model 22
3.2 Signaling System 7 23
3.2.1 SS7 Network Architecture 23
3.2.2 SS7 and the OSI Reference Model 24
3.2.3 SS7-IP Internetworking 30
3.3 TDM over IP 30
3.3.1 TDMoIP Encapsulation 31
3.3.2 Encapsulation Details for several packets switched networks 32
3.3.2.1 UDP/IPv4 32
3.4 SS7 over IP Implementation (SIGTRAN-SCTP) 33
3.4.1 Stream Control Transmission Protocol 34
3.4.2 SIGTRAN Architecture 36
3.4.3 Transporting MTP over IP 38
3.4.3.1 M2UA: MTP2 User Adaptation Layer 38
3.4.3.2 M2PA: MTP2 User Peer-to-Peer Adaptation Layer 39
3.4.3.2.1 M2PA and M2UA Comparison 41
3.4.3.3 M3UA: MTP3 User Adaptation Layer 41
3.4.4 SUA: SCCP User Adaptation Layer 43
3.4.4.1 SUA and M3UA Comparison 45
4 System Implementation **46**
4.1 GRAN Network Architecture 46
4.1.1 GRAN System Services and Operations 49
4.2 Packet Optimized Radio Access System 50
4.2.1 Call Processing 52
4.3 Soft-switching 54
5 Network Optimization: Optimal Routing **56**
5.1 Global Title Translation (GTT) Routing 58
5.2 International Roaming Network 59

5.2.1 Routing and Addressing.. 60
5.2.2 Global Title Translation Scenarios.. 61
5.3 Optimal Routing Proposal.. 63
5.3.1 Proposal-1: Network Virtualization (NV).. 64
5.3.1.1 The Work Flow (with network virtualization).. 64
5.3.2 Proposal-2: Optimized MSRN Assignments (OMA)..................................... 65
5.3.2.1 The Work Flow (Pre OMA)... 66
5.3.2.2 The Work Flow (Post OMA).. 67
5.3.2.3 The Limitations.. 69
6 Traffic Dimensioning in IP-GRAN: Simulation and Analysis.......... 70
6.1 Simulation Enviornment... 70
6.2 The Simulation.. 71
6.3 The Results.. 73
6.3.1 Single TRX.. 74
6.3.2 Multi-TRX... 76
6.3.3 Multi-BTS.. 78
6.4 The Analysis.. 80
6.4.1 Download Jitter... 80
6.4.2 Uplink Jitter... 81
6.4.3 Packet Drop... 81
6.4.4 Bandwidth Requirements.. 82
6.5 Effect of Signaling on Dimensioning... 82
7 Packet Optimized IP GRAN Prototype: Setup and results............... 84
7.1 Proposed Network Architecture... 84
7.2 Test Network Architecture.. 87
7.2.1 Architecture-1: Signaling Aggregator is situated at SeaNet............................ 87
7.2.2 Architecture-2: Signaling Aggregator is situated at MNO's premises........... 88
7.3 Test Setup.. 88
7.3.1 Test parameters.. 89
7.4 Softswitching: Signaling flow... 90
7.4.1 Message Switching Configurations.. 90
7.5 SCTP association between MSC/VLR and global SS7 net.......................... 97
7.5.1 Message switching protocol trace.. 99
7.6 Protocol trace... 108
7.6.1 SCCP trace.. 109
7.6.2 MAP invoke at location update... 112
7.6.3 ISUP trace: MO call setup.. 117
7.6.4 Trace : MT call setup.. 119
7.6.5 RTP/MGCP trace: voice setup.. 122
7.7 Network limitations and optimization... 127
8 Conclusions.. 130
9 Future work.. 132

References.. 133

List of Figures

Figure 2.1 GSM system architecture.. 5
Figure 2.2 Components of GSM radio system.. 7
Figure 2.3 Components of GSM mobile switching system... 8
Figure 2.4 Location update after changing the VLR area... 12
Figure 2.5 Routing calls to a mobile station... 13
Figure 2.6 Routing variants for national MSISDN.. 14
Figure 2.7 Routing for international MSISDN (HLR interrogation from ISC)................... 15
Figure 2.8 Routing through GMSC for international MSISDN.. 16
Figure 2.9 MM connection establishment... 18
Figure 2.10 Overview of outgoing call setup... 18
Figure 2.11 Interrogation of routing information for incoming call....................................... 20
Figure 2.12 Overview of incoming call setup... 21
Figure 3.1 The layers and message types of the OSI Reference Model................................ 22
Figure 3.2 SS7 signaling nodes.. 24
Figure 3.3 SS7 protocol stack and OSI reference Basic ISUP signaling model.................. 25
Figure 3.4 Basic ISUP Signaling.. 28
Figure 3.5 Basic TDMoIP packet format.. 31
Figure 3.6 TDMoIP packet format for UDP/IP.. 32
Figure 3.7 Simpler implementation for signaling transport over IP...................................... 34
Figure 3.8 SIGTRAN architecture model.. 36
Figure 3.9 SIGTRAN Protocol Stack... 37
Figure 3.10 Back hauling with M2UA between 2 distant nodes.. 39
Figure 3.11 Connection between SS7 signaling points to IP signaling point using M2PA... 40
Figure 3.12 Back hauling using M3UA... 42
Figure 3.13 Use of SUA between SG and IP signaling point.. 44
Figure 4.1 Packet Optimized Radio Access Network... 46
Figure 4.2 Statistical multiplexing gain graph.. 47
Figure 4.3 High level system architecture for packet optimized system............................... 51
Figure 4.4 Vertical to layered architecture.. 54
Figure 4.5 Initial network topology vs. Softswitch network topology.................................. 55
Figure 5.1 Traditional routing in mobile networks.. 57
Figure 5.2 GTT routing scheme.. 57
Figure 5.3 Signaling protocol stack for international roaming... 58
Figure 5.4 Mobile GT translated from IMSI and MSISDN... 60
Figure 5.5 Registration and location update with mobile GTT function.............................. 62
Figure 5.6 Mobile terminated call with mobile GTT function... 63
Figure 5.7 NV configuration and call flow scenario... 65
Figure 5.8 Pre OMA calls routing... 66
Figure 5.9 Post OMA calls routing.. 67
Figure 5.10 OMA algorithm for MSRN allocation.. 68
Figure 6.1 Setup and simulated network.. 72
Figure 6.2(a) Bandwidth vs. Packet Drop; Uplink Single TRX site.. 74
Figure 6.2(b) Bandwidth vs. Packet Drop; Downlink Single TRX site...................................... 75
Figure 6.2(c) Bandwidth vs. Jitter; Uplink Single TRX site.. 75
Figure 6.2(d) Bandwidth vs. Jitter; Downlink Single TRX site... 76
Figure 6.3(a) Bandwidth vs. Packet Drop; Uplink Multi-TRX site.. 76
Figure 6.3(b) Bandwidth vs. Packet Drop; Downlink Multi-TRX site....................................... 77
Figure 6.3(c) Bandwidth vs. Packet Jitter; Uplink Multi-TRX site…... 77

Figure 6.3(d) Bandwidth vs. Jitter; Downlink Multi-TRX site.. 78
Figure 6.4(a) Bandwidth vs. Packet Drop; Uplink Multi-BTS site.. 78
Figure 6.4(b) Bandwidth vs. Packet Drop; Downlink Multi-BTS site…................................... 79
Figure 6.4(c) Bandwidth vs. Jitter; Uplink Multi-BTS site... 79
Figure 6.4(d) Bandwidth vs. Jitter; Downlink Multi-BTS site... 80
Figure 7.1 Proposed network architecture.. 85
Figure 7.2 Proposed network signaling and layer Architecture... 85
Figure 7.3 SIGTRAN implementation in SeaNet IP GRAN... 87
Figure 7.4 Test setup.. 88
Figure 7.5 Message switching association configurations.. 91
Figure 7.6 An SCTP Association.. 92
Figure 7.7 SCTP Packet format.. 92
Figure 7.8 SCTP association establishment 1.. 93
Figure 7.9 SCTP association establishment 2.. 94
Figure 7.10 SCTP association establishment 3.. 95
Figure 7.11 SCTP data transfer... 96
Figure 7.12 SCTP path heartbeat.. 96
Figure 7.13 SCTP shutdown procedure.. 97
Figure 7.14 SUA routing... 97
Figure 7.15 Calling and called party in SCCP.. 98
Figure 7.16 RTP transport model.. 123

List of Tables

Table 3.1 M2PA and M2UA comparison........ 41
Table 3.2 M3UA and SUA comparison........ 45
Table 4.1 Statistical multiplexing gain........ 48
Table 6.1 Additional Bandwidth required for lowering packet drop from 5% to 1%........ 81
Table 6.2 Bandwidth requirements........ 82
Table 6.3 Downlink signaling bandwidth requirements for case-1 and in-fill sites........ 83
Table 7.1 SeaNet AB MCC and MNC........ 89
Table 7.2 Signaling Aggregator Parameters........ 89
Table 7.3 Media Gateway Parameters........ 89
Table 7.4 Integrated MSC/VLR/BSC Parameters........ 90
Table 7.5 Subsystem numbers and their functions........ 98
Table 7.6 SUA and SCCP-user supported primitives........ 109
Table 7.6 Latency in satellite link........ 128

List of acronyms and abbreviations

ASG	Access Service Group
AUC	Authentication Center
ACM	Address Complete Message
ANM	Answer Message
BCCH	Broadcast Control Channel
BSC	Base Station Controller
BTS	Base Transceiver Stations
BSS	Base Station Subsystem
ChanSrv	Channel Server
ConnSRv	Connection Server
CC	Country Code
DstRI	Destination Routing Identifier
DstGT	Destination Global Title
DTX	Discontinuous Transmission
DPC	Destination Point Code
EIR	Equipment Identity Register
FISU	Fill-In Signal Units
GMSC	Gateway MSCs
GT	Global Title
GRAN	GSM Radio Access Netwrok
HLR	Home Location Register
ISUP	ISDN User Part
IM	Interworking Manager
IR	International Roaming
IMAS	Integrated Mobile Access System
INAP	Intelligent Network Application Part
ISC	International Switching Center
HLR	Home Location Register
ISUP	ISDN User Part
IM	Interworking Manager
IR	International Roaming
INAP	Intelligent Network Application Part
ISC	International Switching Center
IAM	Initial Address Message
IMSI	International Mobile Subscriber Identity
ISO	International Standards Organization
LAC	Location Area Code
LA	Location Area
LAI	Location Area Identity
LAPD	Link Access Protocol-Channel D
LSSU	Link Status Signal Units
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
MSRN	Mobile Subscriber Roaming Number
MSGX	Message Switing
MSC	Mobile Switching Center

MAP	Mobile Application Part
MSISDN	Mobile Subscriber ISDN Number
MS	Mobile Station
MO	Mobile originated
MM	Mobility Management
MT	Mobile Terminated
MSIN	Mobile Subscriber Identification Number
MGC	Media Gateway Controller
M2UA	MTP2 User Adaptation Layer
M3UA	MTP Level 3 User Adaptation Layer
MSU	Message Signal Unit
NDC	National Destination Code
NSS	Network Switching Subsystem
NV	Network Virtualization
OMA	Optimized MSRN Assignment
OSI	Open System Interconnection
OPC	Origination Point Code
OMSS	Operation and Maintenance Subsystem
PLMN	Public Land Mobile Network
PRN	Provide Roaming Number
PSTN	Public Switching Telephone Network
PSN	Packet Switched Network
RTP	Real-Time Transport Protocol
REL	Release Message
RDD	Roamer Direct Dialing
RLC	Release Complete Message
RTNR	Real Time Network Routing
RF	Radio frequency
SIGTRAN	Signaling Transport
SDCCH	Stand-alone Dedicated Control Channel
SG	Signaling Gateway
SUA	SCCP User Adaptation Layer
SLDP	Signaling Link Probing Daemon
SIM	Subscriber Identity Module
SPC	Signaling Point Code
SrcRI	Source Routing Identifier
SrcGT	Source Global Title
SRI	Send Routing Information
SS7	Signaling System No.7
SSP	Service Switching Point
STP	Signal Transfer Point
SMSS	Switching and Management Subsystem
SCP	Service Control Point
SSN	Subsystem Number
SCCP	Signaling Connection Control Part
TMSI	Temporary Mobile Subscriber Identity
TRX	Transceiver
TCAP	Transaction Capabilities Applications Part
TDM	Time Division Multiplex
TCP/IP	Transfer Control Protocol / Internet Protocol
TDMoIP	TDM over IP

UCS	User Call Server
VAD	Voice activity detection
VLSI	Very-large-sclae integration
VLR	Visited Location Register

1. Introduction

The innovative Internet Protocol (IP)-radio access network (RAN) (hence forth abbreviated as IP-RAN) architecture proposed in thesis work is based upon utilizing IP in both core and cellular networks, specifically the radio access network (RAN). Unlike traditional cellular network infrastructure architectures that use proprietary protocols and mandate a strict Radio Node (RN) to Radio Network Controller (RNC) hierarchy, the proposed IP-RAN architecture uses IP to enable each RN to communicate with multiple RNCs. This one-to-many relationship between RNs and RNCs facilitates scaling, provides inherent reliability, and minimizes the bottlenecks found in traditional architectures.

The proposed architecture uses IP rather than proprietary protocols for communication protocol between Base Transceiver Stations (BTS), Base Station Controllers (BSC), and the Network Switching Subsystem (NSS) of the radio access network (RAN). This architecture delivers carrier-grade mobility, scalability, and reliability, is optimized for efficient signaling/call routing and reduces both capital and operational costs in comparison to proprietary protocol-based alternatives. The 3GPP standards have defined the framework for wireless next generation networking under the title, "Bearer Independent Core Networks (BICN)"; which allows the use of a packet switched network instead of circuit switching even for voice services. BICN defines a physical separation of the control and bearer planes [17]. Conceptualizing the principles of BICN, this thesis adopts softswitching to propose a IP-RAN network architecture by splitting the control (signaling) and user plane (bearer in network element), in order to guarantee more optimal placement of network elements within the network.

This thesis proposes the evolution of TDM-based networks to packet-based networking and implements the proposals of the second generation Advanced Telecommunications Computing Architecture (ATCA) technology to provide a true softswitching topology that includes all the necessary ingredients for a high-density, carrier-grade GSM Radio Access Network (GRAN) that can seamlessly scale to reasonable capacities.

In a traditional RAN architecture, proprietary communication protocols are used over Time Division Multiplexed (TDM) links that connect BTS to the BSC and Base Station Subsystem (BSS) to the NSS. A strict BSS to NSS hierarchy is maintained. Complex, proprietary protocols are then used for communication between the network nodes. Most GSM networks in operation today use this type of architecture [18].

In an IP-GRAN environment as proposed in this thesis, IP-enabled BTS is referred to as Radio Nodes (RN), which communicates with the BSC, referred to as Radio Network Controllers (RNC); using IP as the transport protocol. Operating costs are reduced because backhaul traffic can now be carried over low-cost transport using IP in comparison to traditional TDM (such as E1 or T1) transport. One specific supporting cause for adapting IP-based transport is that there is no longer a need to provide a synchronous network over a large area and thus one avoids the expense of clock distribution and the need for keeping everything synchronized! The entire backhaul transport network can be built using standard, off-the-shelf IP switches and routers [1]. Additionally IP switches and routers (of a given aggregate data rate) are generally much cheaper than the E1 or T1 equipment as the production volumes are much higher and hence the prices are lower. This is also helped by the very large number of vendors, the use of Very-large-scale integration (VLSI) to decrease costs on a Moore's Law curve, and the open nature of the standards which facilitates large numbers of developers & vendors.

The proposed network architecture is based on the concepts of 3GPP's BICN architecture and supports voice over IP in the bearer plane and SIGTRAN (see section 3.4) in the control plane. The idea is to apply packet switching and transport instead of traditional circuit switching in order to consolidate all services and layers onto a single scalable packet infrastructure.

This thesis work embraces the vision of an All-IP converged network; so that mobile telephony is implemented as an IP application in the same way as any other IP based application. This should enable:

- IP transport and routing of all media packets.
- IP transport and routing of signaling (using SIGTRAN).
- Consolidation of voice core transport and routing onto a common IP core.
- Ease in internetworking with the 3GPP IMS architecture (though not discussed in the report as the topic is beyond the scope of this thesis work).

The migration of mobile wireless networks to IP has already begun. The proposed IP-GRAN architecture creates a high performance network infrastructure that can be deployed quickly and cost-effectively to provide a foundation which readily supports the ongoing evolution of the network. Such IP-RAN architecture brings IP into the RAN in order to optimize performance, reliability and scaling. This network simplification allows an operator to support all applications including voice, data, and management on a common packet core infrastructure. The proposed architecture provides a complete IP enabled GSM network solution that is high-density, carrier-grade, and can scale seamlessly to meet growing network capacity requirements without adding growth-related complexity to the network.

1.1 Problem Statement

Telecommunication operators are facing considerable and growing competition for their key service, voice telephony. Competition comes not only from other telecommunication operators but also from an ever-growing number of low-cost operators offering IP based converged services. To address this threat, operators must drastically reduce service delivery costs and at the same time ensure service guarantees. Legacy circuit-switched networks are not cost efficient due to their integrated call control (signaling) and switching architecture; thus, for a service provider it becomes essential to identify a more efficient process for equipment location, updates, and voice termination into peer (often incumbent) carrier networks. Considering, for example, the scenario of inbound roaming; routing calls to a roaming mobile can be very inefficient in utilization of trunks and switching resources.

Rectifying this situation involves 'thinking before doing' in order to clearly envisage the goal; which is where is the target terminal and what is the best way to route the media traffic to it? This thesis tries to achieve the vision of All-IP converged network; thus addresses the problem of routing both voice and signaling efficiently to the location of the most appropriate operator's point of presence.

1.2 Proposed Solution

The proposed solution realizes an All IP converged network. IP is used as the transport protocol in the radio network to realize an IP-GRAN. The following chapters of the thesis will introduce the basic elements of a GSM system (chapter 2), describe the underlying technology (chapter 3), introduce the propose architecture and its implementation (chapter 4), describe how this architecture enables system optimization (chapter 5), testing and evaluation of this new architecture (chapter 6), and some conclusions and future (chapters 7 and 8). The proposals of this thesis emphasis on the remote service areas; specifically maritime GSM network, as that is the core business area of the industrial sponsors of this thesis work, SeaNet AB.

Chapter 4 will also discuss the IP-GRAN network architecture in context of micro-mobility but defaults to use traditional Mobile IP schemes for mobility management. Our proposal for a IP-GRAN system architecture hinges on the assumption that most user mobility is local to a domain, in particular, an administrative domain of the network. Therefore, to achieve optimized routing and forwarding, this thesis work proposes to use Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) for more efficient support of intra-domain mobility.

This thesis discusses system optimization in Chapter 5 with reference to call routing scenarios for roaming subscribers, especially international inbound roamers. Roaming cost has gained significant importance amongst the international regulatory authorities and the recent EU directive in this matter strengthens our stand to include the technical proposals around the same in our thesis work.

Chapter 6 of this report emphasizes on the factors influencing the dimensioning of the link, by taking into consideration a system which uses the IP network in order to deliver voice and signaling to a GSM radio access network.

Chapter 7 of this report constitutes test procedures, their explanation and significance; and detailed presentation of process flows required for the design, implementation, and performance evaluation of an operational IP-GRAN. The scope of performance evaluation, as defined by the industrial sponsor of this thesis work; SeaNet AB, does not require a comparison with legacy GSM network or statistical presentation of data; but rather a operational feasibility study of a working prototype, hence real-time data were acquired and analyzed from this prototype.

2. GSM System Architecture

2.1 Overview

GSM networks are structured hierarchically. A given public land mobile network (PLMN) consists of at least one administrative region, which is controlled by a Mobile Switching Center (MSC). Each administrative region is made up of at least one Location Area (LA) which is also often called the visited area (in the case of a roaming terminal). Each LA consists of cell groups (where each cell is associated with a single BTS) and each cell group is assigned to a BSC. Therefore for each LA there exists at least one BSC in generic system architecture of a GSM PLMN [28]. The combined traffic of the mobile stations in their respective cells is routed through a switch, the MSC. Calls originating from or terminating in the fixed network are handled by a Gateway Mobile Switching Center (GMSC).

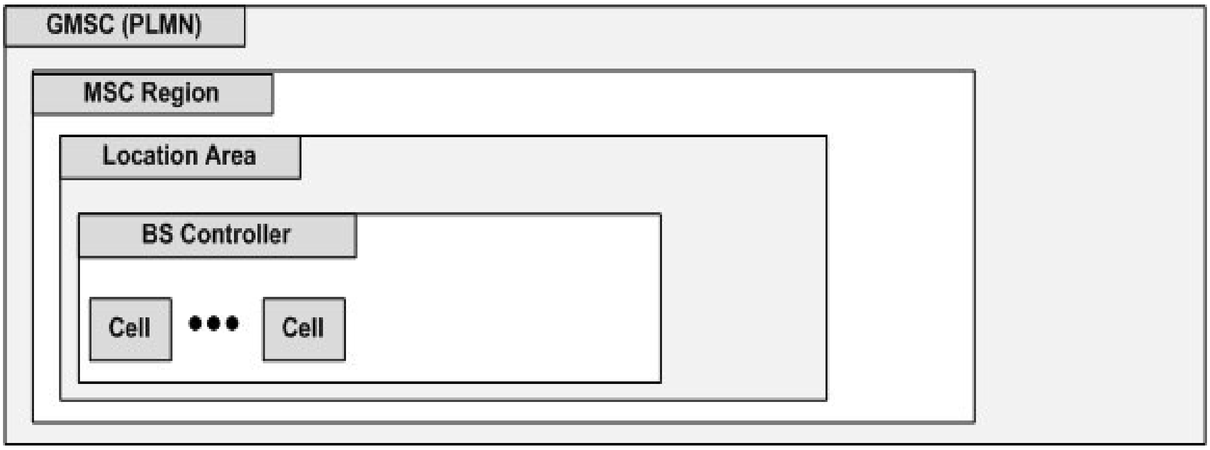


Figure 2.1: GSM system architecture

A set of databases are used to provide call control and network management. These databases are as follows:

- **Home Location Register (HLR)**

  Maintains permanent data (such as user's service profile) as well as temporary data (such as user's current location) for currently registered subscribers. When a user is called, the HLR is queried to determine the user's current location. To reduce the load on HLR, the VLR was introduced to support the HLR by handling many of the subscriber-related queries, such as localization and approval of available features. The HLR continues to deal with tasks that are independent of a subscriber's location.

- **Visited Location Register (VLR)**
  Maintains data of subscribers who are currently in its area of responsibility. Scalability is ensured because there is normally a VLR per MSC. While the HLR is responsible for more static data, the VLR provides dynamic subscriber data management, including caching some of the permanent subscriber data from the HLR for faster access. When a subscriber moves from one location area to another, data are passed between the VLR of the location area the subscriber is leaving to the VLR are of the location being entered; within an operator's network the old VLR transfers the relevant data to the new VLR. When a subscriber roams to a foreign network, the new VLR has to query the subscriber’s HLR for the necessary data.

- **Authentication Center (AUC)**
  Generates and stores security-related data such as keys used for authentication and encryption.

The exact partitioning of the service area, its organization or administration with regard to LAs, BSCs, and MSCs is, however, not uniquely determined and thus has many possibilities for optimization.

2.2 System Architecture

The GSM system has two distinct functions: signaling (for the network operations) and user data traffic. The various subnetworks, called subsystems in the GSM standard, are grouped under three major systems: the radio network, the mobile switching network, and the management network [19]. These three subsystems are the Base Station Subsystem (BSS), the Switching and Management Subsystem (SMSS) or Network Switching Subsystem (NSS), and the Operation and Maintenance Subsystem (OMSS). The BSS and the NSS are discussed in the following sections, where the focus is on their function within the context of this thesis.

2.2.1 Radio Network - Base Station Subsystem (BSS)

All radio-related functions are performed in the BSS, which consists of base station controllers (BSCs) and the base transceiver stations (BTSs).

BSC The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC.

BTS The BTS handles the radio interface to the mobile station. The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTSs are controlled by a BSC.

Figure 2.2 shows the components of the GSM radio network. A GSM cell is the radio coverage area of a BTS; transmitter + receiver = transceiver. The BTS provides the radio channels for signaling and user data traffic in this cell. Thus, a BTS is the network part of the GSM air interface. Besides the radio frequency part (transmitter and receiver equipment) it contains additional components for signal and protocol processing. In order to keep the base stations small, the essential control functions such as handover reside in the BSC. BTS and BSC together form the Base Station Subsystem (BSS). Several BTSs can be controlled together by one BSC (Figure 2.2). Two kinds of channels are provided at the radio interface: traffic channels and signaling channels. BSS handles all of the functions of OSI layer 1. Since otherwise the BTS could not communication with the MS.

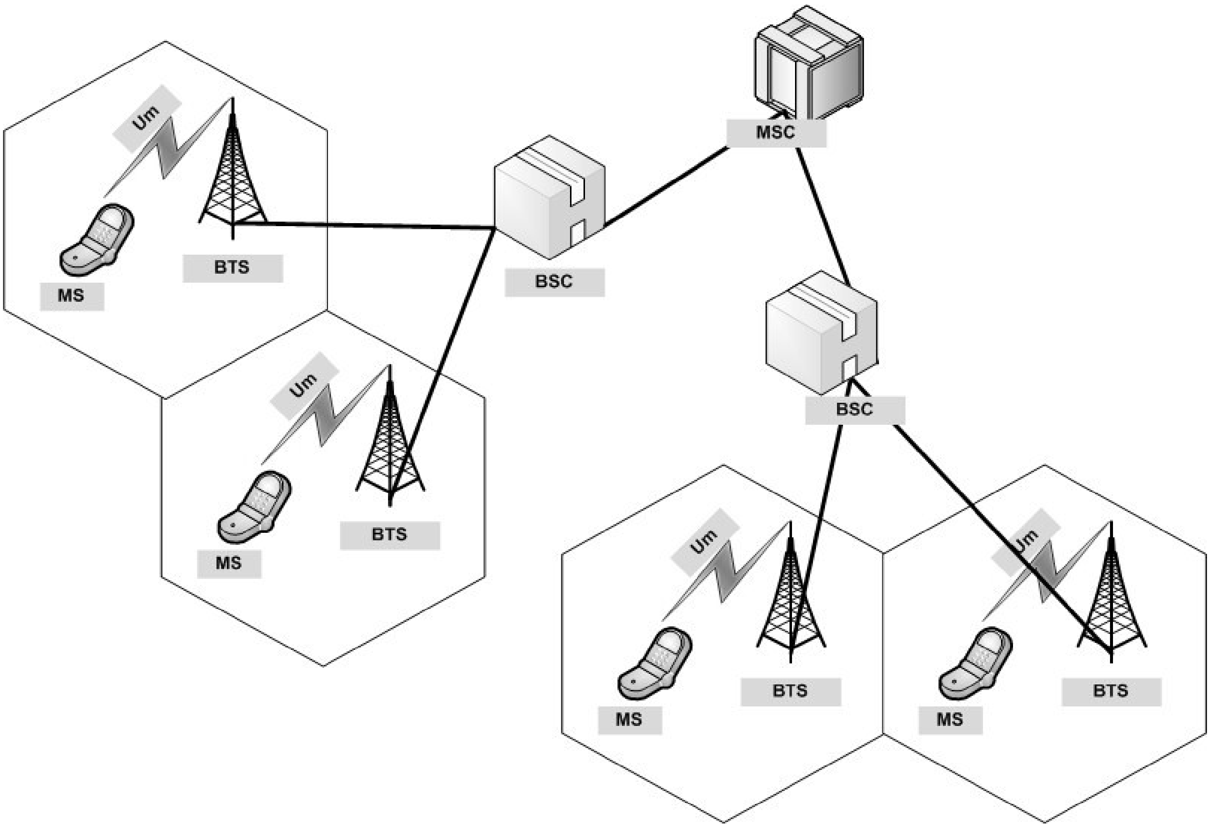


Figure 2.2: Components of a GSM radio network

2.2.2 Mobile Switching Network (MSN) / Network Switching Subsystem (NSS)

The Mobile Switching and Management Subsystem (SMSS) or, the Network Switching Subsystem (NSS) consists of the mobile switching centers and the databases which store the data required for routing and service provision (Figure 2.3) [29]. The NSS carries out switching functions and manages the communications between the cellular network and the Public Switched Telephone Network (PSTN); thus allowing mobile phones to communicate with each other and with telephones in the wider telecommunications network.

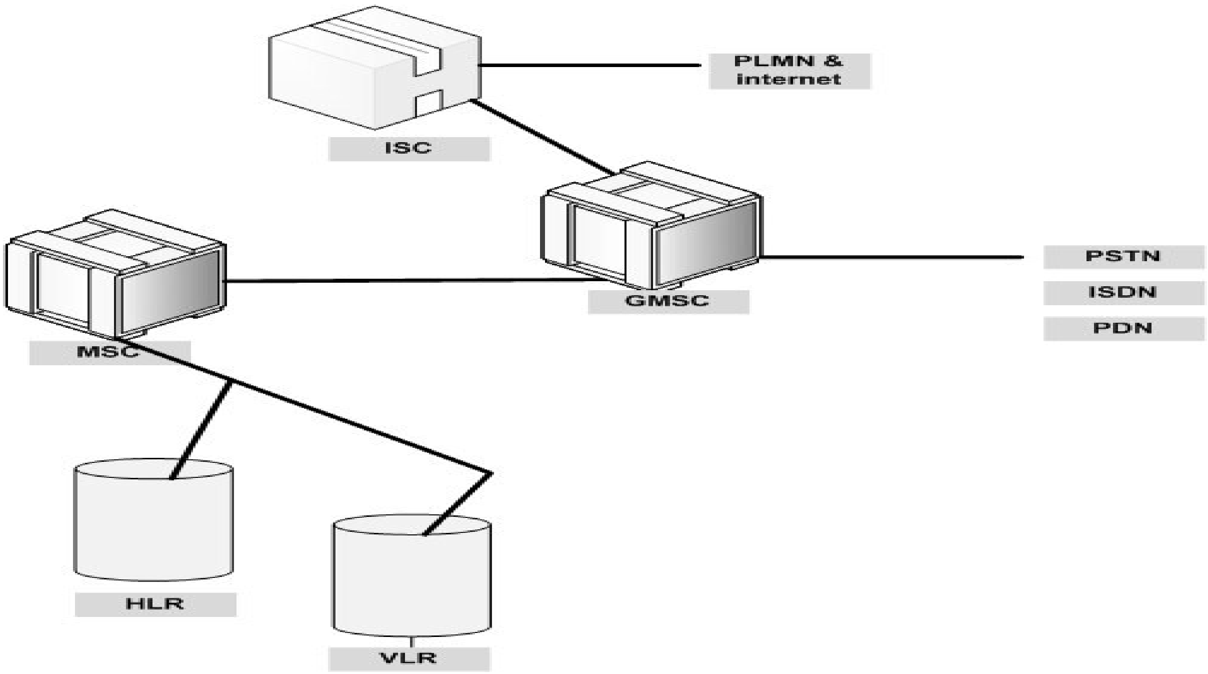


Figure 2.3: Components of the GSM mobile switching network

- **Mobile Switching Center (MSC)**

  The switching node of a GSM network is the Mobile Switching Center (MSC). The MSC performs all the switching functions of a fixed-network switching node, e.g. routing path search, signal routing, and service feature processing, but is more sophisticated in nature. The main difference lies in the fact that the MSC also has to consider the allocation and administration of radio resources and perform mobility management. The MSC therefore has to provide additional functions for location registration of subscribers and for the handover of a connection when a mobile station moves from cell to cell [29].

  MSCs are categorized differently in different contexts, reflecting their complex role within the network. All of these terms could refer to the same physical MSC, but reflect the separate functions which it may need to perform.

- **Dedicated Gateway MSC (GMSC)**

  Pass voice traffic between a mobile network and one or more fixed networks. For an incoming call, the GMSC determines which visited MSC a subscriber who is being called is currently associated with. It also interfaces with the Public Switched Telephone Network. Mobile calls to PSTN and PSTN to mobile calls are routed through a GMSC. Mobile-to-mobile calls within this operator's network simply go through the relevant MSC(s). Mobile-to-mobile calls where the subscribers are in different operators networks will have to go through a GMSC. A GMSC requests the routing information from the HLR in order to route the connection to the local MSC in whose region the mobile station is currently registered.

  An operator may design a network so as not to have any BSS connected to a MSC. Such an MSC will be the Gateway MSC for many of the calls it handles. Routing to the other international networks is done by an International Switching Center (ISC) for the respective country.

- **MSC Server (MSC-S)**

  The MSC Server (MSC-S) is a part of the redesigned MSC concept introduced in 3GPP Release 5 and is a softswitch variant of a Mobile Switching Centre. The MSC Server functionality enables a split between control (signaling) and user plane (Media Gateway; bearer in network element), thus enabling more optimal placement of network elements within the network. The MSC Server and Media Gateway makes it possible to cross-connect traditional circuit switched calls, switched by using TDM over IP.

  Note that as this thesis primarily focuses on the use of softswitching and the associated network components to provide efficient signaling flow and call routing (details of softswitching can be found in section 4.3).

- **Home and Visitor Registers (HLR and VLR)**

  A GSM network utilizes several databases (as outlined in section 2.1). The HLR and VLR communicate with the MSC and constitute towards outlining a NSS. In general, there is one central HLR per GSM network and one VLR for each MSC.

The HLR stores all permanent subscriber data, including the IMSI (International Mobile Subscriber Identity) and MSISDN (Mobile Subscriber ISDN Number in 3GPP terminology). In addition to storing information about the subscriber's subscriptions and permissions, the HLR also contains a pointer to the current location of the mobile station, thus making the HLR as the central location register. This is used for routing the subscribers, for which this HLR has administrative responsibility.

The VLR, as temporary database of the subscribers, stores data associated with all mobile stations that are currently staying in the administrative region of the associated MSC. Each BTS in conjunction with a BSC in the network is served by exactly one VLR; hence a subscriber cannot be present in more than one VLR at a time. The data stored in the VLR has either been received from the HLR, or collected from the Mobile Station (MS). Mobile stations when roaming freely, depending on their current location, may be registered in the VLR of their home network or in a VLR of a "foreign" network (if there is a roaming agreement between both network operators)[29].

The primary functions of the VLR are:

- To inform the HLR that a subscriber has arrived in the particular region served by the VLR.
- To track where the subscriber is within the VLR area (location area) when no call is ongoing.
- To allow or disallow which services the subscriber may use, based on the data received from the HLR of subscriber's home network.
- To allocate Mobile Station Roaming Number (MSRN) during the processing of incoming calls.
- To delete the subscriber record when a subscriber explicitly moves to another region, as instructed by the HLR [18, 29].
- The VLR, though not as its primary function, to control the size of its database; purge the subscriber record if a subscriber becomes inactive whilst in the area of a VLR. The VLR deletes the subscriber's data after a fixed time period of inactivity and informs the HLR (e.g. when the phone has been switched off and left off or when the subscriber has moved to an area with no coverage for a long time).

2.3 Mobility and Switching

International standardization of GSM enables subscribers to move freely not only within their home networks but internationally. Ideally, the subscribers can get access to the special services they subscribed to in their home network, provided there are suitable agreements between the operators. The functions needed for this roaming are called mobility functions and they rely mostly on the Session Management-specific extensions to Signaling System Number 7 (SS7). These extensions are called the Mobile Application Part.

The Mobile Application Part (MAP) procedures relevant for roaming are:

a. Location Registration/Update
b. IMSI Attach/Detach
c. Requesting subscriber data for call setup
d. Paging

The relevant MAP entities for roaming services reside in the MSC, HLR, and VLR. The most important functions of GSM Mobility Management are:

a. Location Registration with the PLMN,
b. Location Updating to report the current location of an MS, and
c. The identification and authentication of subscribers.

These actions are closely interrelated and the mobility data is needed for routing and switching of user connections and for the associated services.

2.3.1 Location Update

Before a mobile station can be called or access services, the subscriber has to register with the mobile network (PLMN). This can either be the home network (where the subscriber has a service contract) or a foreign network provider in whose service area the MS is currently visiting, provided there is a roaming agreement between the two network operators. Registration is only required if there is a change of networks. When the MS changed networks, the VLR of the new network needs to assign a temporary mobile subscriber ID (TMSI) to this subscriber. In order to do so, the subscriber informs the current network of his IMSI and receives a new TMSI by executing a Location Registration procedure. This TMSI is stored by the MS in its nonvolatile storage, such that even after a power-down and subsequent power-up only a normal Location Updating procedure is required [25].

Scenario: Roaming to a foreign network - this involves a change in both location area (LA) and VLR.

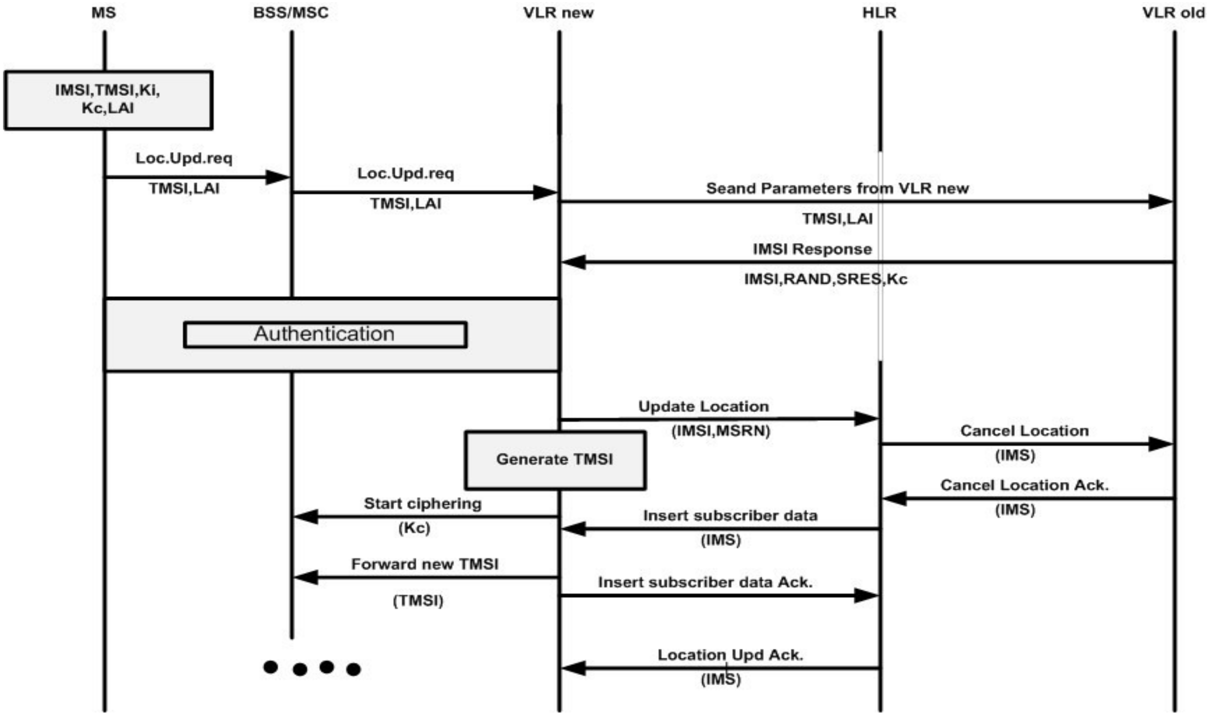


Figure 2.4: Location update after changing the VLR area

Process: The new VLR requests the identification and security data for the MS from the old VLR through the HLR and stores them locally. Only in specific cases, if the old VLR cannot be determined from the old location area identifier (LAI) or if the TMSI is not known in this VLR, then the new VLR may request the IMSI directly from the MS (i.e., initiate the identification procedure). Only after a mobile station has been identified and after the security parameters are available in the new VLR, is it possible for the mobile station to be authenticated and registered in the new VLR, which assigns a new TMSI, and the location information in the HLR is updated. After successful registration in the new VLR (location update accept) the HLR instructs the old VLR to delete its location information about this MS (cancel location)[29].

The location information is stored in the HLR as a MSRN. This MSRN contains the routing information needed for incoming calls, using this information incoming calls are routed to the MS's current MSC. In this scenario, all routing information is transferred to the HLR at the time of a location update. Alternatively, the HLR may simply store the current MSC and/-or VLR in connection with a Local Mobile Subscriber Identity (LMSI), and the actual routing information only determined at the time of an incoming call.

Note that the LMSI is an optional parameter that the VLR assigns to a subscriber on a temporary basis so as to speed-up the search for subscriber data. At the time of location update, the VLR allocates a LMSI and send the same to the HLR together with the IMSI. The HLR simply uses the LMSI to include it together with the IMSI in all messages sent to the VLR concerning a MS.

2.3.2 Call Routing

Scenario: The number dialed (an MSISDN) to reach a mobile subscriber contains no information about the current location of the mobile subscriber. In order to establish a successful connection between the caller and the current location of the mobile subscriber, however, one must determine the current location and the switch responsible for serving the mobile subscriber in their current location.

Process: In order to be able to route the call to this switch, the routing address for this subscriber (MSRN) has to be obtained. This routing address is assigned temporarily to a subscriber by its currently associated VLR. When a call arrives at the GMSC, the HLR is the only entity in the GSM network which can supply this information; therefore it must be interrogated for each connection setup to a mobile subscriber. The principal sequence of operations for routing to a mobile subscriber is shown in Figure 2.5.

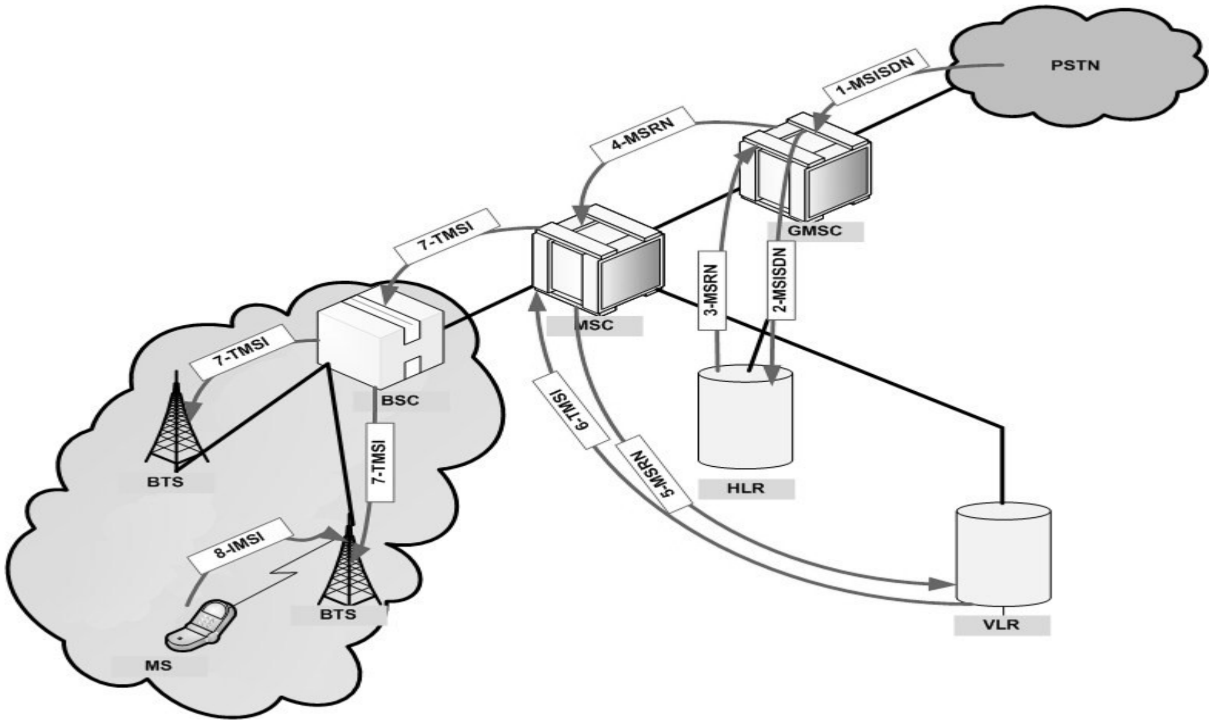


Figure 2.5: Routing calls to a mobile station

a. An ISDN switch analyzes the MSISDN and based on the CC and NDC in the MSISDN can forward the call to the GMSC of the subscriber's home PLMN (step 1).
b. This GMSC can now determine the MSRN for the mobile subscriber by querying the HLR using the MAP (steps 2 and 3).
c. Using the MSRN, the call is forwarded to the local MSC (step 4), which obtains the TMSI of the subscriber (steps 5 and 6) and initiates the paging procedure in the current location area of the mobile station (step 7).
d. After a response to the paging of the mobile station (step 8), the connection can be established [29].

Depending on the capabilities of the associated switching center (whether the call is national or international) and depending on how the MSRN was assigned and stored; several variants for determining the route and interrogating the HLR exist. The following scenarios describe the national or international cases:

a. Routing for national MSISDN

In general, the local switching center analyzes the MSISDN (The analysis of the MSISDN simply identifies the gateway of the subscriber's current network operator) and then interrogates the HLR responsible for this MSISDN (HLR in the home PLMN of the subscriber) to obtain the routing information (Figure 2.6a). The connection can then be established via fixed connections of the ISDN directly to the MSC [29].

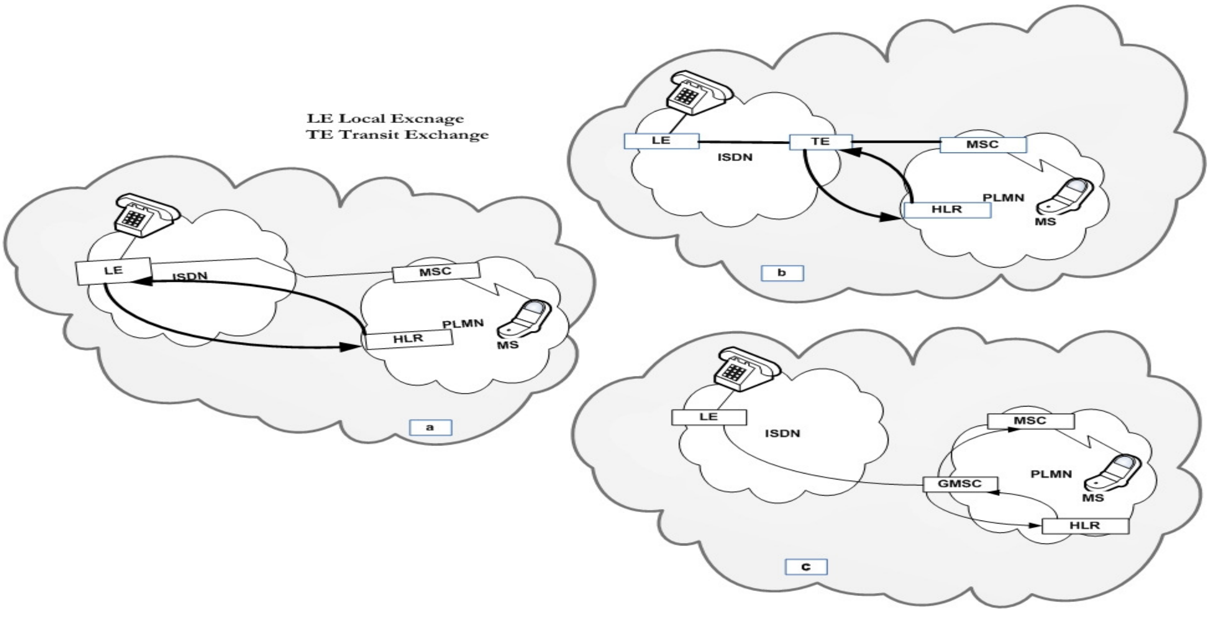


Figure 2.6: Routing variants for national MSISDN

If the local exchange does not have the required protocol intelligence for the interrogation of the HLR, the connection can be passed on preliminarily to a transit exchange, which then assumes the HLR interrogation and routing determination to the current MSC (Figure 2.6b) [29].

If the fixed network is not at all capable of performing an HLR interrogation, the connection has to be directed through a GMSC. This GMSC connects through to the current MSC (Figure 2.6c) [29].

Note that for all the previous three cases, the mobile station could also reside in a foreign PLMN (roaming); the connection is then made through international lines to the current MSC after interrogating the HLR of the home PLMN.

b. Routing for international MSISDN

In this case, the local exchange recognizes only the international country code (CC) and directs the call to an International Switching Center (ISC). The ISC can recognize the National Destination Code (NDC) of the mobile network and process the call accordingly. Figures 2.7 and 2.8 show examples for the processing of routing information [29].

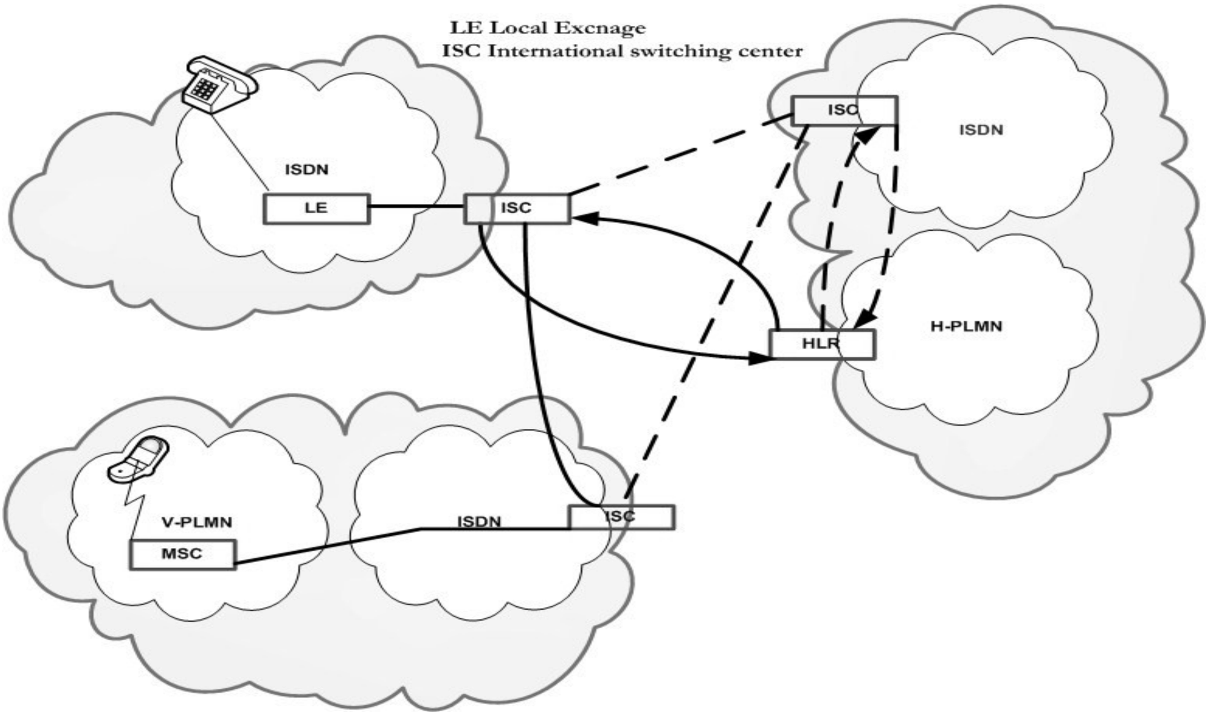


Figure 2.7: Routing for international MSISDN (HLR interrogation from ISC)

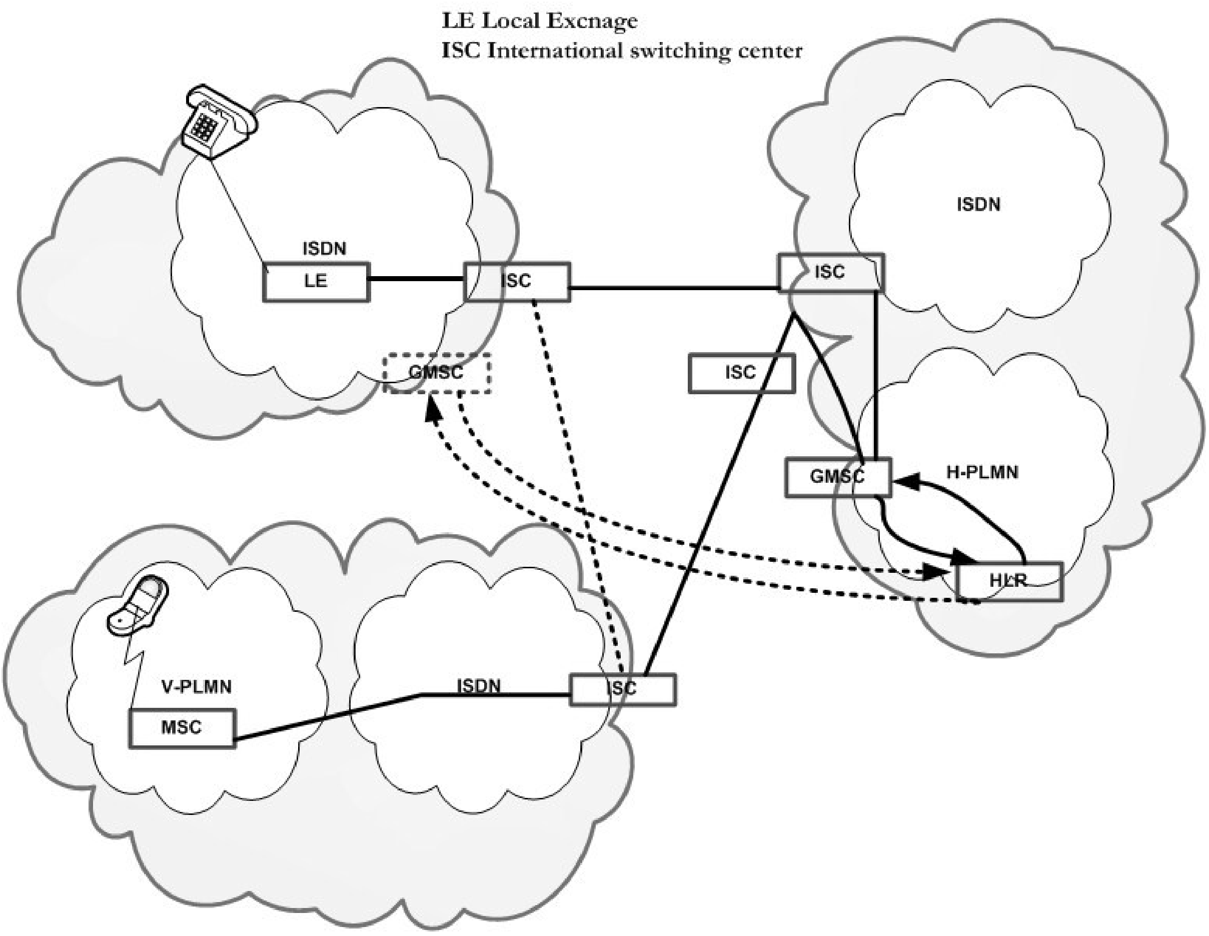


Figure 2.8: Routing through GMSC for international MSISDN

An international call to a mobile subscriber involves at least three networks:

i. The operator's network in the country from which the call originates;
ii. The operator's network in the country with the home PLMN of the subscriber, Home PLMN (H-PLMN); and
iii. The operator's network in the country in which the mobile subscriber is currently roaming, the Visited PLMN (V-PLMN).

In general, the traffic between countries is routed through ISCs; though might not be applicable in case of the operators who have networks in many countries and would not like to route traffic for between their own subscribers via an ISC (optimizing interconnections). This would require switched networks to possess Real Time Network Routing (RTNR) capabilities.

Considering that the traffic is routed through the ISC and depending on the capabilities of the ISC, there are several routing variants for international calls to mobile subscribers. If the ISC performs the HLR interrogation, the routing to the current MSC is performed either by the ISC of the originating call or by the ISC of the mobile subscriber's H-PLMN (Figure 2.7). If no ISC can perform the routing, a GMSC has to be involved, either a GMSC in the country where the call originates or the GMSC of the H-PLMN (Figure 2.8) [5, 18].

2.3.3 MSRN Assignment and Routing

There are two ways to obtain the MSRN:

- Obtaining the MSRN at the time of the location update: In this scenario, an MSRN for the mobile station is assigned at the time of each location update, it is then stored in the HLR. Thus the HLR can immediately supply the routing information needed to switch a call to the local MSC.
- Obtaining the MSRN on a per call basis: The HLR simply knows the identity of the currently responsible VLR. In this case, when routing information is requested from the HLR, the HLR first obtains the MSRN from the currently responsible VLR. This MSRN is assigned on a per call basis, i.e. each call involves a new MSRN assignment.

2.3.4 Call Establishment

The establishment of a connection always requires a verification of the user's identity (i.e., authentication) independent of whether it is a mobile-originated (MO) call setup or a mobile-terminated (MT) call setup. This authentication is performed in the same way as for location updating. The VLR supplements its database entry for this MS with a new set of security data, which replaces the earlier three tuple (RAND, SRES, Kc) [for details about these see [18]]. After successful authentication, the ciphering process for the encryption of user data can start [21, 29].

2.3.4.1 Mobile Originated Call Setup

For Mobile-originated (MO) connection setup (see Figure 2.10), the mobile station makes a connection request to the MSC via a setup indication message, which is a pseudo-message [identify groups of messages]. When the MSC receives the message CM-Service (Call Management) request message from the MS, setup indication message is exchanged between the Mobility Management (MM) entity of the MSC and the MAP entity, indicating a request for an MM connection (see Figure 2.9).

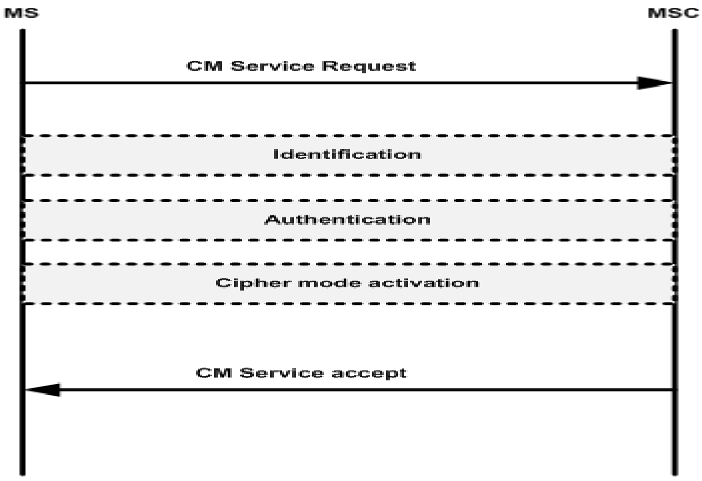


Figure 2.9: MM connection establishment

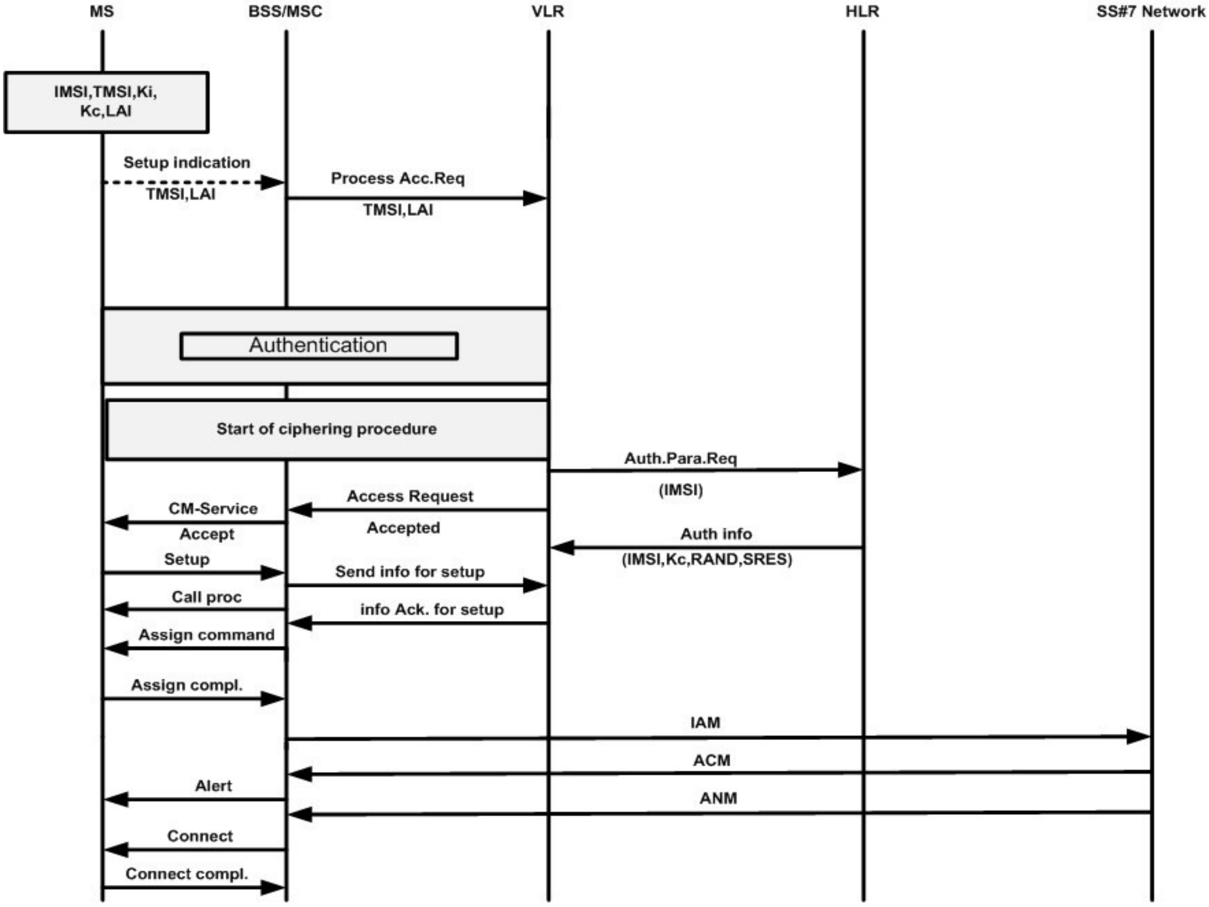


Figure 2.10: Overview of outgoing call setup

Next the MSC signals to the VLR that the mobile station identified by the temporary TMSI in the location area LAI has requested service access (a Process Access request) which is an implicit request for a random number (RAND) from the VLR. . This random number is needed to start the authentication of the MS. This random number is transmitted to the mobile station, which responds with an authentication result (SRES) to the VLR. This VLR now examines this SRES to match it against the SRES which it received from the Authentication Center to determine the authenticity of the mobile station's identity [18, 29].

The ciphering process begins on the air interface after successful authentication, thus the MM connection between MS and MSC will be established (CM-Service accept) via an encrypted link. From this point on all signaling messages are sent in encrypted form. At this point the MS indicates the desired calling target (i.e., the callee's MSISDN) [18, 21, 29].

Once the MS is informed with a call proceeding message that processing of its connection request has started, the MSC reserves a channel for the conversation (user data) and assigns it to this MS (ASSIGN message). The connection request is signaled to the remote network via SS7 using the ISDN User Part (ISUP) message, the Initial Address Message (IAM). When the remote network answers with an Address Complete Message (ACM), the delivery of the call can be indicated to the MS (ALERT message). Finally, when the called party goes off-hook, the connection can be switched through (i.e., with CONNECT, ANS, CONNECT ACKNOWLEDGE messages) [29].

2.3.4.2 Mobile Terminated Call Setup

For incoming i.e., a mobile terminated (MT), connection setup, only the identification of the MSC is really needed in order to route the call to the currently responsible MSC. A call to a mobile station is therefore always routed to an entity which is able to interrogate the HLR for the current routing information in order to forward the call to the relevant MSC. Usually, this entity is a GMSC of the home PLMN of the MS. This GMSC obtains the current Mobile Station Roaming Number (MSRN, an E.164 defined telephone number) of the mobile station by querying its HLR and forwards the MSRN to the current MSC (see Figure 2.11) [29].

Two variants of HLR interrogation occurs depending on whether the MSRN is stored in the HLR or has to be determined by the serving VLR:

a. The interrogated HLR can supply the MSRN directly (routing information).

b. The interrogated HLR has only stored the address of the serving VLR, that it obtained due to the location update. Therefore, the HLR first has to request the current routing information from the serving VLR before the connection to the MS can be established.

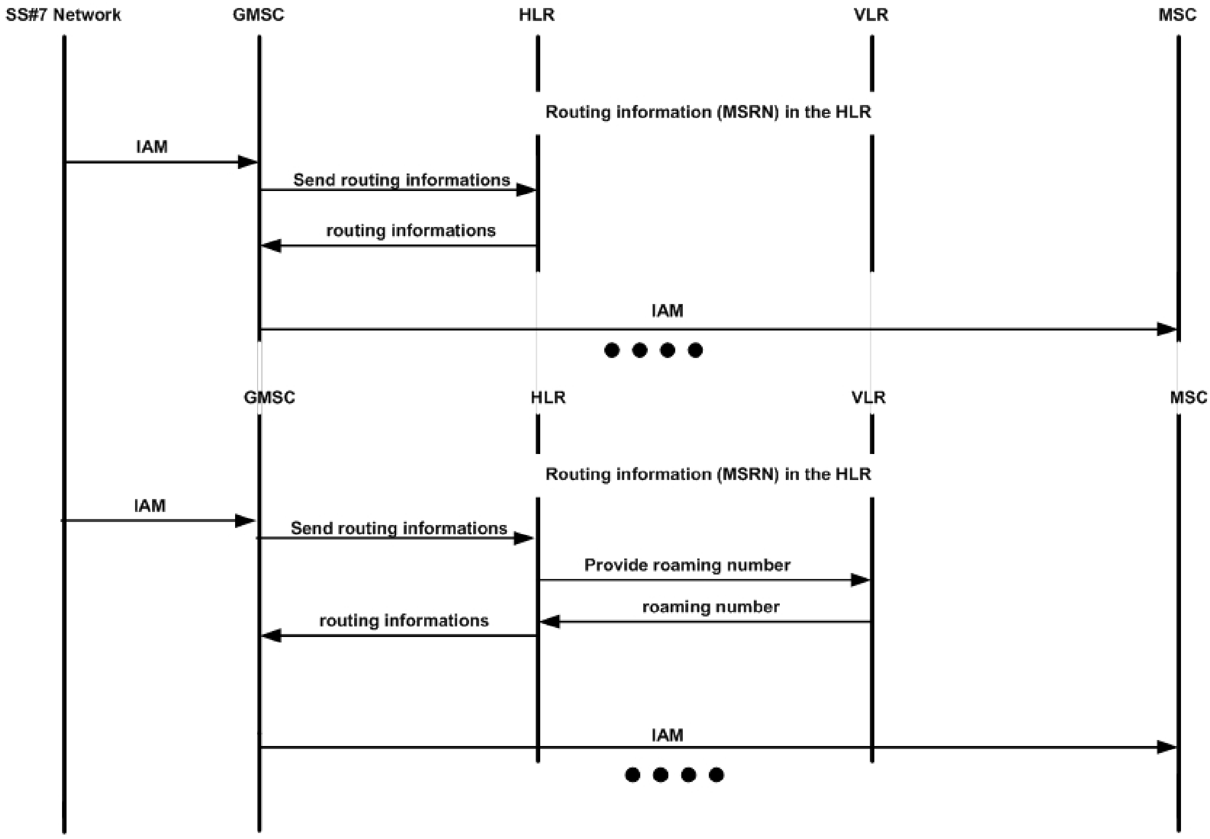


Figure 2.11: Interrogation of routing information for incoming call

Call establishment is again delayed in the local MSC due to the need to determine the exact location of the mobile station within the MSC area (send info for setup, Figure 2.12). The current LAI is stored in the location registers, but an LA can comprise several cells. Therefore, a broadcast (paging call) in all cells of this LA is used to determine the exact location, i.e. cell, of the MS. Paging is initiated from the VLR using MAP. When an MS receives a paging call, it responds thus allowing determination of the current cell [18, 29].

Thereafter, the VLR instructs the MSC to authenticate the MS and to start enciphering the signaling channel. Optionally, the VLR can execute a reallocation of the TMSI (TMSI reallocation procedure) during call setup. Now that the network internal connection has been established, the connection setup proper can be processed (command complete call from VLR to MSC). The MS is told about the connection request with a setup message, and after answering with a call complete, it receives a channel. After ringing (alert) and going off-hook, the connection is switched through (connect, connect acknowledge), and this fact is also signaled to the remote exchange (ACM, ANM) [29].

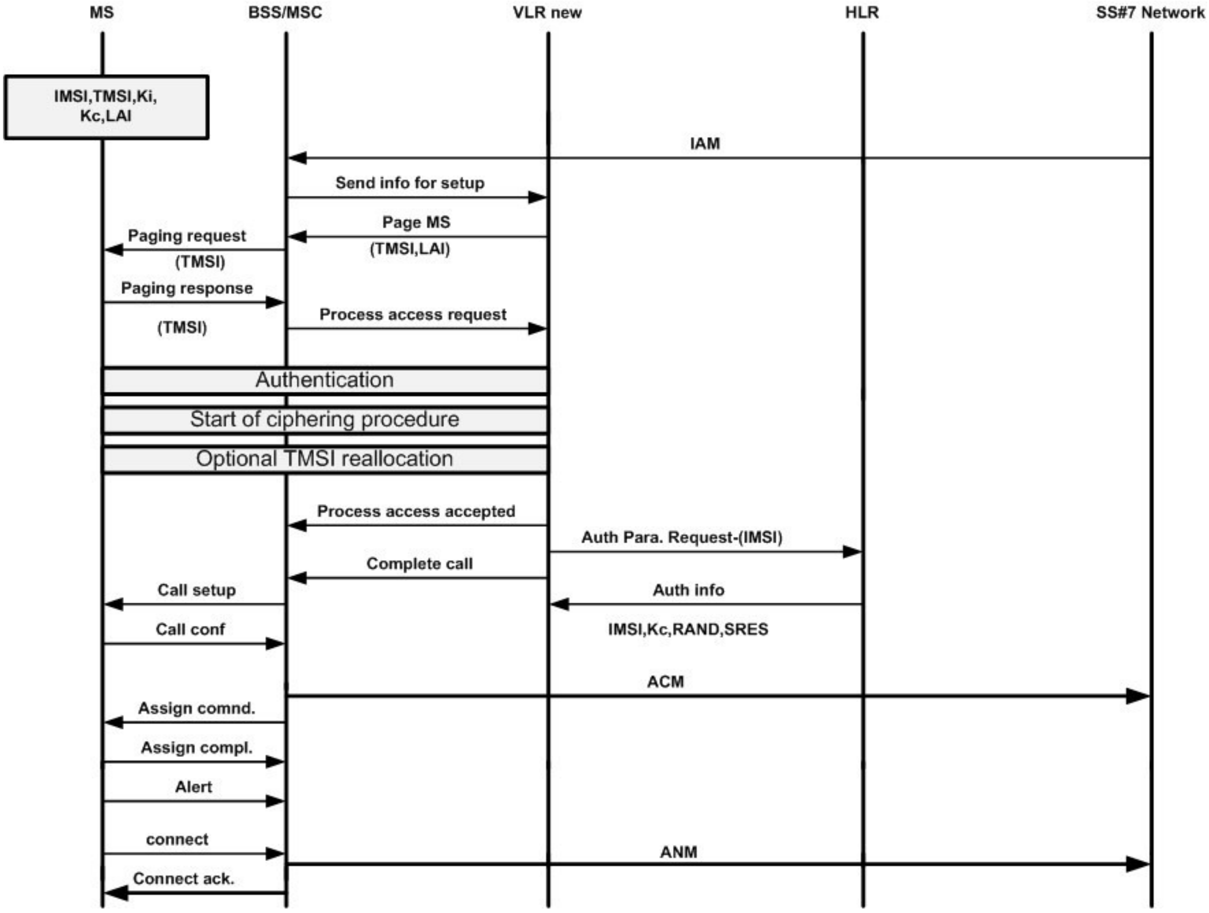


Figure 2.12: Overview of incoming call setup

3. Underlying Technologies

3.1 The OSI Reference Model

The communication process is divided into seven independent layers using OSI (Open System Interconnection) reference model. The following are the general "rules" of the OSI model.

- Each layer work independently, receives a service from the layer immediately below and provides a service to the layer immediately above. The lower layer does not care about the content of the received information.

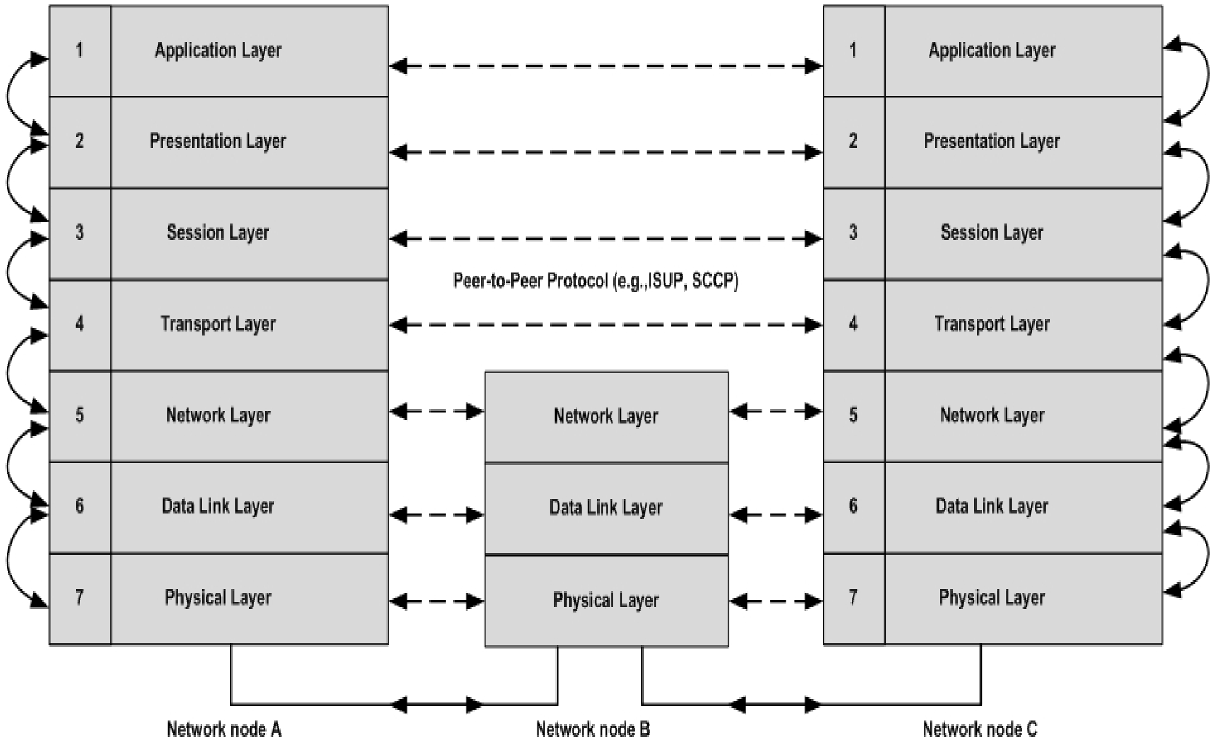


Figure 3.1: The layers and message types of the OSI Reference Model.

- Each layer communicates indirectly with its peer layer at the remote end and directly only with the layers immediately below and above itself.
- If a communications process involves more than two network nodes, the intermediate network node or nodes need only provide the functionality of Layers 1 through 3. As Figure 3.1 shows, network node B is equipped only with Layers 1, 2, and 3. Layers 4 through 7 are required at the end points of a connection only. All other parts of the communication process are available only at the sender and receiver sides.

- The protocols used for Layers 1 through 3 on the interface between A and B are not necessarily the same as those used on the interface between B and C. For example, Layer 2, between the BTS and the BSC in GSM, uses the LAPD (Link Access Protocol-Channel D) protocol, while the SS7 protocol is used between the BSC and the MSC. In that case, network node B would represent the BSC [18].

3.2 Signaling System 7

Common Channel Signaling System Number 7 (SS7 or C7) is a global standard for Telecommunications defined by the International Telecommunication Union Telecommunication Standardization Sector. The standard defines the procedures and protocol by which network elements in the public switched telephone network (PSTN) exchange information over a digital signaling network to effect call setup, routing and control [53]. The role of SS7 network and protocol in relevance of this thesis includes:

- Basic call setup, management, and tear down
- Wireless services such as personal communications services (PCS), wireless roaming and mobile subscriber authentication
- Enhanced call features such as call forwarding, calling party name/number display and three-way calling [53].

3.2.1 SS7 Network Architecture

In a SS7 network each signaling point is uniquely identified by a numeric point code. Signaling messages exchanged between the signaling points, carry the point codes to identify the source and destination of the each message. Routing tables are used by each signaling point, to select the appropriate signaling path for each message based upon the destination point code. There are three kinds of signaling points in the SS7 network:

a. **Service Switching Point (SSP)**

SSPs are switches that originate, terminate or tandem calls (calls processed by two or more switches; inbound to the trunk group on one switch and then routed out of the trunk group via another switch.). An SSP sends signaling messages to other SSPs to setup, mange, and release the voice circuits required to setup a call.

b. **Signal Transfer Point (STP)**

An STP is responsible for routing each incoming signaling message to an outgoing signaling link based on the routing information contained in the SS7 message. The STP acts as a network hub and optimizes the utilization of the SS7 network by eliminating the need for direct signaling links between all signaling points. An STP may perform Global Title Translation (GTT), a procedure by which the destination signaling point is determined from the digits present in the signaling message [53].

c. **Service Control Point (SCP)**

An SCP acts as a centralized database with the MSISDN as the primary key. An SSP sends query message to this centralized database (SCP) to determine how to route a signaling message for call setup. In response, the SCP sends the routing number(s) associated with the dialed number (MSISDN). An SSP may also supply alternative routing number(s) if the primary number is unanswered or busy for a specified time.

Note that STPs and SCPs are customarily deployed in pairs, but that the elements of the pair are not generally co-located (to provide independence, hence increasing availability); they work redundantly to perform the same logical function [52].

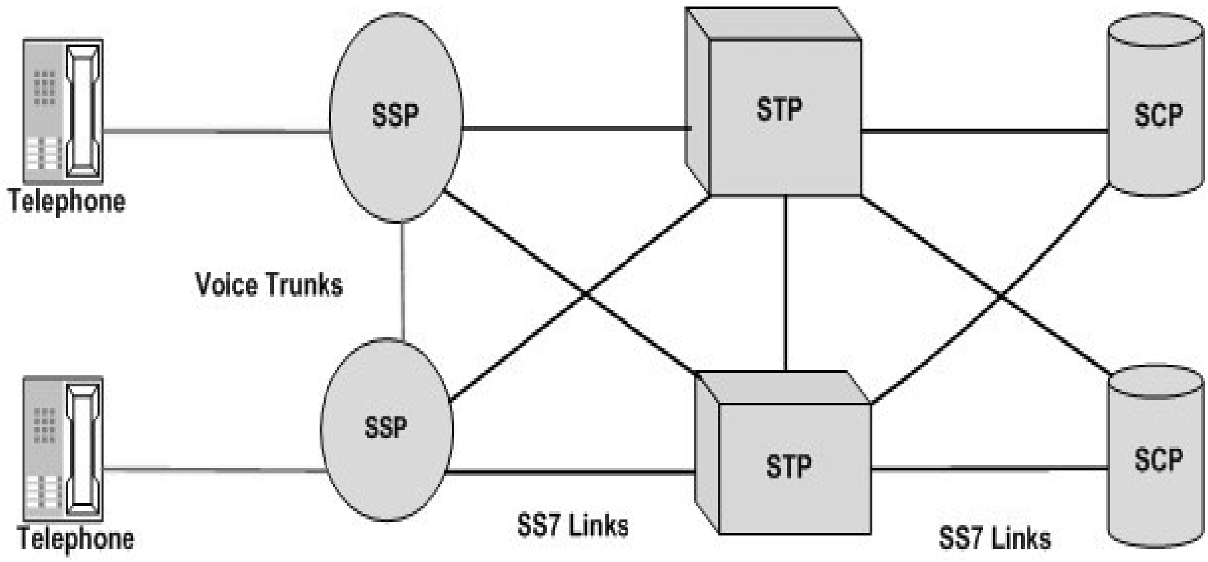


Figure 3.2: SS7 signaling nodes

3.2.2 SS7 and the OSI Reference Model

The hardware and software functions of the SS7 protocol are divided into functional abstractions called "levels." These levels map loosely to the Open Systems Interconnect (OSI) seven layer model defined by the International Standards Organization (ISO) Figure 3.3 [53].

- **MTP Level 1**

  The lowest level, MTP (Message Transfer Part) level 1, is equivalent to the OSI Physical Layer. MTP Level 1 defines the physical, electrical and functional characteristics of the digital signaling link [53].

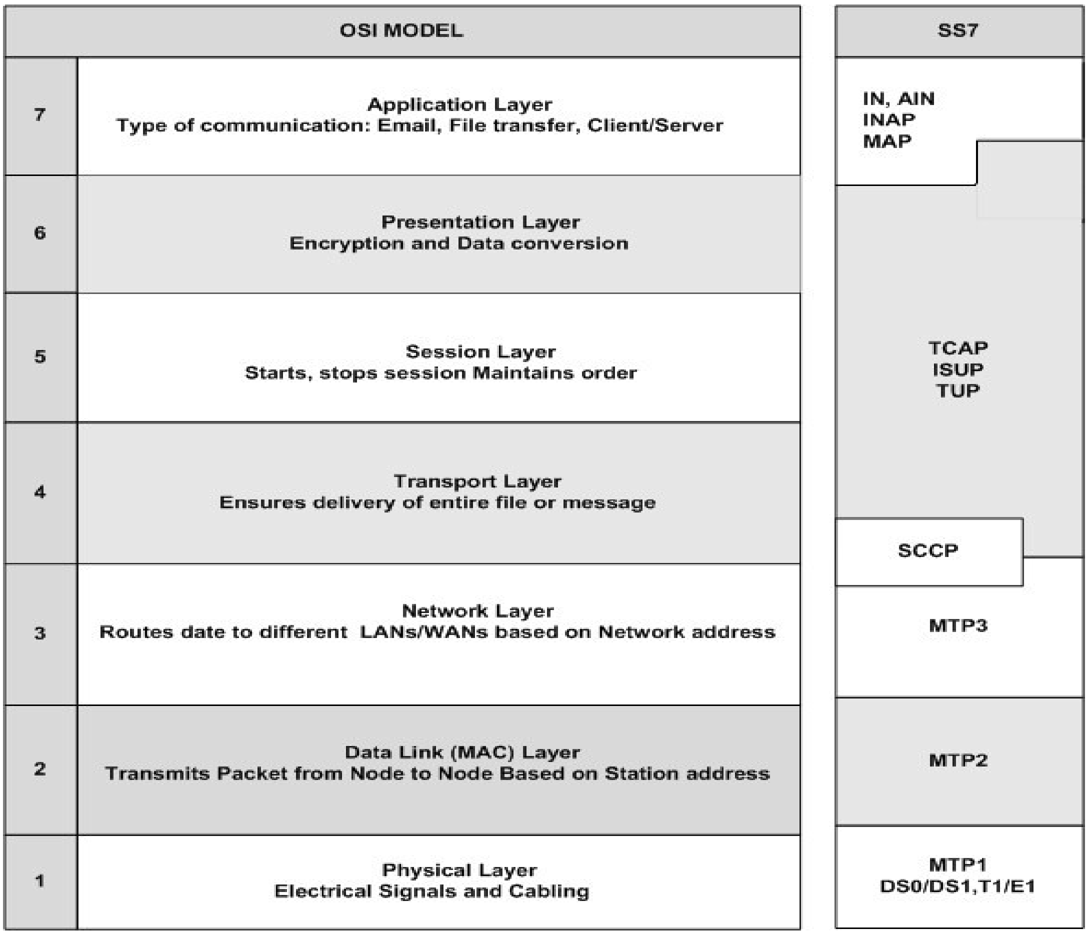

OSI MODEL
7
Application Layer
Type of communication: Email, File transfer, Client/Server
6
Presentation Layer
Encryption and Data conversion
5
Session Layer
Starts, stops session Maintains order
4
Transport Layer
Ensures delivery of entire file or message
3
Network Layer
Routes date to different LANs/WANs based on Network address
2
Data Link (MAC) Layer
Transmits Packet from Node to Node Based on Station address
1
Physical Layer
Electrical Signals and Cabling
SS7
IN, AIN
INAP
MAP
TCAP
ISUP
TUP
SCCP
MTP3
MTP2
MTP1
DS0/DS1,T1/E1

Figure 3.3: SS7 protocol stack and OSI reference model

- **MTP Level 2**

  MTP level 2 is responsible to ensure accurate end-to-end transmission, flow control, message sequence validation and error checking of a signaling message across a link. The message (or set of messages) is retransmitted in case of an error on the signaling link. MTP level 2 is equivalent to the OSI data link layer.

- **MTP Level 3**

  MTP level 3 is responsible to route the signaling message between signaling points in the SS7 network. MTP Level 3 reroutes signaling messages in case of link failure and controls traffic when congestion occur. MTP level 3 is equivalent to the OSI network layer.

- **Signaling Connection Control Part (SCCP)**

  The signaling connection control part (SCCP) provides two major functions that are lacking in the MTP:

I. The first function that SCCP provides is the capability to address the application within a signaling point. The MTP can only receive and deliver messages from a node as a whole; it does not deal with software applications within a node. While MTP network-management messages and basic call-setup messages are addressed to a node as a whole, other messages are used by separate applications (referred to as subsystems) within a node. The SCCP allows these subsystems to be addressed explicitly [18, 52, 60].

II. Global Title Translation: The second function provided by the SCCP is the ability to perform incremental routing using a capability called global title translation (GTT). GTT frees the originating signaling points from the burden of having to know every potential destination to which they might have to route a message. A switch can originate a query, for example, and address it to an STP along with a request for GTT. The receiving STP can then examine a portion of the message, make a determination as to where the message should be routed, and then route it [25, 52]. The STP provides the following functionalities:

a) STPs must maintain a database that enables them to determine where a query should be routed. GTT effectively centralizes the problem and places it in a node (the STP) that has been designed to perform this function.

b) In performing GTT, a STP does not need to know the exact final destination of a signaling message. It can, instead, perform intermediate GTT, in which it uses its tables to find out another STP further along the route to the destination. That STP, in turn, can perform final GTT, routing the message to its actual destination.

c) Intermediate GTT minimizes the need for STPs to maintain extensive information about nodes that are far removed from them. GTT also is used at the STP to share load among paired SCPs in both normal and failure scenarios. In these instances, when messages arrive at an STP for final GTT and routing to a database, the STP can select from among available SCPs. It can select an SCP on either a priority basis (referred to as primary backup) or so as to equalize the load across all available SCPs [25, 52].

d)

- **Transaction Capabilities Applications Part (TCAP)**

  TCAP is responsible to support the exchange of non-circuit related data between applications across the SS7 network using SCCP connectionless service. Queries and responses sent between SSPs and SCPs are carried in TCAP messages. In mobile networks (such as GSM), TCAP carries the Mobile Application Part (MAP) messages sent between mobile switches and databases to support user authentication, equipment identification, and roaming [51, 53].

- **ISDN User Part**

  ISDN User Part (ISUP) is responsible for providing the protocol and procedures that are used to set-up, manage, and release trunk circuits that carry voice and data calls over the Public Switching Telephone Network (PSTN). ISUP can be used for both ISDN and non-ISDN calls. ISUP signaling is not required by a call that originates and terminates at the same switch. Figure 3.4 depicts the ISUP signaling associated with a basic call.

  - **Basic ISUP Call Control:**
    - When a call is placed to an out-of-switch number, the originating SSP switch reserves an idle trunk circuit from the originating switch to the destination switch by transmitting an ISUP Initial Address Message (IAM) (1a). The IAM contains the Originating Point Code (OPC), Destination Point Code (DPC), circuit identification code (circuit "5" in Figure 3.4), dialed digits, and, optionally, the calling party number and name. In the Figure 3.4 below, the IAM is routed via the home STP of the originating switch to the destination switch (1b). The same signaling link(s) are used for the duration of the call unless a link failure forces the switch to use an alternative signaling path.
    - When the IAM arrives at the destination switch, it examines the dialed number, determines if it serves the called party, and if that line is available for ringing. If so, then the destination switch rings the called party line and transmits an ISUP Address Complete Message (ACM) to the originating switch (2a) (using its home STP) to indicate that the remote end of the trunk circuit has been reserved. The STP routes the ACM to the originating switch (2b). Meanwhile the terminating switch provides ringing power to the called party and audible ringing tone to the calling party.

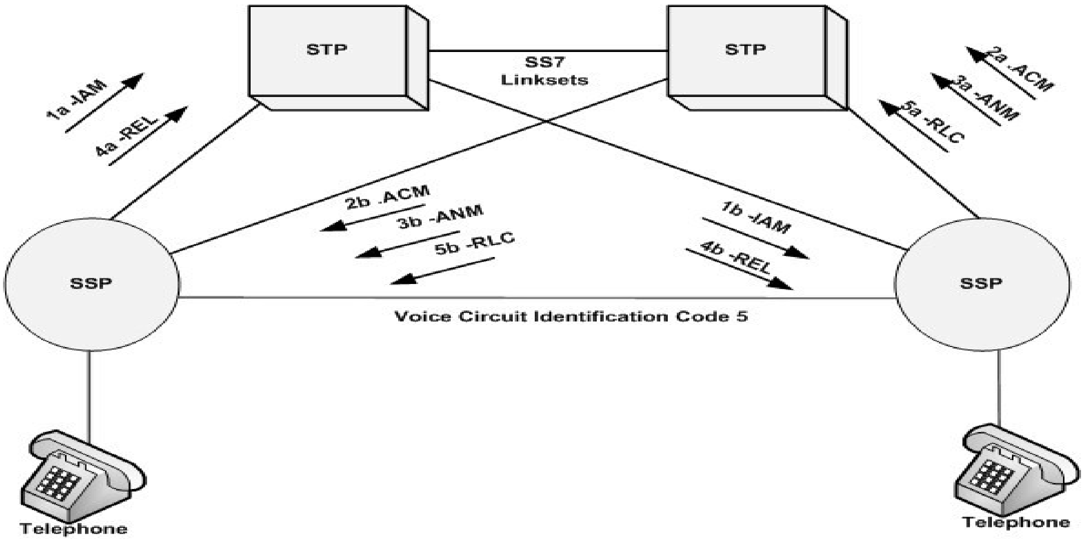


Figure 3.4: Basic ISUP signaling

- In the Figure 3.4 the originating SSP and destination SSP switches are directly connected with trunks. In a scenario where the originating and destination switches are not directly connected with trunks, then the originating SSP switch first transmits an IAM to reserve a trunk circuit to an intermediate switch. This intermediate switch transmits an ACM to acknowledge the circuit reservation request and then transmits an IAM to reserve a trunk circuit to another switch. This process continues until a complete voice circuit from the originating SSP switch to the destination SSP switch is reserved.
- When the called party picks up the phone, the destination SSP switch stops sending ringing tones and sends an ISUP Answer Message (ANM) to the originating SSP switch via its home STP (3a). Then home STP routes the ANM to the originating switch (3b) which verifies that the calling party's line is connected to the reserved trunk, if so, it initiates billing.
- If the called party disconnects the call first, or if the line is busy, then the destination switch sends an ISUP Release Message (REL) to the originating SSP switch indicating the release cause (e.g., normal release or busy). If the calling party disconnects the call first, then originating switch transmits REL message, to release the trunk circuit between originating and destination switches (4a), the STP routes the REL message to the destination switch (4b).
- When the destination SSP switch receives the REL message, the switch disconnects the trunk from the called party’s line, and sets the trunk state to idle. Then the destination switch transmits an ISUP Release Complete Message (RLC) to the

originating switch (5a) to acknowledge the release of the remote end of the trunk circuit. When the originating switch receives (or generates) the RLC (5b), it terminates the billing cycle and sets the trunk state to idle in preparation for the next call [2, 16, 51, 53, 65].

Note that ISUP messages may also be transmitted during the connection phase of the call (i.e., between the ISUP Answer (ANM) and Release (REL) messages [53].

- **Mobile Application Part**

The Mobile Application Part (MAP) is one of protocols in the SS7 suite, it allow the implementation of mobile network (in the case of this thesis, GSM) signaling infrastructure. MAP is an extension of the SS7 protocols to support cellular networks. It defines the operations between the MSC, the HLR, the VLR, the EIR, and the fixed-line network. MAP is used to communicate between the network components (such as MSC, BSC, HLR, VLR, EIR, MS, and SGSN/GGSN in GPRS). This involves the transfer of information between the components using non-circuit-related signaling, for example, MAP signaling is used to enable location updating, handover, roaming functionality, authentication, incoming call routing, and SMS. MAP specifies a set of services and the information flows between GSM components to implement these services [12, 51, 59].

MAP uses TCAP over SCCP and MTP to transfer real-time information (between NSS and BSS components). TCAP correlates individual operations. The TCAP transaction sub-layer manages transactions on an end-to-end basis.

MAP enables a call to be routed to and from the mobile subscriber, and provides all the mechanisms which are necessary for transferring information relating to subscribers roaming between network entities in the PLMN. MAP has several basic functions, including the following:

- MAP enables the GMSC to determine a routing number (MSRN) for an incoming call , by carrying messages to and from the HLR and possibly the VLR.
- MAP enables the MSC via its integrated Visitor Location Register (VLR) to update subscriber status and routing number.
- MAP provides subscriber supplementary service profile and data to switching elements via the VLR [59].

3.2.3 SS7-IP Interworking

The use of SS7 over IP has been more evolutionary than revolutionary in its adoption. Although the ability to transport SS7 over IP has existed for several years, only recently have there been sufficient advances in the technology to make it a truly viable transport alternative to TDM for signaling messages.

Transfer Control Protocol (TCP), although sufficient for the transport of data over IP**,** has some serious limitations when applied to the timeliness requirements of telephony signaling. A new set of standards-based protocols was required to reliably send SS7 messages across an IP network, this protocol was developed by the IETF SIGTRAN working group [54].

3.3 TDM over IP (TDMoIP)

TDM-based circuit switched networking has been the heart of the Public Switched Telephone Network (PSTN) for decades. Some think TDM ' s days are numbered, while others believe that the reliability of this venerable technology and longevity of the installed equipment base means that it will co-exist alongside IP for years to come. Regardless, much of the world's voice traffic is still carried over circuit switched networks and this traffic accounts for a significant portion of carrier revenues [4, 58]. However, data now outpaces voice traffic on nearly all networks.

The challenge of transporting circuit switched trunks over connectionless networks has been addressed by both integrated circuit manufacturers and equipment vendors, with a solution that combines old and new approaches to transporting TDM traffic over new IP, Ethernet or Multiprotocol Label Switching (MPLS) networks [4].

The agreed approach is patterned after the circuit emulation Service over ATM (Asynchronous Transfer Mode). Some have taken ATM cells and packetized the payloads into IP packets. Others have put the TDM channels into the IP payload directly, thus eliminating the segmentation and reassembly step of ATM. Circuit emulation service over IP has parallels to ATM AAL1(ATM Adaption Layer 1) transmission. Both are constant bit rate, both transmit uncompressed voice, and both support structured and unstructured circuit transport [4, 64].

One of the major issues with circuit emulation service over IP or TDM over IP is synchronization -- because in the circuit switched network, timing and synchronization are fundamental to the design and operation of the network. However, this timing is lost when this traffic is carried over a packet switched network. . Thus the timing needs to be restored by other means.

With the proliferation of packet switched networks, carrying telephone and other traditionally TDM based services over these packet switched network, infrastructures has become desirable. The interworking function that connects between the TDM and packet switched network is called a TDMoIP interworking function (IWF). This IWF that encapsulates TDM traffic as packets which are injected into the packet switched network. At the destination another IWF extracts TDM data from packets and generates traffic on a TDM network. Emulated TDM circuits are always point-to-point, bidirectional, and transport the same TDM rate in both directions [4, 64].

Emulation of TDM circuits over the packet switched network can be carried out using pseudo-wires [49]. This emulation must maintain the service quality of a native TDM link; particularly in terms of voice quality, latency, timing, and signaling features; and must be similar to those of existing TDM networks [36].

3.3.1 TDMoIP Encapsulation

The overall format of TDMoIP packets is shown in Figure 3.5. The packet headers (UDP/IP, L2TPv3/IP, and MPLS or layer 2 Ethernet) contain all the information necessary for forwarding the packet from the source IWF to the destination IWF. The packet switch network is expected to be reliable and provides sufficient bandwidth to enable transport of the required TDM data over IP while maintaining the agreed delay, jitter, and loss bounds [64].

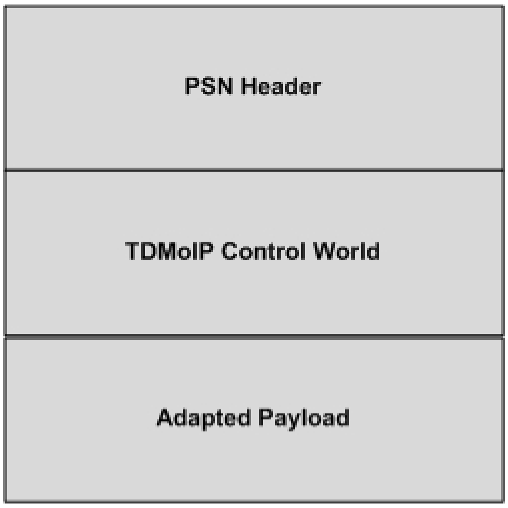


Figure 3.5: Basic TDMoIP packet format

3.3.2 Encapsulation Details for several packet switched networks

TDMoIP pseudo-wires may exploit various packet switched networks, including UDP/IP (both IPv4 and IPv6), L2TPv3 over IP (with no intervening UDP), MPLS, and layer-2 Ethernet. The following subsections will depict the packet format for carrying this pseudo-wire traffic using UDP/IPv4.

3.3.2.1 UDP/IPv4

When using UDP/IPv4, the headers are prefixed to the TDMoIP data (for details see 24, 30, 58). The TDMoIP packet structure is depicted in Figure 3.6,

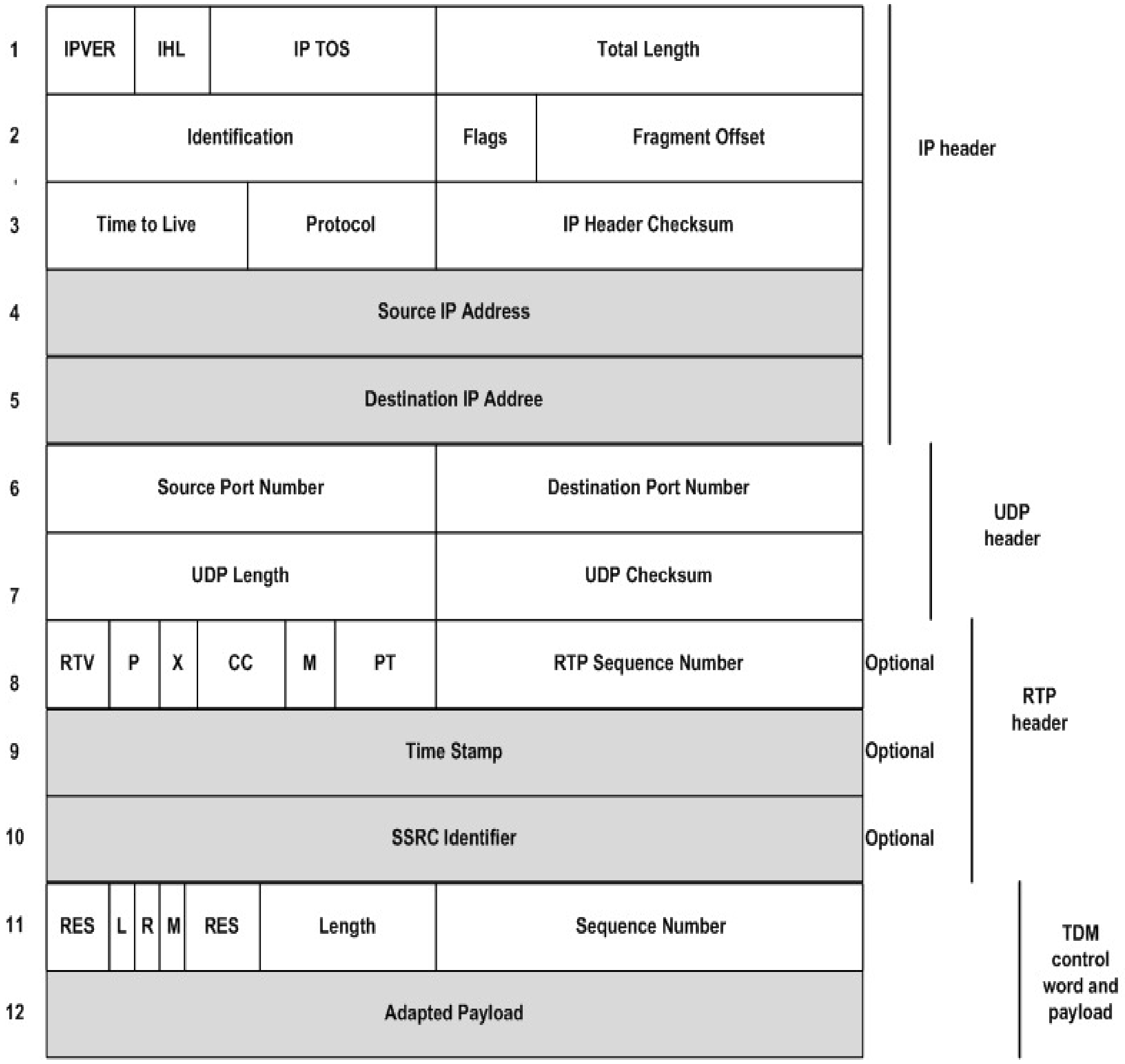


Figure 3.6: TDMoIP packet format for UDP/IP

The first five rows define the IP header; the sixth and seventh rows define the UDP header. Rows 8 through 10 are the optional Real-Time Transport Protocol (RTP) header. Row 11 defines the TDMoIP control word. Source UDP port or destination UDP port can be used to multiplex and demultiplex individual PWs between the nodes.

3.4 SS7 over IP Implementation (SIGTRAN-SCTP)

The ability to offer services over IP, especially in an environment where the bandwidth could be shared by multiple applications, can be very attractive to carriers. If IP connectivity already exists between two points, then leveraging that existing network for SS7 is much easier than having to roll out new, dedicated TDM facilities that might only be used for very limited amounts of SS7 traffic [55]. The reason being espousal of Softswitching in all next generation networks where signaling and media are segregated to reach the destination via the most optimal route which might not be same for both.

Among the many technological solutions to choose from, IP is the most promising media to build new integrated services. Hence, mobile network operators are migrating towards all-IP architecture. This new all-IP architecture includes support for SS7 signaling protocols. Thus IP provides both an effective way to transport user data and for operators to expand their networks and implement new services [55].

The benefits of using an IP network compared to using a legacy TDM–based network are as follows:

- When using signaling gateways to interconnect the SIGTRAN network with a traditional SS7 network (such as an access service group - ASG), there is no need to disrupt the existing SS7 network, and future enhancements are transparent to the existing SS7 network
- SIGTRAN over an IP network doesn't require physical E1/T1 links (which are often provisioned by synchronous digital hierarchy rings). By using new technologies such as IP over fiber, much higher throughput can be achieved and due to the much higher production volumes for data communications equipment the cost is lower!
- SIGTRAN over IP is not constrained to fixed multiples of link capacity as in the SS7 network. This is because the IP network is much more flexible than a TDM-based network, as packets are transported rather that fixed bandwidth circuits [55, 57].

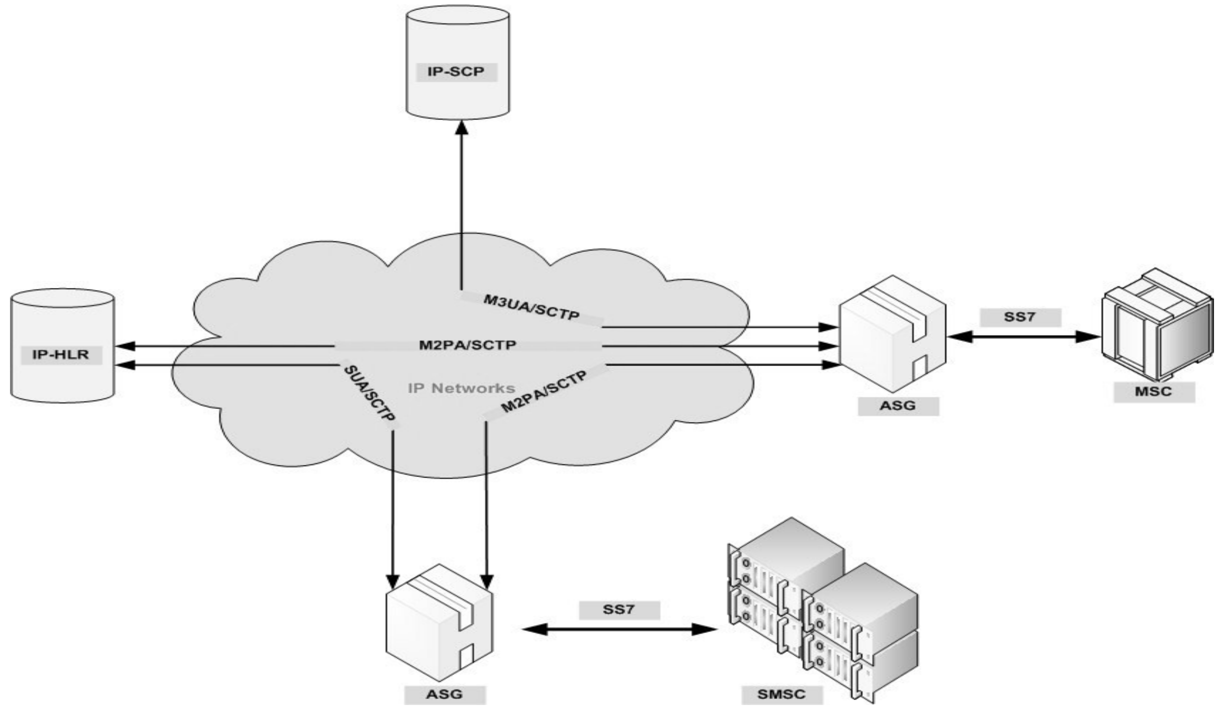


Figure 3.7: Simpler implementation for signaling transport over IP

Figure 3.7 depicts that using SIGTRAN protocols such as an MTP3 user application (M3UA) and a signaling connection control part user application (SUA), the Short Message Service Center [SMSC], IP—Home Location Register [IP- HLR], and so on only requires development at the application layer [55] and avoids the complex SS7 interfaces.

3.4.1 Stream Control Transmission Protocol

The IETF's SIGTRAN (Signaling Transport) suite of protocols, particularly Stream Control Transmission Protocol (SCTP) was specifically designed to meet the requirements of transporting telephony signaling over IP networks. SCTP, as the transport layer, has several features that make it a highly reliable and robust alternative to the TCP or UDP as a transport protocol.

A few of TCP's limitations that have been rectified include:

- TCP provides both reliable data transfer and strict order-of-transmission delivery of data while, some application require reliable data transfer **without** maintaining the sequence and some application need **only partial ordering** of data. In both cases unnecessary delay is introduced due to the head-of-line blocking by TCP, as TCP must wait for the retransmission since it must deliver all bytes in order.

- The task of providing highly available data transfer using multi-homed hosts is simpler as SCTP provides multi-homing and fail-over mechanisms.
- SCTP is designed to avoid many of the denial of service attacks to which TCP was vulnerable.

SCTP's improvements, as described above, over TCP make it much more viable solution for transmission of SS7 over IP networks. To establish an association (SCTP's name for a connection) between two SCTP endpoints, one endpoint provides the other endpoint with a list of its transport addresses (i.e., multiple IP addresses in combination with an SCTP port number) [54]. These transport addresses can be used to send and receive SCTP packets, thus providing multi-homing.

Signaling traffic consists of many independent message sequences between different signaling endpoints. SCTP ensures in sequence delivery between associated end points by allowing signaling messages to be independently ordered within multiple streams (i.e., unidirectional logical channels established from one SCTP endpoint to another). By using separate SCTP streams for each independent message, it is less likely that retransmission of a lost message will affect the timely delivery of other messages in unrelated sequences (thus avoiding head-of-line blocking). Because SCTP avoids head-of-line blocking, the SIGTRAN Working Group recommends SCTP rather than TCP/IP for the transmission of signaling messages over IP networks [54].

There are three types of messages in SS7:

- Message Signal Units (MSUs)
- Link Status Signal Units (LSSUs)
- Fill-In Signal Units (FISUs)

MSUs originate at a higher level than MTP Level 2 and are destined for a peer at another node. LSSUs allow peer MTP Level 2 layers to exchange link status information. FISUs are sent when no other signal units are waiting to be sent across the synchronous link, thus waste of bandwidth is avoided while preserving the ability to detect link failure by use of heartbeat messages in SCTP. FISUs also carry acknowledgment of messages, a function also subsumed by SCTP [54].

In summary, SCTP provides:

- Acknowledged error-free non-duplicated transfer of signaling information

- In-sequence delivery of messages within multiple streams, with an option for order-of arrival delivery of individual messages
- Optional bundling of multiple messages into a single SCTP packet
- Data fragmentation as required
- Network-level fault tolerance through support of multi-homing at either or both ends of an association
- Appropriate congestion avoidance behavior and resistance to denial-of-service and masquerade attacks [51, 54, 55, 57].

3.4.2 SIGTRAN Architecture

The SIGTRAN protocol suite includes the transport protocol SCTP and several user adaptation layers, used to transport SS7 messages over IP networks. The SIGTRAN architecture (shown in figure 3.8) consists of three layers:

1. IP layer,
2. Transport layer (SCTP), and
3. User adaptation layer (e.g. M2PA, M2UA, M3UA, and SUA) [37].

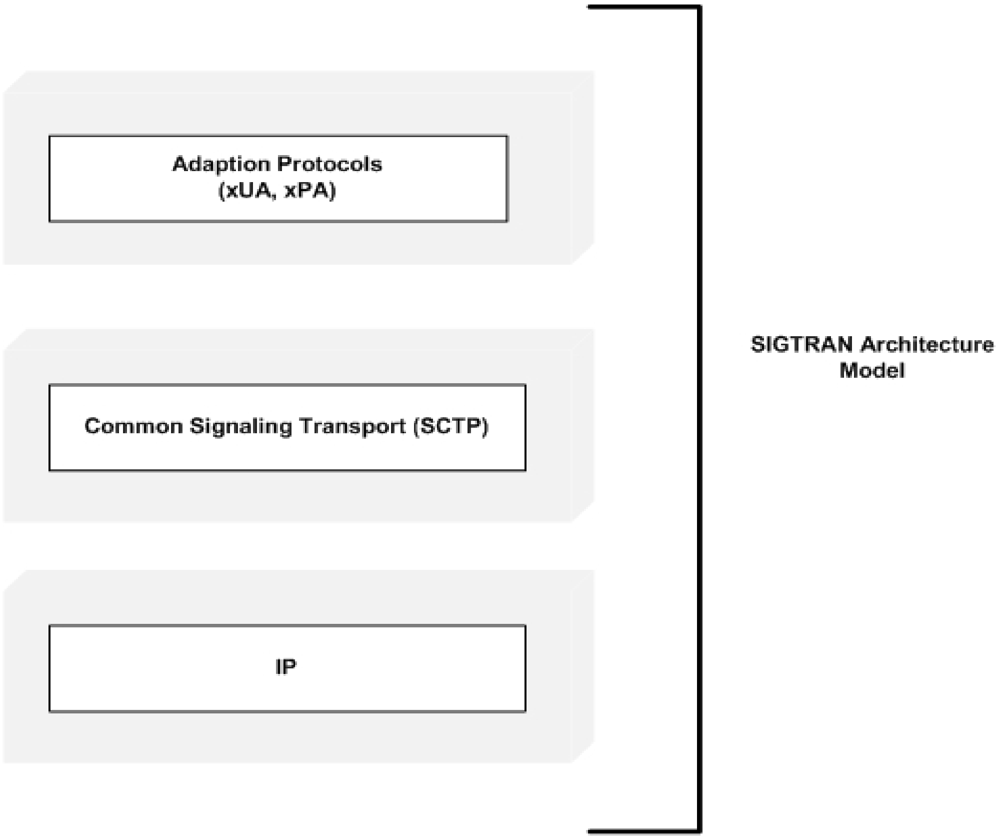


Figure 3.8: SIGTRAN architecture model

In a nutshell, the SIGTRAN protocols provide the means by which SS7 messages can be reliably transported over IP networks. The SIGTRAN architecture identifies two components: the first component is a common transport protocol (SCTP) and the second is an adaptation module which is used to emulate lower layers of the SS7 protocol. For example, if the native protocol is MTP level 3, then SIGTRAN protocols provides the same and equivalent functionality of MTP level 2. If the native protocol is ISUP or SCCP, then SIGTRAN protocols provide the equivalent functionality as MTP levels 2 and 3. Similarly if the native protocol is TCAP, then SIGTRAN protocols provide the same and equivalent functionality of SCCP (connectionless classes) and MTP level 2 and 3 [27].

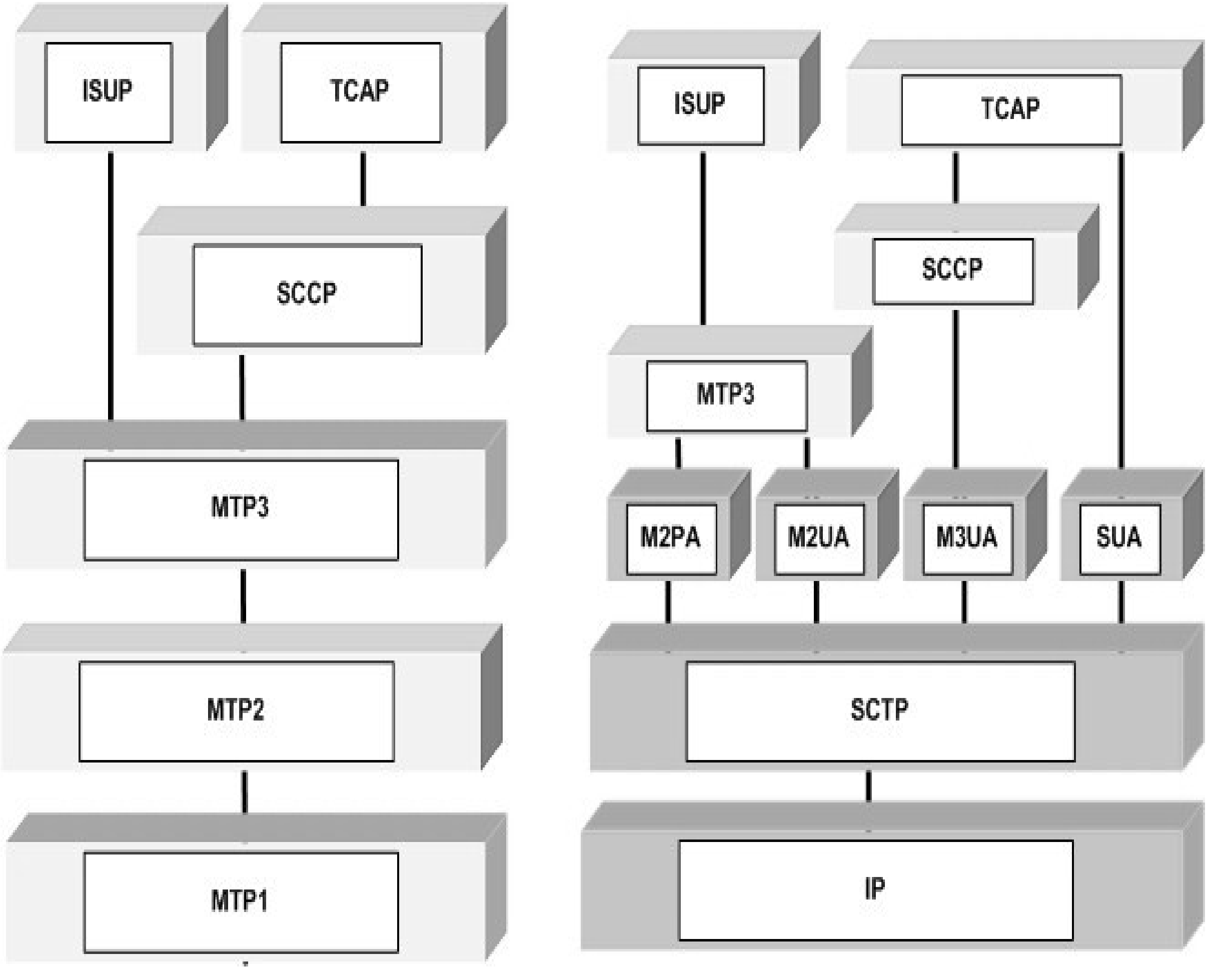


Figure: 3.9 The MTP1 and MTP2 layers in the traditional SS7 stack (left) are replaced by SIGTRAN protocol (right) to enable support of SS7 over IP

In Figure 3.9, three lower layer of the SS7 protocol stack has been replaced with the new SIGTRAN protocols, replace the lower layers of the SS7 stack (MTP1, MTP2 and MTP3), thus enabling transportation over IP. A user adaptation layer enables the SS7 user (MTP3, SCCP, TCAP, ISUP etc.) to be unaware of fact that the original lower SS7 layers have been replaced. Depending on the telephony network, different user adaptation protocols can be chosen depending on their characteristic features [37].

SIGTRAN protocols provide the functionality needed to support SS7 signaling over IP networks, including:

- Flow control
- Using a single control stream provides in-sequence delivery of signaling messages
- Identification of the originating and terminating signaling points
- Identification of voice circuits
- Better error detection, retransmission, and other error correcting procedures
- Recovery from outages of components in the transit path
- Controls to avoid congestion on the Internet
- Detection of the status of peer entities (e.g., in service, out-of-service, etc.)
- Support for security mechanisms to protect the integrity of the signaling information
- Extensions to support security and future requirements [21, 27, 51].

3.4.3 Transporting MTP over IP

To achieve the functional and performance requirements for MTP, the IETF SIGTRAN Working Group has recommended three new protocols: M2UA, M2PA, and M3UA. Each protocol is described below.

3.4.3.1 M2UA: MTP2 User Adaptation Layer

M2UA is a protocol used to transport SS7 MTP Level 2 user (i.e. MTP Level 3) signaling messages over IP networks using SCTP. The M2UA protocol .The M2UA protocol layer provides the equivalent set of services to its users as MTP Level 2 provides to MTP Level 3 [27]. M2UA provides support for:

- MTP2/MTP3 interface boundary
- Communication between layer-management modules
- Support for management of active associations

M2UA is SIGTRAN protocol, used between the Signaling Gateway (SG) and Media Gateway Controller (MGC). The SG uses MTP level 1 and MTP level 2 interfaces to receive SS7 messages from a signaling end point (SCP or SSP) or signal transfer point (STP) in the public switched telephone networks. The SG terminates the SS7 links at MTP Level 2 and transports MTP Level 3 and above to a MGC or other IP endpoint using M2UA over SCTP/IP [27, 51].

The SG maintains the availability state of all MGCs to manage signaling traffic flows across active SCTP associations. Figure 3.10 shows back hauling with M2UA in two distant nodes. The SG and MGC do not know that they are remote and each node thinks that MTP3 is directly communicating with MTP2.

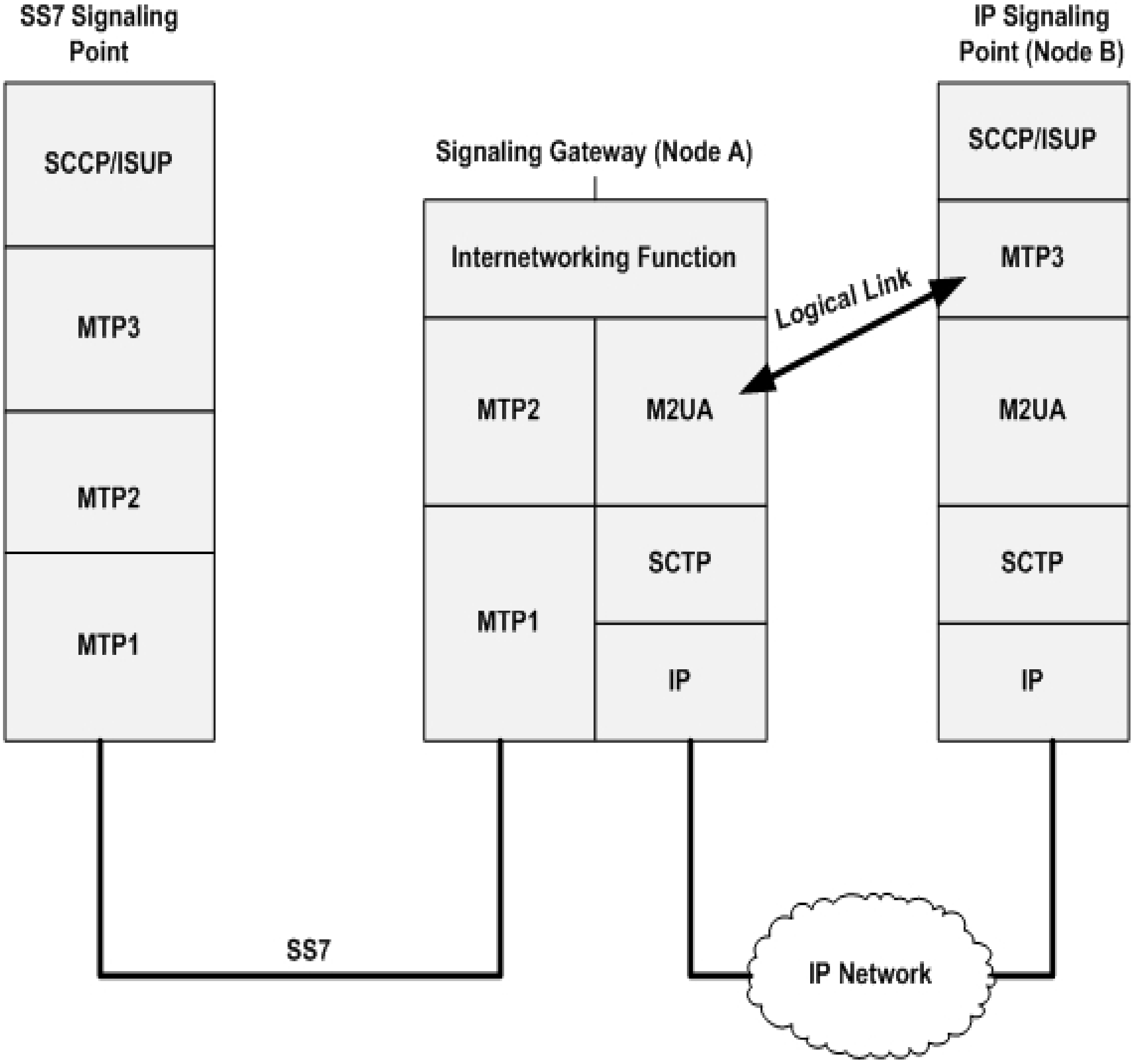


Figure: 3.10 Back hauling with M2UA between 2 distant nodes (Node A and Node B)

3.4.3.2 M2PA: MTP2 User Peer-to-Peer Adaptation Layer

M2PA is a SIGTRAN protocol for transporting SS7 MTP Level 2 user part signaling messages (i.e. MTP level 3) over IP using the SCTP. M2PA supports full MTP Level 3 message handling and network management between any two SS7 nodes communicating over an IP network. IP signaling point functions as traditional SS7 nodes using the IP network. IP signaling point has an SS7 point code. The M2PA protocol layer provides the equivalent set of services as MTP Level 2 provides to MTP Level 3 [27, 51].

M2PA is used between a SG and a MGC, between a SG and an IP signaling point, and between two IP signaling points. Signaling Points may use M2PA over IP or MTP Level 2 over standard SS7 links to send and receive MTP Level 3 messages [27].

Figure 3.11 shows how SS7 signaling connects via an IP signaling point through an SG equipped with both traditional SS7 network and IP network connections. IP signaling point processes MTP3-to-MTP2 primitives and SG act as an STP.

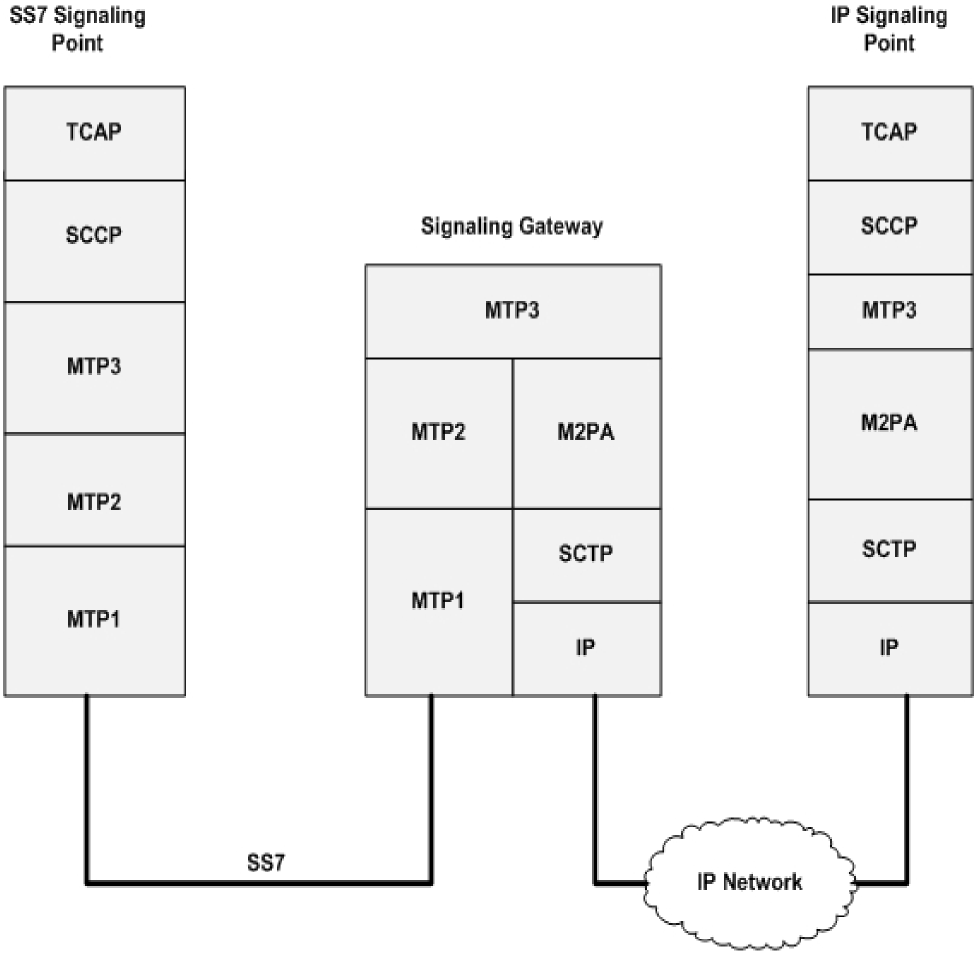


Figure 3.11: Connection between SS7 signaling points to IP signaling point using M2PA

3.4.3.2.1 M2PA and M2UA Comparison

The Table below describes the difference between two protocols.

Table 3.1: M2PA and M2UA comparison [55]

	M2PA	**M2UA**
Point codes	SG is an SS7 node with a point code.	SG is not an SS7 node and has no point code.
Types of links	SG to IP signaling-point connection is an SS7 link (in MTP3 aspects).	SG to IP signaling-point connection is not an SS7 link. It is an extension of MTP2 to a remote node.
SS7 upper layers	SG can have upper SS7 layers, e.g., SCCP.	SG does not have upper SS7 layers because it has no MTP3.
Primitives	IP signaling-point processes MTP3–to–MTP2 primitives	IP signaling point transport MTP3-to-MTP2 primitives to SG's MTP2 (via the interworking function) for processing
Interface with MTP3	Present an MTP2 upper interface to MTP3	Present an MTP2 upper interface to MTP3.
MTP3 data messages	Transport MTP3 data messages	Transport MTP3 data messages
Management	Relies on MTP3 for management procedures	Uses M2UA management procedures

3.4.3.3 M3UA: MTP3 User Adaptation Layer

M3UA is a SIGRAN protocol for transporting SS7 MTP Level 3 user part signaling messages (e.g., ISUP, TUP, and SCCP) over IP using SCTP. SCCP uses M3UA or SUA to carry its user protocols (e.g., TCAP or RANAP messages).

M3UA is used between a SW and a MGC. The SG receives SS7 signaling using MTP as transported over a standard SS7 link. The SG terminates MTP-2 and MTP-3 and delivers ISUP, TUP, SCCP, and/or any other MTP-3 user messages, as well as certain MTP network management events, over SCTP associations to a MGC [27, 51].

The ISUP and/or SCCP layer at an IP signaling point does not know that the expected MTP-3 services are provided by remote SGs instead of locally. Similarly, the MTP-3 layer at a SG does not know that local users are actually remote parts over M3UA. Conceptually, M3UA extends access to MTP-3 services at the SG to remote IP endpoints. If an IP endpoint is connected to more than one SG, then the M3UA layer at the IP endpoint must maintain the status of all the configured SS7 destinations and route messages according to their availability and the congestion status of the routes to these destinations via each SG [51, 54].

The M3UA layer at SG supports the seamless operations of signaling between SS7 and IP networks through internetworking with MTP-3 management functions. For example, the SG indicates to remote MTP-3 users at IP endpoints when an SS7 signaling point is reachable or unreachable or when SS7 network congestion or restrictions occur [27, 54]. The M3UA layer at an IP endpoint maintains the state of all the routes to remote SS7 destination and may request from the M3UA layer at the SG information about the state of a remote SS7 destination. The M3UA layer at an IP endpoint may also indicate to the SG information about the congestion state at various destinations.

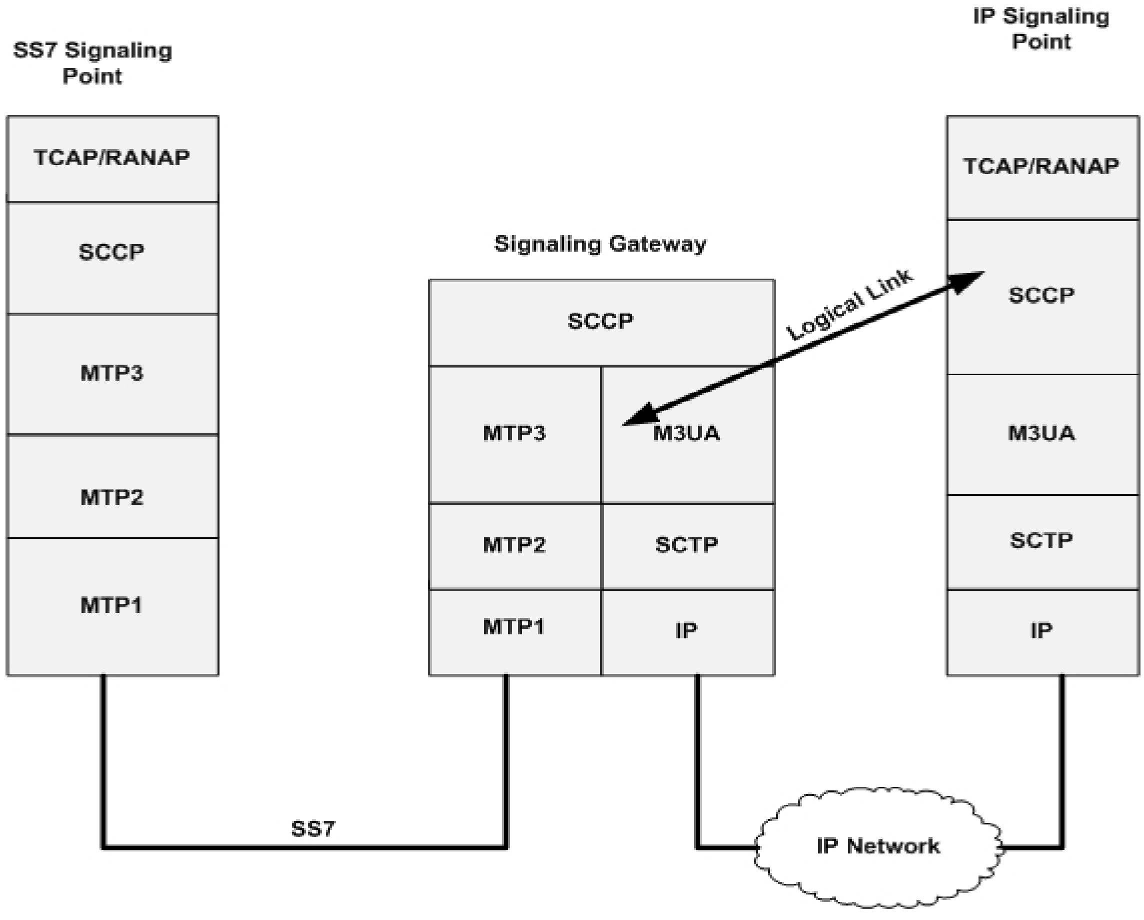


Figure 3.12: Back hauling using M3UA

Figure 3.12 depicts an SG containing a SCCP protocol layer that may, perform the SCCP Global Title Translation (GTT) function for a SCCP message that is addressed to the SG's SCCP. If the result of a GTT for an SCCP message yields an SS7 destination point code (DPC) or DPC/subsystem number (SSN) address of an SCCP peer located in the IP domain, then the SG uses the services of the local M3UA for ongoing routing to the final IP destination using SCTP.

3.4.4 SUA: SCCP User Adaptation Layer

SUA (SCCP User Adaptation Layer) is a SIGTRAN protocol for transporting SS7 SCCP user part signaling messages (e.g., TCAP and RANAP) over IP networks using the services of SCTP. SUA is used between a SG and an IP signaling endpoint and between IP signaling endpoints. SUA supports both SCCP unordered and in-sequence connectionless services and bidirectional connection-oriented services with or without flow control and detection of message loss and out-of-sequence errors (i.e., SCCP protocol classes 0 through 3) [27].

For connectionless transport, SCCP and SUA interface at the SG. From the perspective of an SS7 signaling point, the SCCP user is located at the SG. SS7 messages are routed to the signaling gateway based on point code and SCCP subsystem number [27]. The SG further routes the incoming SCCP messages to the remote IP end points, if redundant IP endpoints exit, then the SG uses a round-robin approach to do load sharing across active IP endpoints.

GTT is performed by the SG to determine the destination of incoming SCCP messages. SG performs routing based on Global Title (GT), i.e. the dialed digits present in the incoming SCCP message.

For connection-oriented transport between an SS7 signaling end point and an IP endpoint, SCCP and SUA interface at the SG to associate the two connection sections needed for connection-oriented data transfer. SG routes the messages to SS7 signaling points based on destination point code (in the MTP-3 address field) and IP endpoints using IP address (in the SCTP header).

SUA can also be used to transport SCCP user information between IP endpoints directly rather than via the SG. The signaling gateway is needed only to enable interoperability with SS7 signaling in the circuit switched network. If an IP resident application is connected to multiple

SGs, multiple routes may exist to a destination in the SS7 network. In this case, the IP endpoint must monitor the status of remote SGs before initiating a message transfer [27, 37, 51, 54, 55].

In this architecture, as portrayed in Figure 3.13, the SCCP and SUA layers interface in the SG. Internetworking is used to provide the seamless transfer of the user and management messages.

For messages destined for an IP-signaling points there are two scenarios:

1. **SG as Endpoint**

   In this case the connectionless SCCP messages are routed based on the point code and SSN. In this scenario the actual location of the SCCP user is regarded as local, hence from the SS7 point of view, the SCCP user is located at the SG.

2. **SG as relay point**

   In this case GTT is executed to determine the destination of the message. In this scenario the actual location of the SCCP user is irrelevant to the SS7 network.

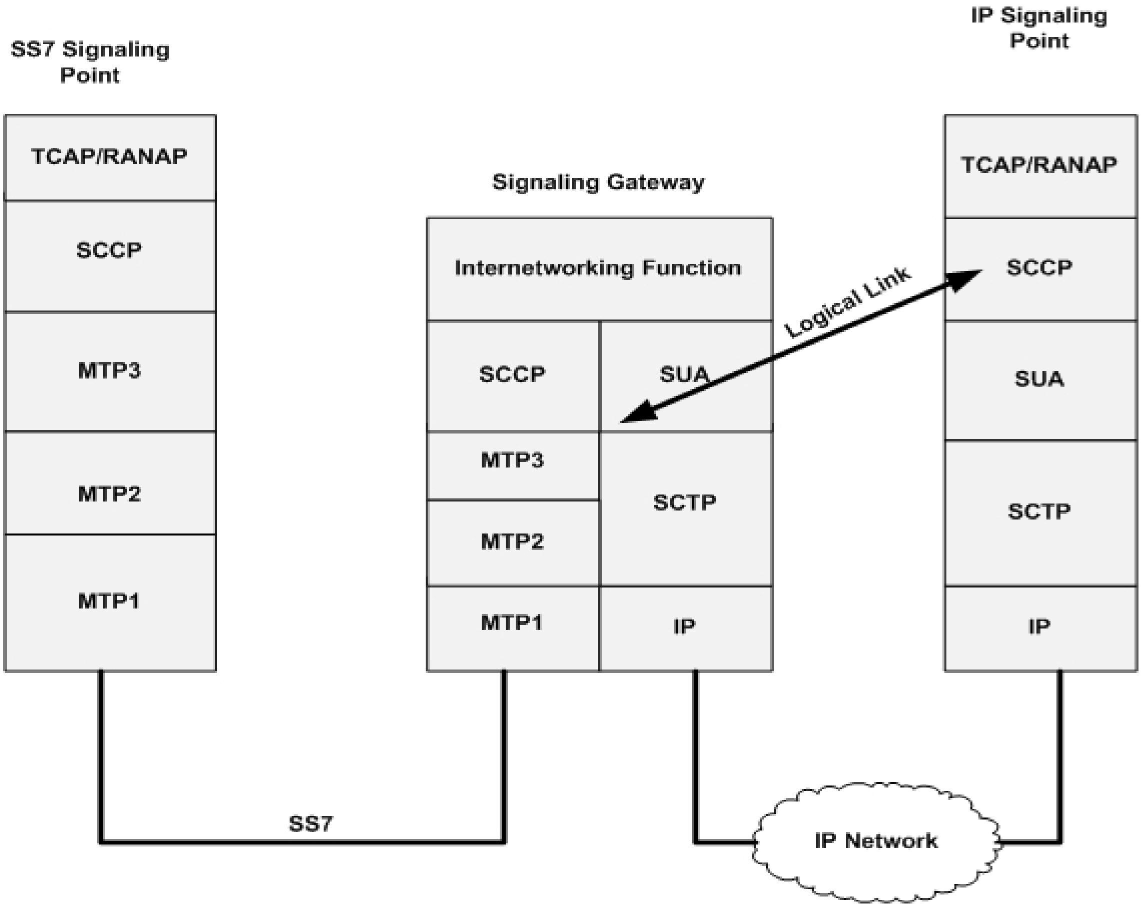


Figure 3.13: Use of SUA between SG and IP signaling point

3.4.4.1 SUA and M3UA Comparison

The protocol stack based on SUA is less complex and more efficient as compared to a protocol stack based on SCCP and M3UA. Consequently, SUA increases the efficiency of the core network and provides simpler implementations.

As from the comparison table below, in general, SUA provides much better scalability, powerful addressing, and more flexible routing capability for signaling network implementation in an all-IP network as compared with SCCP/M3UA.

Table 3.2: M3UA and SUA comparison [55]

	M3UA	**SUA**
SCCP Flavors	The signaling point is required to support different flavors of SCCP if it has to interoperate with different national systems.	This problem is eliminated using SUA.
ISUP Services	Supported	Cannot be supported
Addressing Aspects	Using M3UA each IP node is required to have both the IP address and point code assigned to it.	Using SUA each IP node does not consume scarce point-code resources
Routing Aspects	In M3UA the message is handled from point code to point code.	SUA allows the IP network to route the messages using global title information.
Implementation Complexity	M3UA needs the SCCP services	One protocol layer less. The elimination of SCCP reduces the complexity of the network node (implementation as well as management), therefore reducing costs.

4. System Implementation

Next generation radio access networks will rely heavily on packet transport for voice services. This chapter of the thesis report proposes an Integrated Mobile Access System (IMAS) prototype as the core network element of an integrated IP based radio access network. The IMAS acts as a Mobile Switching Center in standard cellular telephony terminology and includes a call processing system. This chapter also discusses issues with IP-GRAN, presents a generic network architecture based on IMAS to address those issues, and describes a working prototype of the system.

4.1 GRAN Network Architecture

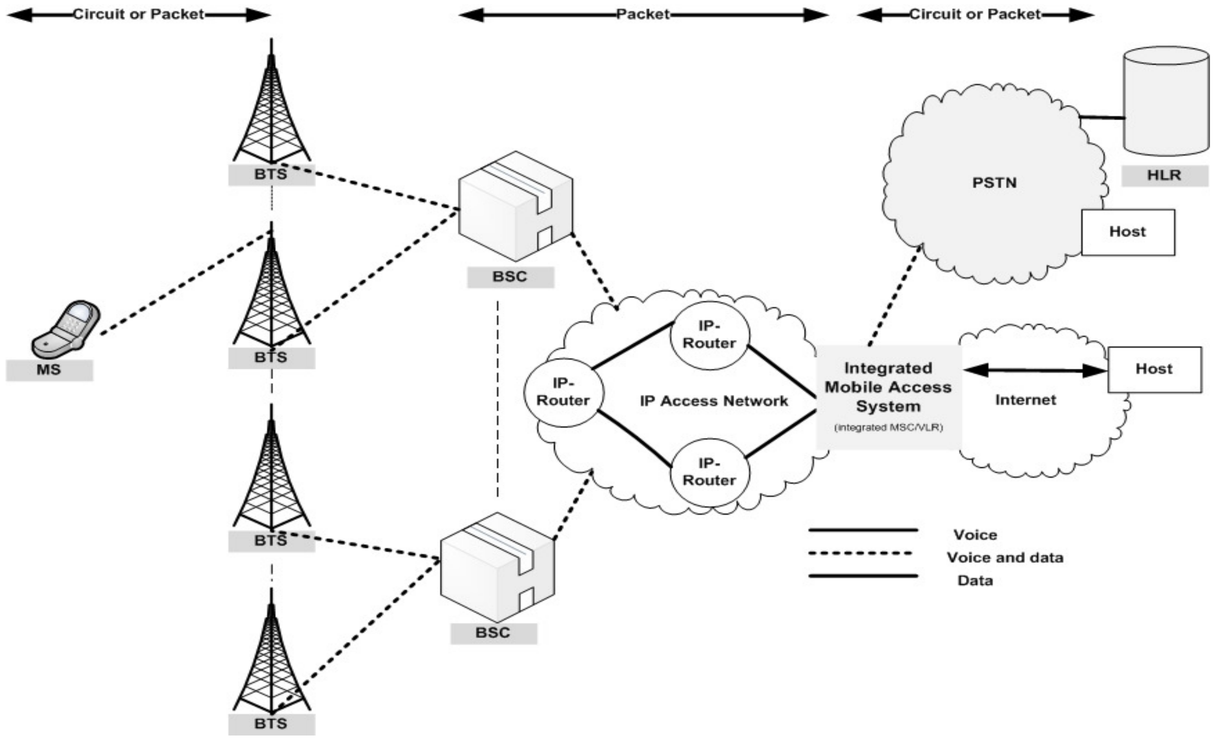


Figure 4.1: Packet Optimized Radio Access Network

The proposed architecture has several benefits:

- First, a single network node is introduced that replaces multiple network nodes in a conventional GSM network, by providing the support for both voice and data application; thus reducing the complexity and cost of managing the network.

- Second, by using a packet backbone network for transport of low bit-rate voice, statistical multiplexing gains may be made by implementing Dynamic Bandwidth Allocation (DBA) techniques; thus reducing the cost of facilities from the BSC to the gateway (or IWF) to the Public Switched Telephone Network (PSTN) [60]. This approach takes advantage of following attributes of a shared telecommunications medium:
  - All users are typically not connected to the network at one time.
  - Even when connected, users are not transmitting data (ex. voice) at all times.
  - Most traffic is "bursty" -- there are gaps between packets of information that can be filled with other user traffic.

This leads to statistical interactions among different traffic sources. The extent of multiplexing gain (spare capacity) is efficiently estimated and the bandwidth (resource) allocation is traded off in an optimal call admission control policy. It is possible to achieve high efficiency of statistical multiplexing for narrowband traffic, e.g., voice, which tends to obey the law of large numbers (assuming single TRX, seven simultaneous calls at full-rate GSM as capacity; the effect of statistical multiplexing can be observed at four simultaneous calls) and have low burst when many sources are superposed together in a high-speed packet/cell multiplexer [33, 44]. The following graph (figure 4.2 is based upon table 4.1) illustrates the statistical multiplexing gains as depicted in one of the Corvil White Paper published in March 2004 [8]:

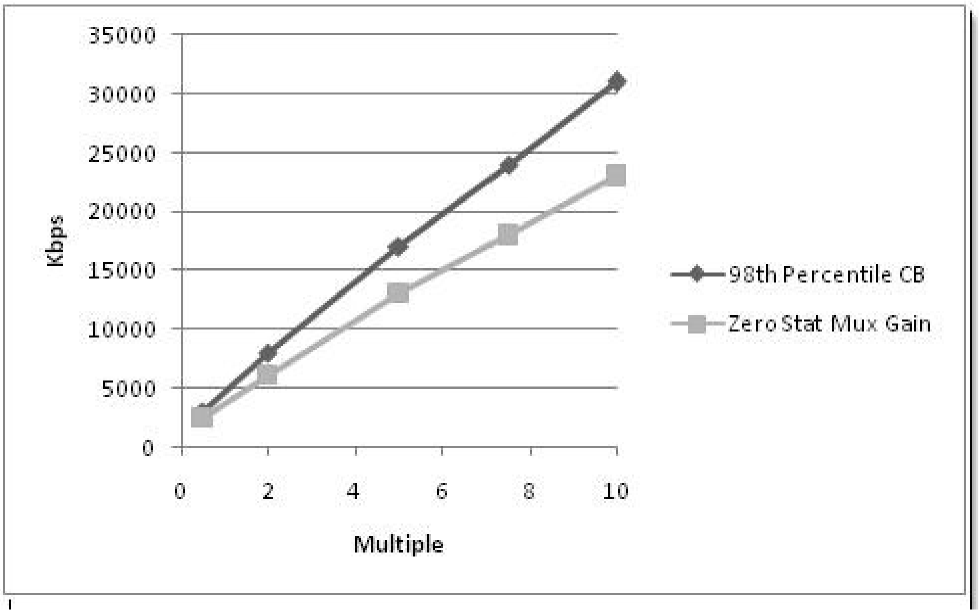


Figure 4.2: Statistical multiplexing gain graph

Table 4.1: Statistical multiplexing gain[8]

Multiple	**1**	**2**	**3**
Statistical Multiplexing Factor	100%	81%	66.31%
98th Percentile CB (Confidence Band)	4.683 Mbps	7.586 Mbps	12.526 Mbps

The graph above estimates the efficiency with which the measured traffic will grow. Here we see that the traffic will not grow linearly, but will multiplex quite well. If one were to assume linear growth then an upgrade to a larger link rate would be required.

To summarize, the difference between the bandwidth requirement of the aggregate and the sum of the per-stream bandwidth requirements is known as statistical multiplexing gain and it underwrites the promised effciency of IP networks. Unless statistical multiplexing can be quantified, the gain cannot be fully exploited and the associated economies of scale go to waste.

Typically with voice activity detection (VAD) enabled, the gain is a factor of two since rarely do both caller and callee talk at the same time. Additionally, there is traffic only if there actually is a call.

- Third, it is possible to support end-to-end voice transport over IP, because the system is based on IP.
- Finally, it is also possible to provide integrated wireless/wireline access with IP-based Quality of Service (QoS) mechanisms because the system is based on IP.

Note that here the mobile access network is always packet-based as the integrated MSC/VLR and the BSC have IP interfaces. However, as shown in Figure 4.1, the wireless link portion could be either packet or circuit-based and the backbone as being IP based. However, it does not say what the underlying physical and network layers are. This leads to four ways in which a cellular service may be offered [60] and the following section describes those as first, second, third and fourth level of service respectively. These four levels are used as terminology to identify four different service architecture designs but are not hierarchical in any way.

4.1.1 GRAN System Services and Operations

The proposed IP based system architecture is based on the following service flow:

1. The first level of service design, utilizes circuit access for A-bis (BTS ↔ BSC) and circuit egress to the PSTN [60]. This is the same kind of service as provided by a mobile network operator today, the only difference is that the access network (BSC ↔MSC) is packet-based rather than circuit based. In this case, only the communication with IMAS is packet-based, hence two media converters are required: one at the IMAS and one at BSC, to transform circuit switched user data into packets and establish an RTP/UDP/IP session between the appropriate BSC and the IMAS [5, 60]. In addition, voice coding/decoding functions are also needed inside the system to transform the voice into a format compatible with the PSTN gateway.

   The signaling and control functions implemented in the integrated mobile access system architecture must be similar to that of a standard MSC/VLR. The call processing must interact with the PSTN for database access (both Intelligent Network (IN) services and Mobility Management (MM) services) and connection control. The call processing must also interact with base station for paging and circuit establishment functions. To perform handoff between BSCs, the RTP/UDP/IP session between this system and the old BSC must be redirected to between the system and the new BSC [5, 60]. Considering the scope of this thesis project with its emphasis on a maritime GSM network, the access network is likely to be small. Thus, handoff will have same performance and efficiency as in current circuit switched networks.

2. The second level of service design, utilizes circuit access from standard cellular telephones and packet egress into the Internet. This is an evolution of first level of service in which the backbone network is also packet-based resulting in cost efficiencies due to reduced tariffs, packet multiplexing, and potentially avoidance of voice transcoding [60]. In this type of network architecture, the BSC acts as Media Gateway and formats the user circuit-switched voice into RTP/UDP/IP packets. In this design, performing inter-BSC handoffs, if required, is complicated. There are several options which are discussed briefly in the following text, and lies outside the scope of this thesis:
   - One option, similar to handoff processing in level one service, is for the end host in the Internet to redirect the RTP/UDP/IP session from the old BSC to the new BSC.

However, this may result in increased delay and packet loss during a handoff, because the packet flow may span a long distance.

- A second option is for the older BSC to serve as an anchor, by extending a new session to the new BSC as the user roams. While this option may result in minimal packet loss during the handoff, the efficiency of the network is reduced as the routing is no longer optimal. Given the specific scope of thesis project, the inefficiency, as mentioned above, has not been analyzed and quantized, but it has been proposed as part of the proposed future work.
- A third approach is to terminate one RTP/UDP/IP session between the end hosts in the Internet and initiate another session between the IMAS and the BSC. This allows local IP mobility support to perform handoffs, resulting in minimal disruption [5, 60].

3. The third level of service design, utilizes a packet air interface along with circuit-egress using the PSTN. This allows a wireless packet device to communicate with a traditional phone. In this scenario, the call processing will be similar to a standard MSC/VLR, with handoffs between the system and mobile device handled locally at the IP layer. In this case, the mobile device terminates the IP flow. In this type of network, the IMAS must act as a media gateway and also perform voice trans-coding [60].

4. Finally, the fourth level of service design, where packet access is end-to-end. Thus, the wireless packet device has the same capabilities as any other Internet attached device. Network servers are used to perform the call processing functions while mobility management (MM) is handled at network layer [5, 6, 11, 28].

4.2 Packet Optimized Radio Access System

The prototype of a Packet Optimized Radio Access System was implemented as part of this thesis project it supports first, second, and fourth level of services: GSM voice using standard GSM handsets, base terminal stations (BTS) and BSCs, GSM service using IP as bearer for signaling to mobile phones, and packet data from an IP-end device. This section, in keeping with the scope of this thesis project, only describe first level of the service design because none of the terminals, radio equipment, and interfaces to the PSTN need to be changed; unless some proprietary technology has been used for some element.

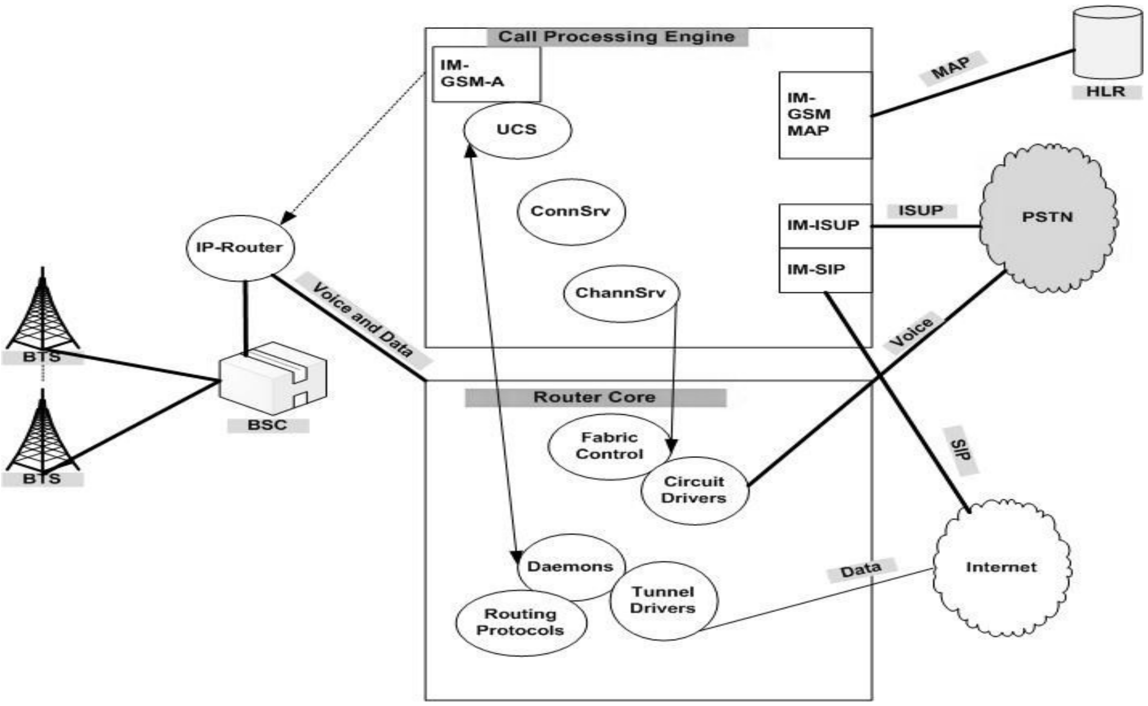


Figure 4.3: High level system architecture for packet optimized system

The high-level system architecture for this packet optimized system is shown in Figure 4.3. This system has two main components: a call processing engine and a router core. In the case of first level of service design (circuit-switched voice), the call processing engine performs MSC and VLR control functions, and controls the router core that acts as a media gateway and performs voice transcoding [60].

Figure 4.3 illustrates the overall structure of a network based on the prototyped implemented as part of this thesis project. The BSC translates voice and signaling information from a circuit switched format to IP packets. For signaling information the standard GSM interfaces from the BSC are tunneled in IP packets to the integrated MSC/VLR. For voice transport, voice samples are encapsulated as an RTP/UDP/IP stream.

For voice communication the access network may connect to the PSTN. To connect to the PSTN, media transformation between RTP voice packets and Pulse Code Modulation (PCM) voice samples is performed. Transcoding is also performed to translate between the compressed wireless CODEC (e.g. GSM speech CODEC) and the PSTN PCM CODEC (e.g. A-law or u-law). For terminating voice on the internet, voice transcoding may or may not be needed, depending on whether different coding schemes are deployed at the end points [60].

The prototype system currently has standard interfaces to GSM BSCs (i.e., using the GSM A-interface), HLRs (MAP), and the PSTN (ISUP). For data, the system provides an IP interface to the Internet. Details of the system operation for voice service are presented in the subsequent sections [7, 10, 41, 43, 60]. As might be expected there is nothing particularly special about providing data service with this architecture.

4.2.1 Call Processing

Call processing can support two types of wireless voice terminals: circuit-switched voice terminals (such as GSM phones) and packet-switched voice terminals (for example, those using with a packet radio interface such as GPRS). The current prototype supports the GSM phones, but it could be extended to support packet-switched voice terminals with the help of a suitable packet voice infrastructure (however, this lies outside the scope of this thesis project). We have emphasized only circuit GSM base voice service.

The call-processing engine is deployed on a set of single board computers to realize the MSC and VLR functions. This call processing engine can be also viewed as a signaling gateway (from a network's perspective) that supports voice over IP. The engine consists of a collection of functionally distributed servers as shown in Figure 4.2. The call processing and mobility management tasks are accomplished by their collaboration [60]. Two classes of servers were introduced:

- Core servers, and
- Interworking managers (IMs)

Core servers handle call processing and MM tasks. Whereas, IMs act as protocol gateways to internal core servers in order to isolate them from the external signaling protocols thereby allowing the core servers to evolve independently of these protocols. IMs also allow core servers to accommodate different standard interfaces (in this case GSM) [60].

In our network prototype, IMs support the GSM-A interface to the BSC (IM-GSM-A), GSM-MAP to the HLRs (IM-GSM-MAP), and ISUP to the PSTN (IM-ISUP).

There are three core servers:

- Channel Server (ChanSrv),
- Connection Server (ConnSrv), and
- User Call Server (UCS).

The ChanSrv is responsible for managing switching device resources, such as transport channels and digital signal processors for voice transcoding. These resources are allocated during call setup and reallocated following a call release. The Chansrv uses Media Gateway Control Protocol (MGCP) [39] to instruct the BSCs and the IMAS about resource allocation by transmitting media gateway control messages [42].

The ConnSrv coordinates the allocation of channel resources to establish a connection to the BSC of the cell in which the MS is currently roaming. The ConnSrv instructs the appropriate ChanSrv to reserve the necessary MSC channel resources and sends messages to external components via the IMs to reserve channel resources external to the MSC. For example, a ConnSrv may reserve network trunk resources using ISUP control messages through the IM-ISUP [5, 60]. When a client moves from an area served by one BSC to another area serving by another BSC, an inter-BSC handover occurs and the new serving BSC gets resources via a ChanServ. Standard handover protocol messages are utilized to reserve radio and terrestrial resources between the BSC and the mobile phone. Additionally, the ChanSrv updates the BSC address on IMAS to redirect traffic to the proper destination [60].

The User Call Server (UCS) manages the registration status of all the mobile devices presently roaming inside the service area of the system. UCS also performs some MM tasks such as paging, handover, mobile user authentication, and ciphering. These mobility management procedures are implemented in UCS so that they can be easily reused for the IP packet data system, if and when required.

The call processing system discussed for wireless circuit-switched access networks above can be extended for IP packet-switched terminals with IP telephony clients supporting protocols such as the Session Initiation Protocol (SIP). This requires changes to the IM interfacing with the BSC, generically called the IM-BSC (this is the IM-GSM-A in our configuration). Transport mobility functions will be handled by the IP layer; however, the IM-BSC will perform the non-transport mobility functions such registration and authentication [60].

In a related work [41], it was shown that a call processing system based on the same design principles as those that are the basis for the system presented here; i.e., high call throughput can be achieved at low latencies and the call processing performance achieved by both circuit switched and packet-switched processing will be same. Further, this related work states that for a pure packet based system, which could be developed extending the fourth level of service design as depicted in this chapter, the achieved call processing performance will be equivalent to any VoIP system.

4.3 Softswitching

IP voice solutions are beginning to make significant inroads among telecommunications network operators because IP voice solutions can deliver quality greater than or equal to traditional telecommunications network, rather than simply best-effort performance. It seems to be very clear that a growing proportion of telephony traffic is getting carried over IP networks, whatever technical challenges may be.

Traditionally, vertical integrated network architectures delivered single services such telephony, television, or data access. IP technology has introduced a converged network architecture enabling service execution, control, and connectivity to be horizontally integrated across multiple access networks. Softswitching [15] is one such scenario where IP technology can efficiently separate the call control and switching functions into different nodes; consequently separating control and connectivity layers, (see Figure 4.4 and Figure 4.5).

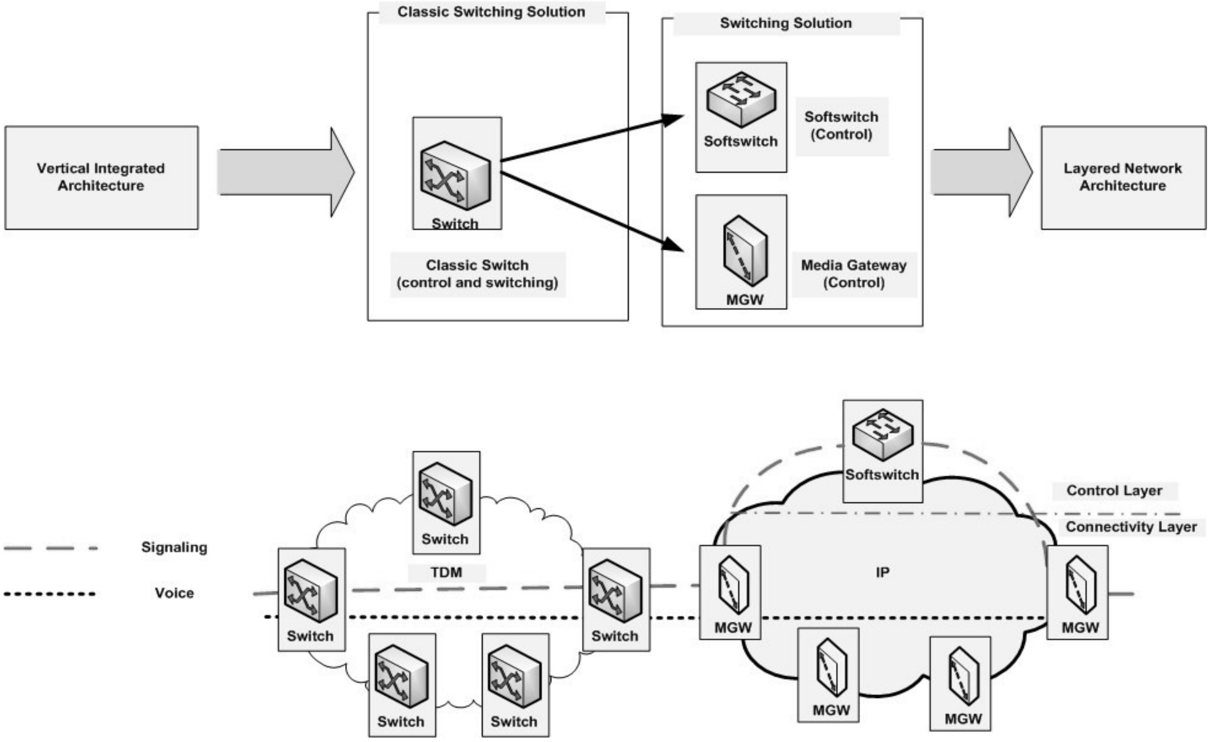


Figure: 4.4 Vertical networks to layered architecture

Softswitching is a critical step in migration to all-IP network architectures. Architectures based on softswitching efficiently support IP transport signaling and voice which were not supported by classical TDM based switching. Softswitches act as control servers for the control layer, where softswitches manage the end--end signaling path between network nodes and other networks to setup a call.

Softswitches control Media Gateways (MGWs) using Media Gateway Control Protocol (MGCP). The MGW is responsible for connectivity to and from the IP backbone network and for media stream processing (such as transcoding). The MGW also provides interfaces to the access nodes and to other networks such as VoIP or TDM [15]. This fundamental characteristic of softswitching supports an evolutionary approach to network development, allowing migration of technologies and services, as the need arises.

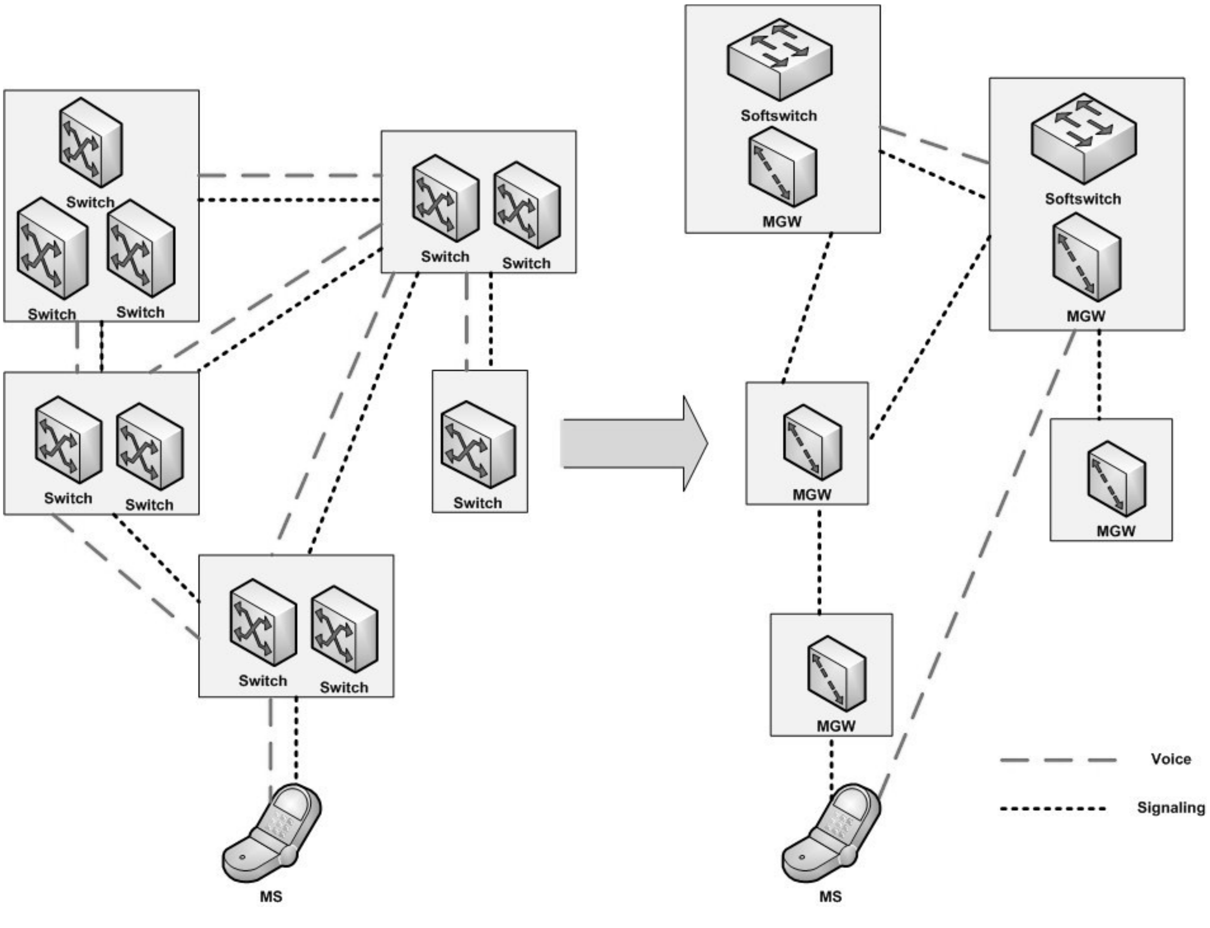


Figure: 4.5 Initial network topology vs. softswitch network topology- all servers are centralized at two main sites

5. Optimization: Optimal Routing

From the perspective of SS7 addressing, each User Part approaches addressing in a different way. The role of MTP (Message Transfer Part) is to reliably transfer messages over the links in a link set. Thus, MTP only cares about the address of the node at the other end of the links. Thus, the only addressing the MTP requires is the SPC (Signaling Point Code) of the node at the end of its links. MTP sees this address as the Destination Point Code (DPC) of all messages it sends over the links. The MTP makes use of the DPC to determine the link for sending the message.

ISUP addressing is somewhat different. In a call control scenario, ISUP addresses a switch at the other end of its trunk which also means using a DPC. However the switch ISUP wishes to communicate with (which is the next switch in a circuit being set up or torn down) is not necessarily or even likely to be located at the other end of its own SS7 links [20].

The responsibility of addressing all other locations lies with SCCP, which could also be used to address the same switching locations as ISUP. Thus SCCP can handle end-to-end signal routing in conjunction with ISUP. However, SCCP is rarely used for switch-to-switch routing; instead ISUP is preferred as it provides complete circuit information for all switches along the voice path. Similar to other user parts, SCCP also makes use of DPC. This address can be used to get a message to any node in the global SS7 network, but this alone is not sufficient. The reason is that at each DPC there is a "system" operating. This system may be a call control application or a database or some other program of some type. Using the DPC as the SS7 address will deliver the message to the "system", but it is not sufficient to deliver the message to the appropriate (database) application. For this purpose, a separate identifier of a subsystem within the system is required; this is the Subsystem Number (SSN). The SSN maybe thought as a database identifier, but it can be used to sub-address any location at which multiple applications are running; hence a switch offering several features may use SSN to separately identify each feature. SSN should thus be treated as an application identifier [20], it is analogous to a port number for UDP, TCP, and SCTP.

The third addressing mechanism is based on Global Title (GT). This brings up the important issue of optimal routing. A Global Title can be viewed as an address to use when the entity doesn't know the destination's actual current address. A Global Title implies the need for translation. In simpler terms, it is an address, but not the address of a node in the SS7 network

(DPC, SSN). The GT translation eventually results in the DPC (and possible SSN) address of an entity currently attached to the network at some point. Because this point of attachment can change and thus a globally valid address is required to be able to address the same entity. This corresponds to the Mobile IP home address for a node in the case of an IP network.

5.1 Global Title Translation (GTT) based routing

Global Title Translation (GTT) based routing is one of the important features for the optimization of routing in mobile wireless networks. The following diagrams (Figures 5.1and 5.2) illustrate the difference between the traditional routing and GTT routing:

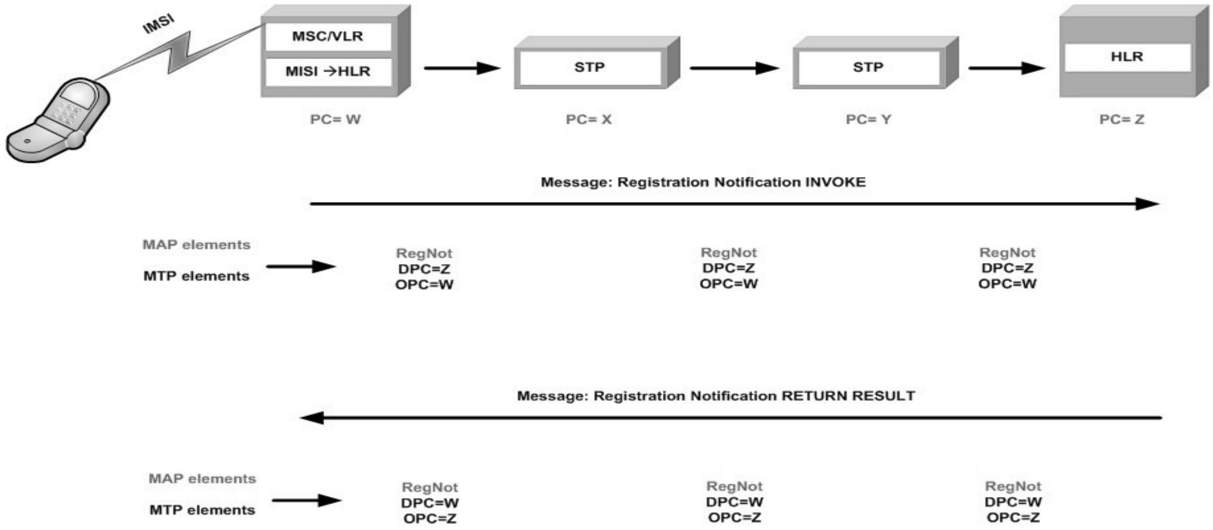


Figure 5.1: Traditional routing in a mobile network

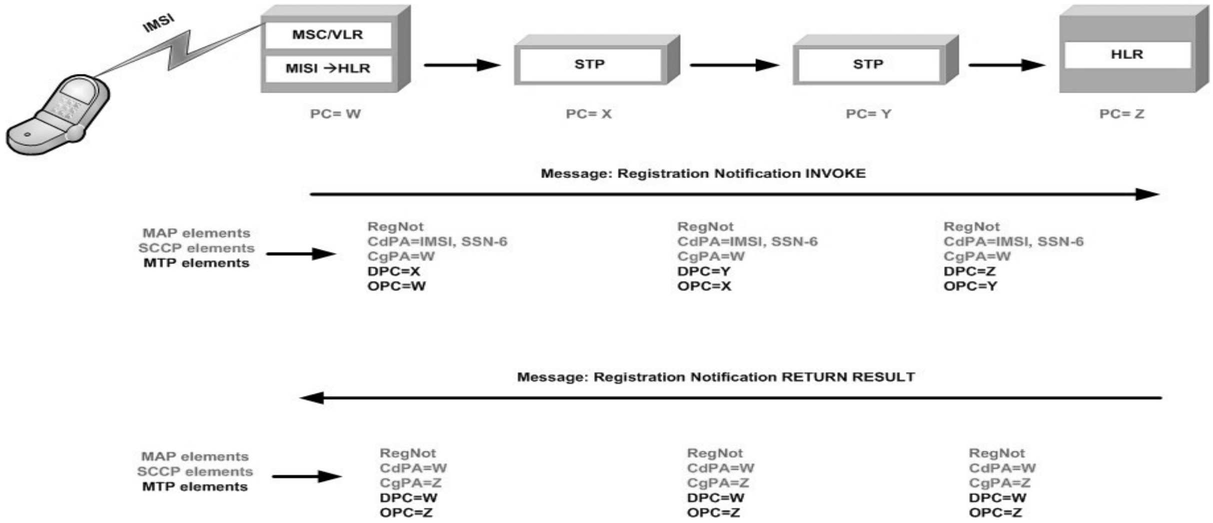


Figure 5.2: GTT routing scheme

As seen from Figure 5.1, the MSC is required to know the point code of the final destination in order to validate a roamer via their Home Location Register (HLR). Because STPs do not store any routing informations, STPs route the message using the point code routing information provided by large routing tables stored in the MSC.

However, in case of GTT routing, as shown in Figure 5.2, the MSC is not required to know the point code of final destination. The MSC only needs to know the point code of the adjacent STP pair and leaves the routing task to the STPs through the SCCP parameters: Called Party Address (CdPA) and Sub System Number (SSN). Based on the IMSI, the CdPA is used in conjunction with SSN number to indicate the routing to an HLR. In the GTT routing scenario, at least one of the STP pairs need to store the routing information to reach the final destination (i.e., the HLR), thus large MSC's tables need not be updated every time a new numbering range belonging to a roaming partner is allocated. Instead, the routing information is updated once in the STPs those control the routing, such as those belonging to the signaling hubs; thus providing simpler route management and the possibility of interconnecting different networks with ease [47].

5.2 International Roaming Network

In mobile communications, a SS7 signaling protocol is defined to transport the signaling messages for international roaming control, as is shown in Figure 5.3.

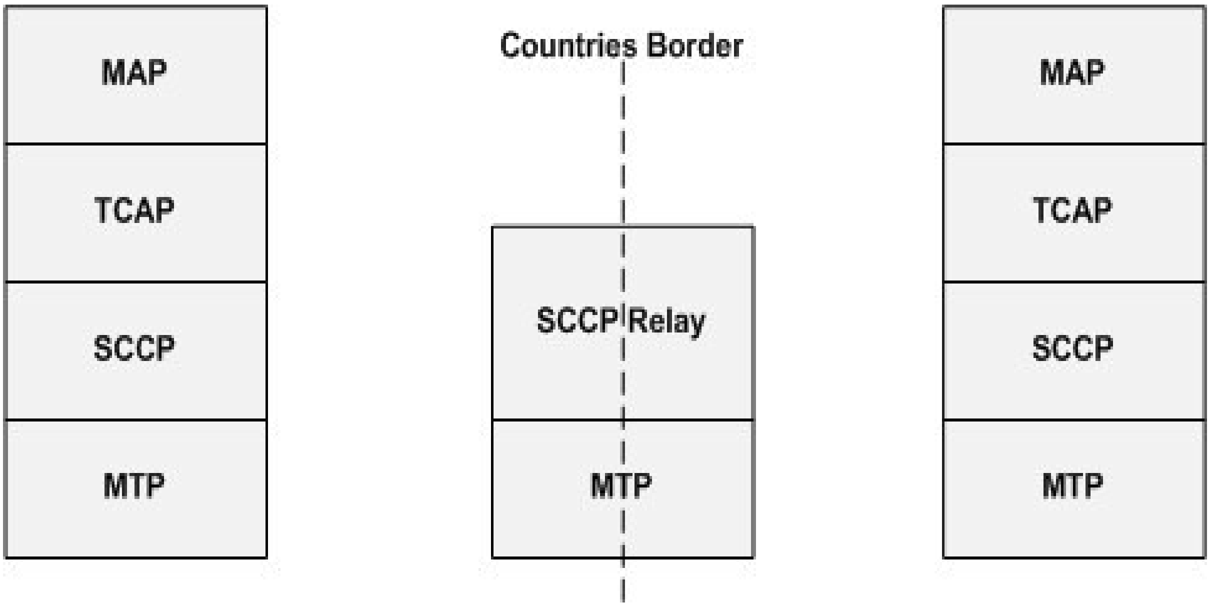


Figure 5.3: Signaling protocol stack for international roaming

MTP transfers connectionless signaling information across the international signaling network to its destination. A signaling point with MTP capability is called a Signaling Transfer Point (STP) (for detailed descriptions refer to section 3.2.1).

In terms of addressing capability, the MTP is restricted to delivering messages to an adjacent node whereas SCCP extends the routing capability to the international signaling network. SCCP performs the translation function (GTT) which translates the SCCP address parameter, global title-containing implicit address information not routable by the MTP, to a point code (DPC, Destination Point Code) and SSN. This Global Title Translation can be performed at the originating signaling point of the message or at an SCCP relay node.

The GTT function supports several numbering plans such as E.164 for ISDN/telephony numbering plan, E.212 for land mobile numbering plan, and E.214 for ISDN/mobile numbering plan. This roaming related data is stored in distributed databases across the international roaming databases. The international roaming database contains the following specific information [48]:

i. The E.164 Country Code (*CC*) and National Destination Code (*NDC*) of an *MSISDN* number.
ii. The E.212 Mobile Country Code (*MCC*) and Mobile Network Code (*MNC*) of an International Mobile Station Identity (*IMSI*) number.
iii. The E.214 Country Code and Network Code (*NC*) of a Mobile Global Title (*MGT*) number.
iv. The Mobile Station Roaming Number (*MSRN*).
v. The international signaling point code (ISPC) used by two standalone/integrated STP nodes which the concerned mobile network is connected to.
vi. The type of exchange used, as the two (two, for redundancy) international gateway nodes, which the concerned mobile network is connected to

5.2.1 Routing and addressing

The *MSISDN*, *MSRN*, *IMSI*, and *MGT* are the four most important numbers for international roaming. In principle, the *MSISDN* should sufficient for any subscriber of the ISDN or PSTN to call any Mobile Station (MS) in a Personal Communication Network. This is because MSISDN consists of the CC+ national mobile number which is equivalent to CC + NDC + SN (Subscriber Number.) Alternatively, an MSRN is temporally assigned to an MS by the VLR with which the MS is registered. This MSRN is stored by the HLR and indexed by the MSISDN. The GMSC uses this MSRN to route calls directed to an MS. The format of MSRN is identical to the

MSISDN [48], however, this represents a temporary number assigned from the pool of the operator's MSRNs and this number is only valid and used within the currently attached network.

Additionally a unique IMSI is allocated to each MS, which is composed of MCC, MNC, and MSIN (Mobile Subscriber Identification Number). The MCC uniquely identifies the country code of the operator who issued the SIM card. The MNC identifies the home PLMN of this MS, while the MSIN uniquely identifies this MS within that operator's network.

The MSISDN and IMSI are used as a GT address in the SCCP for signaling routing to HLR of the MS. The translation scheme is given in Figure 5.4. The {CC + NDC} provides sufficient routing information to address the exact DPC and SSN. In order to access the database HLR for example, the SCCP of the MSC translates the IMSI to the MGT. Next, the SCCP of the integrated STP translates the MGT to the international SPC of the specific DPC which will be the destination address [48].

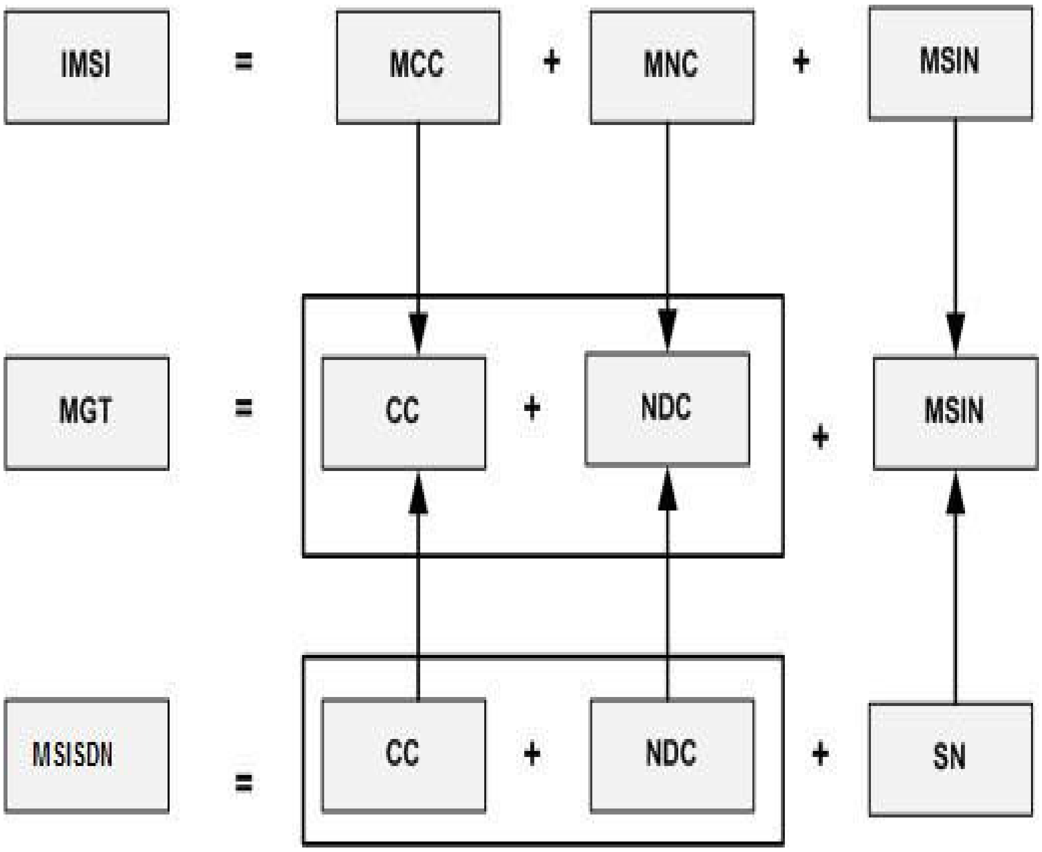


Figure 5.4: Mobile GT translated from IMSI and MSISDN

5.2.2 Global Title Translation Scenarios

a.) Registration & Location Update

Assumption: MS is assumed to roam to a foreign network

The following steps will occur (they are illustrated in figure 5.5) [48]:

- When this MS is first activated in this foreign network it initiates a location registration to the VLR in the visited network.
- This registration message is transferred to the VLR by a location update message.
- Upon receiving this registration message, the VLR checks whether this MS is already registered or not. If MS is not registered, then VLR analyzes the IMSI of MS to determine the home HLR to which MS belong. Next, the visited VLR communicates with the home HLR using the *MGT* derived from the *IMSI.*
- Consequently, the *MGT* is analyzed by the SCCP routing function. The location update message is transmitted to a node in a foreign country based upon the *CC* of this *MGT.* Therefore, the gateway SCCP relay node takes charge of the translation from the originating node and the *SPC* of the subsequent SS7 network is determined. GTT is performed repeatedly in all intermediate SCCP relay nodes until the home HLR can be queried using {*NDC+MSIN*}. The GTT performed by the SCCP translates the SCCP address parameter from a global title to a point code and a subsystem number.
- Upon receiving this location update message, the HLR sends the MS profile data to the visited VLR using the received visited VLR number.
- Finally, the home HLR asks the old VLR to remove the MS data from its database (labelled "cancel MS data" in the Figure 5.5).

b.) Mobile originated call

Assumption: MS is assumed have roamed to a foreign network

The mobile originated call will query the visited VLR database and home HLR database using the same GTT [48], as described in the registration scenario above (see Figure 5.5).

c.) Mobile terminated call

Assumption: MS is assumed have roamed to a foreign network

The following steps will occur when a PSTN subscriber dials the MSISDN of MS (The GTTs performed are shown in Figure 5.6.) [48]:

- The exchange of the PSTN will route the call to GMSC of the MS based upon a GTT of the MSISDN.
- The GMSC performs a GTT on the MSISDN of the called MS to determine the appropriate HLR to interrogate for the present location of this MS.
- Subsequently, this HLR interrogates the visited VLR for a routable address, such as a MSRN.
- The HLR responds to the GMSC with the routing information and *MSRN*.
- Consequently, this call is routed from the GMSC to the exact responsible MSC in the visited foreign network.

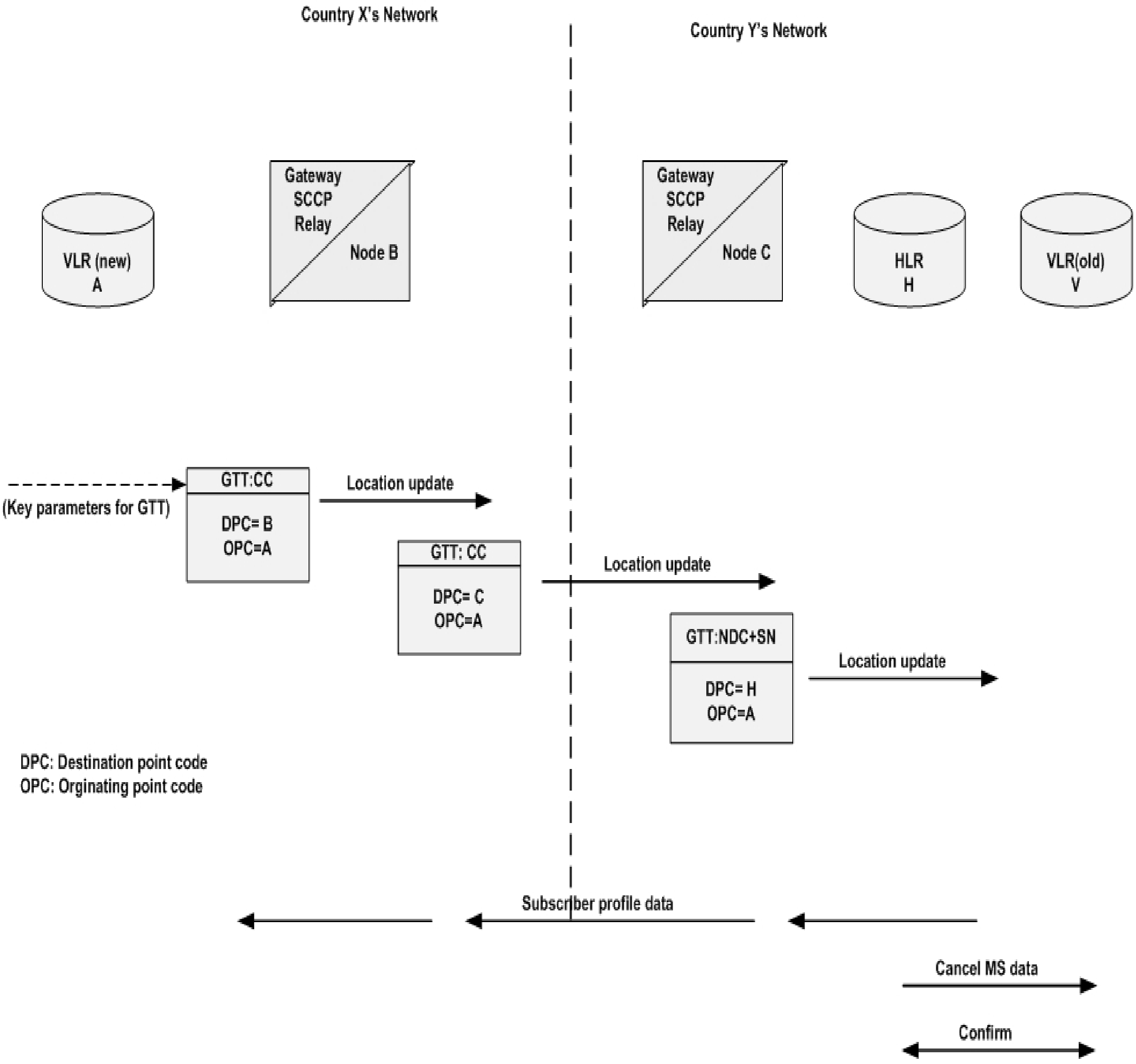


Figure 5.5: Registration and location update with mobile GTT function

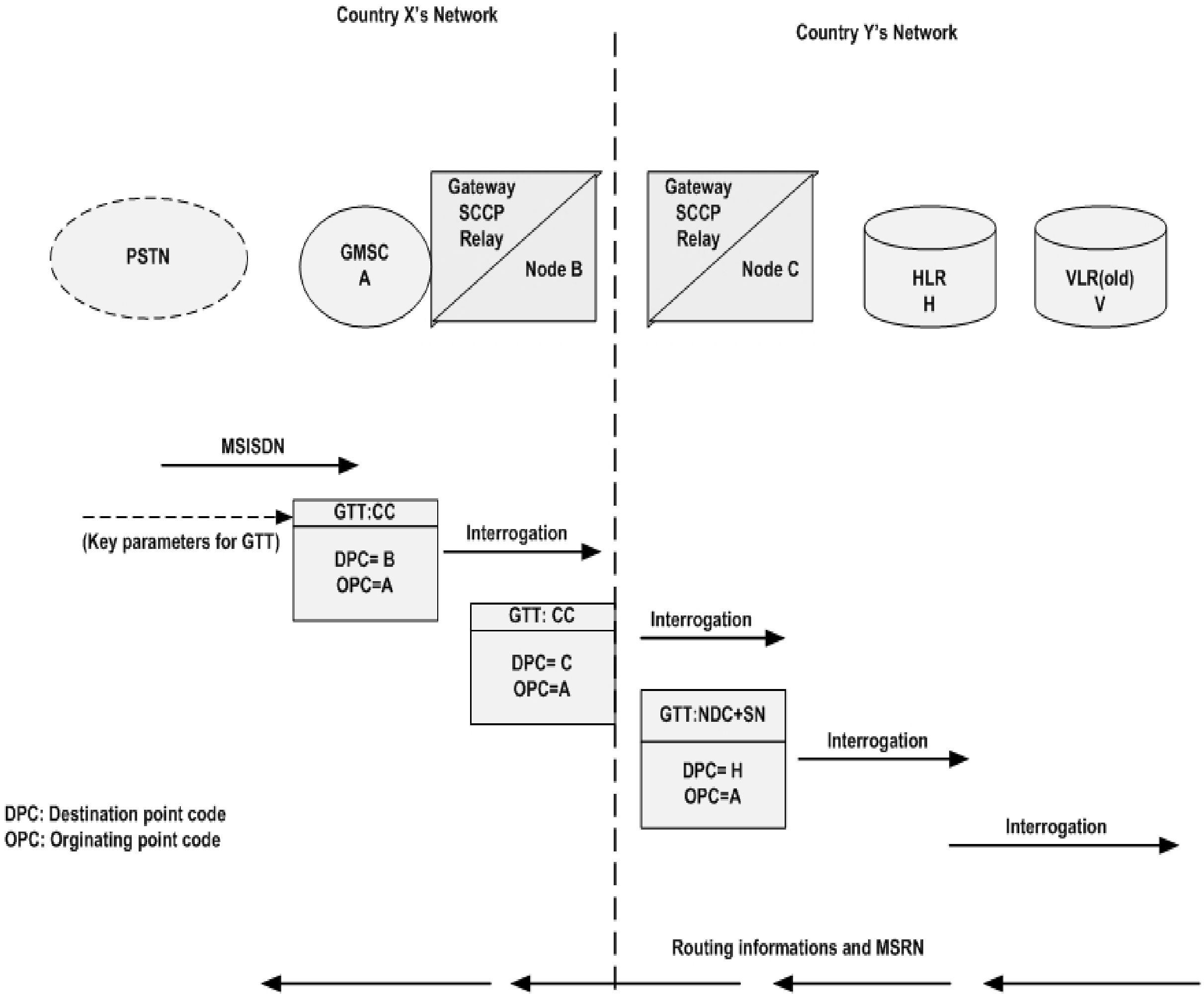


Figure 5.6: Mobile terminated call with mobile GTT function

5.3 Optimized Routing Proposals

Assumption: A mobile stations roams into a foreign network

Problem Statement: When a MS roams to visited network; we will call this MS a roamer. If a caller in the local network wishes to make a call to the roamer, this call will be routed to the roamer's home country and the call will then be routed from the roamer's home country to the visited network. The caller has to pay for the call to the roamer's home country while the roamer has to pay for the dialing leg from his home country to his (current) visited network. This is quite undesirable for both caller and roamer, especially if the call and the roamer are in the same country and even worse if they are in the same network!

5.3.1 Proposal-1: Network Virtualization (NV)

We will assume that we have access to the SCCP gateway of the respective country. In the case of international roaming, all signaling messages are sent through the signaling link and verified by this SCCP gateway. Therefore the SCCP gateway can keep track of the present location, and the subscriber profiles of subscribers who have roamed into this network. The proposed network virtualization solution adds the following three main components:

- A Virtual VLR: To store roamers' profiles.
- A Virtual HLR: Communicate to the serving mobile network using mobile application protocol (MAP).
- A Signaling Link Probing Daemon (SLPD) which is used to constantly monitor the signaling link and capture all SCCP messages.

5.3.1.1 The Workflow (with network virtualization)

- As soon as an roamer performs a location update, the roamer's profile (IMSI, Sub-status, MSISDN, Visited Mobile Switching Centre (VMSC), HLR, etc) are extracted and stored in the Virtual VLR
- When an inbound call reaches the International Telephony Switching Centre (ITSC)/SCCP gateway the Virtual VLR will be queried. The caller and roamer should not be from the same country or the caller should also be roaming. Otherwise, the caller will be in the home network and thus the SCCP will occur in the home PLMN, therefore the network virtualization approach does not work (an explicit reason for considering the second case of Optimized MSRN Assignment, as discussed in section 5.3.2)
- The gateway, by analyzing the B-number (the called number) will look for a prefix of '00' indicating an international call; this initiates a trigger to forward the B-number to the Virtual VLR using (Intelligent Network Application Part (INAP).
- If the B-number is found in Virtual VLR, then the Virtual HLR will utilize the roamer's profile to obtain the addressing of the roaming/serving network. If the B-number is not found in Virtual VLR, then the HLR of the callee will be queried which in turn will query the VLR of the callee's last known serving network (could also be the home network) for a MSRN.
- Based on this information, the Virtual HLR requests the serving network to provide a MSRN in order to initiate the connection.
- The serving network acknowledges the request and provides a MSRN to the Virtual HLR for call setup.

- The B-number will be translated to the acquired MSRN and the result sent back to the SCCP gateway.
- The call will now be setup with the called roamer, thus reducing the two international calls into one local phone call.

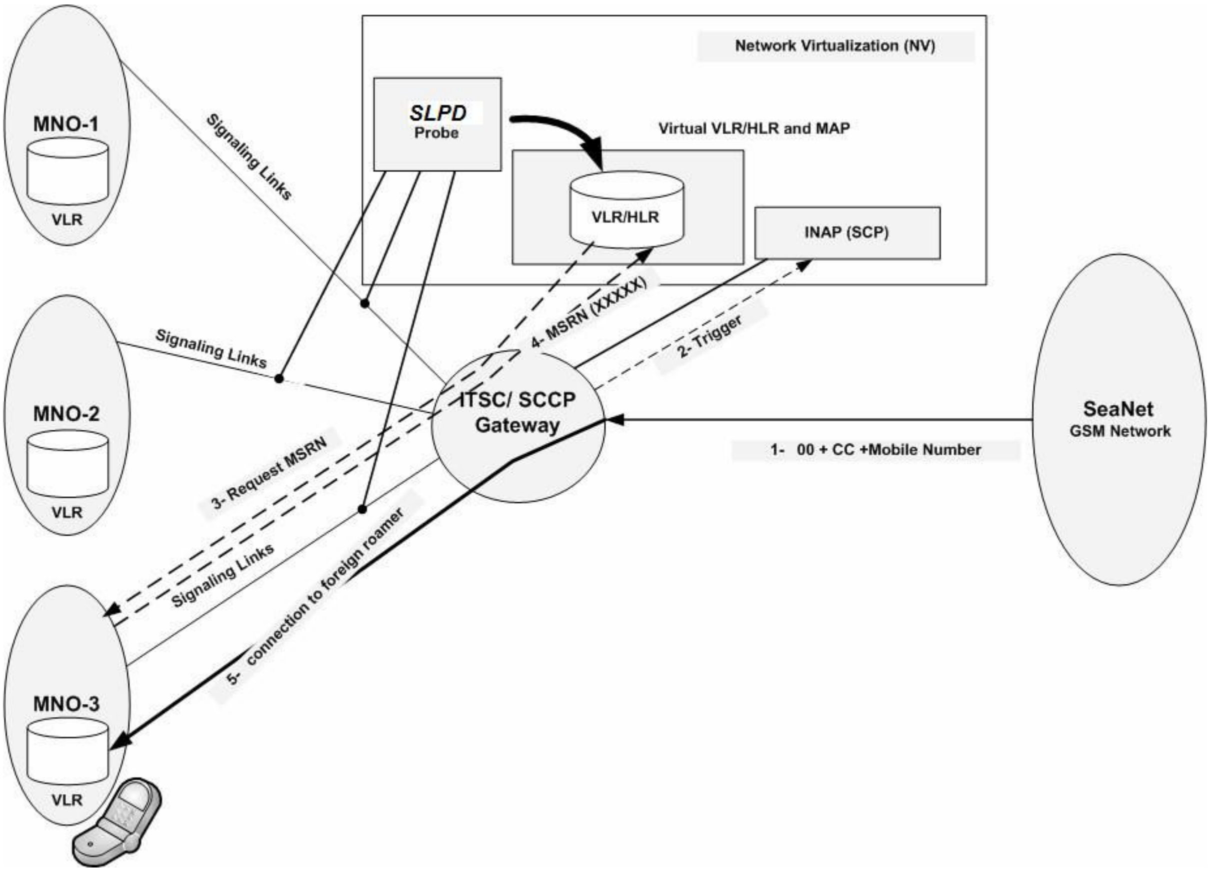


Figure 5.7: Network virtualization configuration and call flow scenario

5.3.2 Proposal-2: Optimized MSRN Assignment (OMA)

Assumptions:

- That it is possible to change the MSRN assignment logic (software) in the MSC to support Optimized MSRN Assignment (OMA).
- Possibility to create and maintain a database within the MSC to support the OMA algorithm.
- International In-bound Roaming.
- That the caller and roamer, both from the same country.
- Visited Network: foreign country.

5.3.2.1 The Workflow (Pre-OMA)

Figure 5.8 shows the case when a roamer is registered in a visited network. We have assumed that the home network and the visited network are in different countries.

The roamer is called by a caller (in the roamer's home network) at his/her mobile number (i.e., MSISDN in GSM nomenclature). The GMSC of the caller sends a MAP message, SRI (Send Routing Information) along with the MSISDN of the roamer to the HLR of home network. The HLR of the home network will now send (via the international SS7 network) a new MAP message, PRN (Provide Roaming Number), along with the IMSI, to the GMSC of the visited network.

The PRN request indicates that the MSC should return a temporary telephone number (MSRN) at which the roamer can be currently reached. The MSC picks up a MSRN from the MSRN series available to it and returns this to the HLR This MSRN has the same CC (ex. +39) as that of visited network. The HLR now returns this MSRN via a SRI to the GMSC of the caller so that it can perform a call setup between the caller and the roamer (i.e., the called party). Based on the MSRN, GMSC of the visited network knows how to reach the roamer via its radio access network.

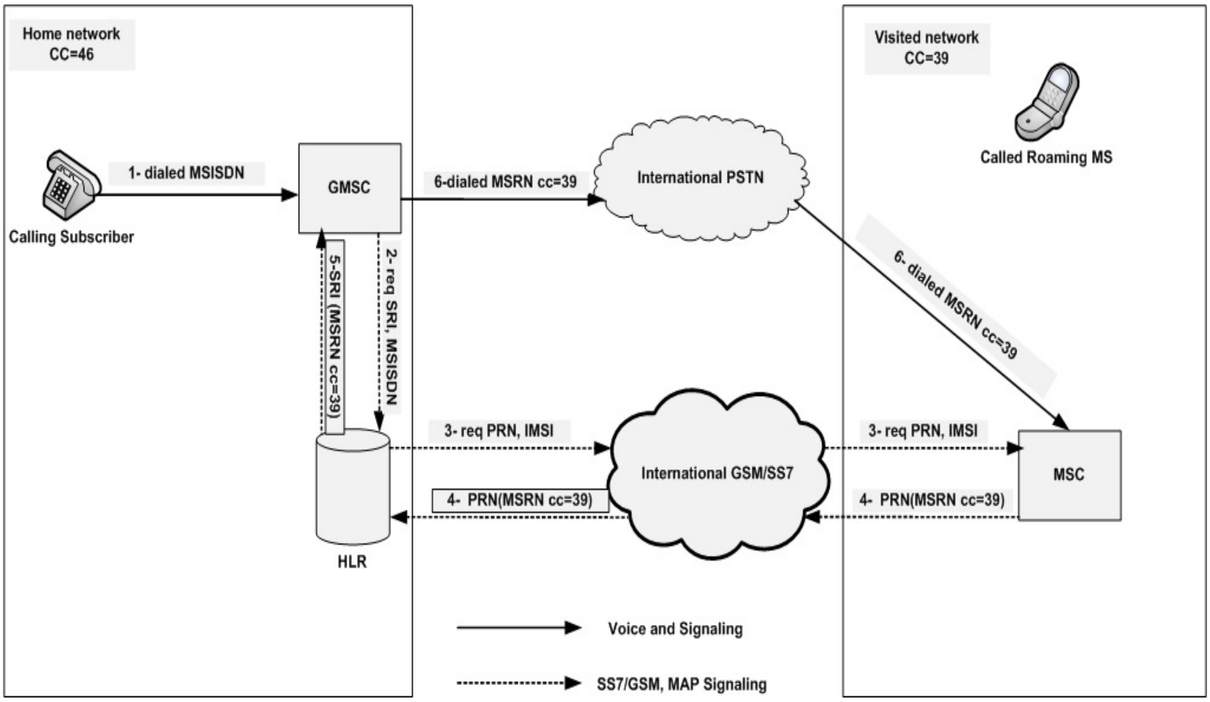


Figure 5.8: Pre OMA call routing

5.3.2.2 The Workflow (Post-OMA)

Figure 5.9 shows the same scenario as Figure 5.8, but with OMA implemented. The OMA algorithm will select and assign MSRN based on a least cost routing algorithm (see Figure 5.10).

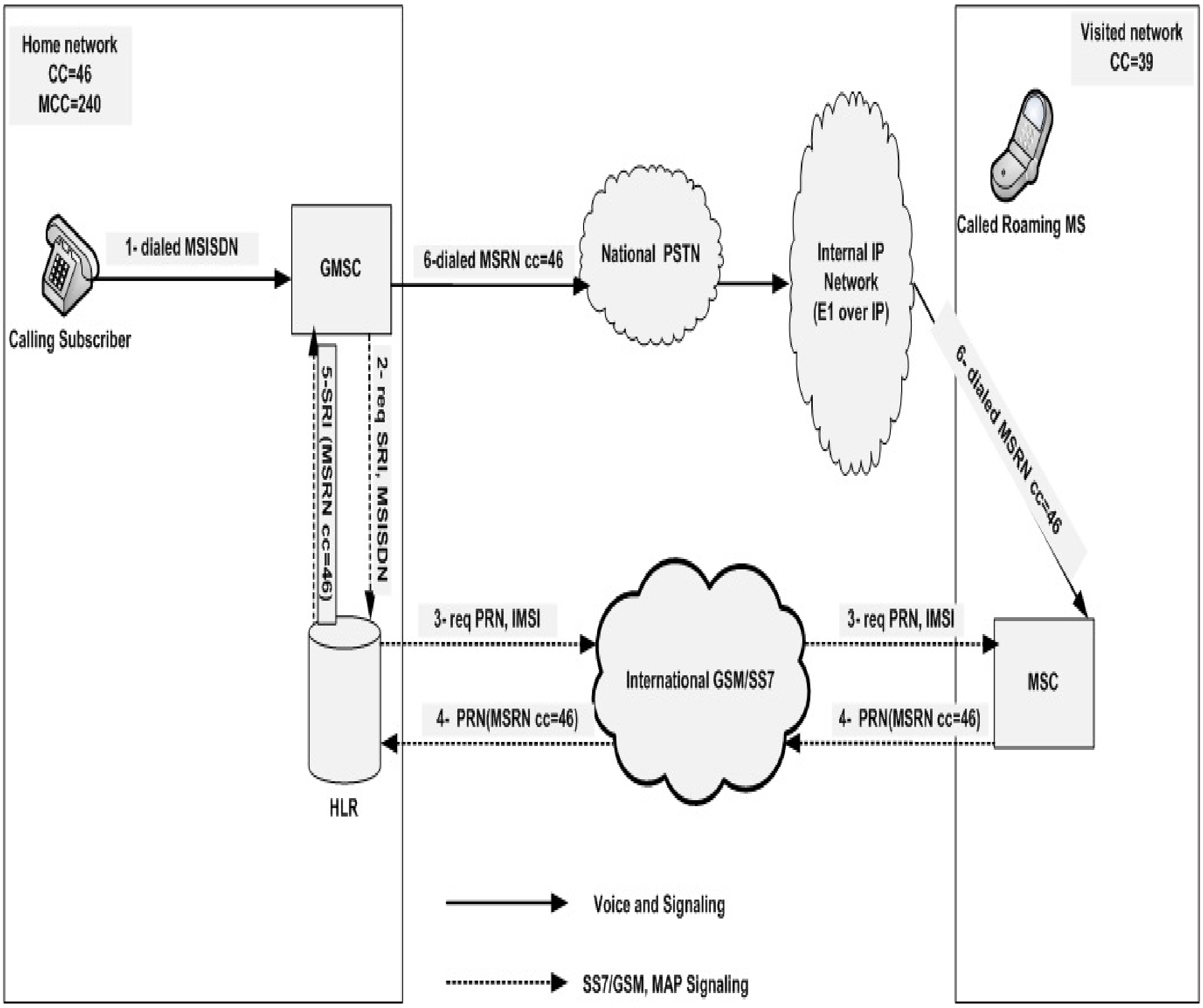


Figure 5.9: Post OMA call routing

One major difference between the architectures in Figure 5.8 and Figure 5.9 is that the assigned MSRN now has the same CC (ex. +46) as that of the home network. Thus the caller will see this as a national call, which is what they expect since we began with the assumption that the caller and callee had the same home network. Considering the workflow described previously, the HLR send a MAP-SRI along with IMSI to the visited network's GMSC for allocation of a MSRN. It is at this point that the OMA algorithm (shown in Figure 5.10) is utilized to allocate the MSRN.

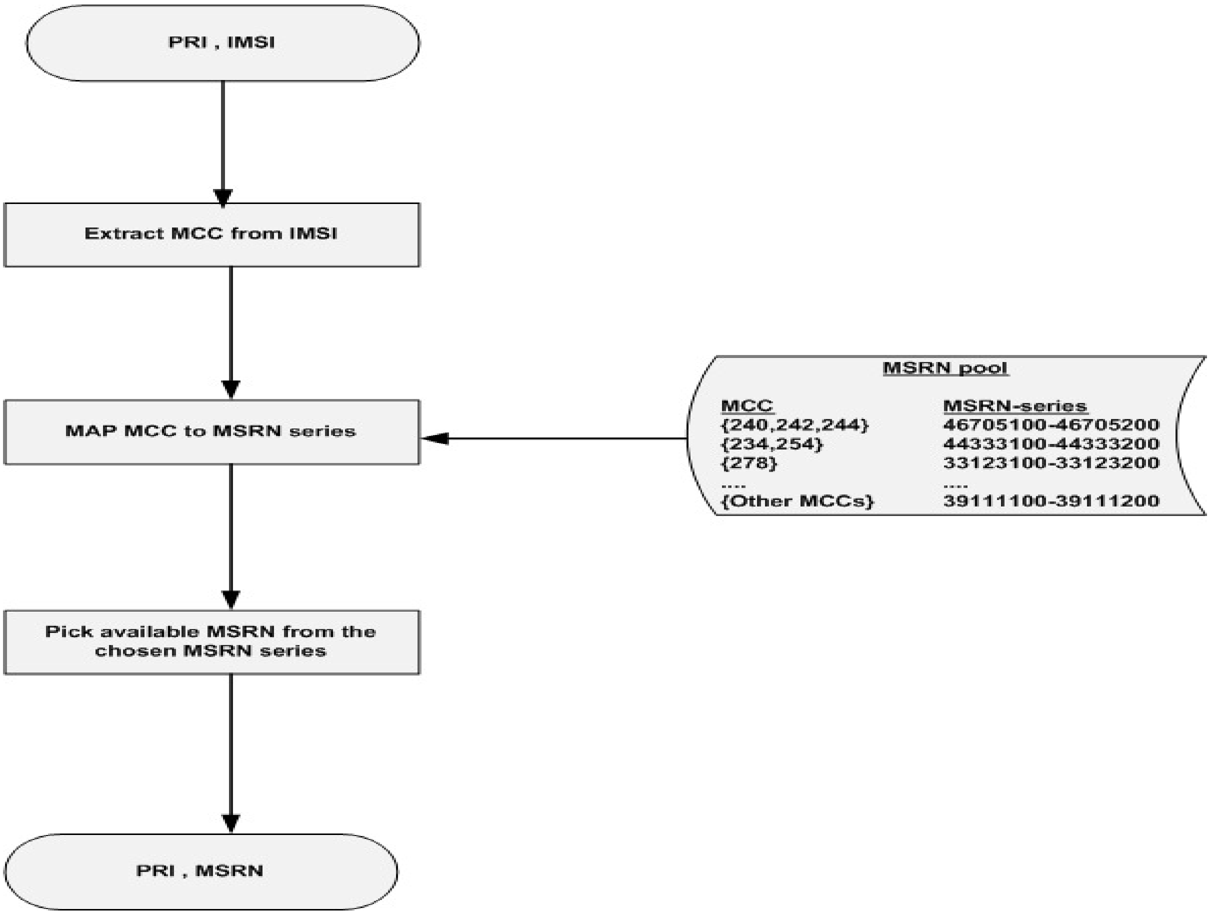


Figure 5.10: OMA algorithm for MSRN allocation

OMA extracts the Mobile Country Code (MCC) of the roamer's network from the IMSI received by the MSC along with MAP-PRN from the home network's HLR for a MSRN. The extracted MCC is used as an index in the OMA's database to acquire a MSRN based on a least cost routing algorithm. The OMA algorithm maps each MCC to multiple set of MSRNs which have the same CC as that of home network or are the best path in terms of least cost routes.

The MSRN which will now be returned by the GMSC in the visited network to the home network's HLR will have the same Country Code (CC), as the home network. The HLR of the home network will return this MSRN to the GMSC of the caller and the call will therefore be terminated in the national telephone network. Based on the terminating number (the MSRN in this case), the call will then be carried over an IP network (perhaps using TDM over IP) to the GMSC of the visited network for eventual call setup to the roamer over the visited network's radio access network.

5.3.2.3 Limitations:

a. The visited network needs an allocation of addresses in the home country's country code! Hence they have to be assigned these by the numbering authority of the home country, which under most circumstances would require that they are a registered operator in this country (not applicable universally). However, with the changing regulatory equation globally, this barrier could also drop in the near future.

b. The size of this allocation is the largest number of subscriber's from this country that can roam into this visited network and receive this optimized call routing. However, these allocated numbers would be used for MSRN allocation which are used just for the duration of call setup and are released back to the pool of available numbers once the call has setup.

6. Traffic Dimensioning in IP-GRAN: Simulation and Analysis

This chapter of our thesis focuses on the factors influencing the dimensioning of the link, by taking into consideration a system which uses the IP network in order to deliver voice and signaling to a GSM radio access network. The two main factors analyzed herewith are packet drop and jitter. The methodological approach is as follows:

- To calculate packet loss and jitter at different load and bandwidth
- To analyze the effects of DTX over the IP link to reduce bandwidth
- To analyze the effects of signaling on the link

6.1 Simulation Environment

In architecture such as the one proposed in this thesis, in the case of remote deployments, discrete individual networks nodes (BTS, BSC) are linked to the main core network via IP links, implemented via IP-VPNs (Virtual Private Networks) and, deployed using IP-over-Satellite inks.

This section focuses upon the necessary parameters required for dimensioning links for IP-GRAN. To achieve this, a packet level simulator *[Courtsey: IP.Access Ltd.]* is used which passes the packets from a UDP server and client through a bandwidth limited VSAT connection. This is done so as to emulate congestion between the two points. Quality of Service parameters such as packet loss and jitter are analyzed for different load and bandwidth scenarios. The effects of discontinuous transmission (DTX) over the IP link are analyzed to reduce bandwidth requirements and in limiting the effects of short periods of congestion. The effects of signaling on the link are also presented in the later part of this section.

The simulation environment includes a number of IP enabled *IP.Access* GSM base stations with up to 4 transceivers (TRXs - transmitters/receivers) in an Ethernet network. A single Ethernet connection supplies both power and traffic to the units. The connection between each TRX and the network is based on standard Internet protocols; the system can thus be easily installed at the same geographic location as that of the BSC and the MSC or remotely. The voice traffic and signaling are routed through a public and/or private IP networks.

Though several configurations are possible; it was mutually agreed with the *IP.Access* that for this simulation purpose the test BTSs' would be placed at their end and the BSC, the MSC and Media Gateway (MG), which provide connection to the PSTN (Public Switching Telephone Network), are sited at SeaNet. Considering the set-up, the IP traffic generated is made up of two components:

GSM-over-1P = Voice-over-IP + Signaling-over-IP

Where Voice-over-IP is RTP streams carried over a UDP connection carrying voice traffic. Signaling-over-IP are channels carried over a TCP/IP connection, which replace the GSM logical channels carried over the A-bis physical and LAPD data link layers. The UDP protocol is used for carrying RTP packets. For a GSM-over-IP system, the payload of each RTP packet is 20ms speech frame, encoded with the full-rate 13kbps speech encoder specified in GSM 6.10 [52].

In the simulation, for the uplink (i.e. packets entering the backbone network), the BTS receives a complete speech frame from the Mobile Station (MS) every 20ms. On the air interface, speech frames received on a timeslot (e.g. TN1) follow immediately the speech frame for TN0. In the downlink (i.e. packets leaving the backbone network), speech packets are generated by the Media-Gateway (MG), which is connected to the PSTN. The speech frames are generated independently of the timing on which they are sent on the air interface; thus, randomizing the delay between RTP sessions.

In this simulation set-up, RTP stream goes through a public network and it is assumed that no congestion is encountered in this network, but each packet is delayed following an exponentially distributed random function. It has been informed by *IP.Access* that the average interval for arrival packet delay is 20ms. The result of such delay is that packets arrive randomly at the BTS, with some packets arriving over 100 ms after the previous RTP packet for the same session. Data transported in the RTP streams is augmented by a control protocol, RTCP [61], on both the uplink and downlink paths.

In the simulation RTCP Sender Report messages are randomly sent within a period of 5 seconds +/- 50% for each call [52].

6.2 The Simulation

The purpose of the simulation presented here is to estimate the bandwidth requirements at the BTS's site and analyze the effects of enabling DTX over the IP link. In an IP-GRAN architecture, voice traffic requires higher bandwidth than traffic due to signaling segregation by softswitching. Thus, the aim of this simulation is to dimension the bandwidth requirements of the RTP streams in *a* realistic network setting.

The simulation network is depicted in Figure 6.1**.** The traffic from the GSM network is relayed from the PSTN by the Media Gateway, through standard TI/E1 connections. The MG is situated at the SeaNet's premises. In order to reach the IP.Access premise, voice packets are passed through a public IP network (VSAT link). As the link between the SeaNet's (acting as MNO) premises and the IP.Access premise, affects the cost of the service; proper dimensioning of this link is required for optimal usage of bandwidth over the VSAT link.

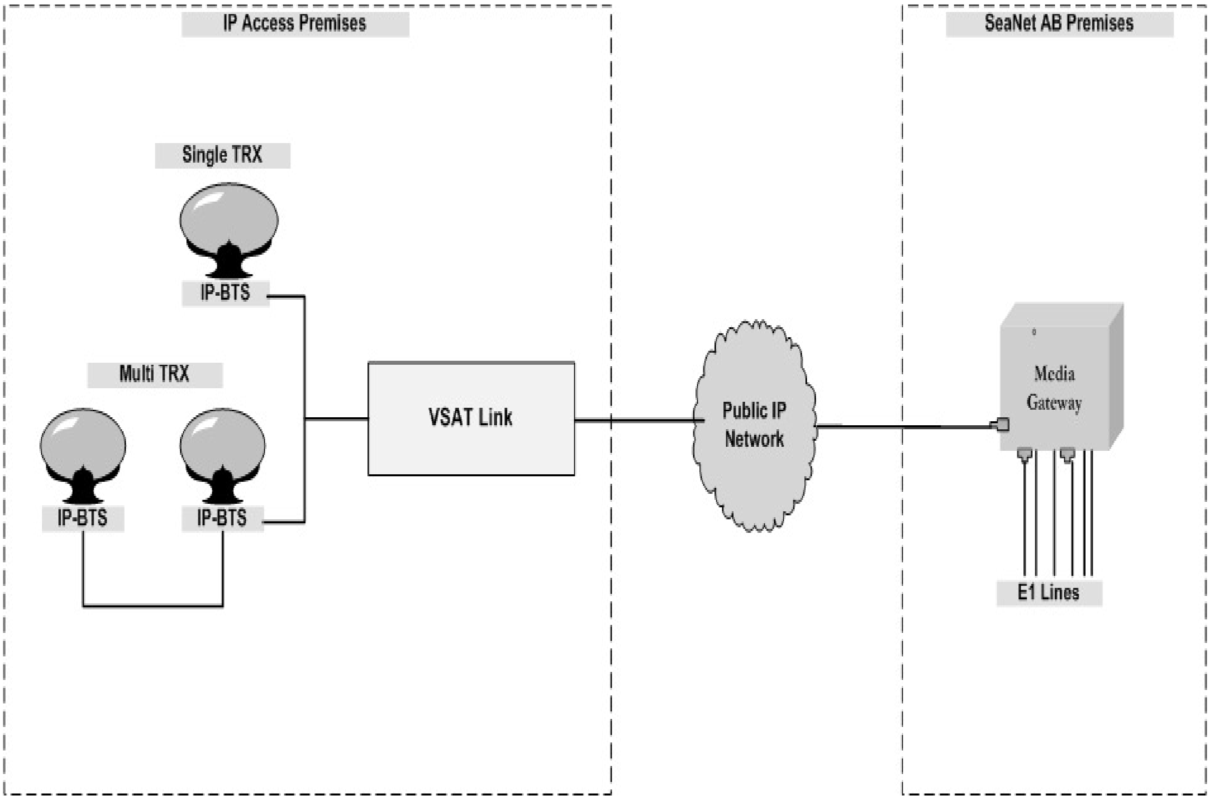


Figure 6.1: Setup of the simulated network

The bandwidth requirements here are quantified by measuring packet drop and jitter. Uplink and downlink RTP traffic are pre-computed off-line, taking into account the scenarios – single talk (talk/silence), double talk, and mutual silence. The steps involved in the simulation process are mentioned herewith:

- A UDP server running on a PC is used to send each RTP packet with the appropriate delay. The packets are passed through a bridge based on the FreeBSD operating system.

- The program **dummynet** is used to simulate bandwidth restrictions, latency and buffer limitation of the network.
- Finally, the packets are received by a UDP client; as this machine also runs the program ***tcpdump,*** the header of the RTP packets and their time of arrival are saved in a file for subsequent analysis.

In order to reduce the CPU work load and increase the accuracy of the time-stamp provided by tcpdump, the UDP client and server are executed on two computers Linux in console mode. When using dummynet, precision in packet delay and bandwidth depends on the following factors: queue size; packets per second traversing the system, kernel tick frequency, and (inversely) the specified bandwidth and delay values. For the bandwidth used in the simulation, a delay of 40ms has shown acceptable delay variation below 1ms [38].

6.3 The Results

The header of RTP packets contains the time-stamp of its creation and a sequence number; together with the time of arrival at destination these are used to compute statistics on packet delay, jitter, and packet drop. The inter-arrival time between packets of the same RTP stream describes the instantaneous effects due to congestion. The jitter buffer on the BTS drops packets with inter-arrival delays bigger than 100ms. In the simulation, downlink packets with delay greater than l00ms are discarded and counted as dropped packets (as they would be perceived by a user) [38]. Simulation assumes full traffic load on all BTSs.

The jitter here is calculated as the statistical variance of the RTP data packet as suggested in the RFC 3550, titled *'RTP: A transport Protocol for Real-Time Applications'*, by the Network Working Group of The Internet Society:

$\mathbf{J(i)=J(i-1) + [\,|D(i-1, i)|\, - J(i-1)] / 16}$, where

J(i-1) is the jitter for the previous sample, and D(i-1,i) is the inter-arrival time between the two packets

Three simulation scenarios are presented, each assumes different requirements for the air interface; and are deemed typical of the deployment of the *IP.Access BTS*:

- Single TRX: used as coverage in-fill or to provide service to a small coverage area.
- One BTS with multiple TRXs: provides higher capacity for an average size coverage area.

- Multi-BTS site: used for providing coverage and capacity in large public or private coverage areas.

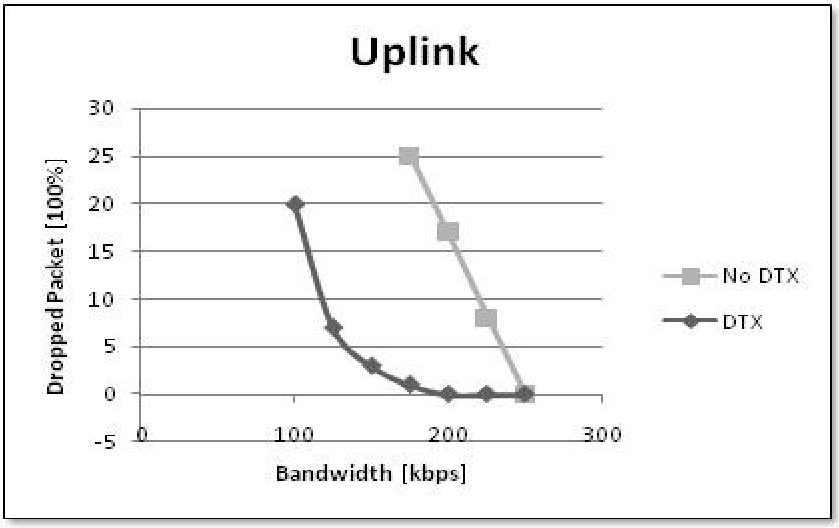
Results from these simulations are used to make generic statements about the effects of congestion on the RTP stream and the effect of using DTX on the IP link. The simulation assumes full traffic load on all BTSs and the following are considered during analysis:

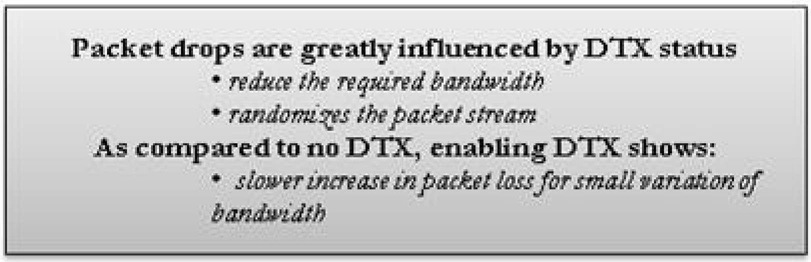
- High latency backhaul link and the traffic is very bursty.
- Having DTX randomizes the traffic and reduces the burstiness of the link.
- Basic priority queuing mechanism implemented on both uplink and downlink's network nodes.

6.3.1 Single TRX

The results of the simulations and the effects of DTX are shown in Figure 6.2 (a, b, c, d). The plots show the statistical variation of packet drop and the jitter (measured as the highest value obtained 99% of the time) against variation of bandwidths in the uplink path

Effect of Packet Drop





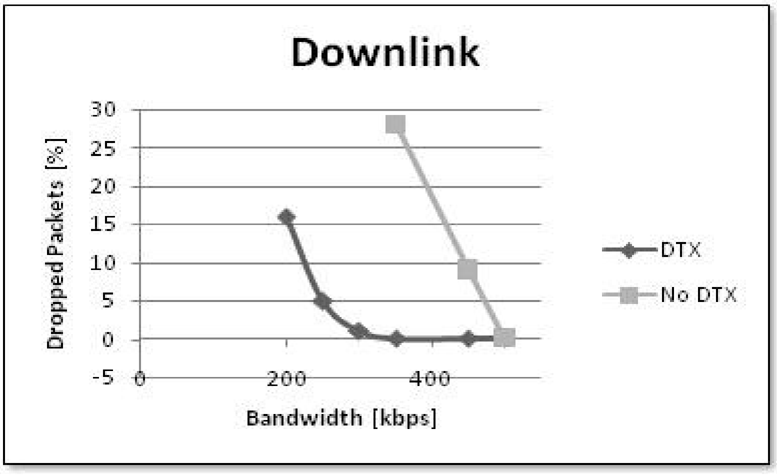
Packet drops are greatly influenced by DTX status

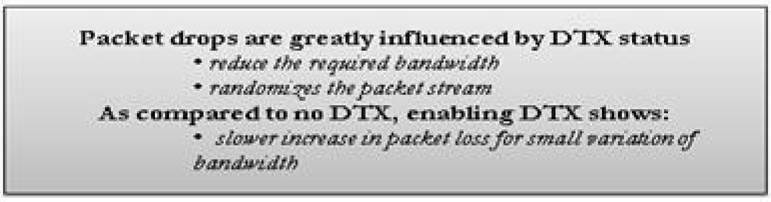
- *reduce the required bandwidth*
- *randomizes the packet stream*

As compared to no DTX, enabling DTX shows:

- *slower increase in packet loss for small variation of bandwidth*

Figure 6.2(a): Bandwidth vs. Packet Drop; Uplink Single TRX site




Packet drops are greatly influenced by DTX status

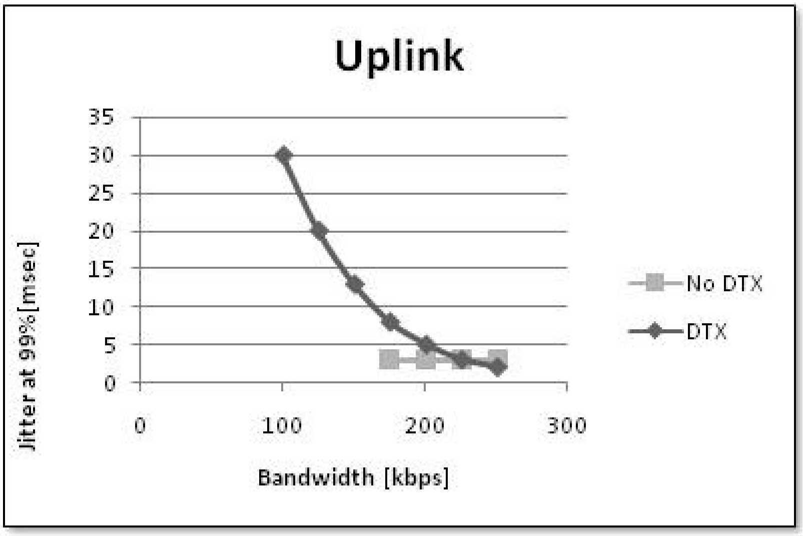
- *reduce the required bandwidth*
- *randomizes the packet stream*

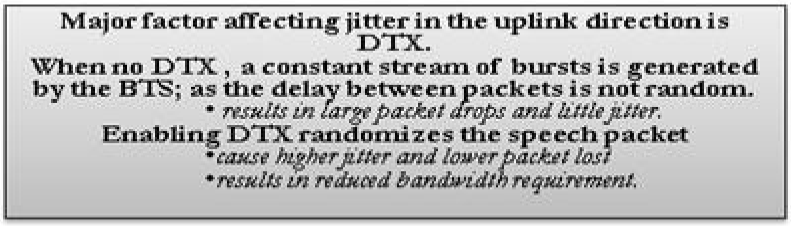
As compared to no DTX, enabling DTX shows:

- *slower increase in packet loss for small variation of bandwidth*

Figure 6.2(b): Bandwidth vs. Packet Drop; Downlink Single TRX site

Effect of Jitter




Major factor affecting jitter in the uplink direction is DTX.

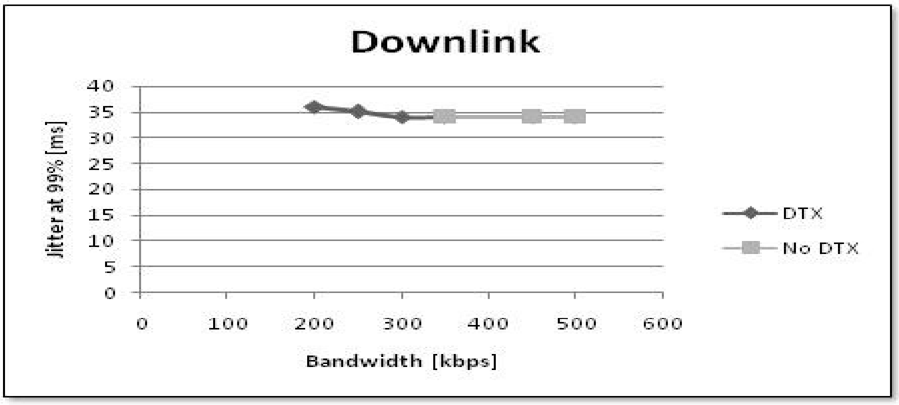
When no DTX , a constant stream of bursts is generated by the BTS; as the delay between packets is not random.

- *results in large packet drops and little jitter.*

Enabling DTX randomizes the speech packet

- *cause higher jitter and lower packet lost*
- *results in reduced bandwidth requirement.*

Figure 6.2(c): Bandwidth vs. Jitter; Uplink Single TRX site



Mostly affected by the delay statistics of the backbone network. Backbone network randomize the time of arrival of each packets

•increases jitter

When using DTX, the silence periods typical of conversational speech, randomize the RTP streams by reducing the number of speech frames

• increases jitter for low bandwidths

Figure 6.2(d): Bandwidth vs. Jitter; Downlink Single TRX site

6.3.2 Multi-TRX

The results of the simulation are shown in Figure 6.3 (a, b, c, d). The site under consideration is composed of 1 BTS with 2 TRXs, with a total of 15 traffic channels (one timeslot on one TRX is assumed to be configured as Broad Cast Control Channel (BCCH) and Stand-alone Dedicated Control Channel (SDCCH)) [According by IP.Access this would be a typical configuration].

Effect of Packet Drop

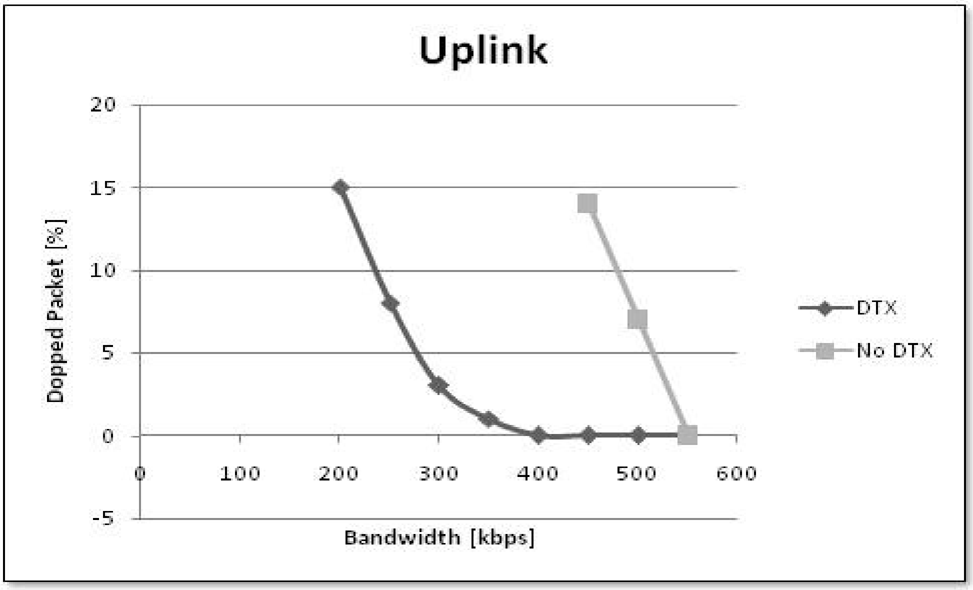


Figure 6.3(a): Bandwidth vs. Packet Drop; Uplink Multi-TRX site

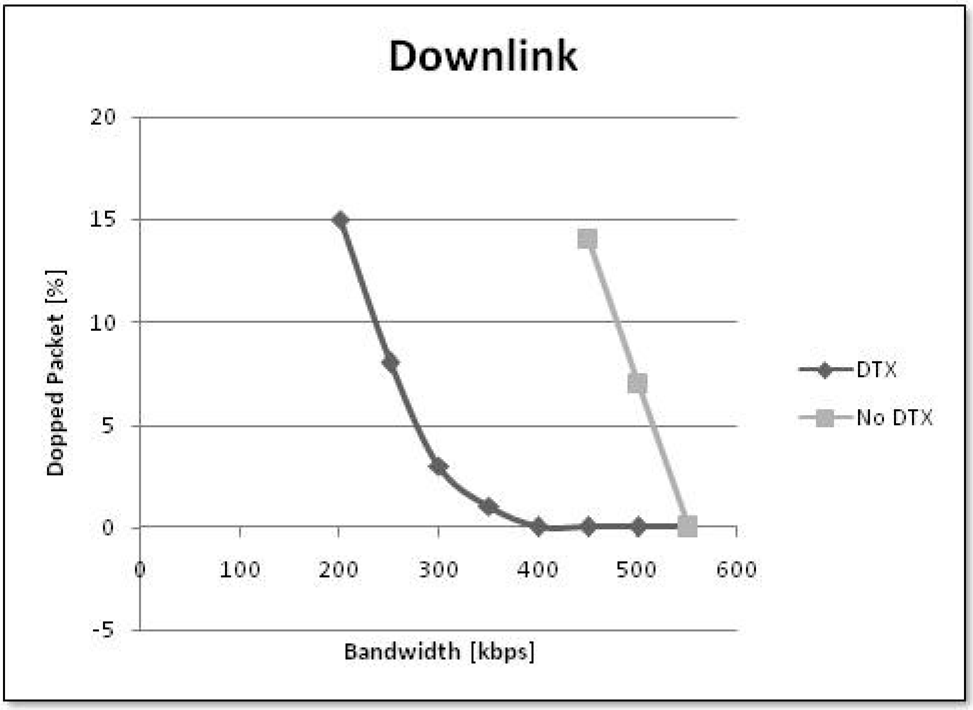


Figure 6.3(b): Bandwidth vs. Packet Drop; Downlink Multi-TRX site

Effect of Jitter

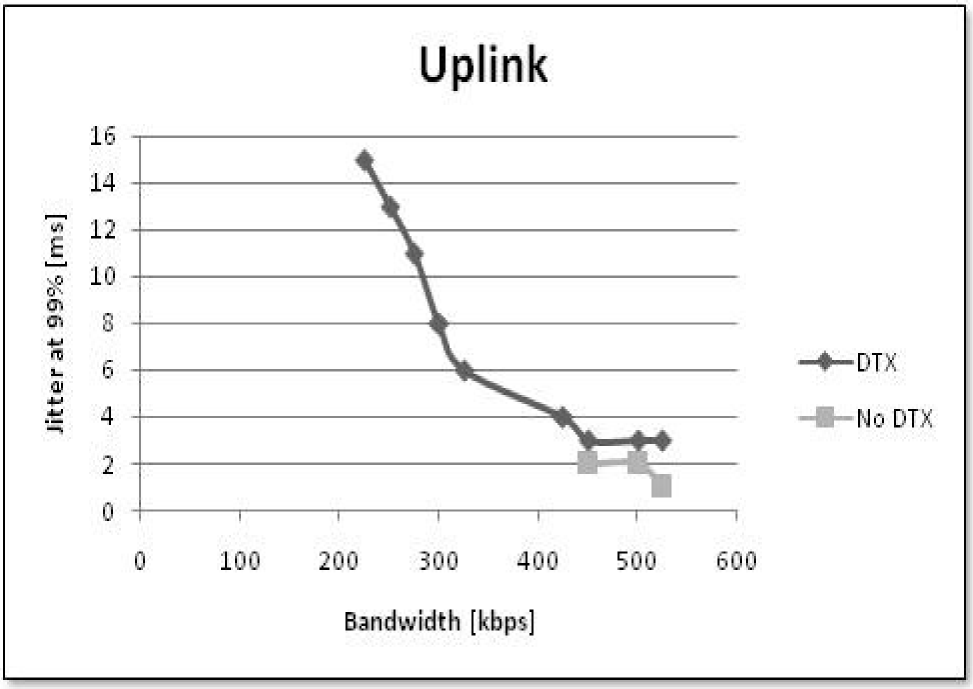


Figure 6.3(c): Bandwidth vs. Packet Jitter; Uplink Multi-TRX site

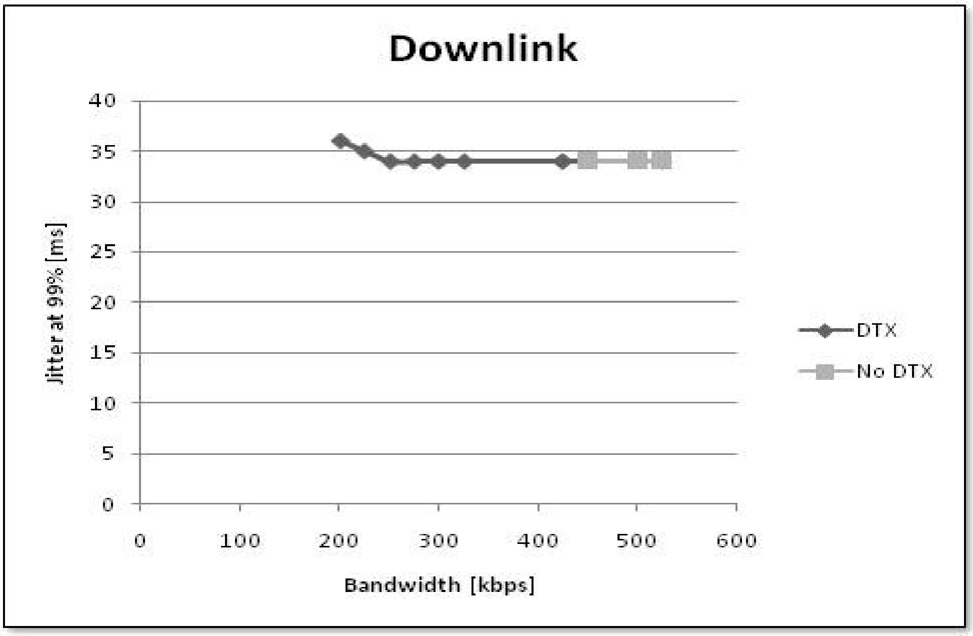


Figure 6.3(d): Bandwidth vs. Jitter; Downlink Multi-TRX site

6.3.3 Multi-BTS

Simulation results in Figure 6.4 (a, b, c, d) shows the drop packets and jitter for a site with 2 BTSs, each composed of 1 TRX, with a total of 14 traffic channels (one timeslot on each BTS is assumed to be a BCCH) [Based upon a typical configuration according to IP.Access].

Effect of Packet Drop

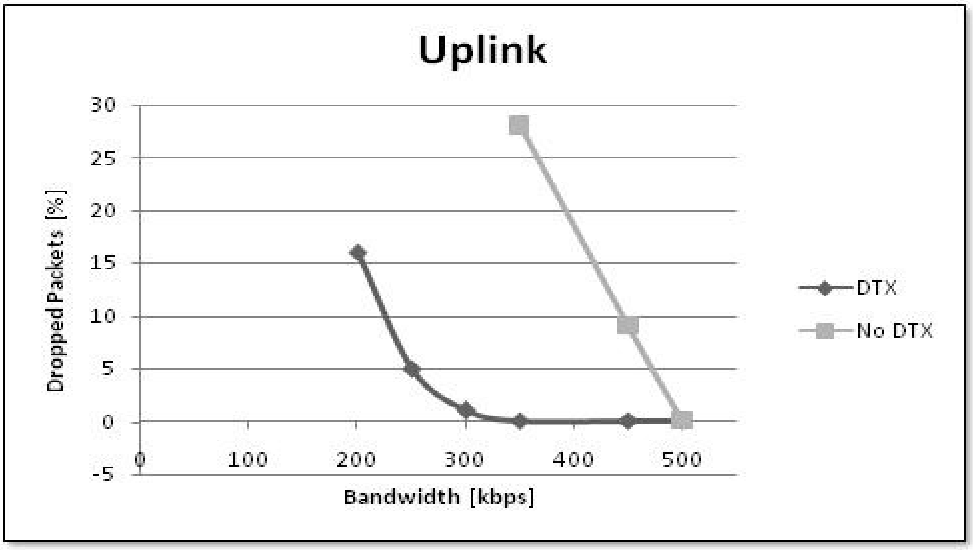


Figure 6.4(a): Bandwidth vs. Packet Drop; Uplink Multi-BTS site

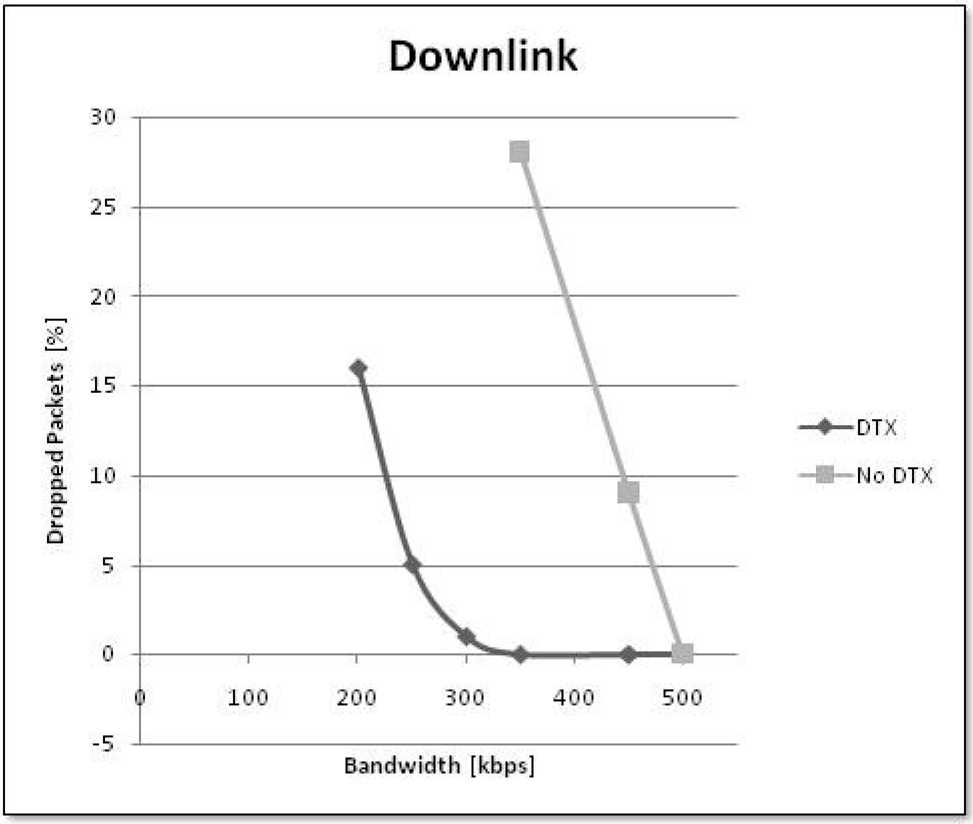


Figure 6.4(b): Bandwidth vs. Packet Drop; Downlink Multi-BTS site

Effect of Jitter

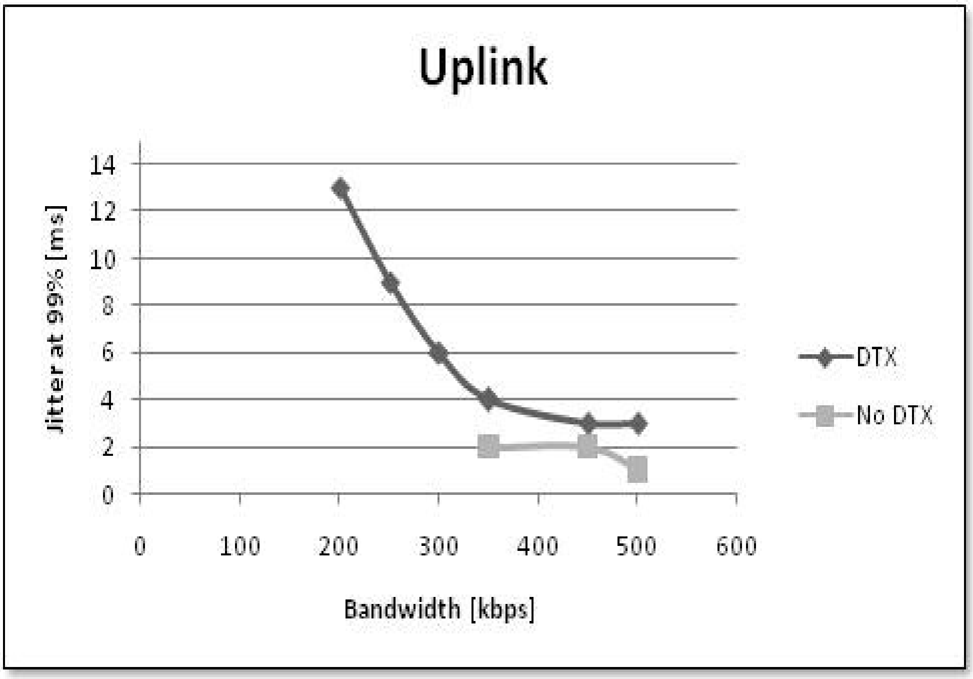


Figure 6.4(c): Bandwidth vs. Jitter; Uplink Multi-BTS site

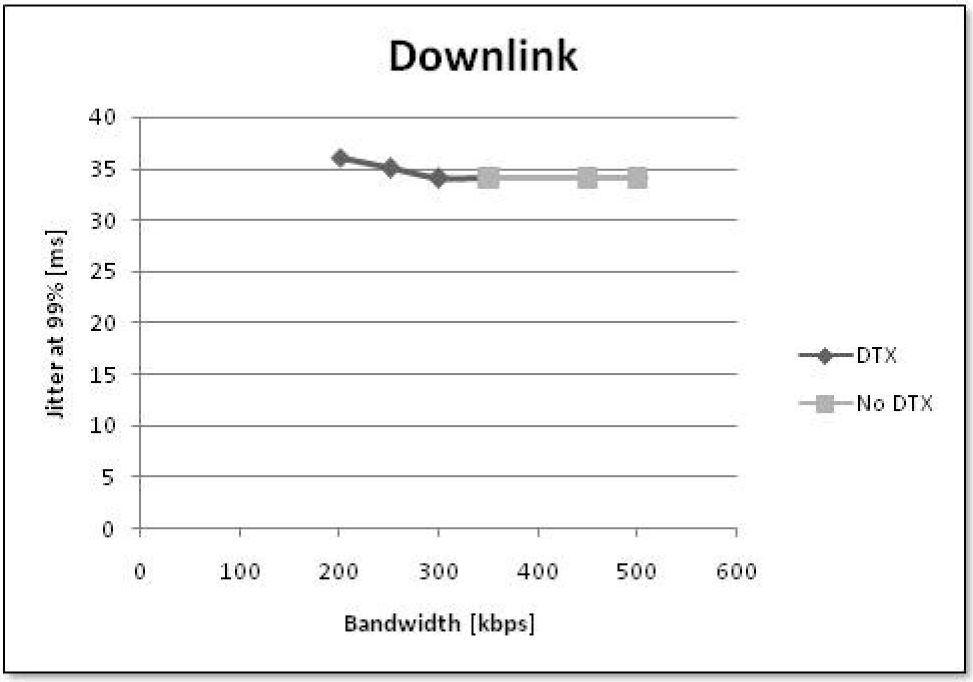


Figure 6.4(d): Bandwidth vs. Jitter; Downlink Multi-BTS site

6.4 The Analysis

From the simulation results presented, it is possible to derive the following conclusions about the network bandwidth requirements at the BTSs' premises.

6.4.1 Downlink Jitter

Downlink jitter is mostly affected by the delay statistics of the backbone network. For an average delay of *20ms,* 99% of the speech frames arrive within 35ms of their transmission. The effect of the backbone network is to randomize the time of arrival of each packet; therefore, increasing jitter. By randomly spreading the arrival delay for each RTP packet, the probability of packet drop at the input to the download is reduced.

When using DTX, the silence periods typical of conversational speech, randomize the RTP streams by reducing the number of speech frames. This increases the jitter for low bandwidths in the sense that a number of speakers may be active at the same time that the variance in needed bandwidth increases; though it would seem as the effect of the reduction in average number of frames. However, the backbone network has a stronger effect on the jitter characteristics, which hides the effects of DTX.

6.4.2 Uplink Jitter

The major factor affecting jitter in the uplink direction is DTX. When no DTX is used, a constant stream of talk bursts is generated by the BTS; as the delay between packets is fixed (and not random). This results in a large number of packet drops (type: bursty) and little jitter (in objective terms and not cumulative effect on the quality of service). On the contrary, enabling DTX randomizes the arrival of speech packets and cause higher jitter and lower packet loss; thus statistically resulting in reduced bandwidth requirement. It is actually the reduction in the number of RTP packets which need to be transmitted that results in the reduction in required bandwidth.

6.4.3 Packet Drop

Packet drop statistics in the uplink and downlink are very similar. As the available outgoing bandwidth decreases the buffer at the bridge is more likely to fill up, therefore causing the bridge to drop packets. Fortunately, ttransferring voice over an IP network has been shown to be highly resilient to packet losses (assuming that a suitable CODEC is used) and it has been observed [61] that speech quality is maintained if packet loss due to congestion is below 5% (assuming no additional error on the air interface). Packet drops are greatly influenced by DTX status, as the use of DTX not only reduces the required bandwidth but also randomizes the inter-arrival statistics of the packet stream. As compared to the no DTX scenario, having DTX results in a slower increase in packet loss for a limited variation in bandwidth. The following table summarizes such gain [52]:

Table 6.1: Additional bandwidth required for lower packet drop rate from 5% to 1%

	Single TRX	**Multi TRX**	**Multi BTS**
No DTX	10kbps	22kbps	20kbps
DTX	24kbps	46kbps	80kbps

Considering the single site, single TRX scenario; for a traffic increase on the link of about 10kbps, a 5% packet drop rate is observed versus a minor traffic loss of 1% with the lower offered rate. With DTX enabled, the traffic increase on the link would need to be about 24kbps in order for the packet drop rate to be increase to 5%. This confirms the fact that DTX makes the system more resistant to variations in bandwidth because of possible congestion at the uplink.

6.4.4 Bandwidth Requirements

Results depicted in section 6.3.3 confirmed the fact that DTX can reduce the bandwidth requirements at the cell site. The following table, however, illustrate the bandwidth ratio required to obtain 1% packet drop for DTX enabled versus not enabled cases.

Table 6.2: Bandwidth requirements

	Single TRX	**Multi TRX**	**Multi BTS**
Bandwidth (no DTX)	240kbps	520kbps	485kbps
Bandwidth (DTX)	160kbps	316kbps	330kbps
Bandwidth ratio	1.5	1.6	1.46

Based upon table 6.2 we can conclude that for the same load with a packet rate of 1%:

Required Bandwidth (with DTX) = approx. $\frac{2}{3}$ x required Bandwidth (without DTX)

6.5 Effect of Signaling on Link Dimensioning

For an IP-GRAN architecture as proposed in this thesis, signaling from various components of the GSM network are carried over a TCP/IP connection. The effect of signaling under various scenarios can be understood as follows:

The bandwidth requirements for carrying such signaling is dependent on the criteria used to design the GSM network. The signaling generated by a GSM network which provides service in a high user density indoor area (Case-1), is different from the signaling traffic generated by a GSM network which provides coverage at a public location (Case-2).

Signaling exchanged between the BTS and BSC in the first case is characterized by a large number of channel assignment and channel release commands from users commencing and ending calls. However, for the second case, signaling includes a large number of location updates or paging messages, which are dependent on user mobility and network design.

Whether the BSC is co-located with the BTS or with the MSC depends on the architecture of the GSM network. If the BSC is placed with the MSC, bandwidth requirements between the backbone IP network and cell site depends on the A-bis interface. If the BSC is located with the BTS, an IP stream carries A interface messages.

The figures presented in following table, were provided to us by IP.Access for the purpose of this thesis. They offer an estimate of the bandwidth requirements for the A and A-bis interfaces for different environments. The parameters used to calculate the traffic over A interface; it is assumed that the BSC controls 50 equal sites. In the in-fill environment, it is also assumed that the location area offers GSM services to 5000 users [52].

Table 6.3: Downlink signaling bandwidth requirements for case-1 and case-2 sites [38]

Interfaces	**Single TRX**	**Multi TRX**	**Multi BTS**
A-bis (case-1)	0.4 kbps	1.4 kbps	0.9 kbps
A-bis (case-2)	1.6 kbps	2.7 kbps	2 kbps
A (case-1 50 BTSs)	18 kbps	58 kbps	22 kbps
A (case-2 50 BTSs)	20 kbps	57 kbps	71 kbps

The estimates shown in table 6.3 take into account factors such as call establishment, call release, handovers, SMS, and paging. Typical usage and call duration are assumed. These estimates show that signaling is a small fraction of the overall traffic load; however, as it is transmitted over a reliable TCP connection, its effect on congested links cannot be ignored

7. Packet Optimized IP GRAN Prototype: Setup and Results

7.1 Proposed Network Architecture

- End-to-end IP compatibility: based on the proposals made in chapters 4 and 6: GSM communications are carried via IP this allows the use of standard open protocol equipment to create service offerings, and enables sharing of the common transmission backbone with other IP based services, such as Internet access. Furthermore end-to-end nature of an IP network allows for direct communication between network nodes, with traffic automatically routed to its destination via the most appropriate route.

- Distributed Architecture: A significant benefit of IP-based Softswitching, as discussed in section 4.3, is that GSM network elements can be located anywhere within the IP "cloud," that is, they can be put where they best suit the requirements of the network. In other words, the traditional architecture of legacy GSM networks is no longer a requirement. This means, for example, that a Media Gateway can be located in one place, such as at a remote secure service provider's facility, while the BSC/BTS infrastructure is only deployed as and where needed. Furthermore, call processing is distributed and intelligent. In the case of satellite back-haul this allows local calls to connect locally (voice path requires no satellite bandwidth), and a mesh satellite network allows all long distance (over satellite) calls to be logically a single hop.

- Signaling flow purely based upon Global Title based routing (sections 5.1 and 5.2), where the originating node does not need to know the point codes of all the signaling nodes which the signaling will traverse, thus avoiding the need to maintain dense routing tables for routing signaling messages across the global SS7 network.

- Optimal Routing for roamers: While the basic concepts have been described earlier in the thesis (section 5.3), some of the details have not been included as they are considered confidential by SeaNet Martitime Communications AB (our employer). A typical deployment for a maritime vessel is shown in figure 7.1. A layered view of such a network is shown in figure 7.2.

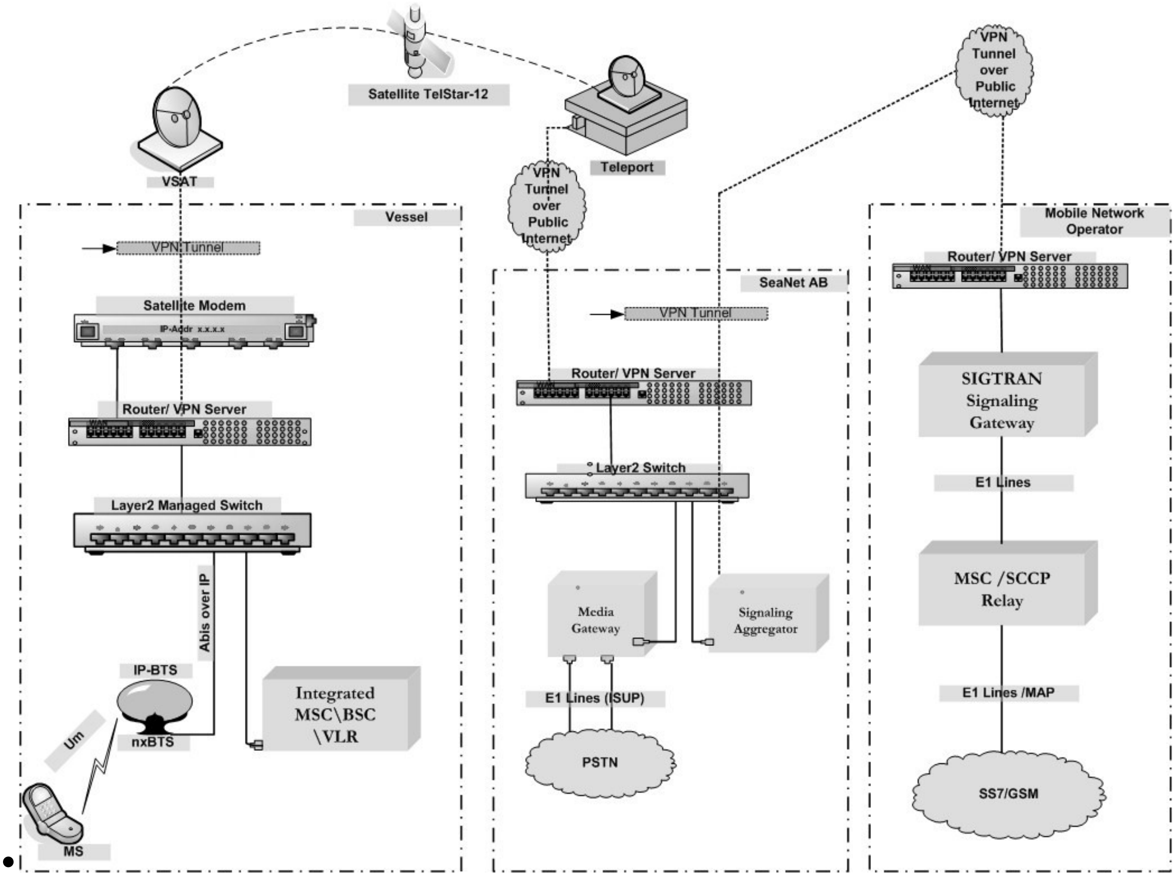


Figure 7.1: Proposed Network Architecture

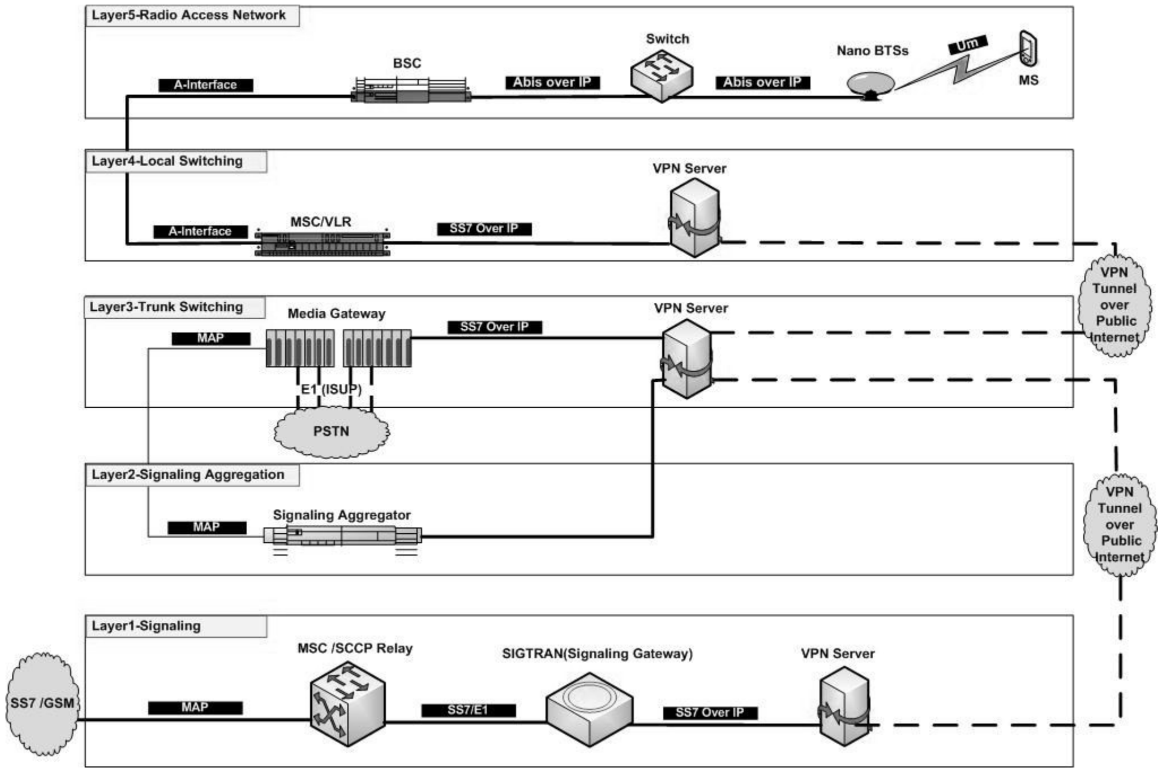


Figure 7.2: Proposed Network Signaling and Layer Architecture

The key aspect of the solution proposed in this thesis is its highly distributed architecture. The use of a packet based, IMAS inspired, GSM architecture allows all the elements of the GSM network to interconnect via a packet (e.g., IP) network, and all elements therefore can make use of, and share, network resources regardless of their location. This allows greater flexibility in the deployment, management, and expansion of a network.

Figure 7.1 shows that a single Media Gateway is deployed at a hub location. From this hub location IP communications links are established with the "Radio Access Networks" (RANs) on-board a maritime vessel. In a maritime scenario, this connection is possible via a satellite link, which is often the only reliable communication media between these areas and the hub location. However, when near to shore or near to another ship, other links can be used. Since these links are simply tunnels for IP traffic backhauling – one could have great flexibility in the choice of link. With this link in place, the on-board Integrated BSC/MSC/VLR system (for the purpose of simplicity, let's call this unit, On-board Mobile Radio Communication System (OBMRCS)) will process calls from, to and between the RANs. This system has intelligent call processing, meaning call signaling goes through the IBMVS; however the actual voice calls are directly routed to their destination. For example, a "local" call within a RAN is switched locally. The voice path does not traverse the IBMVS or make use of any IP backbone bandwidth. This result in a high quality, low latency call, which in a maritime scenario is particularly important due to limited bandwidth available (at reasonable prices) via satellite.

A key advantage to note regarding this approach is the savings due to the sharing of common resources across multiple networks or RANs. The sharing is both in terms of infrastructure and operations. For example, a single centrally located Media Gateway can support multiple RANs. It also allows for significant savings in operations as a single centralized staff supports multiple networks, thereby reducing the number of people and the level of their expertise required in the field. It should be highlighted that the Signaling Aggregator can be located either at an mobile operator's or the service provider's switching center; practically anywhere within the IP cloud as it utilizes SIGTRAN to send SS7 signaling over IP.

SIGTRAN implementation in SeaNet's IP GRAN (see figure 7.3):

- Utilizes SCCP/SUA (SUAP Application Protocol).

- The IP Server Process (IPSP) is an Appilcation Server (AS) process in standard system terminology; except that it uses SUA in a peer-to-peer fashion. An IPSP does not use the services of the signaling gateway.
- This implementation approach is useful for porting an application, orginally designed for ISDN, into an IP enviornment.

A protocol tracer from Zynetix is used to collect traces, concerning SS7 and SIGTRAN traffic, from an operational network. The purpose of presenting these trace is to give a proof of concept for the proposals made in this Master's thesis.

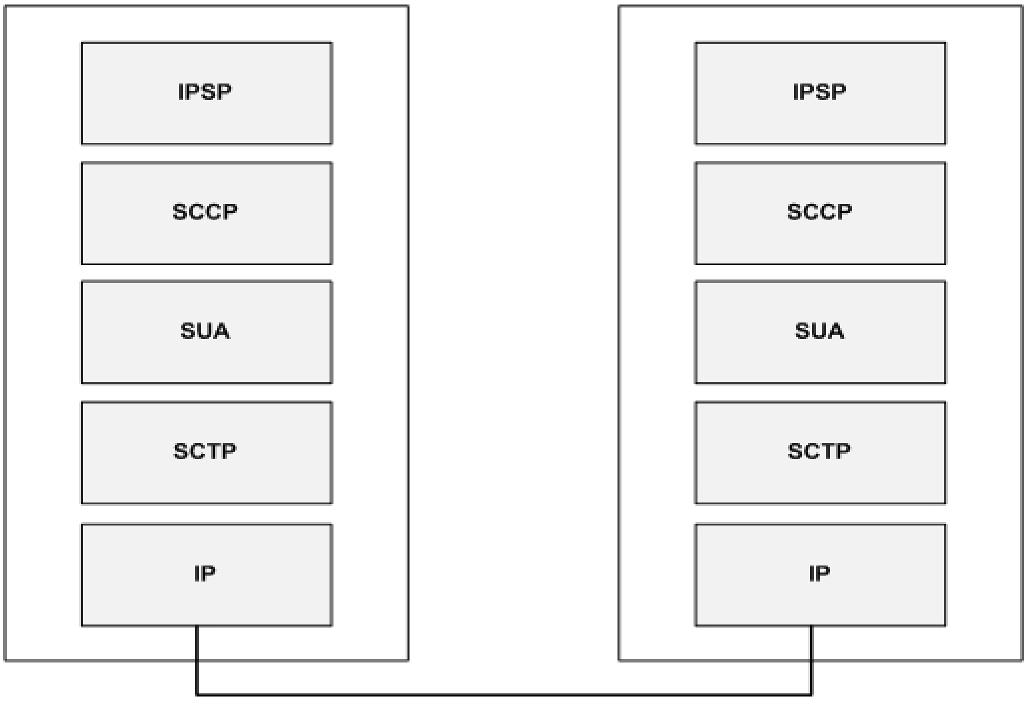


Figure 7.3: SIGTRAN implementation in SeaNet IP GRAN

7.2 Test Network Architecture

7.2.1 Architecture-1: Signaling Aggregator is situated at SeaNet

In this scenario the signaling aggregator is situated locally at SeaNet's premises and connected over SIGTRAN/SUA over SCTP to the mobile network operator's (MNO's) MSC via a signaling gateway as shown in figure 7.1. Pure global title based routing is used. As this architecture was not used in the testing conducted as part of this thesis, further details are not given here. However, details of this approach will be available from SeaNet in the first quarter of 2008.

7.2.2 Architecture-2: Signaling Aggregator is situated at MNO's premises

In the tests performed as part of this thesis project, the signaling aggregator was situated at the MNO's premises and connected over SIGTRAN/SUA over SCTP directly to the media gateway (i.e., without any mediating gateway). The signaling aggregator is connected to the MNO's MSC through a physical E1 interface. For this scenario a combination of global title and point code were used in routing. All the tests were conducted in the environment shown in figure 7.4.

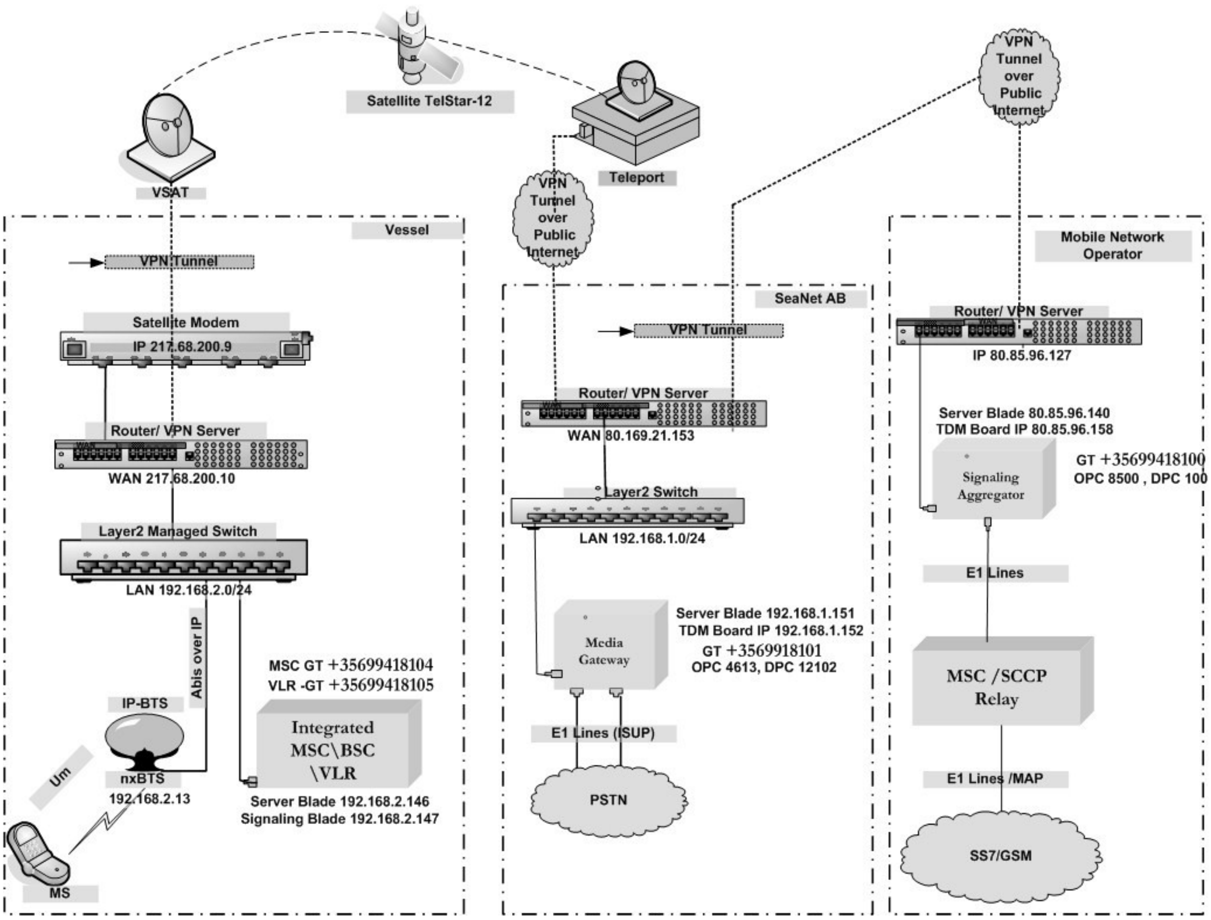


Figure 7.4: Test setup

7.3 Test Setup

All the tests were conducted in an environment where the signaling aggregator was actually placed in the mobile network operator's (MNO's) premises. The following test parameters were used for this testing. The integrated MSC/VLR parameters include E.214 table entries which were used to allow roaming for the test subscriber who used a Vodafone Malta postpaid SIM card in their mobile handset.

7.3.1 Test Parameters

As can be seen in table 7.1, the mobile country code (MCC) which was used is that assigned for Internation Shared Codes, these are allocated to transnational networks (such as satellite networks). The MNC is that allocated to Vodafone Malta Maritime.

As would be expected the global title (GT) shown in table 7.2 has the country code (+356) associated with Malta. While the MSRN range is from that allocated to Sweden (+46) with the city code for Stockholm.

The roaming partner MCC and MNC shown in table 7.4 identifies Malta's vodeafone/Telecell as the mobile operator. A NDC=94 indicates that this is a Malta Telecell number.

Table 7.1: SeaNet AB MCC and MNC

MCC	901
MNC	19

Table 7.2: Signaling Aggregator Parameters

SPC/OPC	8500 (SPC from MNO's range)
GT	+35699418100
SPC/DPC	100 (0-12-4) (SPC from MNO's range)
Server Blade IP address	80.85.96.140
TDM Board IP address	80.85.96.158

Table 7.3: Media Gateway Parameters

SPC/OPC	4613(SPC from Swedish number authorities)
SPC/DPC	12102 (on the national plane)
GT	+35699418101
MSRN Range	+46850534700 – 49
Server Blade IP address	192.168.1.151
TDM Board IP address	192.168.1.152

Table 7.4: Integrated MSC/VLR/BSC Parameters

MSC GT	+35699418104
VLR GT	+35699418105
VLR Camel ship to ship GT	+35699418204 (when implemented)
Server Blade's IP address	192.168.2.146
Signaling Blade's IP address	192.168.2.147
Cell ID 1	10000
Cell ID 2	10001
Cell ID 3	10002
Cell ID 4	10003
Cell ID 5	10004
Cell ID 6	10005
Cell ID 7	10006
Network Color Code	5
Base Station Color Code	0 - 7
LAC (Location area code)	60200
Roaming partner MCC and MNC	278 01
Roaming partner CC of MGT	356
Roaming Partner NDC of MGT	94

7.4 Softswitching: Signaling Flow

The signaling flow based on global title routing was analyzed and observed in three different scenarios as part of this thesis project. The configuration and message flow details are discussed below.

7.4.1 Message Switching Configurations

The Message Switch (MSGX) is used as an internal message switching device for multi-layer switching with in the proposed SS7 network. Essentially acting as a Message Signaling Unit (MSU) bridge, the MSGX transfers MSUs between classic SS7 and SIGTRAN networks. The MSGX moves untranslated messages over a bridging application to an IP counterpart. The counterpart is based on SCCP level traffic. For SCCP, the counterpart is accessed over the SCCP User Adaptation layer (SUA). The process also moves messages from SUA to SCCP. SUA has a role for transporting SS7 SUA user signaling over IP using SCTP and enabling seamless operation between SCCP user peers, Integrated MSC/VLR ↔Media Gateway ↔Signaling Aggregator ↔MSC at MNO (access to global SS7 network), in the IP transaction service space (as shown in figure 7.5).

SCTP allows for transport between peer SCTP users for protocols such as SUA. SCTP is connection oriented in nature and provides a means for SCTP endpoints to provide the other endpoints with a list of transport addresses through which an endpoint can be reached and from which it will originate messages. Also, SUA lifts the restrictions on message size (272 octet) and bandwidth (56k or 64k bits per second links) allowing signaling points to exceed the restrictions imposed by the limitations of SS7 networks of 16 linksets consisting of 64kpbs transport; with SUA eliminating the linkset concept completely.

The test setup also includes MTP-SCCP switching. It is used to provide a clear managed and fully routable SS7 network across the wide area IP network. For example, the MSGX within the integrated MSC/VLR routes signalling and traffic via the media gateway.

The MSGX configurations of the MSC/BSC/VLR, media gateway, and signaling aggregator are defined in the form of associations as shown in figure 7.5. An association refers to an SCTP association which provides the transport for the delivery of SCCP-User protocol data units and SUA adaptation layer peer messages.

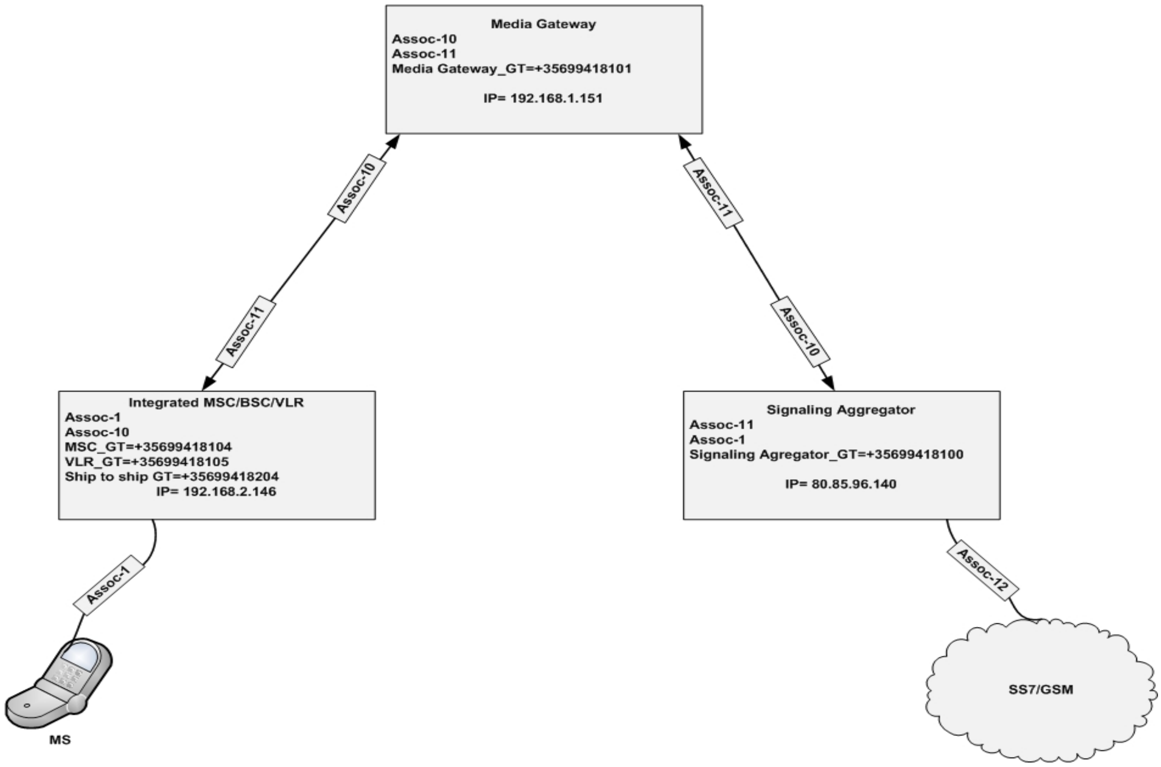


Figure 7.5: Message switching association configurations

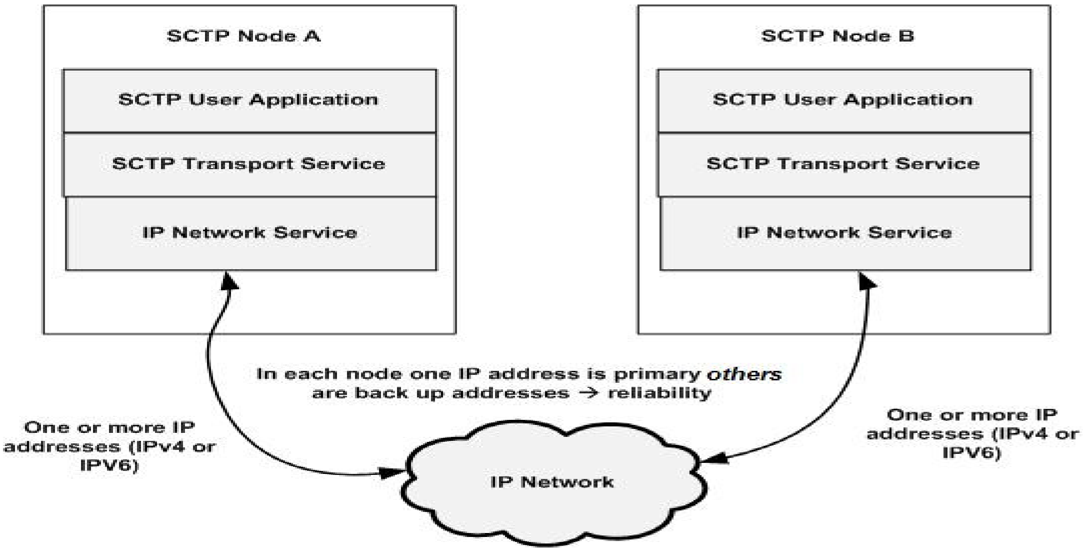

SCTP Node A
SCTP User Application
SCTP Transport Service
IP Network Service
SCTP Node B
SCTP User Application
SCTP Transport Service
IP Network Service
In each node one IP address is primary *others* are back up addresses → reliability
One or more IP addresses (IPv4 or IPV6)
IP Network
One or more IP addresses (IPv4 or IPV6)

Figure 7.6: An SCTP Association

An SCTP association is identified by following parameters:

- IP Address
- Port numbers
- Verifications tags
- Checksums in messages

An SCTP association between two end points (node A and node B) is shown in figure 7.6:

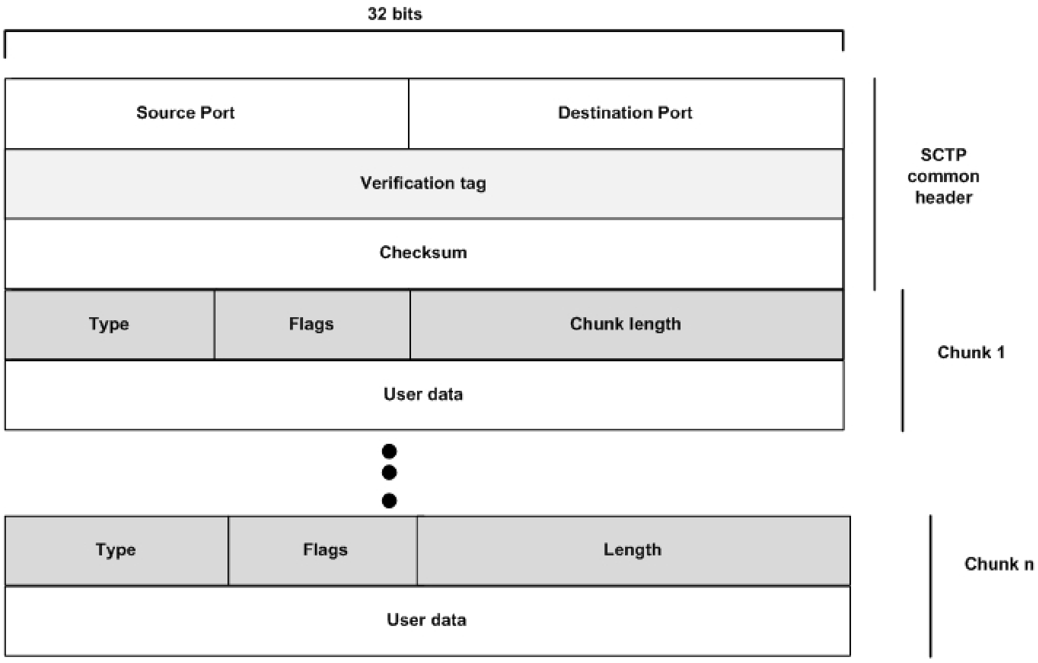


Figure 7.7: SCTP Packet format

SCTP packets have a common header plus control and data chunks as shown in figure 7.7:

- Port numbers similar to those in UDP and TCP.
- During initiation of an association, each end point exchanges the values of verification tags.
- Checksum helps in tackling masquerade attacks.
- Control and data chunks have type flags and length information along with the user information or the control information itself.

SCTP association establishment step1 is shown in figure 7.8:

- Initiate tag gives the value for the verification tag.
- Advertised receiver window (a-rwnd) = buffer space in bytes reserved by initiator for this association.
- TSN= Transmission sequence number (message number).
- Optional: backup address, host name, increase state cookie time etc.

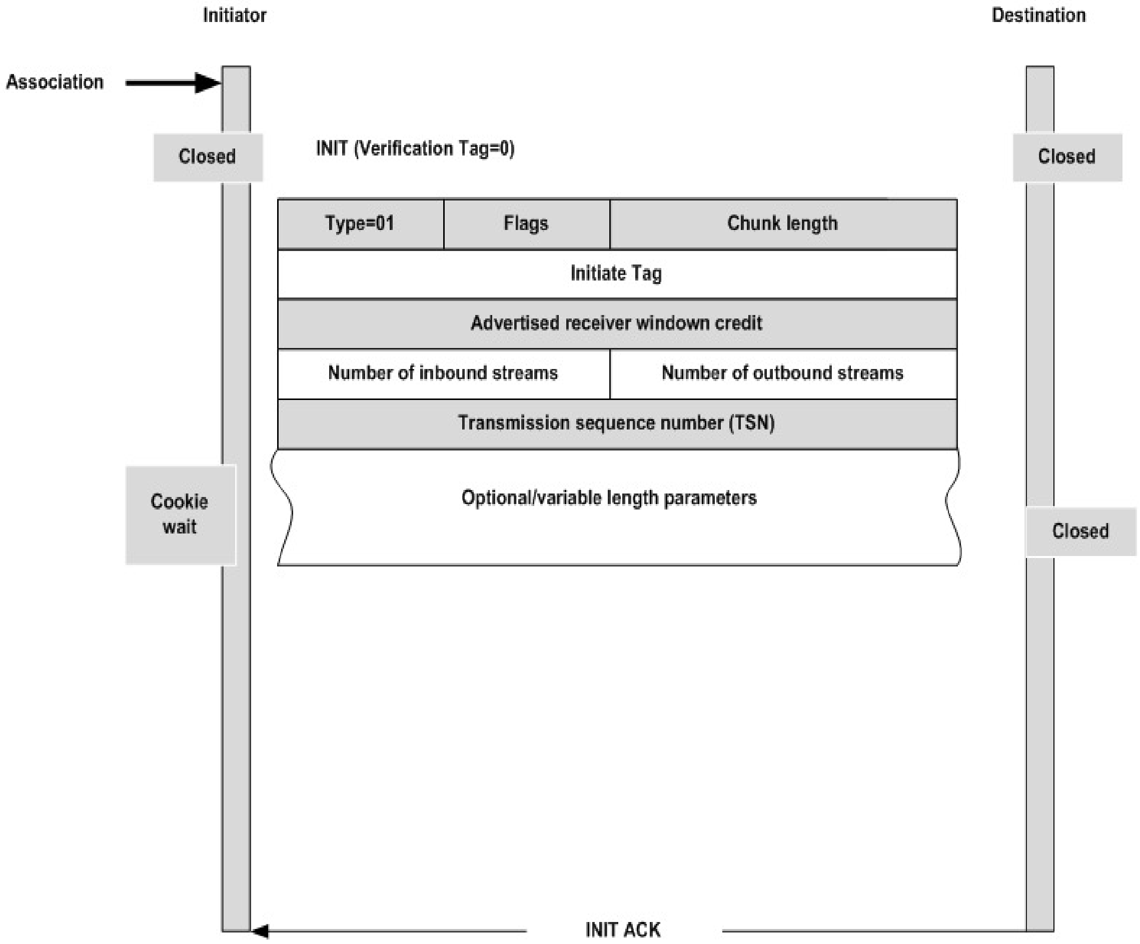
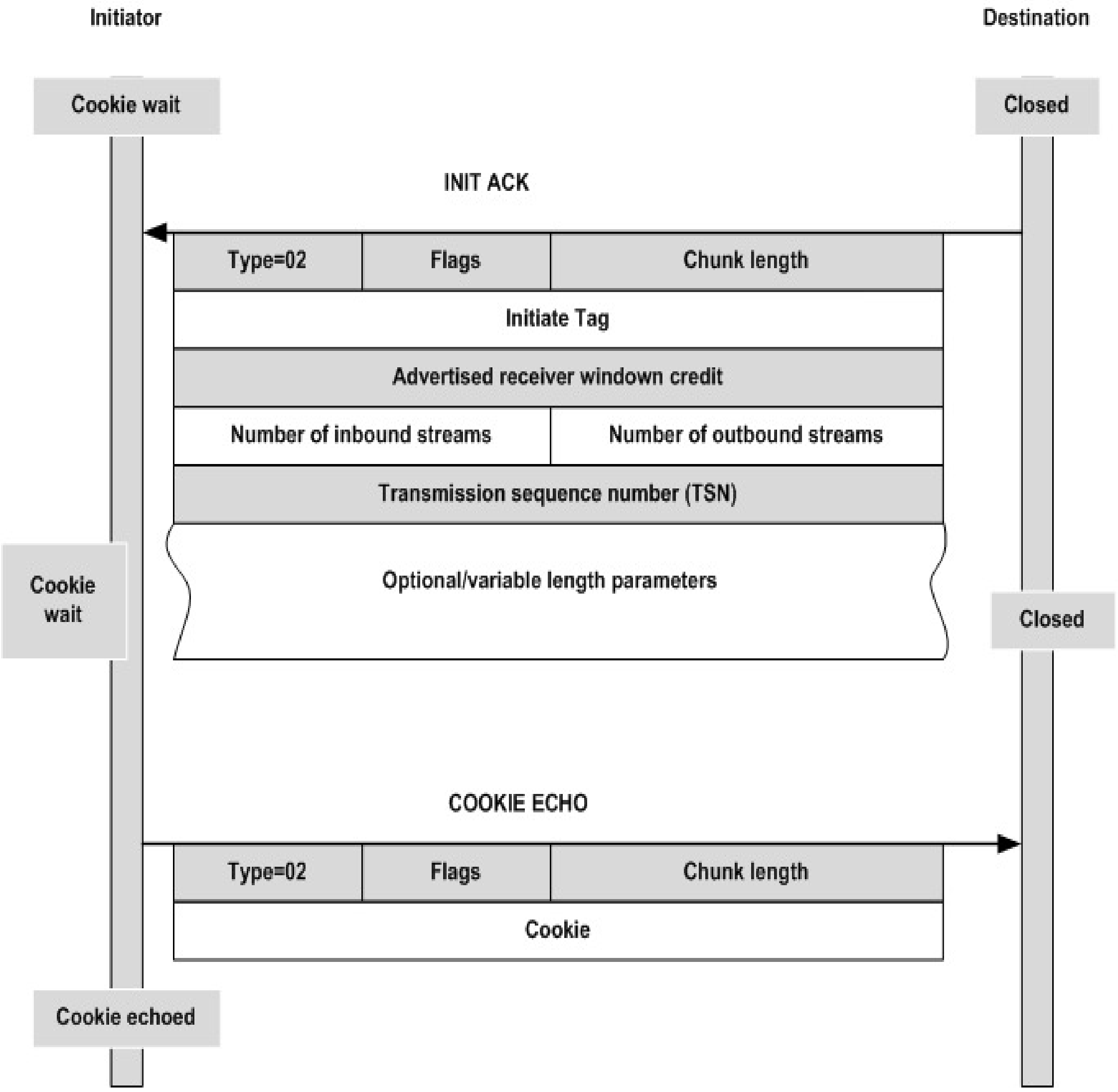

Initiator
Destination
Association
Closed
INIT (Verification Tag=0)
Closed
Type=01
Flags
Chunk length
Initiate Tag
Advertised receiver windown credit
Number of inbound streams
Number of outbound streams
Transmission sequence number (TSN)
Optional/variable length parameters
Cookie wait
Closed
INIT ACK

Figure 7.8: SCTP association establishment step1

SCTP association establishment 2 is shown in figure 7.9:

- The same optional parameters as in INIT.
- One MANDATORY variable length parameter:
  - State Cookie: contain all the informations for the destination to create this association.



Initiator
Destination
Cookie wait
Closed
INIT ACK
Type=02
Flags
Chunk length
Initiate Tag
Advertised receiver windown credit
Number of inbound streams
Number of outbound streams
Transmission sequence number (TSN)
Optional/variable length parameters
Cookie wait
Closed
COOKIE ECHO
Type=02
Flags
Chunk length
Cookie
Cookie echoed

Figure 7.9: SCTP association establishment step2

SCTP association establishment step3 is shown in figure 7.10:

- The destination can now rely on that the initiator is who it claims to be 4-way handshake prevents Denial of service (DOS) attacks like SYN attacks in TCP.
- Transmission control block (TCB) contains association states.

.

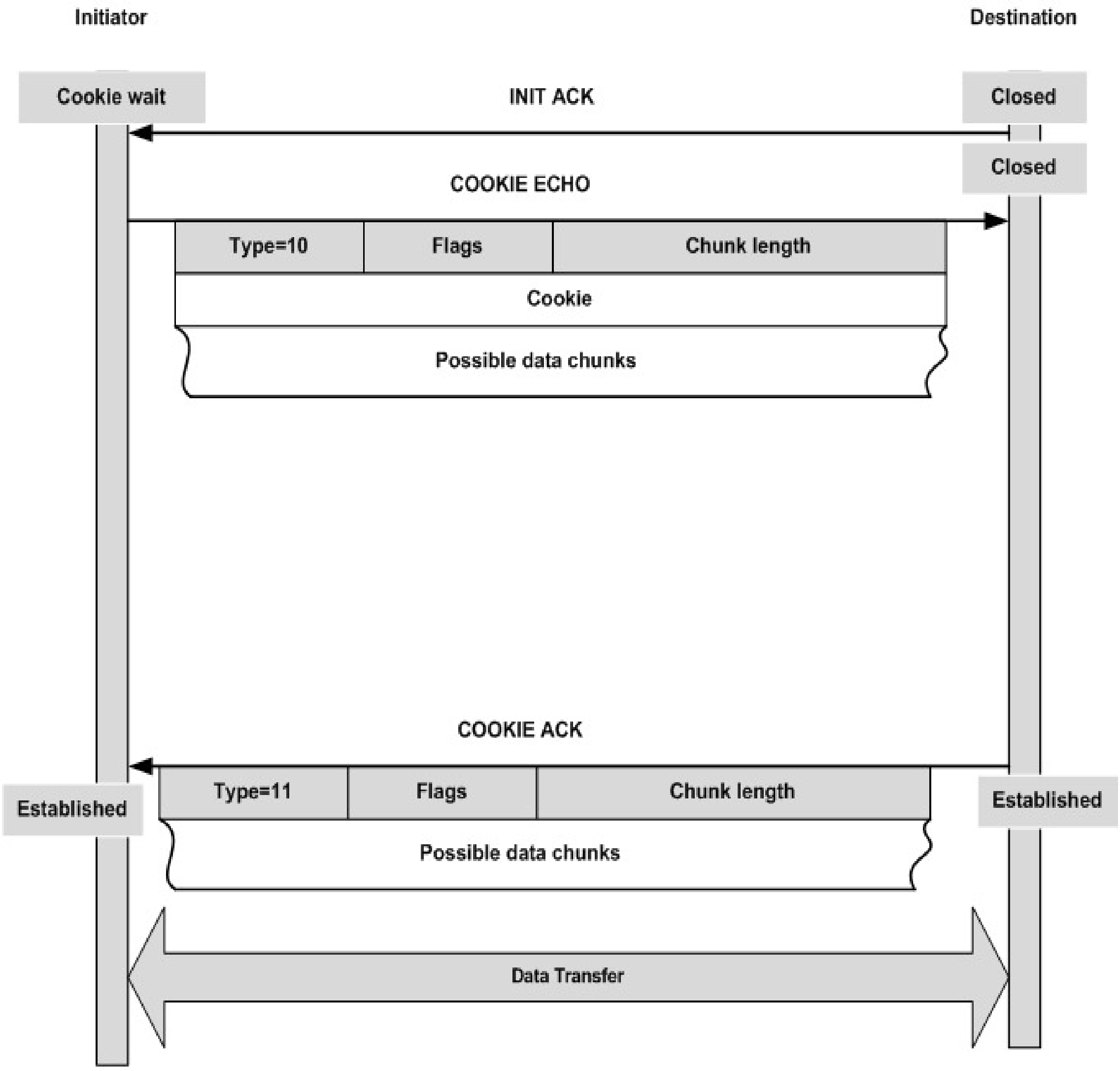


Figure 7.10: SCTP association establishment step3

SCTP data transfer is shown in figure 7.11:

- U- Unordered.
- B- Beginning fragment
- E- Ending fragment
- Transmission sequence number (TSN) - Sequence number of data chunk within an association.
- Selective acknowledgement (SACK).
- Retransmission can be per stream: No Head of line (HOL) blocking.

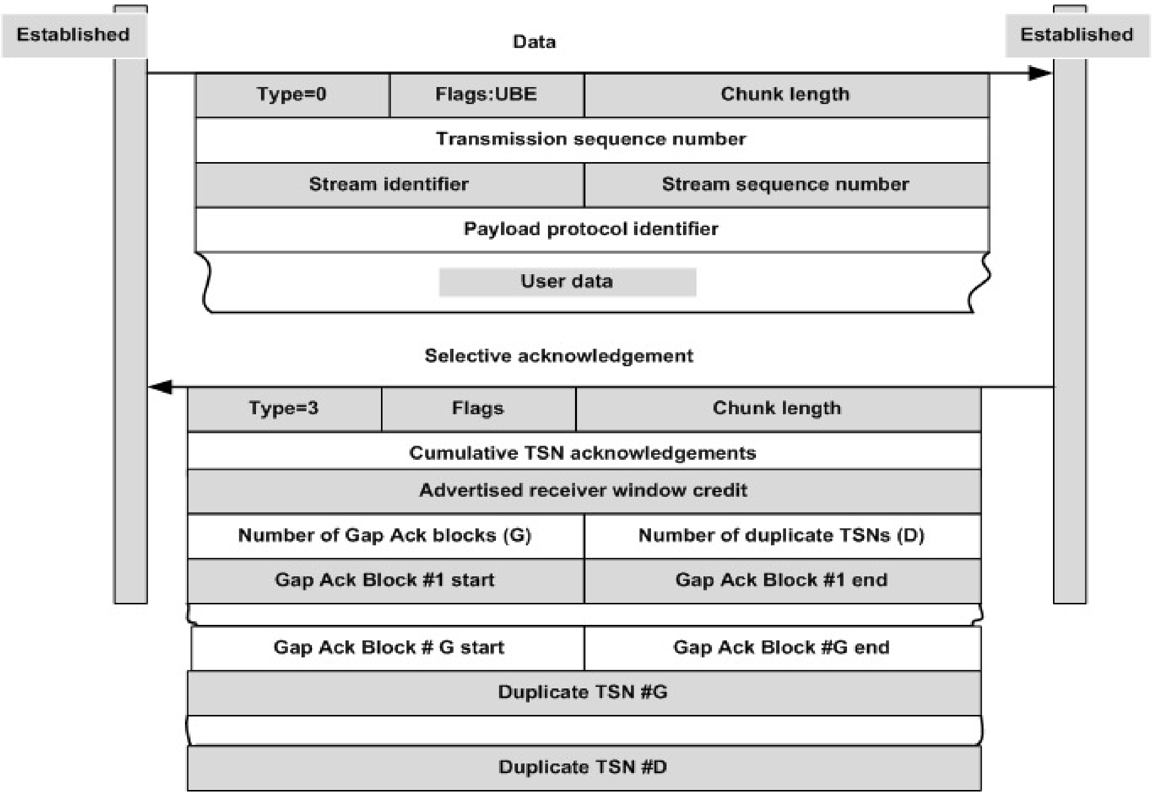


Figure 7.11: SCTP data transfer

Note that SCTP path heartbeat gives information about IP address state is shown in figure 7.12:

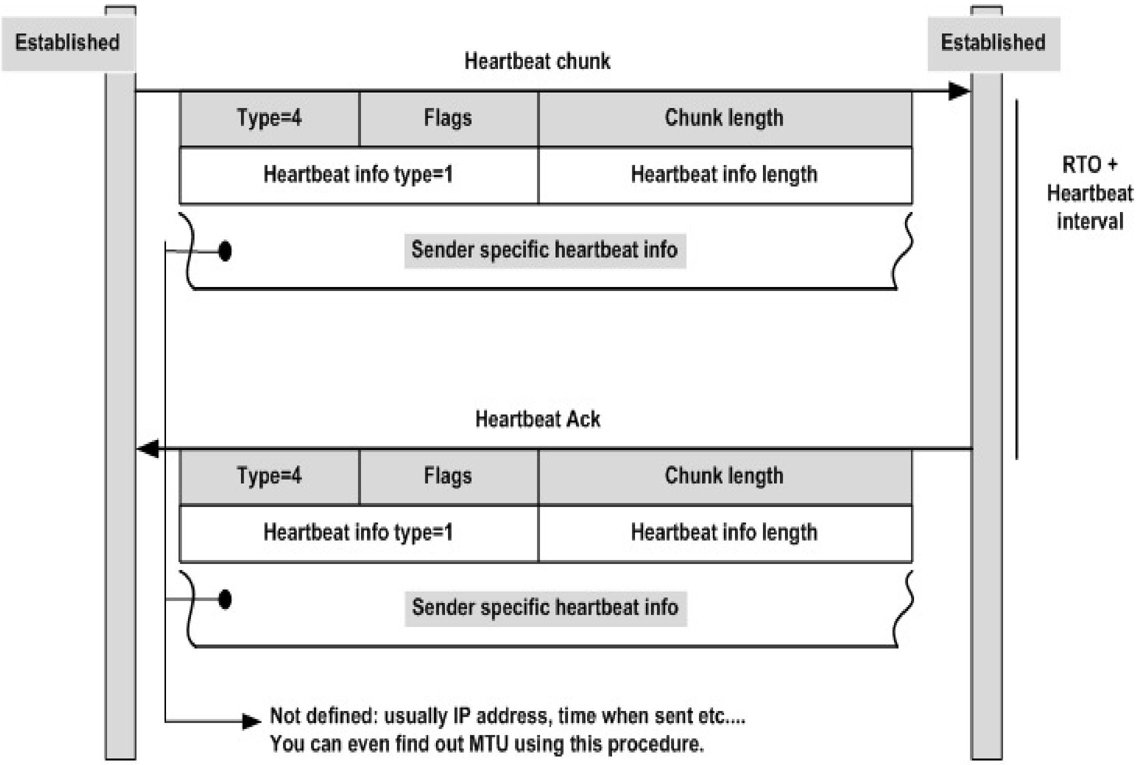


Figure 7.12: SCTP path heartbeat

The SCTP shutdown procedure is shown in figure 7.13:

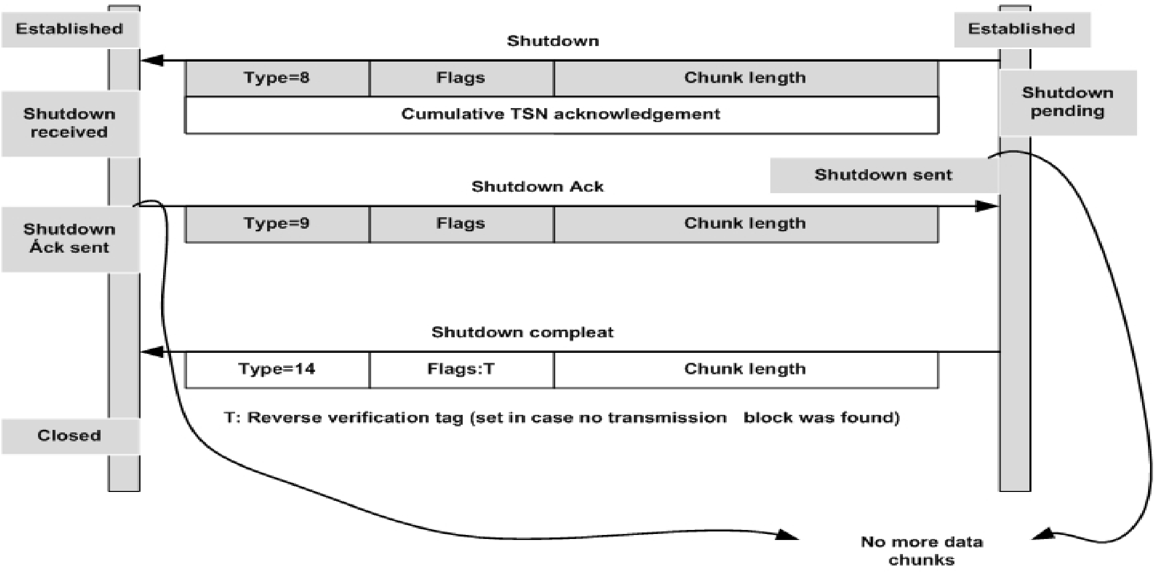


Figure 7.13: SCTP shutdown procedure

7.5 SCTP associations between MSC/VLR and the global SS7 network

MSUs are exchanged between the global SS7 network and the initiating MSC/VLR using SUA routing; as shown in figure 7.5 and figure 7.14. SUA routing is shown in figure 7.14 and figure 7.15 where as table 7.5 shows SSNs and their functions:

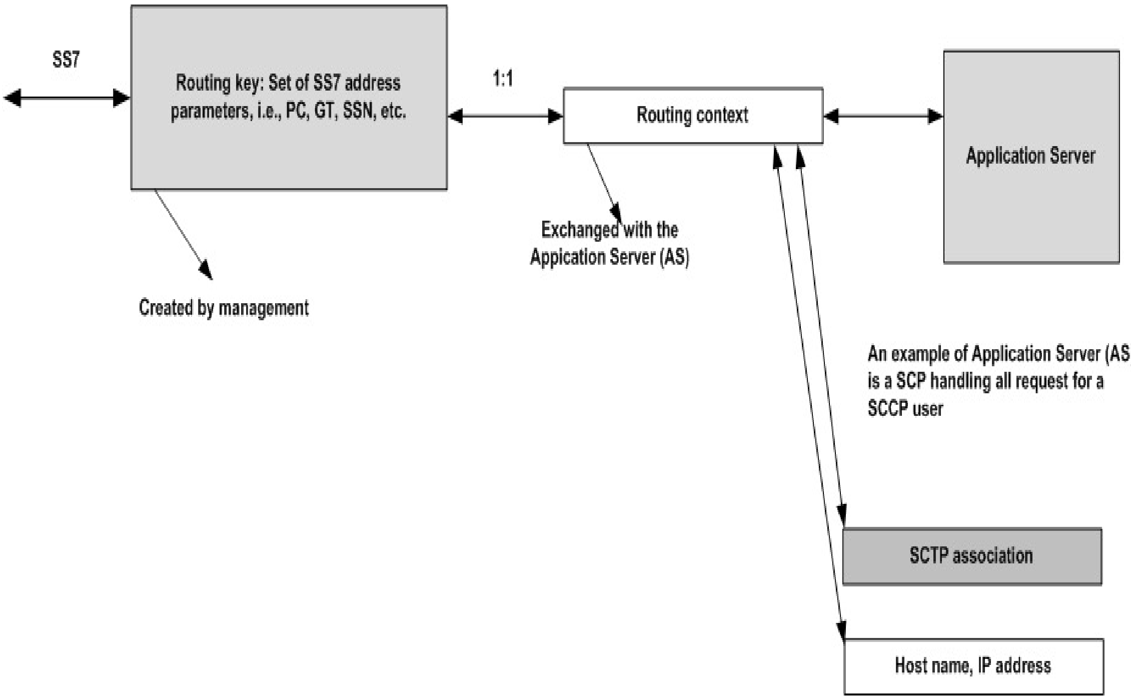

SS7
Routing key: Set of SS7 address parameters, i.e., PC, GT, SSN, etc.
1:1
Routing context
Application Server
Created by management
Exchanged with the Appication Server (AS)
An example of Application Server (AS) is a SCP handling all request for a SCCP user
SCTP association
Host name, IP address

Figure 7.14: SUA routing

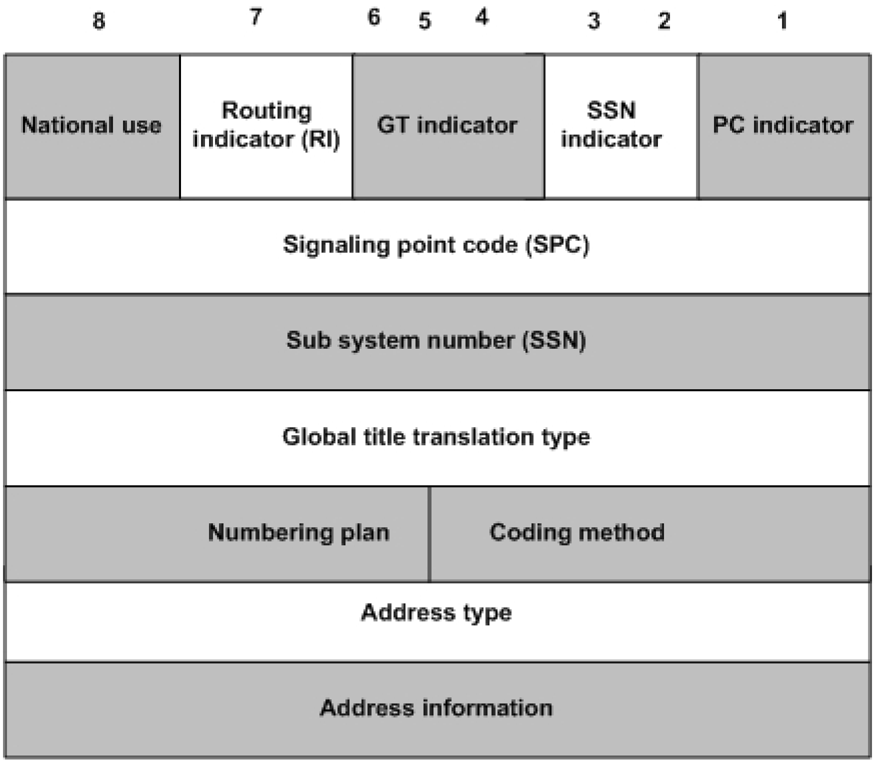


Figure 7.15 Calling and called party in SCCP

Tbale: 7.5 Sub-system numbers and their functions

Sub system number (SSN)	SSN Function
1	SCCP management
2	TUP
3	ISUP
4	Operation and maintenance AP (OMAP)
5	MAP
6	MAP/HLR
7	MAP/VLR
8	MAP/MSC
9	MAP/EIR
10	MAP/Auc
11	ISUP/SS ISUP supplementary service
12—247, 249—252	Reserved
248	MUP (NMT mobile up)
249	OMC
250	BSSAP

7.5.1 Message Switching Protocol Trace

We used the SIGTRAN Protocol Tracer provided by Zynetix Ltd., UK; a technology partner of SeaNet for capturing and decoding this traffic. This software offered the following advantages:

- SIGTRAN decoding was based on the relevant IETF standards.
- Single line decoding; displaying the key information of the entire SIGTRAN message (message type, class…).
- Automatic selection of the protocols above SCTP (IUA, SUA, DUA, M3UA, M2PA and M2UA) depending on the Payload Protocol ID.

Scenario: Location updates message switching traces

The trace shows a location update performed when a roaming mobile subscriber switched on his/her MS for the first time in SeaNet's network. Each of the SS7 messages/MSU is processed as per the MSGX configuration for that respective network element and corresponding traces are collected in real-time.

MSC/VLR → Media Gateway → Signaling Aggregator → International SS7 Net

a.) MSC/VLR → Media Gateway

When the MS tries to register, the request is initiated by the MSC/VLR and sent to the Media Gateway for follow-up processing. As per the principle of message switching where there is no need for a circuit to be established all the way from the source to the destination.

The VLR within the Integrated MSC/VLR/BSC will pass the location update request to the message switch, i.e. into ASSOC-1. The message is then routed to the destination association (destassoc) in this case ASSOC-10, which is associated with the media gateway.

```
# Configuration for the server itself
[SERVER]
ip=192.168.2.146
gctaddr=25
pc=1020  [superficial value; unique  point code is required for point code based routing but  irrelevant in
present cont of GT routing]
```

```
# Configuration for local associations #
# SCCP Module
 [ASSOC-1]  SS7 Module
desc=SS7M
type=dk [Intel's Dialogic / DataKinetics - SS7 Interface]
Protocols=sccp
gctaddr=1
dkmsgtype=0x8001
pc=10   [superficial value; unique  point code is required for point code based routing but  irrelevant in
present cont of GT routing]
gt=35699418105 [This is the global title of the VLR]
destassoc=10
```

The type of the association listed as 'dk' is a simple internal message queuing system, as there is no need for a full blown SCTP when the processes using ASSOC-1 are running in the same system.

The location update request is shown below:

```
softmsc: 144246.575: Received DK message from association 1 (#SS7M)
[144246.575:hhmmss.FSN/BSN, where FSN/BSN=Forward/Backward Sequence Number]
softmsc: SrcGT: 35699418105, DstGT: 356940400123658
softmsc: SrcPC: 8500, DstPC: 100 [SrcPC: Unique PC of the SCP directly connected over E1/TDM
link with MNO's MSC; DstGT: Unique PC of the MNO's MSC]
softmsc: SrcSSN: 7, DstSSN: 6
[SSN= 6 is MAP/HLR and SSN=7 is MAP/VLR; since MSU is originated on LU so DstSSN is
6 and SrcSSN is 7]
softmsc: SrcRI: GT, DstRI: GT
softmsc: Protocol class: 1
```

Although source and destination point codes are set, both source and destination routing identifier (SrcRI and DstRI) are set to GT, thus global titles will be used to route the signaling messages. Here the destination point code (DstPC) being set to 100 is of importance, as it identifies the network element that deals with location update requests within the Mobile network operator's network.

The VLR passed the location update request to the message switch, i. e. into ASSOC-1. The message is then routed to the destassoc listed above, in this case ASSOC-10. Via ASSOC-10, which is defined below, the message is sent to the media gateway over an IP link using the media gateway's IP address. The Subsystem Numbers (SSNs), specify which higher layer application sent the message (in this case 7 indicates the VLR) and which higher application it is meant for (in this case 6 indicates the HLR) at the destination system.

```
[ASSOC-10]
desc=Signaling flow to and from Media Gateway
type=sctp
protocols=sua
init=no
ip=192.168.1.151
local port=10030
remoteport=10300
destassoc=1
pc=100
```

Both local and remote ports need to be specified and must be different to avoid ambiguity as the Media Gateway could have one-to-many associations with different OBMRCS. The local port is used for sending messages; the remote port is used for receiving messages. This identifies the association uniquely.

The corresponding trace is shown below:

```
softmsc: 144246.579: Sending SCTP message to association 10 (MSGX at Media gateway):
softmsc: SrcGT: 35699418105, DstGT: 356940400123658
softmsc: SrcPC: 8500, DstPC: 100
softmsc: SrcSSN: 7, DstSSN: 6
softmsc: SrcRI: GT, DstRI: GT
softmsc: RC: 0
softmsc: Protocol class: 1
```

b.) Media Gateway → Signaling Aggregator

The Location Update request message from the Integrated MSC/VLR/BSC arrives at ASSOC-10 (the Media gateway) and is then forwarded to ASSOC-11, which is the association with the Signaling aggregator. The Location Update request message from the MSC/VLR comes in to ASSOC-10, as defined below:

```
[ASSOC-10]
desc= Signaling flow from and to MSC/VLR
type=sctp
protocols=sua
init=yes
ip=192.168.2.146
localport=10400
remoteport=10040
destassoc=11
log=yes
```

The corresponding trace is as follows:

```
softmsc: 235218.507: Received SCTP message from association 10 (MSGX at MSC/VLR)
softmsc: SrcGT: 35699418105, DstGT: 356940400123658
softmsc: SrcPC: 8500, DstPC: 100
softmsc: SrcSSN: 7, DstSSN: 6
softmsc: SrcRI: GT, DstRI: GT
softmsc: RC: 0
softmsc: Protocol class: 1
```

This is sent to destassoc 11 as specified in the configuration below. The reason is that messages received on remote port 10400 are to be passed on to this destassoc. Later on it will be seen that in the opposite direction, a message coming from assoc-11 will be sent to the MSC/VLR having GT *35699418105* located at 192.168.2.146 over local port 10040.

```
[ASSOC-11]
desc=Signaling flow to and from Signaling Aggregator
type=sctp
protocols=sua
init=yes
ip=80.85.96.140
localport=10100
remoteport=10010
pc=30
```

Note that, if multiple SCTP associations exist between a Media Gateway and various MSC/VLRs; a route based on Global Title matching (Usually this is referred to as Global Title Translation) is needed to route the MSU coming from Signaling Aggregator to the appropriate network.

```
[Route -3]
table=gt
match=35699418105
assoc=10
```

Thus the message is sent on to the Signaling Aggregator.

```
softmsc: 235218.545: Sending SCTP message to association 11 (MSGX at Signaling Aggregator)
softmsc: SrcGT: 447797706111, DstGT: 443859042501390
softmsc: SrcPC: 1082, DstPC: 643
softmsc: SrcSSN: 7, DstSSN: 6
softmsc: SrcRI: GT, DstRI: GT
softmsc: RC: 0
softmsc: Protocol class: 1
```

From ASSOC-11, the message is sent over an IP link to the Signaling aggregator, based on the IP address of the Signaling Aggregator.

c.) Signaling Aggregator → Mobile Network Operator

The location update request message arrives from the Media gateway over ASSOC-11 at the Signaling aggregator. The configuration looks as follows:

```
[ASSOC-11]
 desc=Signaling flow from and to Media Gateway
type=sctp
protocols=sua
init=no
ip=192.168.1.151
localport=10010
remoteport=10100
log=yes
destassoc=1
```

The corresponding trace is shown below:

```
 softmsc: 183230.770: Received SCTP message from association 11
 softmsc: SrcGT: 35699418105, DstGT: 356940400123658
 softmsc: SrcPC: 8500, DstPC: 100
 softmsc: SrcSSN: 7, DstSSN: 6
 softmsc: SrcRI: GT, DstRI: GT
 softmsc: RC: 0
 softmsc: Protocol class: 1”
```

The message is passed onto destassoc 1, which is configured as below:

```
[ASSOC-1] MTP3 Module
desc=MTP
type=dk [Intel’s Dialogic / DataKinetics - SS7 Interface]
protocols=sccp
gctaddr=14
log=yes”
```

The corresponding trace is shown below:

```
 softmsc: 181322.567: Sending DK message to association 1 (MTP3)
softmsc: SrcGT: 35699418105, DstGT: 356940400123658
softmsc: SrcPC: 8500, DstPC: 100
softmsc: SrcSSN: 7, DstSSN: 6
softmsc: SrcRI: GT, DstRI: GT
softmsc: Protocol class: 1
```

From ASSOC-1, the SCCP message is relayed over an E1 link to the MNO's MSC. In this case the association is MTP3, thus destassoc and GT are not used. Instead the routing is done via point codes. In this case the DstPC is the same as the destination PC of the message. Thus the MTP3 application passes it onto the Operator SS7 network for GT analysis.

International SS7 Net → Signaling Aggregator → Media Gateway → MSC/VLR

The result is that the MS requesting to register on the network is identified as a Vodafone MS. The Operator network authenticates the MS as a Vodafone Malta subscriber roaming in the Operator network.

a.) MNO's MSC → Signaling Aggregator

Once the authentication is done, a response message comes back over association 1 from the MNO's MSC:

```
softmsc: 181324.013: Received DK message from association 1 (MTP3)
softmsc: SrcGT: 356940, DstGT: 35699418105
softmsc: SrcPC: 100, DstPC: 8500
softmsc: SrcSSN: 6, DstSSN: 7
softmsc: SrcRI: GT, DstRI: GT
softmsc: Protocol class: 0
```

Now, however, there is no obvious parameter that tells the association-1 what to do with messages coming from outside. Routes are defined as follows for the purpose

```
[ROUTE-1]
table=gt
match=dstgt: 35699418105
assoc=11
```

Though there exists one-to-one connection between the Signaling Aggregator and the Media Gateway, a route is added to avoid ambiguity for each MSC/VLR (GSM network) that the Media Gateway connects to; based on the respective VLR's GT. Based on the destination GT of the message, route-1 says it should be routed over ASSOC-11.

```
softmsc: 183553.457: Sending SCTP message to association 11
softmsc: SrcGT: 356940, DstGT: 35699418105
softmsc: SrcPC: 100, DstPC: 8500
softmsc: SrcSSN: 6, DstSSN: 7
 softmsc: SrcRI: GT, DstRI: GT
 softmsc: RC: 0
 softmsc: Protocol class: 0”
```

Thus the location update message is forward along this route, i.e., forwarded it to ASSOC=11 towards the Media gateway.

e.) Media Gateway →Integrated MSC/VLR/BSC

At Media gateway location update response message comes into ASSOC-11.

```
“Jun 27 19:32:29 softmsc: 183229.535: Received SCTP message from association 11
Jun 27 19:32:29 softmsc:      SrcGT: 356940, DstGT: 35699418105
Jun 27 19:32:29 softmsc:      SrcPC: 100, DstPC: 8500
Jun 27 19:32:29 softmsc:      SrcSSN: 6, DstSSN: 7
Jun 27 19:32:29 softmsc:      SrcRI: GT, DstRI: GT
Jun 27 19:32:29 softmsc:      RC: 0
Jun 27 19:32:29 softmsc:      Protocol class: 0”
```

Note that, if multiple SCTP associations exist between a Media Gateway and various MSC/VLRs; a route based on Global Title translation is needed to route the MSU coming from Signaling Aggregator to the respective networks such route is shown below:

```
[Route -1]
table=gt
match=dstgt: 35699418105
assoc=10
```

The message is now passed on to ASSOC-10 as follows:

```
softmsc: 235221.960: Sending SCTP message to association 10 (MSGX at OSC133)
softmsc: SrcGT: 44385016411, DstGT: 447797706111
softmsc: SrcPC: 643, DstPC: 1082
softmsc: SrcSSN: 6, DstSSN: 7
softmsc: SrcRI: GT, DstRI: GT
softmsc: RC: 0
softmsc: Protocol class: 0
```

Thus the message is sent towards Integrated MSC/VLR/BSC.

e.) Integrated MSC/VLR/BSC

The location update response message arrives into ASSOC-10, which is the only remote association defined at the Integrated MSC/VLR/BSC.

```
softmsc: 165308.131: Received SCTP message from association 10
softmsc: SrcGT: 356940, DstGT: 35699418105
softmsc: SrcPC: 100, DstPC: 8500
softmsc: SrcSSN: 6, DstSSN: 7
 softmsc: SrcRI: GT, DstRI: GT
softmsc: RC: 0
softmsc: Protocol class: 0”
```

Coming in from the outside, it is routed to destassoc (as defined in the configuration shown in section 6.4.2.1 (a)), in this case ASSOC-1; the trace of which is shown as below:

```
softmsc: 144249.314: Sending DK message to association 1 (SS7M)
softmsc: SrcGT: 356940, DstGT: 35699418105
softmsc: SrcPC: 100, DstPC: 8500
softmsc: SrcSSN: 6, DstSSN: 7
softmsc: SrcRI: GT, DstRI: GT
softmsc: Protocol class: 0
```

Where it is passed onto the MS.

7.6 Protocol Trace

Again we have used the SS7 Protocol Tracer provided by Zynetix Ltd., UK; a technology partner of SeaNet. The reasons for using this protocol tracer include:

- ISUP, SCCP and TCAP call trace filters
- Decodes the captured signaling layer-by-layer,
- Automatic selection of the protocols above MTP (TUP, ISUP, SCCP, TCAP) depending on the Service Indicator field.
- Automatically finds all the signaling events related to a specific connection, e.g. an ISUP call or a SCCP connection.

The following filters and call traces used in the context of this thesis project:

- ISUP
  - Message Type
  - Circuit Identification Code
  - Calling Party Number
  - Called Party Number
- Call Trace ISUP
  - SCCP
    - Message Type
    - Global Title
    - Subsystem Number
    - Call Trace SCCP
  - MTP
    - Message Type
    - Originating Point Code

- Destination Point Code
- Service Indicator
- Network Indicator

7.6.1 SCCP Trace

Two types of SCCP implementation exist: SCCP route and SCCP relation. These are conceptually similar to signaling route and signaling relation in MTP respectively. They are defined as follows:

- SCCP route (covered in section 7.5): A SCCP route is composed of an ordered list of nodes where the SCCP is used (origin, relay(s), and destination) for the transfer of SCCP messages from an originating SCCP user to the destination SCCP user.

- SCCP relation: A SCCP relation is a relation between two SCCP users which allows them to exchange data over it. A SCCP relation can consist of one or several SCCP routes.

The following section will show different scenarios of SCCP relation in a context of network architecture as shown in Table 7.6. The following primitives are supported between the SUA and an SCCP-user (a reference to the ITU standard and the sections where these primitives and corresponding parameters are described, is also given):

Table 7.6: SUA and SCCP-user supported primitives

Generic Name	**Specific Name**	**ITU Reference (**ITU-Q.711 **)**
N-CONNECT	Request Indication Response Confirm	Chap 6.1.1.2.2 (Tab 2/Q.711)
N-DATA	Request Indication	Chap 6.1.1.2.3 (Tab 3/Q.711)
N-EXPEDITED DATA	Request Indication	Chap 6.1.1.2.3 (Tab 4/Q.711)
N-RESET	Request Indication Response Confirm	Chap 6.1.1.2.3 (Tab 5/Q.711)
N-DISCONNECT	Request Indication	Chap 6.1.1.2.4 (Tab 6/Q.711)
N-INFORM	Request Indication	Chap 6.1.1.3.2 (Tab 8/Q.711)
N-UNITDATA	Request Indication	Chap 6.2.2.3.1 (Tab 12/Q.711)
N-NOTICE	Indication	Chap 6.2.2.3.2 (Tab 13/Q.711)
N-STATE	Request Indication	Chap 6.3.2.3.2 (Tab 16/Q.711)
N-PCSTATE	Indication	Chap 6.3.2.3.3 (Tab 17/Q.711)
N-COORD	Request Indication Response Confirm	Chap 6.3.2.3.1 (Tab 15/Q.711)

Connection-oriented signaling messages always start with the establishment of a SCCP connection using the N-CONNECT SCCP primitive. Selection of the signaling target is done when the N-CONNECT indication message is received from a signaling source, e.g., an access node. Four different N-CONNECT messages are used to successfully set up a SCCP connection.

The originating SCCP user, i.e., the signaling source sends an N- CONNECT request to the SCCP user application. The terminating SCCP user, i.e., the signaling target receives an N-CONNECT indication from its SCCP layer; the terminating SCCP user returns an N-CONNECT response to the originating SCCP user application. The originating SCCP user receives an N-CONNECT confirm from its SCCP layer.

In addition to the SCCP connection setup with the signaling source, a connection needs to be established with an actual signaling target. This is done before sending the N-CONNECT response to the signaling source.

Whenever a data message is received for an already established connection-oriented signaling, identified by the connection identifier in the message, the SCCP user application will verify the received connection identifier and forward the data message directly using the corresponding outgoing connection identifier.

Finally, each connection-oriented signaling connection is terminated using the N-DISCONNECT primitive. In a nutshell, the SCCP connection setup process is as follows:

1. N-CONNECT request
2. N-CONNECT indication includes called address and a connection identifier;
3. N-CONNECT request includes signaling target MSC and a connection identifier
4. N-CONNECT indication
5. N-CONNECT response;
7. N-CONNECT confirm including connection identifier as that used in step 3.
8. SCCP user application creates entry in connection identification table linking connections with identifier as used in step 2 and step 3 to each other;
9. N-CONNECT response including connection identifier as that used in step 2;
10. N-CONNECT confirm

The data transfer process occurs as follows:

11. N-DATA request;
12. N-DATA indication including connection identifier as that used in step 2;
13. The SCCP user application looks in identification table and finds that the data has to be forwarded to signaling connection with identifier as that used in step 3;
14. N-DATA request including connection identifier as that used in step 3;
15. N-DATA indication;
16. N-DATA request;
17. N-DATA indication including connection identifier as that used in step 3;
18. The SCCP user application looks in identification table and finds that data has to be forwarded to connection with identifier as that used in step 3;
19. N-DATA request including connection identifier as that used in step 2
21. Signaling target decides to terminate connection with N-DISCONNECT request where the related message may include a data part;
22. N-DISCONNECT indication including connection identification as that used in step 3;
23. The SCCP user application looks in identification table and finds that N-DISCONNECT needs to be forwarded to the connection with identifier as that used in step 2; and then deletes the corresponding entry from the identification table;
24. N-DISCONNECT request including connection identifier as that used in step 2;
25. N-DISCONNECT indication, i.e., connection terminated.

The following trace represents the steps involved in SCCP connection establishment, as mentioned above:

```
Jun 27 17:52:50 softmsc: Port-0 Tx to 192.168.1.151:4533:: HBACK
Jun 27 17:52:50 softmsc:
Jun 27 17:52:56 softmsc: Port-0 Rx:: HBACK
Jun 27 17:52:56 softmsc:
Jun 27 17:52:59 softmsc: 165259.903 SCCP user N-CONNECT ind,  Prim: indication,ConnId: 79
Jun 27 17:52:59 softmsc:  CalledAddr  ( 2) 42 fe
Jun 27 17:52:59 softmsc:  UserData    (30) 00 1c 57 05 08 00 09 f1
Jun 27 17:52:59 softmsc:                   91 eb 28 27 20 17 0f 05
Jun 27 17:52:59 softmsc:                   08 00 42 f0 80 00 28 30
Jun 27 17:52:59 softmsc:                   05 f4 2e 80 25 54
Jun 27 17:52:59 softmsc:
```

```
Jun 27 17:52:59 softmsc: 165259.913 SCCP user N-CONNECT resp,  Prim: request,  ConnId: 79
Jun 27 17:52:59 softmsc:
Jun 27 17:53:00 softmsc: 165259.993 SCCP user N-DATA req,  Prim: request,  ConnId: 79
Jun 27 17:53:00 softmsc:  UserData    ( 6) 01 00 03 05 18 01
Jun 27 17:53:00 softmsc:
Jun 27 17:53:00 softmsc: Port-0 Rx:: HB
Jun 27 17:53:00 softmsc:
Jun 27 17:53:00 softmsc: Port-0 Tx to 192.168.1.151:4533:: HBACK
Jun 27 17:53:00 softmsc:
Jun 27 17:53:00 softmsc: 165300.218 SCCP user N-DATA ind,  Prim: indication,  ConnId: 79
Jun 27 17:53:00 softmsc:  UserData    (14) 00 0c 54 12 03 30 18 81
Jun 27 17:53:00 softmsc:                   13 04 60 14 10 00
Jun 27 17:53:00 softmsc:
Jun 27 17:53:01 softmsc: 165301.380 SCCP user N-DATA ind,  Prim: indication,  ConnId: 79
Jun 27 17:53:01 softmsc:  UserData    (14) 01 80 0b 05 59 08 29 87
Jun 27 17:53:01 softmsc:                   10 40 00 21 63 85
Jun 27 17:53:01 softmsc: “
```

7.6.2 MAP Invoke at Location Update

a.) IMSI Authorization

The roamers sends its IMSI (278010400123658) to SeaNet’s VLR (GT =35699418105) and requests authentication. SeaNet’s VLR contacts the HLR (GT 356940) of the roamer by sending a “*DialogueId:73 SendAuthInfoReq*” message corresponding to the IMSI of the roamer and ask for authentication parameters. The HLR responds with a “*DialogueId:73 SendAuthInfoCnf*” message and sends authentication parameters (i.e., Kc, RAND , SRES) to SeaNet’s VLR.

```
Jun 27 17:53:01 softmsc: 165301.519 MAP:: DialogueId:73 OPEN-REQ
Jun 27 17:53:01 softmsc:       DestAddr: AI:0x12 SSN:6 GTType:0 GT:17-356940400123658
Jun 27 17:53:01 softmsc:       OrigAddr: AI:0x12 SSN:7 GTType:0 GT:11-35699418105
Jun 27 17:53:01 softmsc:     ApplContext: (9) 06 07 04 00 00 01 00 0e 02
Jun 27 17:53:01 softmsc:
Jun 27 17:53:01 softmsc: 165301.549 MAP:: DialogueId:73 SendAuthInfoReq
Jun 27 17:53:01 softmsc:         Timeout: 15
Jun 27 17:53:01 softmsc:        InvokeId: 0
Jun 27 17:53:01 softmsc:            IMSI: 278010400123658
Jun 27 17:53:01 softmsc:
Jun 27 17:53:01 softmsc: 165301.572 MAP:: DialogueId:73 DELIMITER-REQ
Jun 27 17:53:01 softmsc:
Jun 27 17:53:02 softmsc: 165302.544 MAP:: DialogueId:73 OPEN-CNF
Jun 27 17:53:02 softmsc:        DestAddr: AI:0x12 SSN:7 GTType:0 GT:11-35699418105
Jun 27 17:53:02 softmsc:        OrigAddr: AI:0x12 SSN:6 GTType:0 GT:11-356940
Jun 27 17:53:02 softmsc:          Result: Accepted
Jun 27 17:53:02 softmsc:     ApplContext: (9) 06 07 04 00 00 01 00 0e 02
Jun 27 17:53:02 softmsc:
Jun 27 17:53:02 softmsc: 165302.597 MAP:: DialogueId:73 SendAuthInfoCnf
```

b.) Authentication and Encryption

The MS receives the RAND (Random Challenge), encrypts it with the Individual Ki (Individual Subscriber Authentication Key) assigned to the MS, and sends the SRES (Signed Response) to MSC. The MSC verifies the SRES, and then the MS generates a Kc (Session Key) utilizing Ki and RAND and sends Kc to the BTS. The MSC also sends the Kc to the MS. The BTS verifies the Kc from the MS and MSC. The over-the-air communication channel between the MS and BTS is now encrypted. This process authenticates the roaming MS to SeaNet's GSM network.

```
Jun 27 17:53:02 softmsc:        InvokeId: 0
Jun 27 17:53:02 softmsc:          RAND-0: 9d 6a 7b 0e 5b 2e 07 9d c0 86 62 49 60 e0 85 ed
Jun 27 17:53:02 softmsc:            Kc-0: 55 dc c7 ae ed d2 a4 00
Jun 27 17:53:02 softmsc:          SRES-0: 0x6fbebf7c
Jun 27 17:53:02 softmsc:          RAND-1: 85 09 40 5e 56 1c d5 8d c5 c0 22 b8 04 f5 3e 5f
Jun 27 17:53:02 softmsc:            Kc-1: 9f 73 39 b4 5d a8 88 00
Jun 27 17:53:02 softmsc:          SRES-1: 0x8db52d92
Jun 27 17:53:02 softmsc:          RAND-2: df b9 a5 f0 5e 89 35 f2 fc 70 54 54 a9 ac 4b 79
Jun 27 17:53:02 softmsc:            Kc-2: f6 dd a5 bb 52 fb 38 00
Jun 27 17:53:02 softmsc:          SRES-2: 0x9b417913
Jun 27 17:53:02 softmsc:          RAND-3: 0d 93 c2 3e 37 33 85 f1 06 b1 f2 39 91 42 d7 6d
Jun 27 17:53:02 softmsc:            Kc-3: 56 80 78 91 aa 1b fc 00
Jun 27 17:53:02 softmsc:         SRES-3: 0x6bc39fb2
Jun 27 17:53:02 softmsc:
Jun 27 17:53:02 softmsc: 165302.734 MAP:: DialogueId:73 CLOSE-IND
Jun 27 17:53:02 softmsc:
Jun 27 17:53:02 softmsc: 165302.827 SCCP user N-DATA req,  Prim: request,  ConnId: 79
Jun 27 17:53:02 softmsc:  UserData    (22) 01 00 13 05 12 00 9d 6a
Jun 27 17:53:02 softmsc:                   7b 0e 5b 2e 07 9d c0 86
Jun 27 17:53:02 softmsc:                   62 49 60 e0 85 ed
Jun 27 17:53:02 softmsc:
Jun 27 17:53:05 softmsc: 165305.501 SCCP user N-DATA ind,  Prim: indication,  ConnId: 79
Jun 27 17:53:05 softmsc:  UserData    ( 9) 01 80 06 05 14 7c bf be
Jun 27 17:53:05 softmsc:                   6f
Jun 27 17:53:05 softmsc:
Jun 27 17:53:05 softmsc: 165305.528 SCCP user N-DATA req,  Prim: request,  ConnId: 79
Jun 27 17:53:05 softmsc:  UserData    (16) 00 0e 53 0a 09 04 55 dc
Jun 27 17:53:05 softmsc:                   c7 ae ed d2 a4 00 23 01
Jun 27 17:53:05 softmsc:
Jun 27 17:53:05 softmsc:
Jun 27 17:53:06 softmsc: Port-0 Rx:: HBACK
Jun 27 17:53:06 softmsc:
Jun 27 17:53:07 softmsc: 165307.171 SCCP user N-DATA ind,  Prim: indication,  ConnId: 79
Jun 27 17:53:07 softmsc:  UserData    (18) 00 10 55 20 0d 06 32 17
Jun 27 17:53:07 softmsc:                   09 33 95 57 06 00 80 41
Jun 27 17:53:07 softmsc:                   11 f2"
```

c.) Location update request confirmation

SeaNet's VLR sends a "*DialogueId:74 UpdateLocationReq*" message to the roamer's HLR , this message is enclosed with IMSI: *278010400123658, MSC: 35699418104, VLR: 35699418105.* The HLR accepts the request and responds with a "*DialogueId: 74 InsertSubsDataInd"* message along with MSISDN: 35699375466 of the MS. Further we can see the exchange of "*DialogueId:74 InsertSubsDataRsp"* and *"DialogueId:74 UpdateLocationCnf"* MAP messages between SeaNet's VLR and the roamer's HLR.

```
Jun 27 17:53:07 softmsc: 165307.234 MAP:: DialogueId:74 OPEN-REQ
Jun 27 17:53:07 softmsc:        DestAddr: AI:0x12 SSN:6 GTType:0 GT:17-356940400123658
Jun 27 17:53:07 softmsc:        OrigAddr: AI:0x12 SSN:7 GTType:0 GT:11-35699418105
Jun 27 17:53:07 softmsc:     ApplContext: (9) 06 07 04 00 00 01 00 01 03
Jun 27 17:53:07 softmsc:
Jun 27 17:53:07 softmsc: 165307.260 MAP:: DialogueId:74 UpdateLocationReq
Jun 27 17:53:07 softmsc:         Timeout: 15
Jun 27 17:53:07 softmsc:        InvokeId: 0
Jun 27 17:53:07 softmsc:            IMSI: 278010400123658
Jun 27 17:53:07 softmsc:             MSC: 11-35699418104
Jun 27 17:53:07 softmsc:             VLR: 11-35699418105
Jun 27 17:53:07 softmsc:    CAMEL Phases: V1 V2
Jun 27 17:53:07 softmsc:
Jun 27 17:53:07 softmsc: 165307.278 MAP:: DialogueId:74 DELIMITER-REQ
Jun 27 17:53:07 softmsc:
Jun 27 17:53:08 softmsc: 165308.213 MAP:: DialogueId:74 OPEN-CNF
Jun 27 17:53:08 softmsc:        DestAddr: AI:0x12 SSN:7 GTType:0 GT:11-35699418105
Jun 27 17:53:08 softmsc:        OrigAddr: AI:0x12 SSN:6 GTType:0 GT:11-356940
Jun 27 17:53:08 softmsc:          Result: Accepted
Jun 27 17:53:08 softmsc:     ApplContext: (9) 06 07 04 00 00 01 00 01 03
Jun 27 17:53:08 softmsc:
Jun 27 17:53:08 softmsc: 165308.247 MAP:: DialogueId:74 InsertSubsDataInd
Jun 27 17:53:08 softmsc:        InvokeId: 1
Jun 27 17:53:08 softmsc:          MSISDN: 11-35699375466
Jun 27 17:53:08 softmsc:
Jun 27 17:53:08 softmsc: 165308.306 MAP:: DialogueId:74 InsertSubsDataRsp
Jun 27 17:53:08 softmsc:        InvokeId: 1
Jun 27 17:53:08 softmsc:
Jun 27 17:53:08 softmsc: 165308.324 MAP:: DialogueId:74 DELIMITER-REQ
Jun 27 17:53:08 softmsc:
Jun 27 17:53:08 softmsc: 165308.380 MAP:: DialogueId:74 DELIMITER-IND
Jun 27 17:53:08 softmsc:
Jun 27 17:53:09 softmsc: 165309.281 MAP:: DialogueId:74 InsertSubsDataInd
Jun 27 17:53:09 softmsc:        InvokeId: 2
Jun 27 17:53:09 softmsc:
Jun 27 17:53:09 softmsc: 165309.691 MAP:: DialogueId:74 InsertSubsDataRsp
Jun 27 17:53:09 softmsc:        InvokeId: 2
Jun 27 17:53:09 softmsc:
Jun 27 17:53:09 softmsc: 165309.715 MAP:: DialogueId:74 DELIMITER-REQ
Jun 27 17:53:09 softmsc:
Jun 27 17:53:09 softmsc: 165309.782 MAP:: DialogueId:74 DELIMITER-IND
Jun 27 17:53:09 softmsc:
Jun 27 17:53:09 softmsc: 165309.866 MAP:: DialogueId:74 InsertSubsDataInd
Jun 27 17:53:09 softmsc:        InvokeId: 3
Jun 27 17:53:09 softmsc:
Jun 27 17:53:10 softmsc: Port-0 Rx:: HB
Jun 27 17:53:10 softmsc:
Jun 27 17:53:10 softmsc: Port-0 Tx to 192.168.1.151:4533:: HBACK
Jun 27 17:53:10 softmsc:
Jun 27 17:53:10 softmsc: 165310.321 MAP:: DialogueId:74 InsertSubsDataRsp
Jun 27 17:53:10 softmsc:        InvokeId: 3
Jun 27 17:53:10 softmsc:
Jun 27 17:53:10 softmsc: 165310.339 MAP:: DialogueId:74 DELIMITER-REQ
Jun 27 17:53:10 softmsc:
Jun 27 17:53:10 softmsc: 165310.390 MAP:: DialogueId:74 DELIMITER-IND
Jun 27 17:53:10 softmsc:
Jun 27 17:53:11 softmsc: 165311.222 MAP:: DialogueId:74 UpdateLocationCnf
Jun 27 17:53:11 softmsc:        InvokeId: 0
Jun 27 17:53:11 softmsc:            HLR: +356940
Jun 27 17:53:11 softmsc:
Jun 27 17:53:11 softmsc: 165311.292 SCCP user N-DATA req,  Prim: request,  ConnId: 79
Jun 27 17:53:11 softmsc:  UserData    (18) 01 00 0f 05 02 09 f1 91
Jun 27 17:53:11 softmsc:                   eb 28 17 05 f4 00 00 d9
Jun 27 17:53:11 softmsc:                   6e a1
Jun 27 17:53:11 softmsc:
Jun 27 17:53:11 softmsc: 165311.335 MAP:: DialogueId:74 CLOSE-IND
Jun 27 17:53:11 softmsc:
Jun 27 17:53:12 softmsc: 165312.714 SCCP user N-DATA ind,  Prim: indication,  ConnId: 79
Jun 27 17:53:12 softmsc:  UserData    ( 5) 01 80 02 05 5b
Jun 27 17:53:12 softmsc:
Jun 27 17:53:12 softmsc: 165312.766 SCCP user N-DATA req,  Prim: request,  ConnId: 79
Jun 27 17:53:12 softmsc:  UserData    ( 6) 00 04 20 04 01 00
Jun 27 17:53:12 softmsc:
```

7.6.3 ISUP Trace: Mobile Originating (MO) Call Setup

- **ISUP/SDP/RTP Setup**

  The traces recorded in this section at the Media gateway for an outgoing call scenario. Initial parts of the trace show Called Party Address (cld) (i.e.,*46736308811*) and Calling Party address (clg) (i.e., *35699375466).* The *"farendinfo=0:192.168.2.146:4532"* parameter shows which remotely connected BSC/MSC/VLR is used to make an outgoing call. The Media gateway transmits an ISUP Initial Address Message (IAM) "*022042.973 ISUP Tx: IAM CctGrp 0 LocalCct 2, Len 25"* to reserve an idle trunk circuit for an outgoing call; IAM also includes cld and clg. The destination ISDN switch examines the cld and determines that it serves the called party; rings the called party's line and transmits an ISUP Address Complete Message (ACM) to the Media gateway "*022048.334 ISUP Rx: ACM CctGrp 0 LocalCct 2, Len 6".* When the called party picks up the phone, the destination switch terminates the ringing tone and transmits an ISUP Answer Message (ANM) to the Media gateway "*022052.678 ISUP Rx: ANM CctGrp 0 LocalCct 2, Len 2"*. Finally if caller hangs-up first, the Media gateway sends an ISUP Release Message (REL) "*Jun 28 03:21:01 softmsc: 022101.885 ISUP Tx: REL CctGrp 0 LocalCct 2, Len 6*" to release the trunk circuit between the switches.

```
"Jun 28 03:20:42 softmsc: Port-3 Tx to 192.168.2.146:4532:: HBACK
Jun 28 03:20:42 softmsc:
Jun 28 03:20:42 softmsc: Port-3 Rx:: setup 0
Jun 28 03:20:42 softmsc: bc-itc=0
Jun 28 03:20:42 softmsc: bc-l1=0
Jun 28 03:20:42 softmsc: cld=11-46736308811
Jun 28 03:20:42 softmsc: clg=11-35699375466
Jun 28 03:20:42 softmsc: farendinfo=0:192.168.2.146:4532
Jun 28 03:20:42 softmsc:
Jun 28 03:20:42 softmsc: 022042.973 ISUP Tx:  IAM  CctGrp 0 LocalCct 2, Len 25
Jun 28 03:20:42 softmsc:  Called number        ( 8) 04 10 64 37 36 80 18 f1
Jun 28 03:20:42 softmsc:  Calling number.      ( 8) 84 11 53 96 39 57 64 06
Jun 28 03:20:42 softmsc:  Trans. medium req.   ( 1) 00
Jun 28 03:20:42 softmsc:
Jun 28 03:20:46 softmsc: Port-3 Rx:: HBACK
Jun 28 03:20:46 softmsc:
Jun 28 03:20:48 softmsc: 022048.333 MSGType 32769 (0x8001), Id 5, St 0, Dst 4,  Src 14, Len 11
Jun 28 03:20:48 softmsc:     c5 05 92 d1 2b 02 00 06
Jun 28 03:20:48 softmsc:     16 34 00
Jun 28 03:20:48 softmsc:
Jun 28 03:20:48 softmsc: 022048.334 ISUP Rx:  ACM  CctGrp 0 LocalCct 2, Len 6
Jun 28 03:20:48 softmsc:  Backwards call ind.  ( 2) 16 34
Jun 28 03:20:48 softmsc:
Jun 28 03:20:48 softmsc: Port-3 Rx:: CRCX 1408 0000@192.168.2.146 MGCP 1.0
Jun 28 03:20:48 softmsc: M: sendrecv
Jun 28 03:20:48 softmsc: C: 2c
Jun 28 03:20:48 softmsc: v=0
Jun 28 03:20:48 softmsc: c=IN IP4 192.168.1.152
Jun 28 03:20:48 softmsc: m=audio 4196 RTP/AVP 98
Jun 28 03:20:48 softmsc: a=rtpmap:98 GSM-EFR/8000
Jun 28 03:20:48 softmsc:
Jun 28 03:20:48 softmsc: Port-3 Tx to 192.168.2.146:4532:: alert 0
Jun 28 03:20:48 softmsc: inbandinfo=1
Jun 28 03:20:48 softmsc: sdp=192.168.1.152:4196
Jun 28 03:20:48 softmsc: farendinfo=0:192.168.1.151:4533
Jun 28 03:20:48 softmsc:
Jun 28 03:20:50 softmsc: Port-3 Rx:: switch 0
Jun 28 03:20:50 softmsc: sdp=192.168.250.254:4026
Jun 28 03:20:50 softmsc:
Jun 28 03:20:52 softmsc: Port-3 Rx:: HB
Jun 28 03:20:52 softmsc:
Jun 28 03:20:52 softmsc: Port-3 Tx to 192.168.2.146:4532:: HBACK
Jun 28 03:20:52 softmsc:
Jun 28 03:20:52 softmsc: 022052.677 MSGType 32769 (0x8001), Id 5, St 0, Dst 4,  Src 14, Len 9
Jun 28 03:20:52 softmsc:     c5 05 92 d1 2b 02 00 09
Jun 28 03:20:52 softmsc:     00
Jun 28 03:20:52 softmsc:
Jun 28 03:20:52 softmsc: 022052.678 ISUP Rx:  ANM  CctGrp 0 LocalCct 2, Len 2
Jun 28 03:20:52 softmsc:
Jun 28 03:20:52 softmsc: Port-3 Tx to 192.168.2.146:4532:: connect 0
Jun 28 03:20:52 softmsc:
Jun 28 03:20:56 softmsc: Port-3 Rx:: HBACK
Jun 28 03:20:56 softmsc:
Jun 28 03:21:01 softmsc: Port-3 Rx:: rel 0
Jun 28 03:21:01 softmsc: cause=16
Jun 28 03:21:01 softmsc:
Jun 28 03:21:01 softmsc: 022101.885 ISUP Tx:  REL  CctGrp 0 LocalCct 2, Len 6
Jun 28 03:21:01 softmsc:  Cause              ( 2) 80 90
Jun 28 03:21:01 softmsc:
Jun 28 03:21:01 softmsc: 022101.975 MSGType 32769 (0x8001), Id 5, St 0, Dst 4,  Src 14, Len 9
Jun 28 03:21:01 softmsc:     c5 05 92 d1 2b 02 00 10
Jun 28 03:21:01 softmsc:     00
Jun 28 03:21:01 softmsc:
Jun 28 03:21:01 softmsc: 022101.976 ISUP Rx:  RLC  CctGrp 0 LocalCct 2, Len 2
Jun 28 03:21:01 softmsc:
Jun 28 03:21:02 softmsc: Port-3 Rx:: HB
Jun 28 03:21:02 softmsc:
Jun 28 03:21:02 softmsc: Port-3 Tx to 192.168.2.146:4532:: HBACK
Jun 28 03:21:02 softmsc:
Jun 28 03:21:06 softmsc: Port-3 Rx:: HBACK
Jun 28 03:21:06 softmsc: “
```

7.6.4 Trace: Mobile Terminating (MT) Call Setup

a.) MAP Trace: Roaming Number Request and Allocation

For an incoming call, the Integrated MSC/VLR/BSC receives a request from the roamer’s HLR to provide the routing information needed to reach the roamer (*MAP:: DialogueId:540 ProvideRoamingNumInd)*. This request includes *IMSI: 278010400123658 and Call Ref Num:*

209A377715 as the session reference. The Integrated MSC/VLR/BSC acknowledges the request with "*MAP:: DialogueId:540 ProvideRoamingNumRsp"* message and provides a MSRN *(MSRN: +46850534704).*

```
"Jan 10 15:18:26 softmsc: Port-0 Rx:: HBACK
Jan 10 15:18:26 softmsc:
Jan 10 15:18:26 softmsc: Port-0 Rx:: HB
Jan 10 15:18:26 softmsc:
Jan 10 15:18:26 softmsc: Port-0 Tx to 192.168.1.151:4512:: HBACK
Jan 10 15:18:26 softmsc:
Jan 10 15:18:31 softmsc: 151831.366 MAP:: DialogueId:540 OPEN-IND
Jan 10 15:18:31 softmsc:       DestAddr: AI:0x12 SSN:7 GTType:0 GT:11-35699418105
Jan 10 15:18:31 softmsc:       OrigAddr: AI:0x12 SSN:6 GTType:0 GT:11-356940
Jan 10 15:18:31 softmsc:    ApplContext: (9) 06 07 04 00 00 01 00 03 03
Jan 10 15:18:31 softmsc:
Jan 10 15:18:31 softmsc: 151831.371 MAP:: DialogueId:540 OPEN-RSP
Jan 10 15:18:31 softmsc:       DestAddr: AI:0x12 SSN:6 GTType:0 GT:11-356940
Jan 10 15:18:31 softmsc:       OrigAddr: AI:0x12 SSN:7 GTType:0 GT:11-35699418105
Jan 10 15:18:31 softmsc:         Result: Accepted
Jan 10 15:18:31 softmsc:
Jan 10 15:18:31 softmsc: 151831.377 MAP:: DialogueId:540 ProvideRoamingNumInd
Jan 10 15:18:31 softmsc:       InvokeId: 1
Jan 10 15:18:31 softmsc:           IMSI: 278010400123658
Jan 10 15:18:31 softmsc:            MSC: +35699418102F
Jan 10 15:18:31 softmsc:           GMSC: +3569411F
Jan 10 15:18:31 softmsc:   Call Ref Num: 209A377715
Jan 10 15:18:31 softmsc:  ORNotSuppInGMSC: Y
Jan 10 15:18:31 softmsc:
Jan 10 15:18:31 softmsc: 151831.385 MAP:: DialogueId:540 ProvideRoamingNumRsp
Jan 10 15:18:31 softmsc:       InvokeId: 1
Jan 10 15:18:31 softmsc:           MSRN: +46850534704
Jan 10 15:18:31 softmsc:
Jan 10 15:18:31 softmsc: 151831.386 MAP:: DialogueId:540 CLOSE-REQ
Jan 10 15:18:31 softmsc:  ReleaseMethod: Normal
Jan 10 15:18:31 softmsc:
Jan 10 15:18:31 softmsc: 151831.392 MAP:: DialogueId:540 DELIMITER-IND
```

b.) SCCP Trace: Call Setup

The routing node sends the data packet including a call setup message and prior to performing the lookup, encapsulates the data packet in a signaling connection control part (SCCP) message to reach to the destination using GT routing over IP link.

```
Jan 10 15:18:31 softmsc:
Jan 10 15:18:33 softmsc: Port-0 Rx:: setup 4
Jan 10 15:18:33 softmsc: bc-itc=0
Jan 10 15:18:33 softmsc: bc-l1=3
Jan 10 15:18:33 softmsc: cld=11-46850534704
Jan 10 15:18:33 softmsc: clg=11-46735107953
Jan 10 15:18:33 softmsc: farendinfo=4:192.168.1.151:4512
Jan 10 15:18:33 softmsc:
Jan 10 15:18:33 softmsc: 151833.891 SCCP user N-UNITDATA req,  Prim: request,  ConnId: 0
Jan 10 15:18:33 softmsc:  CallingAddr ( 2) 42 fe
Jan 10 15:18:33 softmsc:  CalledAddr  ( 2) 42 fe
Jan 10 15:18:33 softmsc:  UserData    (22) 00 14 52 08 08 29 87 10
Jan 10 15:18:33 softmsc:                   40 00 21 63 85 09 04 00
Jan 10 15:18:33 softmsc:                   00 b9 b4 1a 01 06
Jan 10 15:18:33 softmsc:
Jan 10 15:18:35 softmsc: 151835.877 SCCP user N-CONNECT ind,  Prim: indication,  ConnId:
102
Jan 10 15:18:35 softmsc:  CalledAddr  ( 2) 42 fe
Jan 10 15:18:35 softmsc:  UserData    (28) 00 1a 57 05 08 00 09 f1
Jan 10 15:18:35 softmsc:                   91 eb 28 27 16 17 0d 06
Jan 10 15:18:35 softmsc:                   27 03 03 30 18 81 05 f4
Jan 10 15:18:35 softmsc:                   00 00 b9 b4
Jan 10 15:18:35 softmsc:
Jan 10 15:18:35 softmsc: 151835.880 SCCP user N-CONNECT resp,  Prim: request,  ConnId: 102
Jan 10 15:18:35 softmsc:
Jan 10 15:18:35 softmsc: 151835.892 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:35 softmsc:  UserData    (22) 01 00 13 05 12 04 0e 01
Jan 10 15:18:35 softmsc:              bc f0 77 11 5e 7a 90 87
Jan 10 15:18:35 softmsc:              e3 14 c0 b0 61 6d
Jan 10 15:18:35 softmsc:
Jan 10 15:18:35 softmsc: 151835.970 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:35 softmsc:  UserData    (14) 00 0c 54 12 03 30 18 81
Jan 10 15:18:35 softmsc:              13 04 60 14 10 00
Jan 10 15:18:35 softmsc:
Jan 10 15:18:36 softmsc: Port-0 Rx:: HBACK
Jan 10 15:18:36 softmsc:
Jan 10 15:18:36 softmsc: 151836.440 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:36 softmsc:  UserData    ( 9) 01 80 06 05 14 89 9c 7e
Jan 10 15:18:36 softmsc:              b1
Jan 10 15:18:36 softmsc:
Jan 10 15:18:36 softmsc: 151836.444 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:36 softmsc:  UserData    (16) 00 0e 53 0a 09 04 41 37
Jan 10 15:18:36 softmsc:              35 16 da e5 c0 00 23 01
Jan 10 15:18:36 softmsc:
Jan 10 15:18:36 softmsc:
Jan 10 15:18:36 softmsc: Port-0 Rx:: HB
Jan 10 15:18:36 softmsc: “
```

7.6.5 RTP/MGCP Trace: Voice Setup

The Real time protocol (RTP) is a “sub-layer” protocol on top of UDP is shown in figure 7.16. RTP supports the transfer of real-time data amongst the participants of a session. The session is defined by:

- RTP port number (destination port in UDP header of all receivers).
- RTCP (Real Time Control Protocol) port numbers.
- Participant IP addresses.
- RTP transport model (see figure 7.16) includes source, relay, and receiver. The relay will mark itself as the synchronization source.

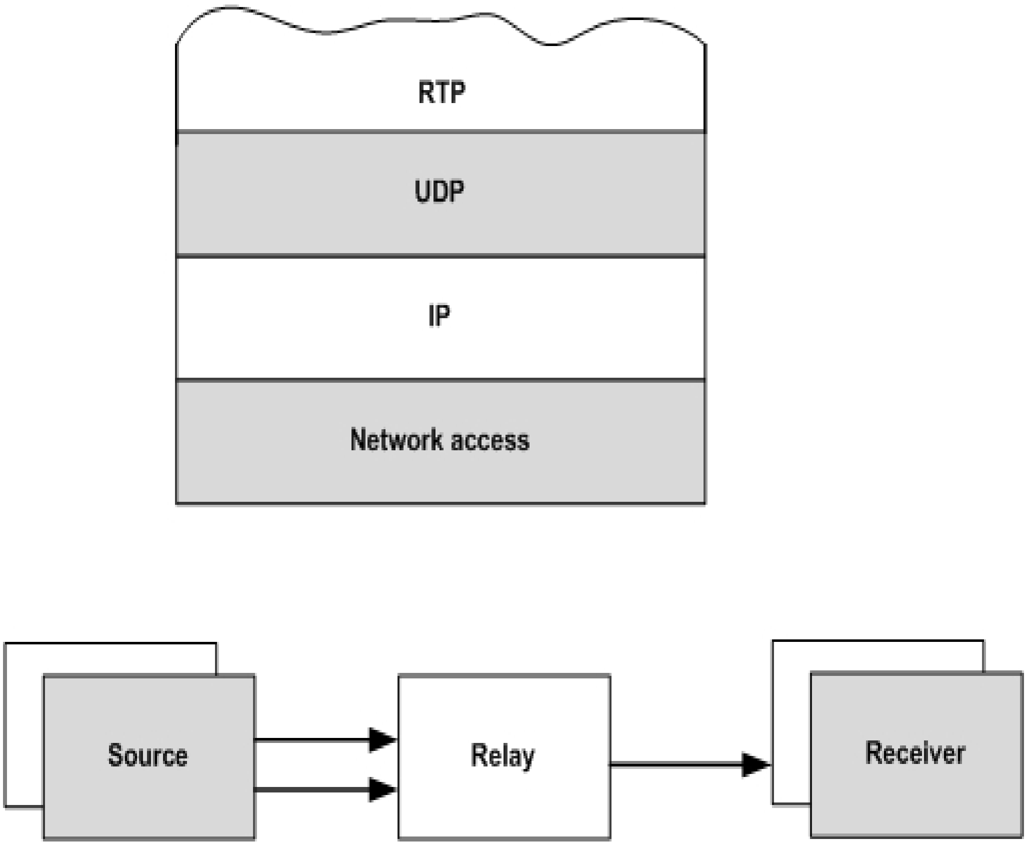


Figure 7.16: RTP transport model

In the trace output here, the SS7 and MGCP trace for voice channel call setup involves a BTS (IP address *192.168.2.200*), the Integrated MSC/VLR/BSC (IP address 192.168.2.146), and a Media Gateway (IP address 192.168.1.151). Media Gateway Control Protocol (MGCP) supports the ability for a call agent to influence the CODEC negotiation by providing a local connection option. This can be part of the ingress Create Connection (CRCX) or the egress CRCX MGCP messages.

The purpose of the trace is to give an example of the protocol in a working scenario template (Note that the address of the media gateway is blacked out to protect its identify - as it is a real commercial gateway.):

```
“Jan 10 15:18:36 softmsc: Port-0 Tx to 192.168.1.151:4512:: HBACK
Jan 10 15:18:36 softmsc:
Jan 10 15:18:37 softmsc: 151837.147 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:37 softmsc:  UserData     (18) 00 10 55 20 0d 06 32 17
Jan 10 15:18:37 softmsc:                    09 33 95 57 06 00 80 22
Jan 10 15:18:37 softmsc:                 18 f2
Jan 10 15:18:37 softmsc:
Jan 10 15:18:37 softmsc: 151837.154 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:37 softmsc:  UserData    (18) 01 00 0f 03 05 04 02 20
Jan 10 15:18:37 softmsc:                 82 5c 07 91 64 37 15 70
Jan 10 15:18:37 softmsc:                 59 f3
Jan 10 15:18:37 softmsc:
Jan 10 15:18:37 softmsc: 151837.853 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:37 softmsc:  UserData    (16) 01 80 0d 83 48 04 06 60
Jan 10 15:18:37 softmsc:                 04 02 00 05 81 15 01 01
Jan 10 15:18:37 softmsc:
Jan 10 15:18:37 softmsc:
Jan 10 15:18:37 softmsc: 151837.862 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:37 softmsc:  UserData    (11) 00 09 01 0b 03 01 08 11
Jan 10 15:18:37 softmsc:                 01 10 33
Jan 10 15:18:37 softmsc:
Jan 10 15:18:38 softmsc: 151838.468 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:38 softmsc:  UserData    (11) 00 09 02 15 00 21 98 2c
Jan 10 15:18:38 softmsc:                 03 40 11
Jan 10 15:18:38 softmsc:
Jan 10 15:18:38 softmsc: 151838.569 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:38 softmsc:  UserData    ( 5) 01 80 02 83 01
Jan 10 15:18:38 softmsc:
Jan 10 15:18:38 softmsc: Port-0 Tx to 192.168.1.151:4512:: alert 4
Jan 10 15:18:38 softmsc: inbandinfo=0
Jan 10 15:18:38 softmsc:
Jan 10 15:18:40 softmsc: 151840.969 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:40 softmsc:  UserData    ( 5) 01 80 02 83 47
Jan 10 15:18:40 softmsc:
Jan 10 15:18:40 softmsc: 151840.972 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:40 softmsc:  UserData    ( 5) 01 00 02 03 0f
Jan 10 15:18:40 softmsc:
Jan 10 15:18:40 softmsc: 151840.983 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:40 softmsc: CRCX 1504 1033@[redacted]gw MGCP 1.0
Jan 10 15:18:40 softmsc: M: sendrecv
Jan 10 15:18:40 softmsc: C: 2f
Jan 10 15:18:40 softmsc:
Jan 10 15:18:41 softmsc: 151841.220 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:41 softmsc: 200 1504
Jan 10 15:18:41 softmsc: I: 27
Jan 10 15:18:41 softmsc: v=0
Jan 10 15:18:41 softmsc: c=IN IP4 192.168.2.200
Jan 10 15:18:41 softmsc: m=audio 4018 RTP/AVP 3
Jan 10 15:18:41 softmsc:
Jan 10 15:18:41 softmsc: Port-0 Rx:: CRCX 1505 0004@192.168.1.151 MGCP 1.0
Jan 10 15:18:41 softmsc: M: sendrecv
Jan 10 15:18:41 softmsc: C: 2f
Jan 10 15:18:41 softmsc: v=0
Jan 10 15:18:41 softmsc: c=IN IP4 192.168.2.200
Jan 10 15:18:41 softmsc: m=audio 4018 RTP/AVP 98
Jan 10 15:18:41 softmsc: a=rtpmap:98 GSM-EFR/8000
Jan 10 15:18:41 softmsc:
Jan 10 15:18:41 softmsc: Port-0 Tx to 192.168.1.151:4512:: connect 4
Jan 10 15:18:41 softmsc: sdp=192.168.2.200:4018
Jan 10 15:18:41 softmsc: farendinfo=4:192.168.2.146:4511
Jan 10 15:18:41 softmsc:
Jan 10 15:18:41 softmsc: Port-0 Rx:: switch 4
Jan 10 15:18:41 softmsc: sdp=192.168.1.152:4520
Jan 10 15:18:41 softmsc:
Jan 10 15:18:41 softmsc: 151841.895 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:41 softmsc: MDCX 1506 1033@[redacted] MGCP 1.0
Jan 10 15:18:41 softmsc: M: sendrecv
Jan 10 15:18:41 softmsc: C: 2f
Jan 10 15:18:41 softmsc: I: 27
Jan 10 15:18:41 softmsc: v=0
Jan 10 15:18:41 softmsc: c=IN IP4 192.168.1.152
Jan 10 15:18:41 softmsc: m=audio 4520 RTP/AVP 98
Jan 10 15:18:41 softmsc: a=rtpmap:98 GSM-EFR/8000
Jan 10 15:18:41 softmsc:
Jan 10 15:18:41 softmsc: 151841.913 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:41 softmsc: 200 1506
Jan 10 15:18:41 softmsc: v=0
Jan 10 15:18:41 softmsc: c=IN IP4 192.168.2.200
Jan 10 15:18:41 softmsc: m=audio 4018 RTP/AVP 3
Jan 10 15:18:41 softmsc:
Jan 10 15:18:44 softmsc: 151844.131 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:44 softmsc:  UserData     ( 8) 01 80 05 83 25 02 e0 90
Jan 10 15:18:44 softmsc:
Jan 10 15:18:44 softmsc:
Jan 10 15:18:44 softmsc: 151844.136 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:44 softmsc:  UserData     ( 9) 01 00 06 03 2d 08 02 e0
Jan 10 15:18:44 softmsc:                    90
Jan 10 15:18:44 softmsc:
Jan 10 15:18:44 softmsc: Port-0 Tx to 192.168.1.151:4512:: rel 4
Jan 10 15:18:44 softmsc: cause=16
Jan 10 15:18:44 softmsc:
Jan 10 15:18:44 softmsc: 151844.269 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:44 softmsc:  UserData     ( 9) 01 80 06 83 6a 08 02 e0
Jan 10 15:18:44 softmsc:                    90
Jan 10 15:18:44 softmsc:
Jan 10 15:18:44 softmsc: 151844.273 SCCP user N-DATA req,  Prim: request,  ConnId: 102
Jan 10 15:18:44 softmsc:  UserData     ( 6) 00 04 20 04 01 00
Jan 10 15:18:44 softmsc:
Jan 10 15:18:45 softmsc: 151845.469 SCCP user N-DATA ind,  Prim: indication,  ConnId: 102
Jan 10 15:18:45 softmsc:  UserData     ( 3) 00 01 21
Jan 10 15:18:45 softmsc:
Jan 10 15:18:45 softmsc: 151845.471 SCCP user N-DISCONNECT req,  Prim: request,  ConnId: 102
Jan 10 15:18:45 softmsc:  DiscReason  ( 1) 00
Jan 10 15:18:45 softmsc:
Jan 10 15:18:46 softmsc: Port-0 Rx:: HBACK
Jan 10 15:18:46 softmsc:
Jan 10 15:18:46 softmsc: Port-0 Rx:: HB
Jan 10 15:18:46 softmsc:
Jan 10 15:18:46 softmsc: Port-0 Tx to 192.168.1.151:4512:: HBACK "
```

7.7 Network Limitations and Optimization

Every design has limitations, hence optimizations are required. There are many technical challenges involved with implementing a quality mobile telephony phone system over satellite links in an IP infrastructure. Often good network optimization techniques become the deciding factor in an operator's ultimate success. The key issues with respect to network optimization involve minimizing the effects of satellite delay, maximizing the utilization of satellite resources, and optimizing the differing and often conflicting requirements of multiple services and protocols which need to be integrated in concatenated networks.

The best design for a particular network is determined by past experience, research, simulation, testing, and monitoring; and contributed to this thesis. Potential limitations associated with this architecture are based on the introduction of a fixed roundtrip satellite transmission delay of 650 milliseconds in the IP cloud, and the difference in error characteristics associated with satellite based transmission when compared to terrestrial based transmission systems normally assumed for the development of the protocols which were used. Care must be taken to insure that each protocol can accommodate these differences. In order to reduce the effects introduced by the satellite delay, the network design must attempt to minimize the points where multiple exchanges in protocol handshaking would cause network bottlenecks, such as implementing techniques to reduce the number of signaling or control messages required in protocol exchanges.

Quality of service techniques are also required to be implemented (though not covered within the scope of this thesis) to reliably handle the network traffic with an appropriate order of precedence (e.g., network signaling traffic is more important than an internet access request). Finally, optimum utilization of satellite resources requires a careful grooming of the protocols to assure optimum packet structure. This is needed because in services like GSM over IP, the payload of the IP packet (voice) is almost of the same size or even smaller than the header. Over the end-to-end connection, comprised of multiple hops, these protocol headers are extremely important but over just one link (hop-to-hop, ex. VSAT link) these headers serve no useful purpose. It is possible to compress those headers, and thus save the bandwidth and use the expensive resources efficiently. IP header compression also provides other important benefits, such as reduction in packet loss and improved interactive response time

The traditional GSM architecture, with a satellite link for backhauling of GSM traffic; uses satellite channels for the traffic, call setup, and Abis signaling. The softswitch architecture, as proposed in this thesis, uses satellite channels only for the call setup and as needed to carry call traffic.

The table 7.6 below summarizes the number of satellite voice channels required per type of call, as well as the delay introduced into the voice path for these calls. In addition the traditional architecture will introduce a 650ms delay in the Abis signaling impairing mobility performance (depending upon where the mobility management is performed).

Table 7.7: Latency in Satellite link

	Softswitch Architecture	**Traditional MSC**
Local Calls		
Satellite channels per call	0	4
Satellite delay (round trip)	0 ms	1300 ms
Long Distance Calls		
Satellite channels per call	2	2
Satellite delay (round trip)	650 ms	650 ms

The table 7.7 shows that the traditional architecture requires four (4) satellite voice channels, or two (2) full duplex satellite voice circuits, to complete a single local call (i.e., a call between two subscribers in the same local region), while the softswitch architecture requires none. This has a significant impact on the amount of satellite bandwidth required for the network. This is a very important factor because satellite bandwidth is a recurring charge for operation of the network. Furthermore, all local calls suffer substantial delay due to the double satellite hop resulting in degraded voice quality. The effect of this will depend upon the faction of calls which are local MS to local MS calls. We will elucidate this further in the example to follow.

The traditional MSC architecture has inherent impediments to the growth of the remote radio access network as shown in the following example:

In the traditional architecture we will require a duplex satellite channel (E1 over IP over VSAT) for each end of the call. For a local call terminating in another network, this could mean two (2) duplex satellite channels for each mobile channel. For a network with 500 mobile radio channels and 10% long distance calling, we would require 450 satellite channels if all local calls are mobile to mobile on the network and 900 satellite channels to support the local calling terminating on another local network. In comparison, only fifty (50) satellite channels are required to support the actual long distance calling [48, 38].

The proposed softswitch architecture requires only the 50 channels for long distance calls. In terms of satellite bandwidth, each channel requires a minimum of two (2) sub-channels each of 13.4 kbps of bandwidth on the satellite or 26.8 kbps per channel. One can see from the figures above that the traditional architecture requires 10 to 20 times more softswitch architecture.

8. Conclusion

There is no widely accepted blueprint or off-the-shelf solution for designing an efficient cellular network for remote service areas. A prudent, forward looking Radio Access Network design must take into account current voice requirements and limited data traffic while minimizing network operating expenses or capital equipment outlays. The best design for a particular network is determined by past experience, research, simulation, testing and monitoring; and all of which were involved this thesis project.

The architecture proposed in this thesis provides a complete IP enabled GSM network solution for remote service areas that can scale seamlessly, in order to meet network capacity growth requirements without adding growth-related complexity back to the network. This thesis embraces the vision of the All-IP converged network, where mobile telephony is implemented as an IP application in the same way as any other application.

The IP-GRAN proposed here takes advantage of two of the most used communications technology to date: the Internet and the GSM standards. In case of remote service areas, having satellite communication as the preferable and at times the only available access network, lowering the costs of the network connections between cellular sites and the core network has an impact on the uptake of the technology. Chapter 6 of this thesis also presented some of the issues involved in dimensioning the links for RAN traffic over IP.

In the proposed architecture, which is based on the concept of softswitching; voice traffic is carried over RTP streams; whereas, signaling is carried over TCP or SCTP links. A packet simulator was used to simulate the most important characteristics of the system such as packet size, inter-arrival delay, and the control channel (RTCP); and effects of congestion on the RTP streams were studied. The effect of DTX on bandwidth requirements was also studied

It was observed that link congestion has the greatest effects on packet loss. However, by employing DTX on the RTP streams, the system will require lower bandwidth (perhaps only 2/3 of the bandwidth required when not employing DTX) and the system is more resilient to short congestion periods. This observation is critical for transporting GSM traffic over VSAT link from a remote service area from the perspective of limited bandwidth availability and a desire for efficient utilization of the satellite link which is rented. Also, an overview of the factors influencing the dimensioning of traffic due to signaling was presented. Chapter 5 proposes two Global Title Translation based routing schemes, NV (Network Virtualization) and OMA (Optimized MSRN Assignments); specifically emphasizing providing low cost call setup alternatives during international roaming.

Chapter 4 of this report introduces a key network element for a wireless (cellular) packet network, called Integrated Mobile Access System (IMAS); which is conceptually based on an IP router. It provides MSC functionality for voice users and offers network simplification to support all applications including voice, data and management on a common packet core infrastructure. A basic implementation of IMAS is discussed which supports voice service from standard GSM terminals, using an IP network for the wired portion of the mobile access network. Although the system presented here is a prototype for a network using a pure IP access network, its key concepts, modularized call processing, and mobility management at the network layer in a localized manner; can be applied to other types of networks; such as end-to-end IP networking for wireless data applications, but needs further study.

Finally a test setup of an IP-GRAN was configured for a Maritime GSM implementation as a remote service area network. The setup was brought into operational state and traces were recorded using a protocol tracer in real-time. These traces were then used to explain various processes involved in running a IP-GRAN, in keeping with the proposals and observations made in the previous chapters of this thesis. Also, another purpose was to present a working example as a proof of concept for the proposals made in this Master's thesis project.

As a concluding remark, we clearly foresee that in the near future cellular networks will increasingly be based on packet switching technology. The trend has already begun. To successfully support data applications on a large scale, and to allow the rate of growth seen on the wired Internet, these networks will required to be inherently packet based as opposed to simple packet overlay networks. The key to success will lie in choosing a suite of network components with the flexibility and performance characteristics that enable the mobile network operator to pursue all available options and implement those which best address present and future technological and commercial concerns. Our thesis work has tried to address some of the issues in that regard and hopefully has contributed by making some proposals for how to realize this vision.

9. Future Work

The cost of the links connecting the backbone network and a remote GSM network has a major effect on the uptake of IP based Radio Network Access technology.

Through simulation, it is shown that discontinuous transmission for the voice traffic offers a reduction in the bandwidth requirements and makes the system more resilient to, short periods of congestion. Therefore, we propose as future work an exploration in depth of the effect of signaling over a congested link.

Also, a remote RAN's performance and scalability is limited when pursued as a traditional GSM network architecture. The distributed softswitch architecture described in this thesis proposes a significant improvement in network design and architecture. However, a lack of resources hindered us from digging deeply into issues such as satellite bandwidth cost, delay characteristics in the voice channel, mobility (i.e., handover) performance, and call termination to wireline networks. A statistical study of the aforesaid factors is thus proposed as future work; to analyze the implications, individually and with respect to others, with regard to optimizing the proposed IP-GRAN both in technical as well as commercial terms.

Furthermore, the emergence of SIP based network infrastructure provides a new medium for telecommunication carriers for providing voice, data, and other services. Although the legacy telephony network is based on circuit switched technology, SIP exploits the widely available packet switched network architecture, thus the transition to SIP requires a complete revamping of the existing networks (such as has been begun by BT in the UK). Future work on convergence of SS7 and SIGTRAN with SIP in the IMAS architecture to achieve peering of a GSM network with the global VoIP network should certainly generate some significant interest and effects.

References

[1] All-IP Next Generation Networking Solutions at NSS19, Accessed May, 2007. http://www.nortel.com/solutions/wireless/collateral/nn115740.pdf.

[2] ANSI T1.113-2000, Signaling System Number 7, ISDN User Part.

[3] Agilent Technologies, Optimizing Your GSM Network Today and Tomorrow, Application Note 1344, Access Jan, 2007.
http://cp.literature.agilent.com/litweb/pdf/5980-0218E.pdf

[4] Bruce Ernhofer, Making the Packet Connection with TDMover-IP: A Technology Primer, Zarlink Semiconductor, Accessed Feb, 2007.
http://www.analogzone.com/nett0809.pdf.

[5] CDPD Forum, Cellular Digital Packet Data System Specification, Release 1.1, 1995.

[6] CCITT Recommendation Q.1051-Q.1063, "Public Land Mobile Network Mobile Application Part and Interfaces," 1988.

[7] C. E. Perkins, "IP Mobility Support," IETF RFC 2002, October 1996.

[8] Corvil White Paper, An Overview of the Capabilities and Applications of CorvilNet, Year March, 2004
http://www.cisco.com/warp/public/732/partnerpgm/docs/corvil_wp_corvilnet.pdf

[9] Digital Cellular Telecommunication System, General Packet Radio Service (GSM 02.60, Version 6.1), ETSI, 1997.

[10] Digital Cellular Telecommunication System, Enhanced Data Rates for GSM Evolution Project Plan and Open Issues for EDGE (GSM 10.59, version 1.6), ETSI, 1997.

[11] Digital Cellular Telecommunication System, Network Architecture (GSM 3.02, version 6.1), ETSI, 1997

[12] ETSI ETS 300 343 ed.1 (1994-07) Integrated Service Digital Network (ISDN); Signaling System Number 7; ISDN User Part (ISUP) version 1; test specifications.

[13] ETSI ETR 256 ed.1 (1996-03) Integrated Service Digital Network (ISDN); Signaling System Number 7 (SS7); Telephone User Part "Plus" (TUP+) [CEPT recommendation T/S E(1988)].

[14] ETSI ETS 300 599 ed.9 (2000-12) Digital cellular telecommunication system (phase2) Mobile Application Part (MAP) specifications (GSM 09.02 version 4.19.1).

[15] Ericsson Efficient Softswitching white paper August, 2006.
http://www.ericsson.com/technology/whitepapers/8107_efficient_softswitching_a.pdf

[16] GSM over IP Picocells for in building coverage and capacity, IP Access, Accessed Feb, 2007.
http://www.ipaccess.com/products/datasheets/BSC_24-01-07.pdf.

[17] GSM-UMTS next generation voice core literature/brochures, Accessed May, 2007. http://www2.nortel.com/go/solution_assoc_detail.jsp?segId=0&parId=0&doc_id=0&catId=0&rend_id=99pt&contOid=100203895&prod_id=58921&locale=en-US

[18] Gunnar Heine, *GSM Networks: Protocols, Terminology and Implementation*, Artech House, January 1999; ISBN 0890064717.

[19] GSM 02.69 Voice Broadcast Service (VBS), Stage 1.

[20] Global Title, Accessed Jan, 2007.
http://www.ss7.com/GlobalTitle.pdf .

[21] GSM definition and overview by International Engineering Consortium, Accessed Aug, 2006.
http://www.iec.org/online/tutorials/gsm.

[22] Integration of SIP and SS7 for VoIP: Opportunities and Challenges, TMCnet,

Accessed July, 2007.
http://www.tmcnet.com/sip/0307/feature_articles_integration_of_sip_ss7_forvoip.htm

[23] ITU-T Specifications of Signaling System No. 7 – Signaling connection control part (SCCP), Functional description of the signaling connection control part, Q-711 March,2003
http://www.item.ntnu.no/fag/ttm4130/stottelitteratur/T-REC-Q.711.pdf

[24] ITU Recommendations Q.716, Signaling connection control part (SCCP) performances.
http://www.nmedia.net/docs/ccitt/1992/q/q716.txt

[25] Introduction to GSM by Performance Technologies, Accessed January, 2007. http://www.pt.com/products/gsmintro.html.

[26] Information Science Institute, University of Southern California. IETF RFC791 Internal Protocol Darpa internet program protocol specification, September, 1981.

[27] Interworking Switched Circuit and Voice-over–IP Networks, Accessed Jan 2007 http://www.iec.org/online/tutorials/ip_in/topic01.html.

[28] ITU Recommendations Q.700-Q.795, "Specifications of Signaling System No. 7," 1989.

[29] Jörg Eberspächer, GSM *Switching, Services & Protocols*, 2nd edition 2001, John Wiley and Sons LTD, Toronto.

[30] J. Postel, ISI, IETF RFC768 User Datagram Protocol, August, 1980.

[31] Jyhi-Kong Wey, Wei-Pang Yang, and Lir-Fang Sun, "Traffic impacts of International roaming on mobile and personal communications with distributed data Management" Mobile Networks and Applications, Volume 2, Issue 4, January 1997, pages 345-356.

[32] Klaus Turnia, Josephus Kuster, and Dimitrios Papadimitrious, Signaling in a mobile cellular communication network with pooled MSCs, US Patent Issued on August 3, 2004
http://www.patentstorm.us/patents/6771983.html

[33] K. Sriram, Methodologies for Bandwidth Allocation, Transmission Scheduling, and Congestion Avoidance in Broadband ATM Networks, Room 3H-607, AT&T Bell Laboratories, Holmdel, N.J. 07733 Year 1992
http://www.antd.nist.gov/~ksriram/weighted-FQ-Globecom-1992-00276647.pdf

[34] L. Zhang, S. Deering, D. Estrin, S. Shenker, and D. Zappala, "RSVP: A New Resource ReSerVation Protocol," IEEE Network, Volume 7, Number 5, September 1993, pp. 8-18.

[35] Laila Daniel, Reliability and Availability in Stream Control Transport Protocol (SCTP), Research Seminar on Real Time and High Availability, November, 2001.
http://www.cs.helsinki.fi/u/kraatika/Courses/sem01a/daniel-slides.pdf

[36] M. Riegel, Siemens AG, IETF RFC4197 Requirements for Edge-to-Edge Emulation of Time Division Multiplexed Circuits over Packet Switching Networks, October, 2005.

[37] Mia Immonen, SIGTRAN: Signaling over IP — a step closer to an all-IP network, Master's thesis Royal Institute of Technology (KTH), Stockholm, Sweden, IMIT/LCN, 15 June, 2005.
ftp://ftp.it.kth.se/Reports/DEGREE-PROJECT-REPORTS/050619-Mia-Immonen-with-cover.pdf.

[38] M.Fiacco and A.Lvanov, Traffic dimensioning for GSM-over-IP services, IP Access Ltd. CPCL, Capital park, Fulbourn, Cambridge CB1 5XE, UK, March, 2004.

[39] N. Greene, M. Ramalho, and B. Rosen, Media Gateway Control Protocol Architecture and Requirements, Request for Comments (RFC): 2805 , Year April, 2000
http://www.ietf.org/rfc/rfc2805.txt

[40] Public Network Signaling Tutorial, Comp TEK, Accessed August 2007.
http://www.comptek.ru/ss7/tutorial.html

[41] R. Ramjee, K. Murakami, R. W. Buskens, Y-J. Lin, and T. F. La Porta, Design Implementation and Evaluation of a Highly Available Distributed Call Processing System, Accessed December, 2007.

http://www.springerlink.com/index/n7363k4345254115.pdf.

[42] RADVISION White Paper, Implementing Media Gateway Control Protocols, Year 27, 2002 http://www.radvision.com/NR/rdonlyres/1C34D0AA-C455-428B-A839-306926516053/0/ RADVISION Media -GatewayControlProtocol.pdf

[43] R. Ramjee, T.F. La Porta, S. Thuel, K. Varadhan, and S-Y. Wang, HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks. Accessed May, 2007. http://www.ieee-icnp.org/1999/papers/1999-30.pdf

[44] Robert Boorstyn and Almut Burchard, J org Liebeherr y Chaiwat, and Oottamakorn, Statistical Multiplexing Gain of Link Scheduling Algorithms in QoS Networks , Technical Report: University of Virginia, CS-99-21 July 1999. http://www.cs.virginia.edu/~techrep/CS-99-23.pdf

[45] Richard Adams, and John Loughney, Sigtran, SUA 14 editorial suggestions, Accessed August, 2007. http://www1.ietf.org/mail-archive/web/sigtran/current/msg01587.html

[46] Robby de Candido, Selektiv tilldelning av Mobile Station Roaming Number, Application submitted to Swedish patent office.

[47] REF- International Forum on ANSI-41 Standards Technology Published for IFAST by Alliance for Telecommunications Industry Solutions March, 2003. http://www.ifast.org/files/Journal/ifastjournal-march2003.pdf.

[48] Research & Development Group, IP Access Ltd. UK, Accessed August, 2007. http://www.ipaccess.com

[49] S. Bryant and P. Pate IETF RFC3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture, March, 2005.

[50] S. Assawaboonmee, C. Chayawan, and S. Pungvora-asn, "Roamer direct dialing (RDD)", IEEE Region 10 Conference TENCON 2004, Volume C, 21-24 Nov. 2004, pages: 41 – 43, Digital Object Identifier 10.1109/TENCON.2004.1414701, http://www.ieeexplore.ieee.org/iel5/9709/30648/01414701.pdf.

[51] *SS7, Protocol, Architecture & Services*, Cisco Press, August 02, 2004,ISBN-10: 1-58705-040-4.

[52] Signaling System 7 (SS7), International Engineering Consortium, Online Education, Web ProForums, Accessed Aug, 2007. http://www.iec.org/online/tutorials/ss7/.

[53] SS7 Tutorial, Performance Technologies tutorials, Accessed Aug, 2007. http://www.pt.com/tutorials/ss7.

[54] SS7/IP Interworking Tutorial, Performance Technologies tutorials, Accessed Aug, 2006. http://www.pt.com/tutorials/iptelephony/.

[55] SS7 over IP Signaling Transport & SCTP, International Engineering Consortium , Online Education, Web ProForums, Accessed Aug, 2006 http://www.iec.org/online/tutorials/ss7_over.

[56] Stephen Yablonski and Steven Spreizer, Enabling Modern Telecommunications Services via Internet Protocol and Satellite Technology, Presented to PTC'04, Honolulu, Hawaii, USA Accessed May, 2007 http://www.globecommsystems.com/pdf/CS-PTC04-Hosted-Switch.pdf

[57] Stream Control Transmission Protocol (SCTP), International Engineering Consortium , Online Education, Web ProForums, Accessed Aug, 2006 http://www.iec.org/online/tutorials/sctp/.

[58] Time Division Multiple Accesses (TDMA), International Engineering Consortium, Online Education, Web ProForums, Accessed Aug 2006. http://www.iec.org/online/tutorials/tdma/.

[59] TelecomSpace, Telecom Tutorials and Forum, Mobile Application Part (MAP),

Accessed Feb, 2007
http://www.telecomspace.com/ss7-map.html.

[60] Thomas F. La Porta, Kazutaka Murakami and Ramachandran Ramjee RIMA: Router for Integrated Mobile Access, Bell Labs, Lucent Technologies, The 11th IEEE International Symposium on Volume 1, PIMRC 2000 Issue , 2000 Page(s):315 - 321 vol.1.
http://www.ieeexplore.ieee.org/iel5/7069/19062/00881440.pdf.

[61] T.Scheerbarth, I.Kliche and H.Klaus, "Relationship between MOS and R values for Results for VoIP Simulation" ETSI TIPHON 14, Tempory document 64, Year July, 1999.

[62] Understanding the clear channel codec configuration in the Cisco PGW 2200, document ID: 27820, Accessed August, 2007.
http://www.cisco.com/warp/public/788/products/pgw-clear-channel.pdf

[63] W.D.Ambrosch, A.Maher, and B.Sassceer. "*The Intelligent Network Berlin*", Springer-Verlag New York, Inc, Year of Publication: 1989 ISBN:3-540-50897-X.

[64] Y(J) Stein, R.Shashoua, R.Insler, M.Anavi , IETF Draft, Pseudo Wire Emulation Edge-to-Edge (PWE3), Last Version: Tdmoip-06.txt Tracker Entry Date: 05-Dec-2006.

[65] Zynetix Maritime GSM Solutions, Accessed Feb, 2007.
http://www.zynetix.com/downloads/zynetix_maritime_gsm.pdf.

COS/CCS 2007-24

www.kth.se