IMS Interworking

BORIS IV. KALAGLARSKI
AND
EMILIO DI GERONIMO

KTH Information and
Communication Technology

Master of Science Thesis
Stockholm, Sweden 2007

COS/CCS 2007-15

IMS Interworking

Boris Iv. Kalaglarski & **Emilio Di Geronimo**

bika@kth.se emiliodg@kth.se

Supervisor & Examiner:

Professor Gerald Q. Maguire Jr.
KTH / Royal Institute of Technology

Industry Advisor:

Sven Sjölinder, PhD
Ericsson AB, IP Infrastructure

Stockholm
2007

Abstract

The goal of this project was to analyze the IP Multimedia Subsystem (IMS) with respect to the interworking functionality between two or more IMS domains belonging to different operators. The thesis presents an overview of IMS, its purpose, the circumstances and the environment in which it has evolved, and a look into some of the challenges that lie ahead. Through careful examination of the history of the mobile communications and of IMS itself, the thesis attempts to give the reader a full and comprehendible understanding of what IMS is, what its purpose is, and why it came into existence.

The thesis considers the different models of IMS interworking, as they are currently envisioned by the standardisation bodies and the telecom industry. This analysis aims to identify some of the problematic aspects of the IMS Interworking and to suggest concrete areas for further investigation, which will contribute to the future successful IMS development and deployment.

The report looks into such aspects of IMS interworking as the DNS, different models for ENUM DNS resolution; security issues and technical challenges of security with respect to the network as a whole and some of the IMS network elements in particular, such as the DNS. This thesis also presents the findings of the authors, regarding the challenges of interworking between networks built to support different versions of the IP protocol.

The thesis focuses on the areas of interest, mentioned above, as these have been identified as being of particular significance in connection with the further development of the IMS architecture.

Sammanfattning

Målet med denna uppsats var att analysera IP Multimedia Subsystem (IMS) med fokus på samverkan mellan två eller flera IMS domäner som tillhör olika operatörer. Examensjobbet beskriver en övergripande bild av IMS, dess målsättning, förhållanderna och miljön som den har utvecklats i och några utav utmaningarna som ligger framöver. Uppsatsen försöker med hjälp av bakgrundsfakta om mobiltelefonins historia ge läsarna förståelse om vad IMS är, syftet med det och varför det existerar.

Uppsatsen beskriver olika samverkningsmodeller av IMS som grundar sig i modeller från de olika standardiseringsorganen samt från telecomindustrin. Målet med denna analys är att identifiera några problemaspekter samt presentera konkreta områden att fortsätta arbeta på gällande IMS och dess gällande samverkan mellan olika operatörer. Detta kan bidra till fortsatt framgång med utvecklingen samt utspridningen av IMS.

Uppsatsen tar upp samverkningsproblem med IMS så som DNS, olika uppslagsmetoder av ENUM DNS, säkerhetsfrågor och säkerhetstekniska utmaningar med fokus på nätverket samt några IMS nätverkselement som DNS:en. Uppsatsen lägger också fram författarnas slutsatser gällande samverkan av de olika nätverken med olika versioner av IP protokollet.

Examensjobbet fokuserar på de olika områderna som är ovan nämnda, då de har blivit identiferade med speciell betydelse för att kunna fortsätta att framgångsrikt utveckla IMS arkitekturen.

Acknowledgements

The authors would like to express their gratitude to all colleagues within the vast organisation of Ericsson AB and all experts from the GSM Association, Telia Sonera, and Nokia whose help has been invaluable! Without their advice, comments, suggestions and kind help, the work on this project would have been much more difficult!

Special thanks go to our industrial advisor for this project, Sven Sjölinder, for his endless and tireless efforts to help and aid the authors of this project.

Our thanks, respect and gratitude go to Mr. Bengt Henriques, for believing in us and giving us the chance of a lifetime!

Our gratitude goes to Professor Gerald Q. Maguire Jr. from KTH, who was the academic advisor, supervisor, and examiner for this Master Thesis. Thank you for your endless patience, for your guidance, and advice along the way!

Dedications

I would like to thank everyone that has supported me during the thesis project. Especially I would like to express my thanks to my family, especially my parents Britt-Inger and Michele, who always have been there for me at any time, my little brother André and my big brother Micke. This project could not be done without your support. And of course I want also to thank all of my friends that have been supporting me on the way.

Emilio

I would like to express my eternal gratitude and love for my mother, father, and brother! This has been one of the hardest tasks and probably the biggest challenge so far in my life. Thank you for your awesome support, and for believing in me, every step of the way! Also, I could have never achieved this, without the help and support of my friends who have been the most amazing bunch of people, I have ever encountered!

Thanks, to all of you!

Boris

Executive summary

For the last two decades, the mobile telecommunication industry has been in a constant evolution and improvement. With the introduction of the analogue systems for mobile communication a new page in the history of the communication was turned. The rapid development of many different systems in numerous geographical regions showed that this was a technology trend with great potential. Nevertheless, it also showed that without standardisation and a common system it was impossible to connect the different systems or it was economically unwise to do so. The design of the pan-European network for mobile communications based on digital technology – GSM, proved to be extremely successful. It is also one of the representatives of the so called mobile communication systems of second generation (2G).

Less than a decade ago, the 3rd Generation Partnership Project (3GPP) organisation was established in order to further the development of the GSM platform into the so called third generation (3G) mobile communication system. The major difference between 2G and 3G systems is the introduction of packed switched data communication as opposed to being purely circuit switched communication, as well as the much higher rate of transfer for both voice and non-voice data. There have been numerous steps and new technologies introduced, which have incrementally transformed the older 2G systems into early 3G systems. This process is ongoing even today, with the latest developments dubbed “Evolved 3G”.

The aim of the 3G mobile systems is to bring together two of the most successful human inventions – telephony and the Internet. A key element in this endeavour is the IP Multimedia Subsystem (IMS). Its task is to merge the wireless and the wired worlds. IMS is a platform or architecture which controls access to such services as web, e-mail, video conferencing, and other data exchange for the mobile users of third generation mobile systems. From the user's point of view this access should be seamless and effortless to use. Furthermore, IMS gives service providers the freedom and flexibility to develop and deploy new services easily with minimal changes, if any, to the network architecture.

In spite of being a new platform, IMS must deal with the inherited limitations from both worlds it is trying to merge, i.e., the circuit switched and the packet switched domains. As part of the process of becoming a standard and hopefully a true success, it has to solve issues regarding backward compatibility, addressing, name and number resolution, security, quality of service, different IP protocol versions, roaming, interworking, etc. Many of these aspects, are taken for granted in the Internet world, however, they are significantly different in the mobile communication world. Thus it is very important for IMS to be able to provide the internetworking which the Internet has shown is such a successful model.

There are two main models for IMS Interworking: the Peer-to-Peer model and the Hub model. Each has its advantages and disadvantages, but it is perhaps more important to understand that they are seen as complementary to each other and are also likely to be consecutive in time. Both of the models make different technological demands upon the surrounding environment. Nevertheless, they both have to deal in one way or another with the above mentioned limitations inherited from the underlying technologies in the wireless and the Internet worlds.

Regardless of the model that is chosen, solving these problems will be necessary for the success of IMS and the third generation mobile systems.

Table of Contents

Table of Figures

Abbreviations and acronyms

3GPP	Third generation partnership
AAA	Authentication, Authorization and Accounting
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
API	Application Programmatic Interface
AS	Application Server
B2BUA	Back-to-Back User Agent
BG	Boarder Gateway
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
CEPT	Conference of European Posts and Telegraphs
COPS	Common Open Policy Service
CSCF	Call Session Control Function
DiffServ	Differentiated services
DNS	Domain Name System
DoS	Denial-of-service
ENUM	Telephone Number Mapping
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
EU	European Union
FW	Firewall
GGSN	GPRS Gateway Support Node
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GRX	GPRS Roaming Exchange
GSM	Global System for Mobile Communications
GW	Gateway
HFC	Hybrid Fiber Coaxial
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IBCF	Interconnect Border Control Function
I-BGF	Interconnect Border Gateway Function
I-CSCF	Interrogating-CSCF
IETF	Internet Engineering Task
IMS	IP Multimedia Subsystem
IM-SSF	IP Multimedia Service Switching Function
IP	Internet Protocol
IPsec	IP security
IPX	IP exchange
ISBC	Interconnect Session Border Controller
ISIM	IP Multimedia Services Identity Module
ISUP	ISDN User Part
ITU	International Telecommunication Union
IWF	Inter-Working Function
MGCF	Media Gateway Control Function
MGW	Media Gateway
MMS	Multimedia Messaging Service
MRF	Media Resource Function
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MTP	Message Transfer Part
NAI	Network Access Identifier
NAT	network address translation
OSA	Open Service Access
P-CSCF	Proxy-CSCF
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PLMN	Public land mobile network
PLMN	Public land mobile network
PSTN	Public switched telephone network
PUI	Public User Identifier
QoS	Quality of Service
RADIUS	Remote authentication dial-in user service
RTCP	RTP Control Protocol
RTP	Real-time Transport protocol
SBG	Session Border Gateway
SCS	Service Capability Server
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SGC	Session Gateway Controller
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLF	Subscription Locator Function
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPDF	Service Policy Decision Function
TCP	Transmission Control Protocol
THIG	Topology Hiding Inter-network Gateway
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TrGW	Transition Gateway
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Universal Resource Locator
WLAN	Wireless local area network

1. Introduction in mobile communications

During the early 1980s, analog cellular telephone systems developed at a great rate. This was particularly true in Scandinavia and the United Kingdom. Soon many countries followed suit, which resulted in many *different* systems being developed and used. This situation was not desirable since it limited the market size for equipment, thus preventing the economies of scale from reducing the price for handsets and infrastructure equipment. Furthermore, each of these systems worked only in a certain geographical area and they were not compatible with each other, which was not desirable in an ever more united Europe. [1]

1.1. Global system for mobile communications (GSM)

In 1982, the GSM group was formed to address these obstacles. It was created by the *Conference of European Posts and Telegraphs* (CEPT) and the initials stood for "Groupe Spécial Mobile". Its goal was to develop a pan-European public land mobile system. Later on, a decision was taken to change the name, but to keep the initials.

During the mid-1980s, lots of discussions were held in order to decide what type of system should be built, specifically should it be analog or digital. There were multiple field trials which resulted in the adoption of digital communication for GSM. Soon many countries developed their own solutions, which led to disagreement of which one should be used. After intervention from the EU, all member states decided to implement the standard recommended by CEPT. In early 1987, a competition was organized in Paris where eight different systems competed. A system developed by scientists from the Norwegian University of Science and Technology won the competition.

In 1989 the responsibility for GSM development was transferred to the *European Telecommunication Standards Institute* (ETSI) and by 1990, the first GSM specification was ready. It amounted to more than 6000 pages. Commercial service was started in mid-1991 in Finland, by the company *Radiolinja*.

In 1998, the *3rd Generation Partnership Project* (3GPP) was established. Its original goal was to produce specifications for the next generation of mobile networks. Later, 3GPP took over the responsibility to develop and maintain the GSM specification as well, since ETSI became a partner in the 3GPP. Thus 3GPP adopted a model of evolving GSM, rather than defining a completely new system. [2]

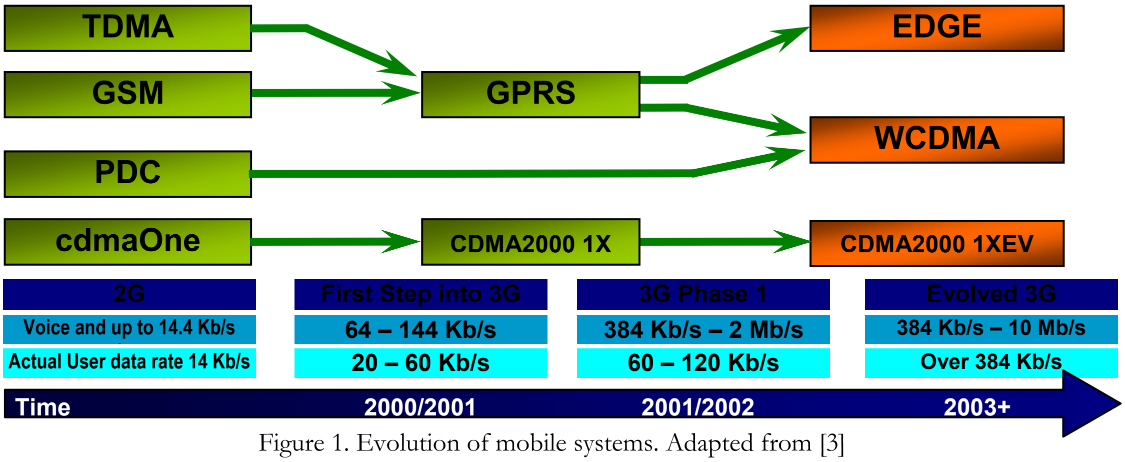


Figure 1. Evolution of mobile systems. Adapted from [3]

1.2. General packet radio service (GPRS) roaming exchange network

One definition of the roaming is:

> *"Roaming is defined as the ability for a cellular customer to automatically make & receive voice calls, send & receive data, or access other services when traveling outside the geographical coverage area of the home network, by means of using a visited network."* [4]

In order to provide roaming service, mobile operators had to decide how to connect data flows between the different networks. There are three main approaches to resolving this problem:

1. Direct connections between the participating mobile operators (Intranet)
2. Connection through the Internet
3. Indirect connection by connecting to GPRS Roaming Exchange (GRX), which is a private network, designed especially for the needs of inter-connecting GPRS operators.

The first solution – direct connection – provides the best connectivity, security, and reliability. Nevertheless, it is usually the most expensive and has significant scaling problems as it requires pair wise connections between the participating operators. The second solution, where the mobile operators interconnect their respective networks through the Internet is often inexpensive, but it has security challenges and no guaranteed QoS. As a result mobile operators generally have chosen the third option – to interconnect through a third party network – the GRX. This solution offers the best balance between quality and security. [5]

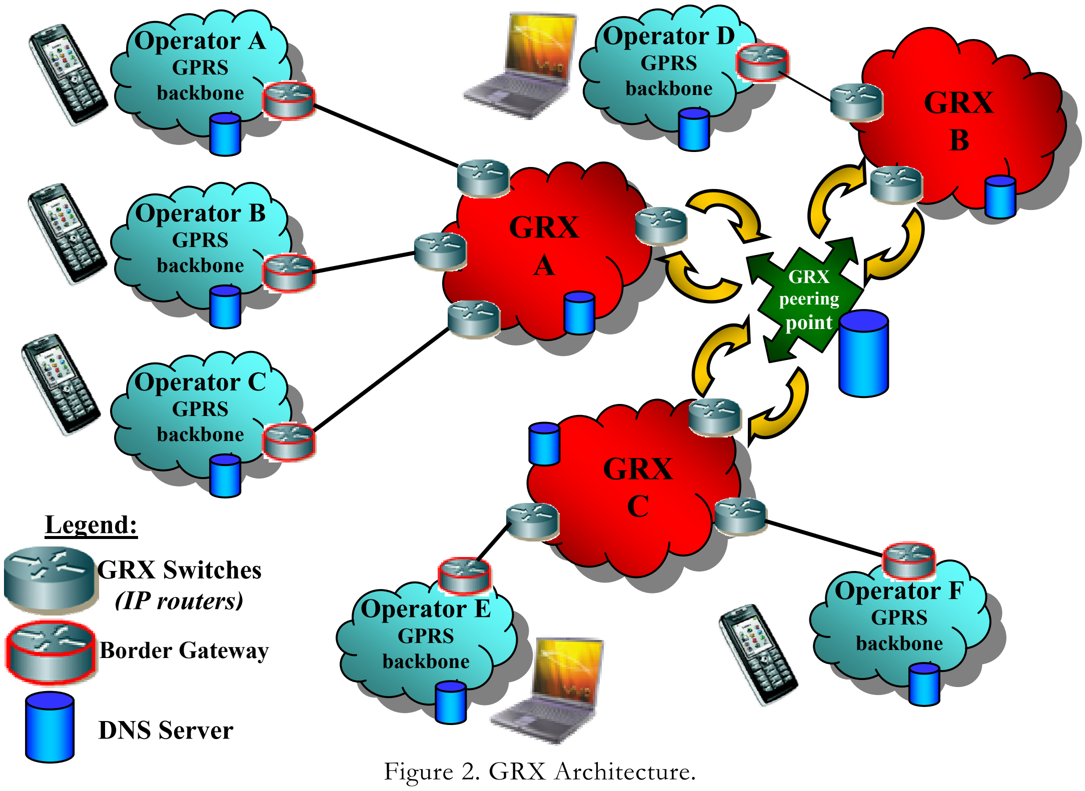


Figure 2. GRX Architecture.

The GRX providers are usually IP service providers with extensive international IP infrastructures. They have implemented a GRX Network, essentially a private IP network, which support specific tunneling protocols and offer service according to a service level agreement (SLA) with their customers.

A GRX network is similar to the Internet with respect to its structure and architecture. It is a layer 3 network, which means that packets are routed within the network to their destination. Border gateways are deployed at the border of each operator's domain. These have a specific function which will be explained in Chapter 3. As indicated in Figure 2, every GPRS and GRX operator has its own DNS server. This DNS is crucial for the support of IP based services such as GPRS roaming, inter-PLMN MMS delivery and IMS interworking. Requirements and detailed guidelines are given to the carriers by the GSM Association in its reference documents IR.34 *Inter-PLMN backbone guidelines* [13] and IR.67 *DNS Guidelines for operators* [22]. The types of entries in these DNSs vary based on where in the whole hierarchy of the DNS system the server is. In general, these could be records containing information about domain names used within the community, pointing to the authoritative DNS for each of the domains, providing mapping between the name of service nodes (such as SGSNs, GGSNs, and MMSC) and their respective IP address. Furthermore, with the help of naming authority pointer records (NAPTR) a mapping between telephone number of a subscriber and corresponding URIs for different services available to that subscriber could be facilitated through the ENUM service, etc. ENUM is described further in section 5.3.

Despite the similarities with the Internet, the GRX network functionality is totally separated from the public Internet for security reasons, through utilization of reserved space of the public IP addresses and domain names not included in the public domain name space. The public IP addresses used within the GRX cannot be and must not be resolved by the public DNS hierarchy and vice versa – the GRX DNS hierarchy must not be able to resolve any IP addresses which belong to the public Internet. The internet routers should not know how to route traffic to the IP addresses used in the inter-PLMN networks.

As mentioned above, the reasons are to meet the security requirements of the GRX network. Although each of the GPRS operators implements its own security measures at the border of its domain, the GRX network is assumed secure and trusted in a sense that no outsider should be able to access the network other than the GRX and GPRS operators. Nevertheless, each operator is responsible for screening the traffic towards his BG, and to allow only specific traffic to enter his network.

Another issue that the GRX and GPRS operators are facing is the transition to IPv6. The currently used IP version 4 address space is a limited resource. Although the GPRS operators have employed numerous techniques to manage IP addresses within their domain, with the introduction of new IP architectures such as the IP Multimedia Subsystem (IMS), it is becoming obvious that the future of mobile communications depends on the successful deployment of IPv6 network functionality. IMS was designed from scratch with IPv6 in mind. The new services that utilize peer-to-peer traffic between the mobile users demand simpler network functionality and use of public IP address if possible. Currently GRX networks utilize version 4 of the IP protocol. Although, in the near future the use of IPv4 will not pose significant obstacles to the operation of the GRX (since IPv6-in-IPv4 encapsulation could be used to tunnel traffic through the GRX), eventually IPv6 must be introduced to resolve the current addressing limitations, thus allowing for transformation of GRX into IPX. This transition from IPv4 to IPv6 will be subject to bilateral agreements between the GRX operators themselves and the GRX operators and PLMN operators. This process could take years and requires changes in the network infrastructure in the parts of it where IPv6 is not supported.

With deployment of SIP based services within the mobile community, another question has arisen – should the GRX network become accessible from the public Internet, e.g. should SIP clients and other applications in the public Internet be allowed to reach SIP clients running on mobile terminals? The most logical answer to this question is positive, but the difficulties which this introduces are not simply technical. For example, the assumption that the GRX network is completely secure and protected against malicious actions (since not everyone is allowed to connect to it) – would be jeopardized. If the GRX is open to regular ISPs, this could undermine the assumed security and trust within the GRX network, because the inter-PLMN infrastructure would be exposed to the security risks that are common to the public Internet. This could be perceived as a flaw of the GRX network design.

Therefore, in order to achieve such a connection between the ISPs and the GRX infrastructure, the respective parties must take appropriate measures to guarantee the security of the GRX networks. This could be done by deploying adequate firewalls and BG functionality at the border of their networks, thus satisfying the requirements which the GSM Association laid out in their reference document IR.34:

> *"For security reasons, GPRS intra- and inter-PLMN backbone networks shall remain invisible and inaccessible to the public Internet. Generally Internet routers shouldn't know how to route to the IP addresses advertised to the inter-PLMN networks. In other words, inter-PLMN service providers and PLMN operator networks shall be totally separated from public Internet."* [13]

Another problem is how to guarantee QoS across the different domains. While there are some mechanisms used within the GPRS community to assure a certain level of QoS, there is no reliable mechanism which could provide the equivalent QoS level within the public Internet.

A guaranteed level of QoS is an important competitive advantage for the operators, if they are to benefit from delivering the services existing on the public Internet. In order to deliver guaranteed level of QoS the operators need to be able to differentiate between the different types of services since they generate different traffic and are sensitive to a different extent to packet losses and delays. For example, voice and video calls are affected by delays and packet losses, resulting in low quality of the conversation and customer dissatisfaction. On the other hand, web-browsing and e-mail are services which are much more tolerant to such traffic impairments.

DiffServ is one method to guarantee QoS on large networks such as the Internet. It deals with bulk traffic flows, rather than single reservations or single data flows. It is suitable when operators negotiate a Service Level Agreement (SLA), where the different classes of traffic, their amounts, and the guarantees for each class are defined. But DiffServ is not enough when end-to-end QoS has to be guaranteed, because of the different way every router on the network interprets the prioritized traffic. In addition, all routers along the path must be able to interpret DiffServ, which may not be the case in large networks and this issue should be addressed while negotiating SLA.

When DiffServ is used, the sender sets the “type of service” field (also known as DiffServ Code Point (DSCP)) in the IP header of the packet to an appropriate value. The higher the number, the better is the class of the data. From this point forward, all that the routers along the way have to do is to give priority to packets with a higher number class of data over the packets with lower class of data. The receiver can monitor the traffic and if larger volume of certain class of traffic is detected than negotiated in the SLA, the sender might be subject to sanctions in accordance with the negotiated contract.

2. IP Multimedia Subsystem (IMS) – introduction

The growth of the Internet and its popular services is forcing telecom operators to provide comparable services to their subscribers. The traditional voice service that runs over the circuit switch network is no longer enough to attract mobile users to spend money with their cellular network operator. These operators want to use IP based networks to provide new more attractive services for their users. These new set of services will in a first phase only be available via the cellular networks and it has to support roaming. To support such a closed ("walled garden") model required the design of a whole new network architecture called IMS. This new telecom technology is an “operator knows best” design. If IMS will be a success or not depends on if the customers will accept this technology as next generation telecom network or if the mobile operators may need do rethink the design. Another technology model that IMS is threatening by is Internet telephony provided by big companies like Ebay/Skype, Microsoft, and Google. This free telephony service can be accessed through WiFi hotspots or other IP-based access networks [30].

IMS stands for IP Multimedia Subsystem. It is a standardized network architecture that is designed to merge cellular networks and the Internet. The third generation partnership (3GPP) has standardized IMS. The purpose of this converged network is to provide a platform for all kinds of multimedia services, both basic calling services as well as enhanced services. The services include among others video sharing and Push-to-talk over Cellular [26]. IMS is designed to make it easy to develop and deploy new services. Additionally, two or more services can be integrated in to one new service. IMS uses open standard IP protocols to enhance the compatibility between IMS and the Internet. The goal is to deliver multimedia services between the fixed- and the cellular networks and within the networks themselves, but *without making these services available to the public internet or allowing new operators on the public internet to provide services to the fixed and mobile telecommunications users.* The reason not to allow these new operators to offer services to these users is *that the mobile access operators want to keep their monopoly or near monopoly positions* [6].

3GPP has defined a list of requirements that IMS must fulfill. Where IMS is defined as:

“An architectural framework created for the purpose of delivering IP multimedia services to end-users.” [6].

These requirements state that the framework needs to support IP Multimedia sessions, quality of service (QoS), interworking with the Internet and the circuit switched network, roaming, operators’ ability to strong control the users’ services, and that new services do not need to be standardized [6].

The second requirement above concerning Quality of Service (QoS), means that the user is to be guaranteed a certain amount of bandwidth and bounded packet delay. Traditionally packet-switched networks only provided best-effort delivery, which means that the IP packets are not guaranteed to arrive at the destination without loss or corruption of packets or even within any specific time bound. Of course higher layer protocols can be used to provide reliability if it is desired, but this is the reverse to the usual model for circuit switched telecommunication where it is assumed that the network provides *in order delivery of bits with a bounded delay* further more the error rate is determined by the links used and error bounds are based upon engineering and management selections of the appropriate link. Another contrast is that of availability of services, in the circuit switched model you either have the service or you do not, while in the packet switched model you may have at least some low quality service even in the worst of conditions [6].

Cellular networks have emphasized roaming as a service. In IMS this means that a user can be in a foreign country (or non-home operator's network) and still be able to use his/her mobile operator's services (i.e. Video sharing, Push-to-talk over Cellular, etc.) [6].

With the introduction of IMS, a mobile access network operator will have the ability to monitor each service which a user is using. This will make it easier for the operator to apply specific business model for each service as part of a use-by-use cost model, while controlling what kind of services the user is allowed to use. The advantage is that users will be able to compare the price of each service between the different operators, and this will enhance the competition between the operators to retain and attract subscribers. However, if the user is using a service that is not provided by the mobile network operator, then the operator will only be able to see how much data is sent over the packet network to/from the user. If the majority of users use these services, then these users may prefer a flat rate model. It is up to the operator which business model to use, such as: flat rate, time-based, service based, or QoS based. However, it is important not to force a user to use only this operator's service, because this would violate the competition rules in Europe. In the first stages of the deployment of IMS, all IMS cellular phones will also support circuit switch calls, thus providing calls to the emergency numbers, which are not yet supported in IMS [6].

The signaling protocol that is used in IMS is SIP (Session Initiation Protocol), and it works over multiple transport protocols (e.g., TCP, UDP, and SCTP). Further details on SIP can be found in section 2.1.1.

2.1. The main protocols in IMS

When 3GPP started to consider what protocols should be implemented in IMS they first considered protocols that had already been developed by ITU-T and IETF. This approach led to the use of the SIP. This session control protocol is the basic protocol underlying IMS [6].

An equally important protocol is the Authentication, Authorization, and Accounting (AAA) protocol for accessing networks or accessing services. 3GPP chose the Diameter protocol [6] for use in IMS. Diameter is an upgrade of the RADIUS [6] protocol. Unlike RADIUS, diameter can be transported over a reliable transport protocol like TCP and secured via IPsec. Diameter was developed so it could be used in any application environment. The protocol is a peer-to-peer protocol and it has negotiation support. Another reason for choosing diameter is to enhance support for roaming [6].

A client-server protocol that is able to exchange policy information between a server and its clients is Common Open Policy Service (COPS)[27]. A policy server, called the P-CSCF node (further details on the main nodes in IMS can be found in section 2.3) acts as a Policy Decision Point (PDP) and the client is the GGSN which acts as a Policy Enforcement Point (PEP). COPS uses TCP as its reliable transport protocol. 3GPP chose COPS as their policy protocol [6].

The media protocol used to transport audio and video in IMS is the Real-time Transport protocol (RTP) [28]. This is used together with the RTP control protocol (RTCP). The control protocol's primary function is to report the QoS statistics of the senders and receivers. RTP is transported over the unreliable transport protocol UDP. IMS itself does not provide any security for the media. The reason for this is that assumption that each radio link provides its own encryption and that all nodes in the IMS core are trusted. However, if a user wants to be guaranteed integrity and does not trust the IMS core or the access network (which may be especially true when roaming), the user could use the Secure Real-time Transport Protocol (SRTP) [29].

IMS uses IPsec for both its access security protocol and network security protocol. IPsec provides security at the network layer. The protocol is used between the P-CSCF and the user's terminal.

2.1.1. The signaling protocol SIP

As was mentioned above IMS is based on the SIP session control protocol. SIP is based upon two successful protocols: HTTP and SMTP. It was standardized by the Internet Engineering Task Force (IETF). Its main purpose is to establish multimedia sessions over an IP network. SIP has several important properties. It is a text based protocol (just like HTTP) and it is a rendezvous protocol, which means that its only task is to establish a session, thus the actual exchange of media is independent of SIP. This means that the media traffic does not need to travel along the same path as the signalling traffic did. IMS makes it possible for the operator to implement third parties services in their networks. This means that the new services need to be written for IMS standards instead for multiple standards depending on the network. Unlike, the circuit switched network where the services need to be standardized to be guaranteed to work between different operators' network. An example of such a service is the Short Message Service (SMS)[22]. Allowing non-standards should reduce the time needed to introduce a new service, but if the operator that provides the service wants to monitor that service for the user, then it will probably delay the deploy of the new service. SIP uses a client-server model in the sense that a SIP entity can be a User Agent Client (UAC), a User Agent Server (UAS), or both depending on the situation. SIP messages are either requests (from a client) or responses (from a server) [6].

The Session Description Protocol (SDP) is carried in the body of the session initiation request. It is a text based protocol which describes a proposed session. SDP is used together with SIP to negotiate what media CODECs both parties support, to establish QoS in both direction, and to specify the IP address and the port number the user agent wants each media stream to be delivered to [6].

2.2. Identify subscribers and services in the IMS

To uniquely identify subscribers or terminals PSTN networks use a sequence of digits to identify a specific telephone. In PSTN networks a user is called by a particular phone at a particular place. In the GSM world a called user uses a mobile handset. GSM operators use a sequence of digits to identify a subscriber (the so called IMSI). GSM supports the ability of the user to change from one handset to another by moving their subscription from one device to another. With IMS a called user utlilizes a user's agent which decides which of the user's multiple devices should be sent information about the incoming call. In IMS each subscriber is identified by one or more public user identities which are used for SIP routing. A public user identity is either a SIP URI or a TEL URI. The latter is needed if a PSTN user wants to call an IMS user or vice versa. The SIP URI might look like: "sip:first.last@operator.com" and a TEL URI: "tel:+46-70-526-34-45". For authentication purposes IMS uses Private User Identities. A key purpose of identification is to determine the relevant subscription for billing purposes [6]

During registration of a user agent it is mandatory to use a SIP URI and not a TEL URI. The reason for this is that TEL URI does not identify the domain name of an operator and a TEL URI is non routable address. With the domain name it is easy to find which network operator a user belongs to. However, it is possible to include a telephone number in a SIP URI with this format: "sip:+46-70-526-34-45@operator.com". Each IMS user is assigned one or more private user identities called a Network Access Identifier (NAI). The form of an NAI is: username@operator.. This private user identity is not used for SIP routing, but is only used for authentication within the IMS. This private NAI is stored in an ISIM (IP Multimedia Services Identity Module). The ISIM resides in a smart card called a Universal Integrated Circuit Card (UICC). Each ISIM contains one private user identity, at least one public user identity, an URI to the relevant operator's domain, and a long-term secret. The secret is used for authentication purposes and for calculating integrity and cipher keys [6]

To identify services in an application server they are named with a Public Service Identity. This public service identity can be either a SIP URI or a TEL URI address. If it is a TEL URI, then a PSTN user will be able to use this IMS service. While SIP URI will be used by non-PSTN users, since almost all SIP entity in IMS will contain a SIP URI [6].

2.3. IMS components

IMS consists of a collection of functions with standard interfaces [6]. Every function can be divided over several nodes or a single node may contain a number of functions. The most common approach is to have one function per node (this keeps things simple).

The most important node in the IMS is the home subscriber server (HSS). It is a database that contains all necessary information concerning subscribers. The network operator needs this information to be able to charge a user for a specific service he/she uses. The information includes among other things the network location of a user (e.g., the IP address of the terminal), along with authentication and authorization data for a user. The authentication data is generated as authentication vectors [6]. Authentication and authorization information is keyed upon the private user identity that identifies a subscriber. The subscriber authenticates using the shared the long-term secret. If there is more than one HSS in an IMS core, then a Subscription Locator Function (SLF) is used to determine which HSS a user's records are in. The HSS is always in the home network. Figure 3 shows an overview of the nodes in the IMS core [7].

The first contact node of the IMS domain an IMS terminal encounters is with the Proxy-Call Session control function (P-CSCF). This is a SIP server and one of three main nodes in the IMS core. All three nodes have different tasks to perform and utilize SIP signalling [6].

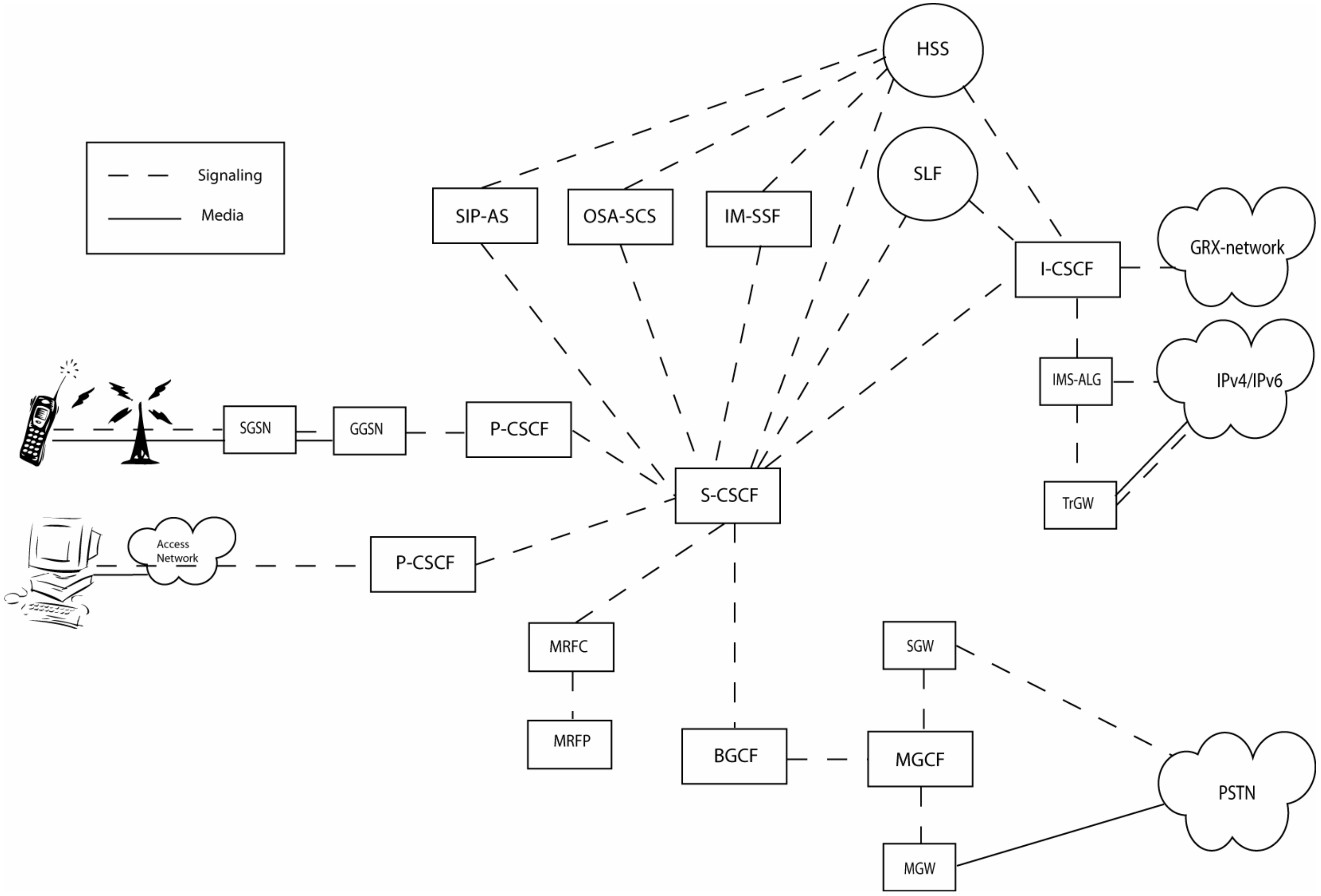


Figure 3. IP Multimedia Subsystem (IMS) CORE – Home network

The P-CSCF acts as a proxy server for both in-coming and out–going traffic to this IMS terminal (also known as User equipment (UE)), hence all signalling traffic to and from an IMS terminal will traverse the P-CSCF. In other words the P-CSCF acts as a gatekeeper with regard to the IMS terminal. As a gatekeeper it will provide integrity protection and a filter mechanism to verify the validity of all SIP requests to or from the UE. Another important function of the P-CSCF is IMS registration and authentication of an IMS subscriber. After the P-CSCF has authenticated an IMS terminal the rest of the nodes in the IMS core do not need to authenticate the UE again, because these other nodes trust the P-CSCF. The P-CSCF will if necessary establish a specific quality of service (QoS) for the media streams. The P-CSCF can be located in the home network or in the visited network. If in the visited network, then the originating IMS domain needs to authenticate the P-CSCF node. In the early stage of IMS deployment the P-CSCF will be placed in the home network. The disadvantage with this placement is that the media has to first go to the home network and then to the destination. This means that the user is forced to send all their SIP traffic through their home P-CSCF in a visited network. The reason to place the P-CSCF in the home network, when introducing IMS, is that in the current GPRS packet network the GGSN (Gateway GPRS support node) is in the home network. The media traffic traverses always through the GGSN that is why the media needs to go via the home network in the fiffers stage of IMS. Currently both the GGSN and the P-CSCF have to be in the same network. The basis is that a user will normally use a home network Access Point (GGSN) to access the home network IMS domain. When the user is roaming he/she will use the visited network access point or the home network access point. If the subscriber uses the home network access point then he/she will use the home network's P-CSCF node and if in the visited network he/she will use the visited network's P-CSCF node (IR.65[14] section 4). To support a P-CSCF in the visited network the GGSN needs to be upgraded to be 3GPP Release 5-compliant, but not all the mobile access network operators will deploy IMS at the same time [6].

The second main node in the IMS core is the Interrogating-CSCF (I-CSCF). The I-CSCF is placed at the edge of the IMS domain to communicate with other IMS domains. Because of security aspects and because the I-CSCF is the first contact point to other IMS domains, the I-CSCF implements a functionality called Topology Hiding Inter-network Gateway (THIG). Therefore the I-CSCF encrypts some sensitive information about the domain in the SIP messages, hiding among other bits of information the domain's capacity and number of IMS servers. The I-CSCF acts as a proxy server. When another IMS domain wants to find an entity within a destination domain associated with an I-CSCF it will learn the address of this I-CSCF from the DNS in the IMS core (how the DNS infrastructure and naming scheme actually works is explained in *chapter 5*) and will forward the SIP message to the I-CSCF for this destination domain. Another difference from the P-CSCF, is that the I-CSCF has an interface to the HSS and the SLF. These two interfaces are needed for the I-CSCF to route the incoming SIP message to the destination node within the IMS domain [6].

The third central node in an IMS is the Serving-CSCF (S-CSCF). It is an UAS and it also handles the registration of subscribers (i.e., it is a SIP registrar). The S-CSCF maintains a binding between the current IP address of the terminal and the user's public user identities. Just as the I-CSCF, the S-CSCF also has an interface to the HSS and the SLF. These two connections from the S-CSCF to the HSS and SLF are needed to be able to download the authentication vectors of a subscriber to the S-CSCF from the HSS. The authentication vectors provided by the HSS are needed to authenticate the IMS terminal to grant access to download the user profile to the S-CSCF from the HSS. The user profile tells the S-CSCF about the service profile associated with this NAI (user), the service profiles are implemented as a set of triggers that activate when some conditions are fulfilled. These conditions involve requests for one or more services. Some of these requests may need to be routed via specific application servers to provide the user with the requested service. This is the why the S-CSCF and the P-CSCF needs to inspect all the SIP signaling that goes to and from the IMS terminal. The S-CSCF also needs to inform the HSS which S-CSCF is allocated to handle this subscriber; subsequently each terminal will send registration requests to the same S-CSCF and the P-CSCF. Another important task is to provide SIP routing services to the user. The S-CSCF translates between TEL URIs and SIP URIs. The network operator has the ability to implement policies regarding what the user is authorized and not authorized to do within this IMS, these policies are enforced by the S-CSCF node [6].

Both the I-CSCF and the S-CSCF are located in the home network. The P-CSCF can be located either in the home network or in the visited network. All three are able to be distributed over multiple nodes to achieve redundancy and scalability [6]

Another type of SIP entity in IMS is the various Application Servers (ASs). These servers provide services which are hosted by operators. These can utilize one or more computational servers. There are different types of application servers. The most common will be the SIP AS, as all future services will be developed to utilize this server. The SIP AS resides inside the operator’s domain. Thus is an operator offers to host third party services, this third party needs to be trusted by the operator. However, if a third party wants to host a service external to the operator’s domain, then another type of AS, called the Open Service Access-Service Capability Server (OSA-SCS) is used. It interfaces with the Open System Architecture (OSA) [23] Application Servers using Parlay [24]. There is an API between the OSA AS and the OSA API, but it works much like a SIP AS. A very useful application server which reuses existing GSM services (including SMS and MMS) is called the IP Multimedia Service Switching Function (IM-SSF). All application servers act either as a SIP proxy server, a SIP user agent (UA), a SIP redirect server, or as a SIP Back-to-back User Agent (B2BUA) [6].

An important node in the IMS core concerns the media flow, this is the Media Resource Function (MRF). It is used to play audio/video announcements, provide multimedia conferencing (bridging), Text-to-speech conversation (TTS) and speech recognition, and Realtime transcoding of multimedia data [7]. The media resource functions are divided over two nodes: the Media Resource Function Controller (MRFC) and the Media Resource Function Processor (MRFP). The MRFC node handles the signaling and it controls the MRFP. The node that takes care of the media is the Media Resource Function Processor [6].

The IP Multimedia subsystem needs to support IMS users that call PSTN or PLMN users. Hence the Breakout Gateway Control Function (BGCF) is implemented to gateway these calls from IMS. The BGCF’s main task is to route signaling and media traffic from an IMS terminal to a user in a circuit-switched network domain. The BGCF does not enable a PSTN user to call an IMS user (i.e., for an incoming call). Instead a PSTN gateway provides this functionality. The PSTN gateway provides an interface to the PSTN circuit switched network. This gateway is divided over three nodes: the Signaling Gateway (SGW), the Media Gateway Control Function (MGCF), and the Media Gateway (MGW). The MGCF is the main node of the PSTN gateway, as it converts the SIP signaling to either ISUP over IP or BICC over IP. It also monitors use of the resources in the MGW. The MGW gateways media from the PSTN network to/from the IMS network. It converts RTP audio to pulse coded modulation (PCM) coded audio (typically G.711 with u-law or A-law coding) or the reverse in the other direction. The SGW converts signalling over the transport protocol SCTP to MTP, in order to pass ISUP messages from the MGCF to the PSTN network [6].

When IMS was designed it only supported IPv6. However, when IMS was close to deployment IPv4 and NAT were nearly ubiquitous, thus a lot of work has been done in SIP to traverse NATs. However, all IMS domains need to understand both IPv4 and IPv6 because the network operator might not have introduced IPv6 yet (for more information about IP version issues in IMS see *chapter 7*). Thus two nodes were introduced: the IMS Application Layer Gateway (IMS-ALG) and the Transition Gateway (TrGW). The IMS-ALG takes care of the control plane traffic and the TrGW handles the user plane traffic [6].

3. Interworking concepts

In order to be commercially viable for the network operators the IMS architecture, among many other aspects, must provide for transparent and reliable services across domain borders. Until recently, IMS has been developed with the main focus on deployment *within* the domain of a single operator. Therefore, while its functionality is well defined, developed, and standardized to some extent, the focus of the work has never been primarily on the interaction between two or more IMS domains (be they mobile or fixed operators). This is “terra incognita” and only recently, have steps been taken to explore the issues including the benefits and the drawbacks that might arise from this type of interaction. This is due to the fact that IMS is still a very new platform and until recently all efforts were concentrated on standardization of a single IMS domain rather than *interworking between* IMS domains.

3.1. Interworking Models

There are two main models of interworking between two or more IMS domains, envisioned by the standardization bodies, as well as the mobile operators and the telecommunication industry. These are the “***Peer-to-peer model***” and the “***Hub model***”. These two models are alternatives and at the same time, complementary to each other. Although the technology for implementing each of these approaches exists even today, it is a common belief that each of these models will evolve as the development and the deployment of the IMS architecture as a “de facto” standard continues. Peer-to-Peer is expected to precede the Hub model because of its less complicated technical requirements. In other words, the introduction of each of these models is likely to be sequential in time.

An IPX (IP exchange) is a closed inter-service provider IP network offering low and predictable delay and guaranteed QoS in a secured environment. [13] Such an IPX itself is an evolution and further development of the existing GRX network which helps to interconnect different PLMN operators. The requirements for IPX service providers are the same as for GRX providers, i.e., the IPX network must comply with the GSMA Inter-PLMN Backbone Guidelines [13], and the security requirements outlined in the same document.

The existence of IPX networks is a necessity for the implementation of the “Hub model”. The “Hub model” is facilitated by introducing an IPX Proxy. This is a SIP proxy with capabilities for providing better security, QoS, and a means for traffic management and media-flow interworking. An IPX should not be mistaken with existing IP exchanges since the purpose and functionality of the latter is simply to facilitate the routing of the IP traffic between operators, while the IPX will provide the means to control the traffic more intelligently, taking decisions based upon the requirements for each particular session, as opposed to just routing based on source and destination addresses. A possible drawback is that such analysis and decision making could introduce additional delay of the traffic and could increase the overall cost.

IMS Interworking will follow a similar pattern to the phases which GSM Roaming and GPRS interworking have shown in the past. In the beginning, because of the small number of mobile operators which have a fully functional IMS domain, interworking between them could be handled through bi-lateral agreements based upon direct business relationships. This is very similar to what happened when the first GSM operators decided to implement roaming between their networks. In later stages, when the number of IMS domains has increased significantly, these bi-lateral agreements would be a hindrance as they do not scale. As the current number of mobile operators is almost 700, it would be virtually impossible to handle all of the pair-wise agreements between them in a convenient way. Therefore at this stage it will be necessary to introduce the "Hub model", which to a great extent is what happened with the introduction of the GRX transit network years ago in order to implement roaming and interworking services globally. Tunneling of traffic between operators via the existing GRX network is a short-term solution and is likely to be adopted in the initial stages of the IMS deployment. Nevertheless, since IMS places many new requirements on the interconnecting networks in terms of QoS, security, increased traffic, and new services the network is most likely to transform into IPX which is better suited to handle the control and user traffics because of the additional functionality of the IPX-proxies. Best effort routing via public internet is not a desirable long-term solution as it does not provide the overall QoS required for IMS. Perhaps, if the IMS interworking traffic is in a very small scale, then Internet could be used as an interconnecting network. This, however, will not be possible in case users require guaranteed level of QoS based for example on different price plans.

3.1.1. The peer-to-peer model

A peer-to-peer model is most likely to be the first of the two approaches for IMS Interworking to be deployed. There are several reasons for this – the small number of interacting parties involved in the initial stages of the IMS Interworking, avoiding significant changes in the existing GRX network or business relationships, most IMS Interworking will happen first "locally" or "regionally (nationally)" and only after some time will evolve into true "international" IMS Interworking, etc. This model provides for quick and relatively easy interaction between several mobile operators in one region, with potentially different business models, while at the same time taking the necessary first steps towards global IMS Interworking. However, there are already several, though not many, international operators and Mobile Virtual Network Operators (MVNO) who could start introducing IMS throughout all their networks dispersed in different geographical regions. Peer-to-peer is a compelling choice for an initial model (time-wise), because of its simplicity, and the minimal technological changes that have to be introduced before a successful IMS Interworking takes place. Figure 4 illustrates an IMS peer-to-peer architecture.

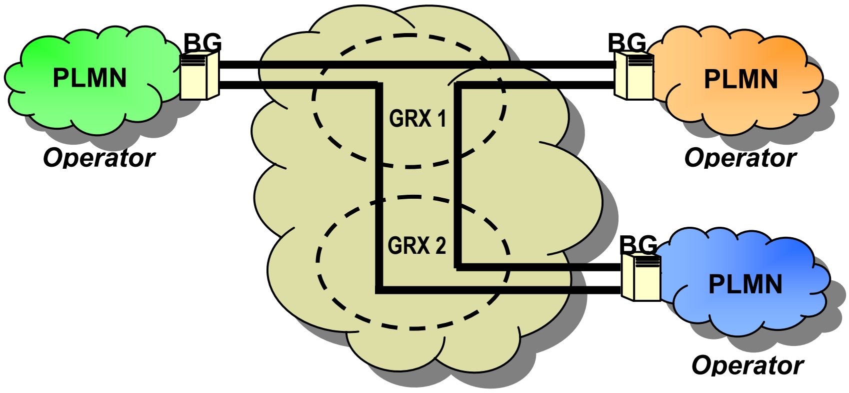


Figure 4. Peer-to-peer IMS Interworking architecture

In the figure shown above, there are three different mobile operators. Each one of them has its own IMS domain within the PLMN it operates. In this case of IMS Interworking the traffic is exchanged between the operators utilizing the existing GRX network infrastructure. Each operator has a service level agreement (SLA) with its peers to provide a specific quality of the service. As it is shown in Figure 4, all of the traffic is exchanged through GRE tunnels over the GRX network (simply using IP routing). This means that both control traffic and user traffic are encapsulated at the border of the PLMN domain by the border gateway and routed through the GRX network to its destination.

The advantages of this method for interworking include, but are not limited to:

- Simple deployment
- Transparent to GRX - as it is simply more IP traffic
- Low cost interworking (as no changes in the GRX are required) and no changes are necessary in the agreements between the mobile operators and their respective GRX operators.

Hence this model is likely to be the one that will be realized in the initial stages of the IMS interworking.

Some of the disadvantages are:

- Difficult to guarantee Quality of Service (QoS) across the borders of the different domains. While the GPRS operators have SLAs with the GRX service providers, the GRX network is a best effort transport network. There is no means to steer the traffic based on its characteristics or requirements. Concrete and controlled QoS is what the current GRX lacks.
- No possibility of session based management of the traffic within the GRX network. Again, the lack of such management is restricted since the operators cannot guarantee end-to-end negotiation of the QoS. In order to do that, future applications must be able to negotiate required QoS level between origin and destination nodes and the data packets must be transported through the whole network according to the negotiated level of QoS in order to guarantee the required end-to-end QoS. However, this might introduce some delay and additional cost.
- When the number of interacting parties increases significantly, handling of the pair-wise IMS traffic agreements required by this model of interworking will become unmanageable, even though the number of SLAs between the PLMN operators and the GRX operators will continue to increase linearly.

It must be mentioned that in addition to the above scenario, there are other scenarios for peer-to-peer interconnect between the IMS domains of different PLMN operators, e.g. leased lines. In this case, the business model on which the interworking is based will be entirely dependant on the physical parameters of the leased line between the two operators, and the GRX will not be utilized as a transport network. Additionally, this “alternative” means of interconnection will introduce significant financial burdens on the operators, who will pass this along through a higher price for the service to the end customers. While the peer-to-peer scenario evades some of the above mentioned disadvantages, it is still not a scalable solution from PLMN operators' point of view.

A very important role in this model of interworking is the so called Border Gateway (BG) which resides at the border of each operator's network. In the ETSI TISPAN standards the BG is called an Interconnect Session Border Controller (ISBC). It incorporates and implements three functional elements of the IMS architecture [8]:

- **Interconnect Border Control Function** (IBCF) provides overall control of the boundary where different operators interconnect. The IBCF provides some level of security to the IMS core since it performs a Topology-Hiding Inter-network Gateway (THIG) sub-function, described in section 2.3 and 6.5.1. In addition to the signalling-based topology hiding it also provides IPv4-IPv6 interworking and session screening based on the source and destination addresses. This means that the IBCF will make sure that correct translation between the protocols is done if necessary and that the necessary traffic would be admitted through the firewalls in both directions with the required parameters. When connecting to non-SIP or non-IPv6 networks, it implements an Inter-Working Function (IWF) and performs bandwidth and admission control. The IBCF interacts with the Interconnect Border Gateway Function (I-BGF) to control the borders of the domain at the transport layers via network address/port translation (NAPT), pinhole firewall, and other functions.
- **Inter-Working Function** (IWF) – used when signalling protocol translation is necessary between the SIP-based IMS network and other networks using H.323 or different SIP profiles.
- **Interconnect Border Gateway Function** (I-BGF) – provides control over the border between different networks on layer 3 and layer 4. This is the function which provides the pinhole firewall and NAT/NAPT functionality, which protects the IMS core of the operator's network by hiding the IP addresses of the service elements in the network and at the same time performs packet filtering at the IP address/port level. Some of the additional functions of the I-BGF include the QoS measurement of the media flows and QoS management of both packets and bandwidth.

Overall, the Session Border Controller (SBC) provides security, scalability, and manageability.

Security is provided by protecting the IMS core from DoS attacks through continuous monitoring and discovering of malicious signalling or media flows, or protecting against non-malicious overloading.

The SBC facilitates scalability by providing functions to reduce the load on the IMS core elements for such intensive tasks as the NAT and the encryption management. When using IPv6 the need for NAT is eliminated, similarly if end-to-end encryption is employed, then most of the encryption load is eliminated as well.

Manageability is achieved by reducing the number of network elements since it includes several IMS functions and by providing performance management such as QoS monitoring for the media flows. This is the model used in most contemporary implementations of SBC. While it is suitable for small-scale deployments, incorporation of several functions into one node could be obstacle to scaling. The carriers might like to have the signalling processing centralised and separated from the handling of the media flow. The latter is better situated closer to the user in order to minimise network delays.

3.1.2. The Hub model

The Hub model of Interworking is likely to be the second choice for deployment (time wise) since it is more demanding from a technology point of view and places additional requirements on the GRX network beyond what exists today. Nevertheless, it is safe to conclude that this model of interworking is likely to become dominant when IMS is widely deployed and the number of peer-to-peer SLAs becomes difficult to manage. Thus this is the most probable scenario for global scale IMS interworking. Figure 5 illustrates the Hub model architecture.

The existing internet exchange points do not provide the functionality this model requires. There are numerous reasons for this, but probably the most important is that these exchange points do not meet the requirements laid down for the IPX by the GSM Association. Nowadays exchange points lack the functionality to deliver the services expected from an IPX network. They cannot provide the guaranteed QoS, accountability, increased manageability and security since they lack mechanisms to do that. The need for increased manageability is introduced by the requirement for traffic separation and session control by the IPX-proxies.

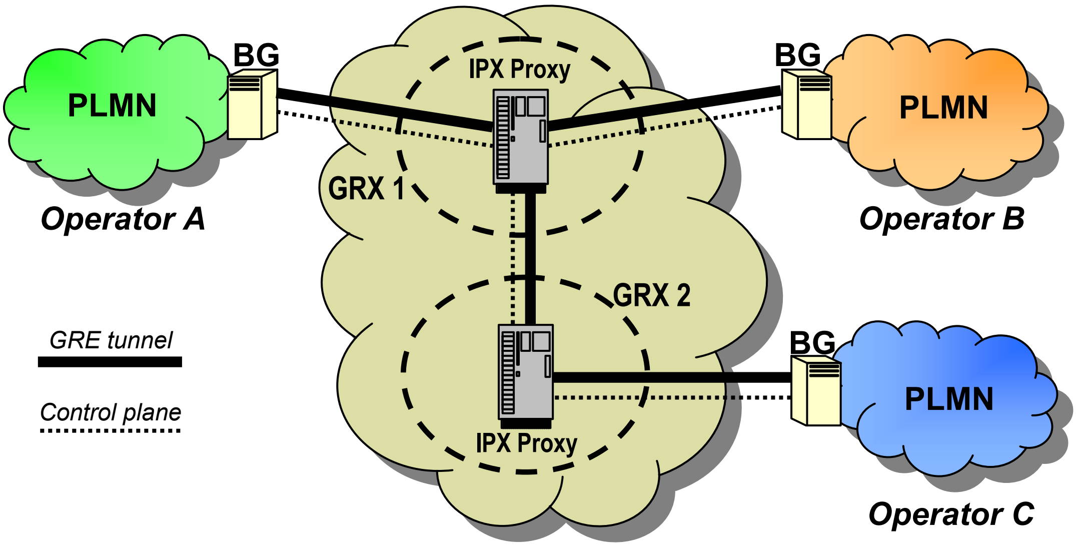


Figure 5. Hub model of IMS Interworking architecture

Similar to the peer-to-peer model, there are three different mobile operators, each of them with their corresponding PLMN and IMS. A Border Gateway (BG) is present on each border where the PLMN is connected to the GRX network, since they provide the operators with some security and network management.

This architecture introduces two new elements as shown in the Figure 5. The first is the so called IPX proxy or IP Exchange proxy and the second is the separate handling of the control plane traffic. The significance of each will be discussed in the following paragraphs.

The introduction of a new service node (the IPX proxy) in the GRX operators' networks is the most significant change made to the GRX network. In order to deliver the services expected from it the IPX proxy will employ functionality similar to that implemented in the service border gateways. With this change, the GRX network becomes more manageable and sophisticated. The proxy also provides for inter-carrier charging, although this breaks the possibility of end-to-end encryption of the traffic. Obviously, this presents a trade off between the subscribers' desire to have high and guaranteed QoS and the security measures taken to protect the traffic. Instead of being looked upon as a disadvantage, this could be also interpreted as an opportunity for even further diversification of the business model of the operators. It assumes the role of a hub, to which all of the clients of a particular IPX operator are connected. All proxies within the evolved network are connected to each other, thus providing connectivity between carriers.

The separate handling of the control plane (signalling) traffic from the user traffic is probably one of the most significant changes in this architecture in comparison with the peer-to-peer model. It is a direct result of the IPX proxy introduction. By examining the control (signalling) traffic, the proxy can make better decisions about the traffic routing, not only based on the source and destination addresses, but also taking into consideration the characteristics of the expected traffic. It also performs bandwidth management on a per tunnel basis, and QoS bandwidth admission control on a per tunnel basis to enforce the SLA and to guarantee that not too much traffic is put on the network links when there is no capacity for that. Usually the interconnecting operators tend to over-dimension their networks in order to be prepared for unexpected surge in the traffic load. Although over-dimensioning is not cost efficient, in some cases it could be considered better choice than the complex additional processing of the traffic, which results in additional delays and increased cost. A balance should be found between deploying of new resources and better management of the existing ones. The IPX proxy uses DiffServ to prioritize QoS traffic over its underlying best effort network. If a limit is reached and the network cannot cope with the amounts of traffic marked as high priority, then either the network capacity must be increased or the network should perform admission control and if bandwidth is not available, new sessions will not be permitted. Alternative is to let the media traffic, which is the resource-hungry traffic to be transported as best effort traffic, and only certain classes be marked as high priority, based on the operator's business model.

There are also some limitations and technical difficulties as well in the case of the evolved GRX network. One such limitation is the speed with which the GRX operators will introduce the new IPX functionality. Currently approximately 20 GRX operators exist globally, and it is expected that they will become IPX operators as well. This depends mostly on the cost of the new equipment and the demand for IPX services from the mobile operator community. In fact, the mobile operators are the main driver for the changes in the GRX network. With the introduction of all-IP network services, the current network topology and functionality of GRX does not meet the demands of the mobile carriers for quality, security, and accountability. The GRX as it exists today is bound to become a hindrance to the development and introduction of new services, unless it changes and become an IPX network. To mention but one reason, the GRX lacks security mechanisms, since it is assumed that all connected parties are trusted and no malicious actions are taken to compromise the network. This assumed trust and security are no longer guaranteed if the GRX is to be opened to all multimedia IP networks to interconnect.

Another issue is the changed and more sophisticated functionality of the DNS and ENUM services that are required for the IMS Interworking. These services are essential for the operators, since their network must be able to resolve telephone numbers (Tel URI) into SIP URI and vice versa in order to be able to establish IMS session across different domains and to help with the number portability issues. IPX will have to provide the Root DNS tree and the records populated in the databases within IPX DNS hierarchy for successfully implementing complete ENUM DNS based number portability solution. In addition, the mobile operators' view is that every user has a telephone number as a unique identifier and based on this number the PLMN network will be able through ENUM and DNS to find out the corresponding URI for all services available to the customer, such as VoIP.

Another important aspect is the usage of different versions of the IP protocol in the different parts of the topology. Operators who have sufficient numbers of IPv4 addresses would still use that address space, even though their core network elements are likely to be able to implement IPv6 already, in order to reduce the investments needed to reconfigure and to avoid possible interworking problems. Others, such as the operators in China (where IPv4 address space is extremely limited) will push for an all-IPv6 solution. This asymmetry in the situation of the mobile operators is the cause of many incompatibilities which in order to be overcome requires additional functionality such as NAT/NAPT, which increases the complexity of the network topology. It is a better solution to deploy IPv6 instead of NAT/NATPT, since the latter introduces the need to do special processing on all packets and as a result add delay. So the conclusion is that a transition to IPv6 should be made a soon as possible.

To conclude, before the Hub model is widely deployed many problems must be overcome, in order to motivate such a significant change. Nevertheless, there is no doubt, given the successful solution of all of these problems the Hub model of IMS Interworking has much to offer to all parties.

4. IMS Trials

Within the GSM Association (GSMA) there have been several tests or trials regarding interworking between IMS domains. GSMA has gathered expert groups from different companies and organizations to work with these interworking issues. The main objective of these trials has been to verify compatibility of different mobile access operators' IMS-networks. There are a number of different (1) vendors of IMS terminals, (2) mobile access operators, (3) GRX-providers, and (4) companies that develop SIP based applications; all of these players have to test their equipment for interoperability. When problems occur they should be forwarded to the relevant parties for investigation. This interoperability testing is very important to assure success of IMS services. The first trials have been done between several countries in Europe, but later expanded to include countries in Asia and in North America. Two different interworking models have been tested in the trials. These are the peer-to-peer model and the hub based model. Test campaigns of different TEL URI architectures have been done. These later campaigns tested different ENUM architectures with either the mobile operators by themselves handling the ENUM queries or a third party like an IPX Proxy operator handling the ENUM queries for a mobile operator. These tests were done in order to fasiciliate the feasibility to use an IPX proxy provider to provide ENUM service for an operator. Using ENUM, a TEL URI is converted to a SIP URI, thus making it possible for a PSTN user to set up a voice session to an IMS user. In all the trials the configurations were very simple in order to facilitate interoperability. Additionally the quality of service between the operators was not tested.

The first trials took place in the first quarter of 2005 in Europe [9]. In this trial the interconnection architecture was the focus. Both architectures were tested. The tests were between six mobile access operators using equipment from three major infrastructure vendors in different countries in Europe. The hub model was tested early in the trials to ensure that the IPX worked well from the beginning. That is why only one IPX proxy was tested in this first phase in the GRX network (see in figure 7). The experiments in both the peer-to-peer model and the hub based model tested different multimedia services, including Session-based video streaming, Session-based Gaming, and Voice Immediate Messaging. These tests were successful and showed basic IMS interoperability. The peer-to-peer structure and the IPX proxy (hub based) models are showed in Figure 6 and Figure 7.

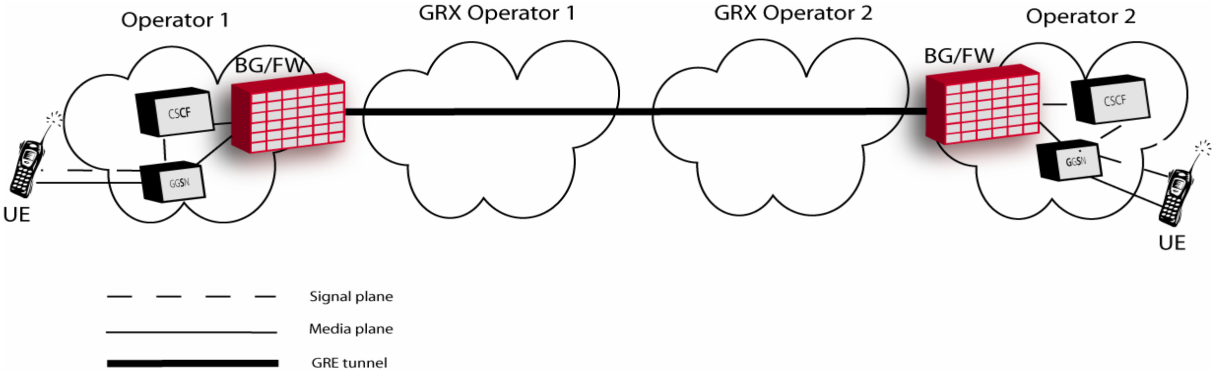


Figure 6. peer-to-peer

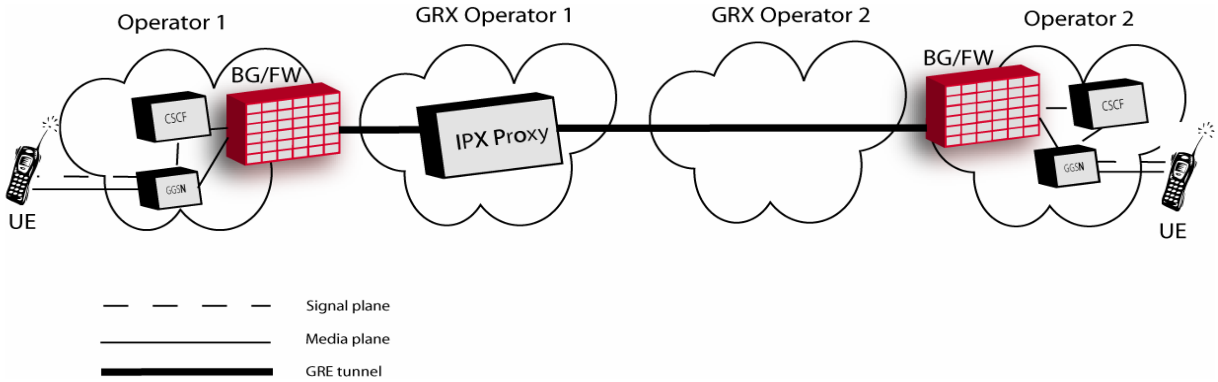


Figure 7. IPX Proxy

After the first quarter of 2005 trials expanded to Asia [10]. In these trials hub-to-hub connectivity including interworking between IPv6 IMS systems and between IMS IPv6 systems and IMS IPv4 systems were tested. Compatibility with existing billing systems and performance management systems were also included in these trials. The hub-to-hub model that was tested is showed in Figure 8. These tests also successfully demonstrated interworking between GRX providers via the inter-hub connectivity and interworking between mobile network operators. The trials in the second half of 2005 included verifying ENUM compatibility between operators. In the last quarter of 2005, GSMA demonstrated the use of TEL URIs as the destination address for user equipment.

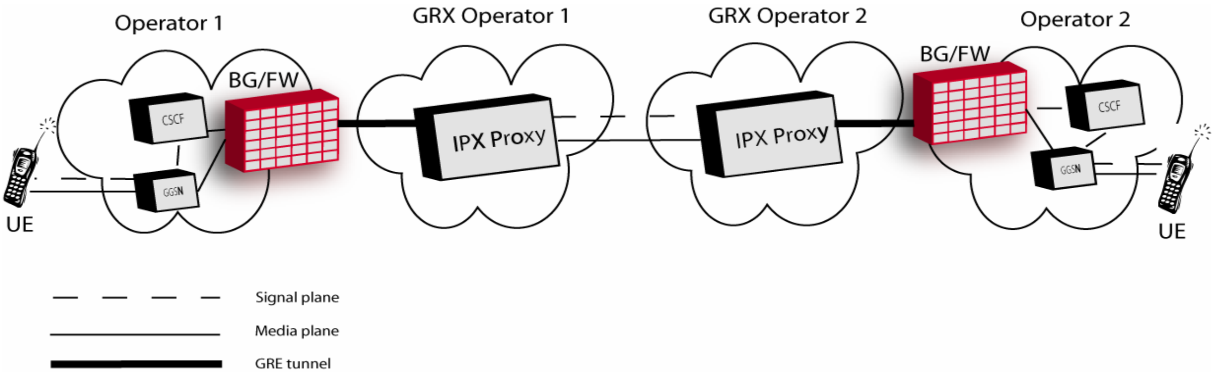


Figure 8. hub-to-hub

The last trial was a superset of all previous trials. This testing occurred in the first quarter of 2006 and it included three continents (Europe, Asia and North America) [11]. The main multimedia service that was tested across the national boundaries in this trial was Video Share services. Video share allows users to share their video clips or show live videos during a voice call to the called user.

In the second quarter of 2006 there were video share interoperability trials in China [25]. All the multimedia service tests were successful. The successes of all the trials from 2005 and later have proven the high level of interoperability. Additionally, multimedia services have been shown to work with equipment from different suppliers. Various trials will continue throughout 2006.

5. Carrier (Infrastructure) Domain Name System (DNS)

The Domain Name System (DNS) is one of the technologies on which the contemporary Internet heavily relies. Without DNS, it is doubtful at best if the Internet would have achieved the vast presence and importance it has today. Specified in several RFC documents, most notably IETF's RFC 1034 [64] and RFC 1035 [65], its job is to store and associate many types of information with *domain names*. As IP addresses are associated with interfaces and not nodes, it is important to note that domain names are associated with IP addresses and hence not necessarily associated with a node. A domain name is an alpha-numerical representation associated with a network interface, which is used when referring to an interface, instead of its hard to remember numerical IP address. The most important function of the DNS is to provide a translation between a specific domain name and the corresponding IP address to which that name should be associated. In addition to being easy for humans to remember, such a name representation of an interface, the domain name also allows for change of the geographic and network attachment point of a network node, thus effectively changing its IP address while keeping the same name, which makes the change largely transparent from user's perspective.

The move to the so called *All-IP world* has pushed many networking concepts and technologies, originally designed for the public Internet, to be adapted and introduced in the area of mobile communications. The great benefit is that through this adoption of well-known, tested technologies the gap between the wired and the wireless domains could be bridged, thus providing services to the mobile users, which already are taken for granted by users connected to the Internet. Apart from being vital for the global Internet, DNS as a technology has found important applications in the mobile world as well. It is critical for such services as the GPRS roaming, MMS, and IMS. One distinct difference of the DNS used within the mobile community is that its hierarchy is separated from that of the public Internet for security reasons – on the Internet everyone connected to the network has capability of interrogating the public DNS, while the DNS in the GRX network is only available to the "closed" community of service providers.

The following paragraphs deal with the implementation of the DNS functionality by the mobile operators and the GRX service providers. The DNS functionality of each mobile operator connected to the DNS of the public Internet is not within the scope of this document.

5.1. DNS Hierarchy

The DNS hierarchy is a well-know structure. Nevertheless, there are different components and functionalities in use at the different sites. The following paragraphs will introduce the general DNS hierarchy as well as its modifications and use in a mobile operator's environment.

5.1.1. Internet's Domain Name System

A domain name usually consists of two or more labels separated by a dot ('.') character. The least significant domain is on the left (the beginning of the domain name), and the most significant is at the end of the name (the last label on the right side). The most significant domains are also known as the *top-level domains*. This hierarchy is shown in Figure 9.

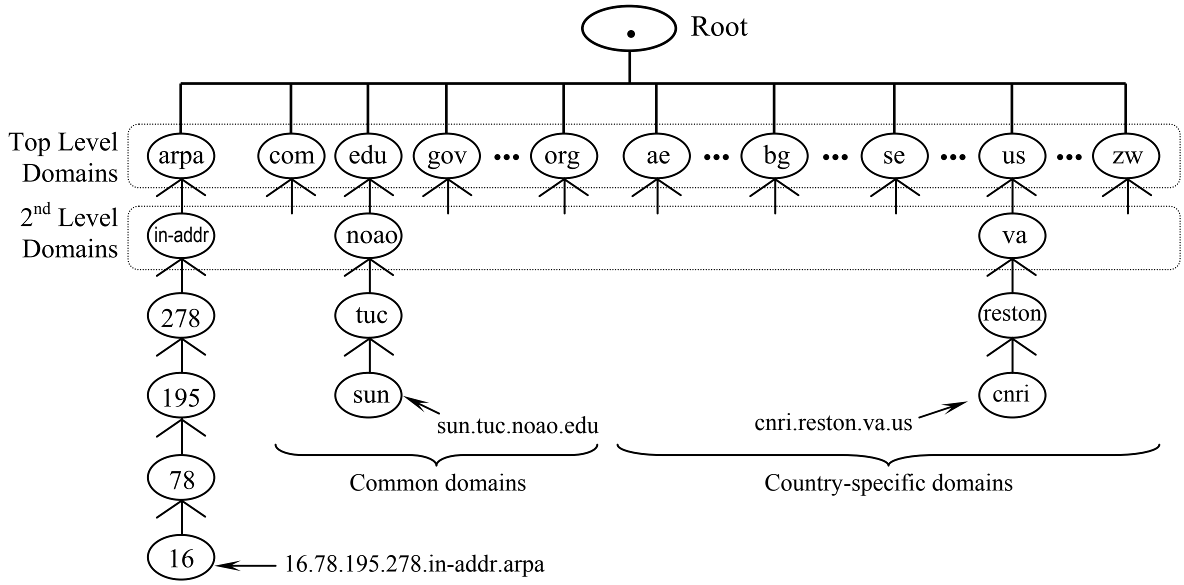


Figure 9. Domain name system – hierarchy

The Root domain holds information about all of the top-level domains (TLD). Associated with each of the TLD is one or more Nameservers, which hold information about all sub-domains belonging to that particular TLD.

A DNS Resolver, or as it is also known a DNS Client, is an entity that tries to resolve a domain name into an IP address or vice versa on behalf of the user. The resolver is normally connected to the local DNS server, which attempts to do the DNS look-ups on behalf of the resolver. It does so, by either looking in its own locally stored cache of previous queries or by forwarding the query to another DNS server. It is common that all DNS Servers cache results from previous queries for further use. The cache is kept for a preconfigured amount of time, which the server learns when it receives a response to a DNS query, after which it expires and future queries must be resolved by the usual DNS look-up process.

For security and redundancy reasons, there are two types of DNS Servers defined – master servers and slave servers. The master DNS server is the one that is currently authoritative for a particular domain and is serving all the queries. The slave DNS server is waiting to step in, in case there is a failure and the master DNS Server becomes unavailable. Usually, each domain has one master DNS server and one or more slave DNS servers. The information between them is shared, kept up to date, and synchronized in order to minimize disruption of this service.

Since there are billions of devices connected to the Internet, one could imagine that the amount of DNS queries is enormous. This could potentially threaten the integrity of the DNS hierarchy since the Root domain would be overwhelmed with DNS queries. In reality, there are thirteen Root DNS Servers which agree to accept DNS updates form the Internet Corporation for Assigned Names and Numbers (ICANN) accredited name brokers. ICAN itself operates the I-root server in California.

The naming concept is to use the letters from the English alphabet A to M dot character ('.') root-servers ('.') net. The reason why there are not more than 13 servers is due to the minimum size packet, which all internet nodes must be able to process, which leads to 512 byte payload limited for UDP [62]. The geographical sites that host the different servers could change when the circumstances demand such a change. In recent years, many countries and regions have started to host *mirrors* of one or more Root DNS Servers in order to improve the quality and availability of the service. Most of these mirror sites are located in South-East Asia.

5.1.2. DNS in PLMN IMS site

The DNS functionality at a mobile operator's site is characterized by the specific relationship an operator has with its customers and peers. Figure 10 shows a schematic of the main DNS traffic flows in operator's network.

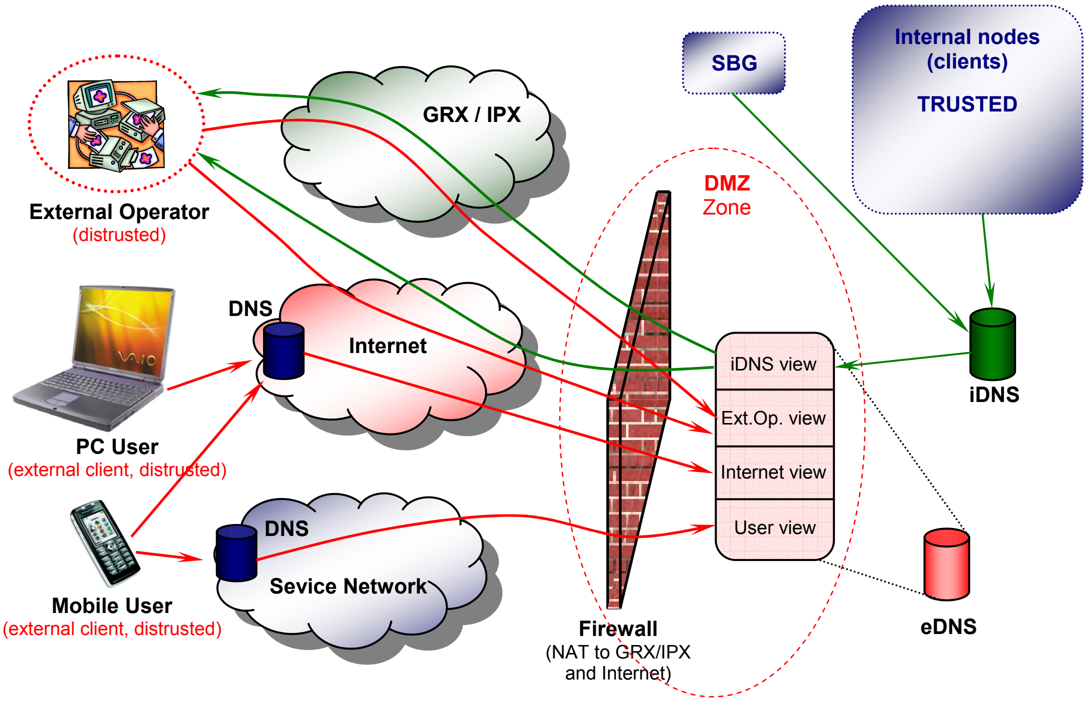


Figure 10. DNS functionality at operator's site

Probably the first fact to mention is that the DNS functionality in the operator's network is split into several parts. An operator has its core network, which has interfaces to other mobile operators, the Internet, and its own subscribers. Each one of these interfaces requires different DNS services, as explained in the following paragraphs.

The core network (CN) of an operator is considered to be one of their most important assets. The entire business of that operator depends on the reliable and uninterrupted service this CN provides. To guarantee such high availability and to guarantee security the DNS which serves the CN is split in two parts: the so called *internal DNS* (iDNS) and the *external DNS* (eDNS). As the names suggest, the iDNS serves internal clients while the eDNS serves the external clients. These two categories are probably better defined respectively as *trusted* and *distrusted* clients.

The *internal* or *trusted* clients are usually the network nodes, which comprise the operator's CN. For all their DNS needs, they rely on the iDNS only. These nodes should not query any DNS other than the iDNS. Furthermore, when the address of an internal node is requested by a node external to the CN, the response to that query should be handled through the eDNS functionality.

The eDNS resides in the operator's CN, but it has the responsibility to provide service to the external DNS hierarchies. As it is shown on Figure 10, the eDNS could be configured to provide different "views". A view allows the DNS server to provide different functionality depending on the client accessing it. So in a way, the *iDNS view* within the eDNS would provide information about the nodes in the CN only to those clients, which match the current list of allowed clients. The *external view* would serve for example, other network operators, which generate DNS traffic to this operator. The *Internet view* would serve clients that reside in Internet, or other DNS servers situated in the public domain, as part of the Internet DNS hierarchy. Finally, the *user view* would serve the operator's own subscribers whenever they require DNS services, e.g. in case the UE has to resolve FQDN of P-CSCF during the P-CSCF discovery phase, or in case the Subscriber wants to resolve public Internet domains/IP addresses.

Different mobile operators could interconnect in several different ways, for example through the dedicated inter-operator network GRX/IPX or through the public Internet if they so choose. In Figure 10, the red colored arrows represent the inbound traffic flows, while the green colored arrows represent the outbound traffic flows. For simplicity, the outbound traffic for Internet clients and the operator's own subscribers is omitted. As it is also shown in the same figure, both Internet clients and the operator's subscribers do not interact directly with the eDNS. Instead, they utilize the existing DNS functionality in their respective networks.

The Firewall shown in Figure 10, provides additional security and protection, thorough its NAT/NATPT functionality, thus effectively "hiding" the addresses of the vital network nodes and minimizing the risk exposure. The NAT functionality is also necessary because of the different types of IP addresses required by the different networks. The eDNS is usually situated in the so called *Demilitarized Zone* (DMZ zone), while the iDNS responsible for the IMS core network, is placed behind the IMS Firewall, not shown on figure 10, for simplicity. DNS architecture in the GRX / IPX network

The DNS hierarchy of the GRX domain has been debated for many years. Name and address resolution have always been a challenge that the GRX and GPRS operators have faced. In the last couple of years there have been improvements and a move towards a single master root DNS, which mimics the DNS hierarchy of the public Internet. While a *single* DNS root is necessary for the public Internet in order to keep it consistent and to keep it as a global network, as argued in RFC 2826 [63], this document does not preclude private networks, such as the GRX, from operating their own private DNS hierarchy.

Figure 11, displays the DNS architecture as it is implemented within the GRX/IPX network. The justification for such architecture is the requirement for complete separation of the GRX's DNS from the public Internet DNS.

The master root DNS contains information about the registered sub-domains used within the GRX community. It is populated with information by the operators, GRX service providers, or GRX operators acting on behalf of an operator.

Policing and validation is conducted by the GSM Association to assure the accurate delegation of sub-domains [22]. This root DNS is necessary in order to provide global interworking between GPRS operators. Furthermore, the GPRS operators have been struggling to find a proper model for an ENUM service to be deployed as well. With the introduction of SIP based services it has become imperative to resolve telephone numbers (expressed as a Tel URI) into a SIP URI and vice versa. Currently, as stated in IR.67 [22], several models for Carrier ENUM (where operator or also called private ENUM) have been developed. There is ongoing discussion within the community which model is most suitable for a Carrier ENUM on GRX. ENUM is also important for tackling such issues as the mobile number portability. More about ENUM is given in section 5.3.

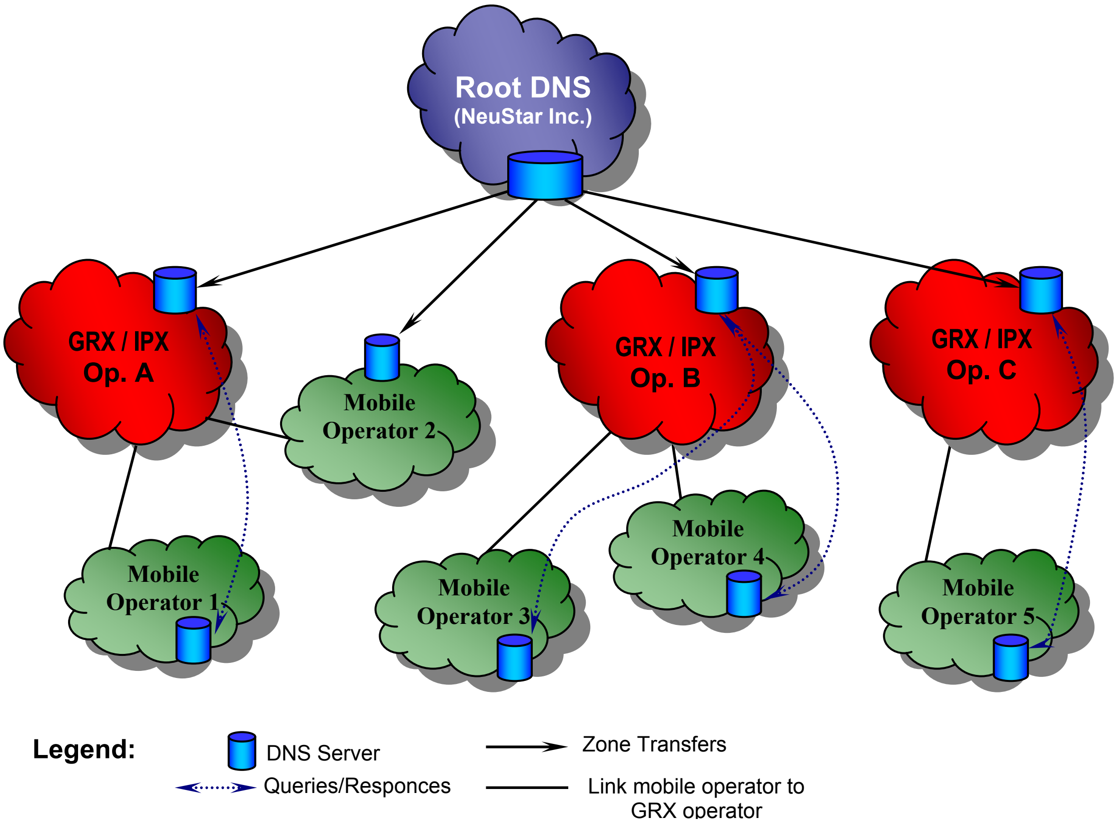


Figure 11. DNS architecture in GRX / IPX network

The GRX operators provide to their connected GPRS operators a root DNS service. This root DNS is known as slave root DNS is operated by the GRX service provider and must be replicated within the GRX network to provide redundancy. It is not mandatory that the slave root DNS is operated by a GRX operator. Instead GPRS operators might choose to provision their own slave root DNS. All slave root DNSs are synchronized with the “back-end” master root DNS server in a process known as *Zone Transfer*, which is necessary to ensure the information integrity throughout the GRX and GPRS networks. This DNS is necessary in order to resolve the name of the access points, authoritative DNS servers, and other equipment such as border gateways, SGSNs, and GGSNs, etc. into an IP address to facilitate the interworking between the different network operators.

All of the network nodes within the GRX and GPRS networks, which have to be visible from outside their network, must use unique public IP addresses on their respective interfaces. This requires that each operator has a unique address space reserved from an official Internet addressing authority. The reason is that the current NAT implementations cannot change/translate the IP address of packets carried inside a GTP tunnel. This could be a problem in roaming scenarios when the SGSN's IP address in PDP context activation request is carried inside a GTP tunnel.

5.2. DNS Requirements

Because of the nature and the specifics of the networks in the mobile world, there are numerous requirements that need to be satisfied before DNS could be utilized successfully in the interworking scenarios. The main reference document for such requirements is the GSM Association's PRD IR.67 [22]. Furthermore, each document describing new IP services to be deployed in the mobile networks contains DNS guidelines specific to the services in question. Examples of such documents are IR.52 MMS Interworking Guidelines [23] and the IR.65 IMS Roaming and Interworking [14]. Since DNS is already in use within the GRX community and the mobile operators have been using it, it is likely that some of the requirements are already satisfied, while others need to be implemented for successful IMS interworking.

5.2.1. GPRS Network specific

R1 - The master and the slave DNS servers within the operators' networks should be separated physically to enhance the availability of the service.

R2- The DNS must support new sub-domains of type *.mnc<MNC>.mcc<MCC>.3gppnetwork.org* in order to be able to support SIP clients on terminals which do not have access to an ISIM. The values of *Mobile Number Code* (MNC) and *Mobile Country Code* (MCC) are given to the operator by *International Telecommunication Union Telecommunication Standardization Sector* (ITU-T) and their national numbering authority. These domains are usable only inside the GRX network.

R3 - The DNS needs to support the domain *.e.164enum.net* in order to facilitate the carrier ENUM functionality. Numerous sub-domains are defined, which follow the ITU-T E.164 number hierarchy of *Country Code* (CC), *National Destination Code* (NDC) and *Subscriber Number* (SN). This domain is usable only inside the GRX network.

***R4* -** ENUM service is needed to be able to convert a TEL URI (E.164) into a SIP URI.

R5 - Support for NAPTR type of records is necessary because of the ENUM service. SRV resource record functionality is needed to resolve SIP URIs to SIP servers, to provide for load balancing, announcement of the port the SIP server is using, and if necessary to support domain name rewriting.

R6 - The DNS software needs to handle big files. This is due to the files of the ENUM service, which could contain enormous numbers of resource records.

R7 - The DNS must be dimensioned with respect to the expected traffic volume increase. This applies to both the hardware and software as well as for the speed of the corresponding interfaces.

R8 – The GPRS operator’s DNS is connected to the GRX network, but must not be reachable from the Internet nor should it be able to resolve domains which belong to the public Internet.

R9 – DNS needs to support both IPv4 and IPv6 addresses, reserved for use within the GRX, and not visible to the public Internet. DNS server which provides responses with *A* and *AAAA* records must also be reachable with both versions of the IP protocol.

5.2.2. GRX/IPX Network specific

All of the above cited DNS requirements specific for a GPRS network are valid for the DNS implementation in the GRX/IPX network as well. Requirements 10 to 12 are cited separately to emphasize on the specific importance of each of them.

R10 - The master and the slave DNS servers within the GRX operators’ networks must be separated physically to provide redundancy. The usual requirements for secondary and primary DNS servers are valid as well.

R11 - The DNS needs to support the new domain .3gppnetwork.org in order to be able to resolve the corresponding operators’ sub-domains for each of the services introduced under this domain such as IMS. This domain is usable only inside the GRX network.

R12 - The GRX DNS hierarchy must not be reachable from the Internet and vice versa.

5.3. ENUM

ENUM stands for Telephone Number Mapping. IETF have defined a mechanism for converting a E.164 number, also known as Tel URI into an address, which could be used in IP network environment. Described in RFC 3761 [24] it defines the way the E.164 numbers are stored and related to services available to a specific number by means of DNS. This mechanism is known as ENUM.

The process of translating a Tel URI into a domain name consists of several steps, and could be described as follows:

At first, the number is written in its full form, including the country code:

+46789123456

In case the number is in a national format, it must be converted into international format (by removing the leading characters and adding the country code and the + sign) prior to attempting ENUM resolution.

After that, the + sign is removed and the digits are separated by a dot (“.”) character:

4.6.7.8.9.1.2.3.4.5.6

The next step is to reverse the order of the digits and to append at the end the appropriate top level domain:

6.5.4.3.2.1.9.8.7.6.4.e164.arpa , or

6.5.4.3.2.1.9.8.7.6.4.e164enum.net .

The first TLD - *e.164.arpa*, is used when the so called public ENUM is used, while the second TLD – *e164enum.net*, is used when the private or as it is also known – the Carrier ENUM is used.

The International Telecommunication Union (ITU) utilizes a specific zone, namely "*e164.arpa*" for use with E.164 numbers. This domain name is used for the public ENUM service, which utilizes the public DNS infrastructure on Internet. The idea is that any international phone number could be translated into a Universal Resource Identifier (URI) by following the algorithm described above. Then, with the help of DNS, this URI could be resolved into one or more internet addresses for services such as Voice-over-IP (VoIP). There is another type of ENUM referred to as Private or also Carrier ENUM, mentioned in the previous paragraph. There are several differences between the public and the private ENUMs, but the most significant is that the private ENUM uses "*e164enum.net*" for a top level domain, which is owned by the GSM Association, and it utilizes the private DNS infrastructure on GRX, instead of the public one on Internet.

The following table gives a comparison between the public and the private ENUMs.

Table 1. Comparison between Public and Carrier (private) ENUM

	Used DNS tree	**Purpose of the ENUM**	**Accessed by**	**Top Level Domain**	**Data populated by**	**Respon-sibility for updates**	**Type of data**
Public ENUM	**Public DNS, the same as on the Internet**	To provide on-line directory service for end users	Public, anyone	**E164.arpa**	Users, it is a voluntary process. Users can choose what data to add or remove	**Users - could be out of date**	May contain personal information, may contain technical data as well
Carrier ENUM	**The GRX / IPX DNS hierarchy. Only available within the operator community**	To provide routing enabling technology	Only by members of the operator community. Not reachable by the end users or Internet users	**e164enum.net**	Operators	**The owning operator**	Strictly technical data, crucial for the services. No personal data.

The available services for a particular E.164 number are stored in the DNS by using a *Network Authority Pointer* (NAPRT) record. They are defined in RFC 2915 [25], and could be used by other services as well. NAPTR records contain one or more URIs which point to the services available to the resolved E.164 number. One example is returning a SIP URI that corresponds to a specific Tel URI, to be used be IMS services.

The NAPTR records, their structure and functions are described further in section 5.3.3.

5.3.1. ENUM DNS structure

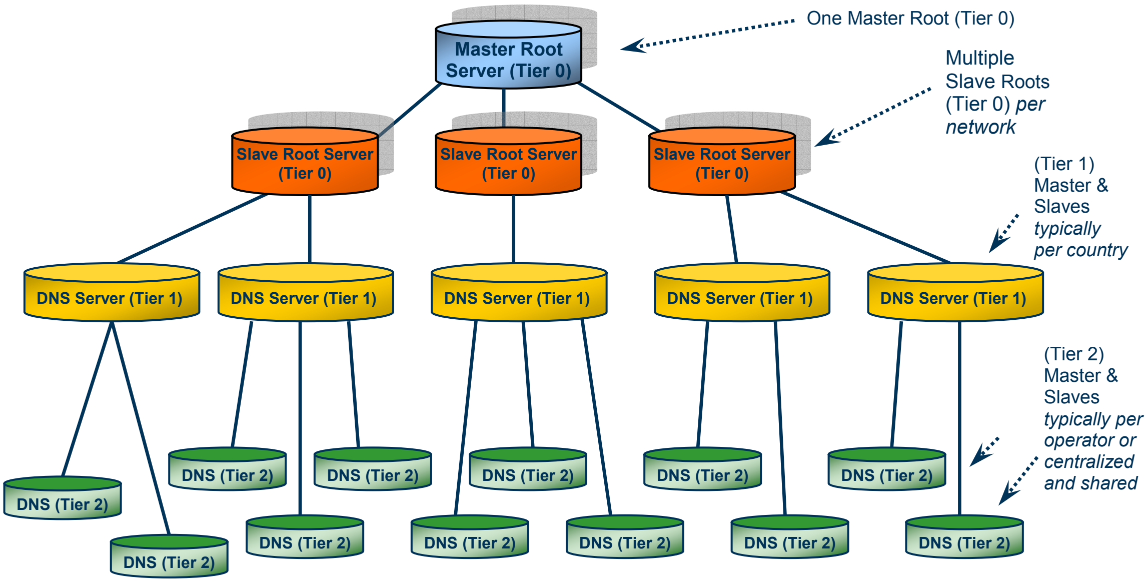
Similar to the DNS hierarchy, the ENUM structure is represented by a single tree. This was designed, in order to secure proper integration with the DNS hierarchy and to provide for a scalable solution. The ENUM hierarchy usually consists of three levels, also known as *tiers*. Figure 12, shows the ENUM tiers and how it is integrated within the DNS tree.

The first of tiers, the one that is on top of the tree, is *Tier 0*. This tier is responsible on a global level, usually integrated with the Root DNS. It is authoritative for the top level domain – either *e.164.arpa*, or *e164enum.net*. It contains pointers to the next level in the hierarchy – *Tier 1*.

Tier 1 is usually deployed on a country level, meaning that it is authoritative for a country code. It is integrated with the DNS that is authoritative for the whole country. An example could be a domain name such as *6.4.e164.arpa*, for a country code +46.

The third and lowest level in the ENUM Tier hierarchy is *Tier 2*. It is usually deployed on a per operator basis, meaning that it serves only a particular PLMN operator. Another alternative is to have centralized Tier 2 for all PLMN operators within one country. However, given that there is extensive number portability, it is better to facilitate Tier 1 instead of Tier 2 servers for ENUM resolution.

The tiers could be combined or further separated if it is necessary or the circumstances in some country demand such separation, or a service, e.g. Number Portability requires it.


One Master Root (Tier 0)
Master Root Server (Tier 0)
Multiple Slave Roots (Tier 0) per network
Slave Root Server (Tier 0)
Slave Root Server (Tier 0)
Slave Root Server (Tier 0)
(Tier 1) Master & Slaves typically per country
DNS Server (Tier 1)
DNS Server (Tier 1)
DNS Server (Tier 1)
DNS Server (Tier 1)
DNS Server (Tier 1)
(Tier 2) Master & Slaves typically per operator or centralized and shared
DNS (Tier 2)

Adapted from: GSM Association IR.67, *DNS Guidelines for Operators v1.2*

Figure 12. Overall structure and distribution of the ENUM Tiers with respect to the Infrastructure DNS hierarchy.

Although all of the necessary functionality exists today, it is important to mention that there is no implementation of a Carrier ENUM yet. There are ongoing discussion within the GSM Association and other institutions, about how to provide the Carrier ENUM functionality within GRX/IPX.

5.3.2. Mobile number portability

Mobile number portability (MNP) is the process which enables a customer of one PLMN operator to switch to another PLMN operator while retaining their telephone number. A similar portability exists for the old, wire-line telecoms, where it is called Local number portability (LNP) or simply Number Portability (NP). Since small differences exist in the way porting is handled in the wired and wireless worlds, it is important to refer to the mobile number portability as MNP.

Currently, MNP and LNP are implemented by using centralized (in most cases) databases, on a national level. Number portability as a service is applicable only within one country. Porting numbers internationally has not been defined. These databases are populated with the ported numbers and, a routing number to the recipient network is given.

When a user dials a number, the network checks if this is a local number or not. If it is a local number, then a query to the national NP database is made, to find out whether the number has been ported or not. If the number indeed has been ported, the NP database responds with the new number including the routing number necessary to reach the recipient network. Then the call is routed towards the network responsible for terminating the call. If there is no information about this number is in the national NP database, then the network tries to route the number further and establish a call, based on the original routing information provided by the number.

To be able to support successfully the number portability function, most networks employ the mechanisms known as *All Call Query* (ACQ) and *Onward Routing* (OR) (also known as *call forwarding*).

The ACQ means that the originating network checks the number in the NP database and then routes the call directly to the terminating (recipient) network. It is regarded as the most complicated way to provide NP, and is associated with high cost when using legacy databases. Despite this, for example in Sweden it is the requirement method. On the other hand, OR method is regarded as the simplest way to introduce NP. This method means that the originating network connects to the donor network and in case the number has been ported, the donor network must route further and complete the call. This method is considered to be a short-term solution while the ACQ method is seen to be a long-term solution. The latter requires a centralized NP database to which all operators are connected, and while this poses some technical difficulties, it also requires significant managerial efforts and cooperation on a national level. Nevertheless, there are such entities that operate nowadays. There are variations of these methods, called *Query on release* and *Call drop back.*

All of the above describes a complicated way of delivering NP functionality, using external databases and methods which impose technical, managerial, and financial burden on the PLMN operators.

The GSM Association has proposed a new, different approach to providing MNP using only the ENUM DNS mechanism. This method is explained in the following section.

5.3.3. MNP Scenarios with Carrier ENUM

Number portability is a service available within a single country, as was mentioned before. As a consequence, the implementation of the service is specific for that country and may differ from the implementation in another country. Nevertheless, there are two major organizations that the NP implementation could belong to. The first one is where a central database is used to store the information (either in one place or locally to each operator) and the second choice is where centralized database does not exist and information is distributed between the operators. The GSM Association has outlined 4 different scenarios, which could be used to implement MNP using ENUM DNS [22].

5.3.3.1 Scenario 1: Centralized authoritative database

This scenario uses a combined Tier 1 and Tier 2 of the ENUM structure, thus effectively creating one ENUM DNS, which is authoritative for all subscribers in a country. All URIs and URLs are centrally stored and managed.

> For example, if a subscriber of mobile operator (MO1) in Sweden has a number *+46789123456*, his SIP URI (used for IMS) could be:
>
> *sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org*

This SIP URI will be provisioned in his ENUM record in the centralized MNP database:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
        6.5.4.3.2.1 NAPTR 10 10 ”u” ”E2U+SIP”
                ”!”^.*$!sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org!”.
```

If this customer moves to another operator, MO2, in the same country, then his record in the centralized database will be modified to reflect the change in his SIP address:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
        6.5.4.3.2.1 NAPTR 10 10 ”u” ”E2U+SIP”
                ”!”^.*$!sip:+46789123456@ims.mnc002.mcc240.3gppnetwork.org!”.
```

The obvious result in this scenario is that the data-fill for such centralized DB could be enormous. The widely used BIND DNS might not be capable of coping with such a load. This requires that specialized ENUM DNS must be used [22].

The scenarios with centralized database stipulate that all subscriber numbers have to be provisioned in the database, no matter whether they are ported or not. This is valid both for this scenario and for Scenario 4, described in paragraph 5.3.3.4.

The above scenario is most suitable for countries, which already have a centralized NP database.

5.3.3.2 Scenario 2: Change of domain name in URIs/URLs in Tier 2

This scenario describes solution where the ENUM Tiers are kept separate, but is similar to Scenario 1, because it also involves changing the individual NAPTR record corresponding to a specific Tel URI, to reflect the change of operators.

> For example, if a subscriber of mobile operator (MO1) in Sweden has a number *+46789123456*, his SIP URI (used for IMS) could be:
>
> *sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org*

This SIP URI will be provisioned in his ENUM record in the MO1’s Tier 2 DNS:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
        6.5.4.3.2.1 NAPTR 10 10 ”u” ”E2U+SIP”
                ”!”^.*$!sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org!”.
```

If this the customer moves to another operator, MO2, in the same country, then his record in the MO1’s Tier 2 DNS will be modified to reflect the change in his SIP address:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
```

```
          6.5.4.3.2.1 NAPTR 10 10 ”u” ”E2U+SIP”
                    ”!”^.*$!sip:+46789123456@ims.mnc002.mcc240.3gppnetwork.org!”.
```

The big disadvantage of this solution is that a recipient network is absolutely dependent on the donor operator to correct its records at the time when the number is ported, and in all future instances, when new services are available to the subscriber in the recipient network, but the donor network must change its NAPTR records to provision for these new services.

Also, in order to provide MNP solution, in this scenario, all PLMN operators who offer number portability as a service, must have their Tier 2 ENUM DNS fully operating. If a new operator wants to join the MNP mechanism, it also must have its ENUM DNS fully provisioned, prior the activation of the MNP service, which is generally a regulatory requirement in most countries today.

Given the manner in which the NAPTR records are distributed among the operators, it is safe to conclude that this option is more suitable for countries which have never used centralized NP database. The disadvantage is that the operators become too mutually dependent, since even if an operator's own DNS is working their customer might not be able to get calls unless the donor's DNS is working as well.

5.3.3.3 Scenario 3: Redirection at Tier 2

In this scenario, Tier 1 and Tier 2 of the ENUM structure are also kept separate. However, the Tier 2 DNS server stores for each ported number a redirection pointer for all incoming queries, effectively redirecting the query to the recipient network. This redirection is realized by using single NS record, which when returned to the DNS resolver will result in a new DNS query, towards the recipient network’s ENUM DNS.

> For example, if a subscriber of mobile operator (MO1) in Sweden has a number *+46789123456*, his SIP URI (used for IMS) could be:
>
> *sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org*

This SIP URI will be provisioned in his ENUM record in the MO1’s Tier 2 DNS:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
          6.5.4.3.2.1 NAPTR 10 10 ”u” ”E2U+SIP”
                    ”!”^.*$!sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org!”.
```

If the customer moves to another operator, MO2, in the same country, then his record in the MO1’s Tier 2 DNS will be modified to reflect the change in the following manner:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
                    6.5.4.3.2.1  IN  NS  dns1.mnc002.mcc240.e164enum.net
```

In the DNS server of MO2, this user will be provisioned with a record, which would look as follows:

```
$ORIGIN 6.5.4.3.2.1.9.8.7.6.4.e164enum.net.
          NAPTR 10 10 ”u” ”E2U+SIP”
                    ”!”^.*$!sip:+46789123456@ims.mnc002.mcc240.3gppnetwork.org!”.
```

The advantages and disadvantages of Scenario 2 are valid for Scenario 3 as well. All of the operators must have their ENUM DNS started. Nevertheless, in this scenario, the recipient operator still depends on the donor operator to implement the changes in its records, but here this dependence is only once, since the actual NAPTR records for a subscriber are managed by the recipient operator.

5.3.3.4 Scenario 4: Central re-direction database

Similar to Scenario 1, this scenario requires combining Tier 1 and Tier 2 of the ENUM structure. What is different is that instead of having all numbers in the country provisioned in the central database with their respective NAPTR records, the database contains only a redirection pointer towards the corresponding operator's DNS. This is similar to Scenario 3. As a result all NAPTR records concerning a specific subscriber are kept and managed by the subscribed operator.

> For example, if a subscriber of mobile operator (MO1) in Sweden has a number *+46789123456*, then the record in the centralized database could be:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
                6.5.4.3.2.1  IN  NS  dns1.mnc001.mcc240.e164enum.net
```

This record will be provisioned in the ENUM record of the MO1's Tier 2 DNS:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
        6.5.4.3.2.1 NAPTR 10 10 ”u” ”E2U+SIP”
                ”!”^.*$!sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org!”.
```

If this customer moves to another operator MO2 in the same country, then his record in centralized DB will be modified to reflect the change in the following manner:

```
$ORIGIN 9.8.7.6.4.e164enum.net.
                6.5.4.3.2.1  IN  NS  dns1.mnc002.mcc240.e164enum.net
```

In the DNS server of MO2, this user will be provisioned with a record, which would look as follows:

```
$ORIGIN 6.5.4.3.2.1.9.8.7.6.4.mnc002.mcc240.e164enum.net.
        NAPTR 10 10 ”u” ”E2U+SIP”
                ”!”^.*$!sip:+46789123456@ims.mcc240.e164enum.3gppnetwork.org!”.
```

This scenario gives full control over the NAPTR records, to the recipient operator, and at the same time, eliminates the dependence on the donor operator to update its records. Only the Tier 1 ENUM DNS, must update the redirection pointer to reflect the change in the subscriber's mobile operator.

Figure 13 shows ENUM hierarchy, implemented in two countries X and Y. Country X has implemented the Distributed storage approach, described in Scenarios 2 and 3, while country Y has implemented the centralized MNP DB solution.

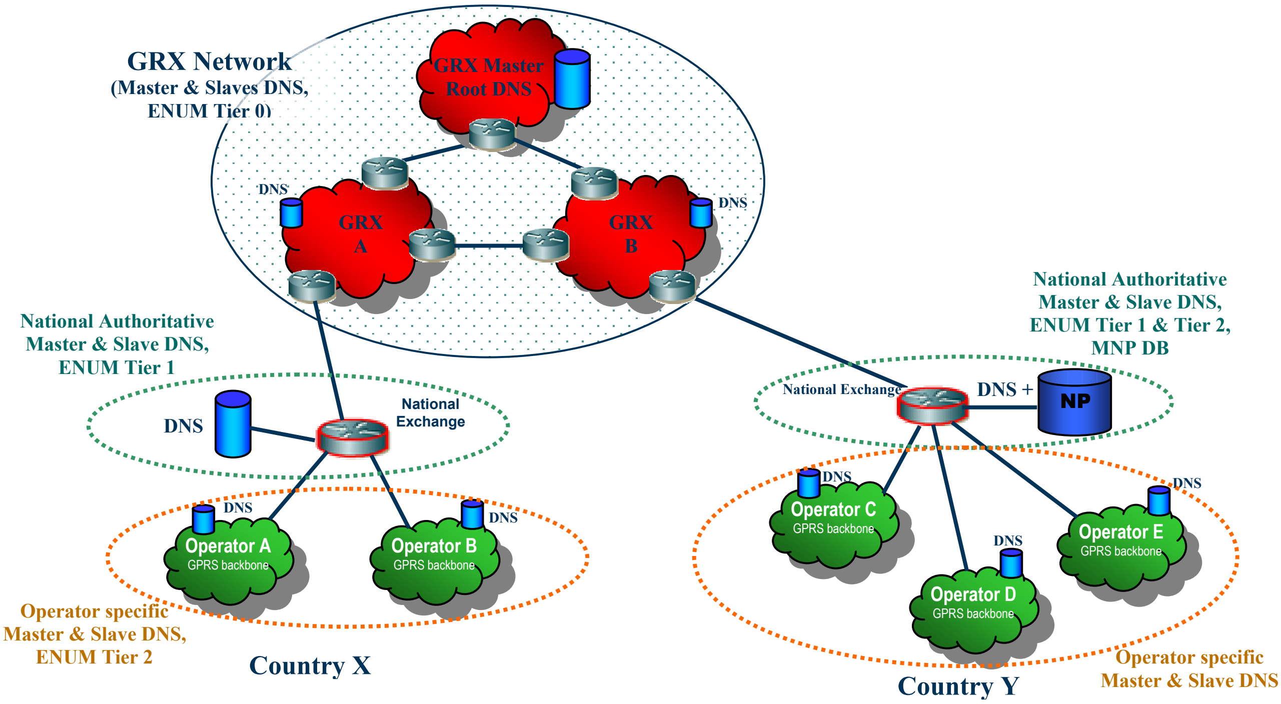


Figure 13. ENUM hierarchy, MNP with Distributed storage and Centralized NPDB solutions

The main concerns about the above described scenarios are the size of the data-fill, which a centralized database might have, the requirement that all numbers in the country must be provisioned in the centralized DB, which might be controversial, since many operators consider the customer base to be sensitive information (although this information could be dynamically obtained by the other operators simply by performing DNS look-up for every number assigned to that operator), and last but not least – the increased number of DNS queries necessary, for example, to resolve a Tel URI into SIP URI and to implement MNP.

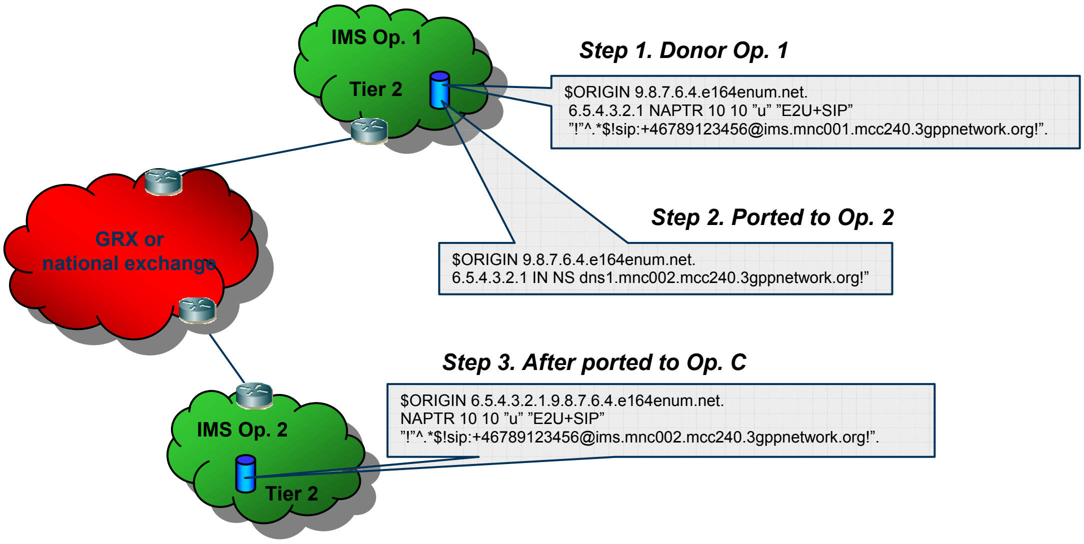
5.3.4. MNP with Distributed database

As it was mentioned before, the distributed ENUM DNS MNP database approach is considered to be a short term solution for providing MNP service. Its advantages are that it does not require expensive infrastructure and significant level of cooperation on a national level. On the other hand the big disadvantage that this approach has is that it always makes the recipient network dependent either totally or to some extent on the donor operator.

This approach does not scale well. It might work in countries with 2 or 3 PLMNs and small amount of subscribers, but in case of bigger countries, where more than 5 operators might be present and the total customer base could be tens of millions, the distributed number portability database could prove a real obstacle and a management burden.

There is not much space for improvements, when a distributed approach is selected for providing MNP. In this case, the originating network must always contact the donor network, which then will have to decide whether to terminate the call, or to respond with further information and return routing information to the originating network, which will have to decide how to route the call further to the actual terminating network.

Still, Scenario 3 – Redirection at Tier 2, has obvious advantages over Scenario 2, since in this case, the recipient operator is dependent on the donor operator only while the number porting is in progress. Once the donor operator has populated its database with the correct routing pointer towards the DNS of the recipient operator, the latter have full control over the services it can offer to the ported subscriber.



```
$ORIGIN 9.8.7.6.4.e164enum.net.
 6.5.4.3.2.1 NAPTR 10 10 ”u” ”E2U+SIP”
 ”!”^.*$!sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org!”.
```

```
$ORIGIN 9.8.7.6.4.e164enum.net.
6.5.4.3.2.1 IN NS dns1.mnc002.mcc240.3gppnetwork.org!”
```

```
$ORIGIN 6.5.4.3.2.1.9.8.7.6.4.e164enum.net.
NAPTR 10 10 ”u” ”E2U+SIP”
”!”^.*$!sip:+46789123456@ims.mnc002.mcc240.3gppnetwork.org!”.
```

Figure 14. MNP, Redirection at Tier 2, Distributed storage solution.

Figure 14 illustrates Scenario 3 – redirection at Tier 2, described in paragraph 5.3.3.3.

In the beginning – step 1, Operator 1 has the authority over the provisioning records for a subscriber. After this subscriber decided to move to Operator 2, its donor operator must implement changes in its records, introducing the redirection pointer towards the recipient operator’s DNS – this is step 2. In step 3, the recipient operator has provisioned a NAPTR record for the ported subscriber in its DNS. With this step, number is considered ported.

5.3.5. MNP with Centralized database - modification proposal

The centralized database models for providing MNP are considered to be more sophisticated than the solutions with distributed storage on the NP information. In addition, it must be mentioned that most of the countries which have number portability implemented already, have done it using a centralized database on a national level. This approach has its advantages such as centralized storage and management and clear procedures to check if the number has been ported or not.

On the other hand, it introduces higher requirements towards the infrastructure and the capacity for processing and management. As it was already mentioned, the centralized database solution has one characteristic that concerns the mobile operators. It is the requirement to have the records for every customer of every operator stored together at combined Tier 1/Tier 2 centralized DB. This requires that operators reveal information about their customer base, which they consider as confidential information. In addition, Solution 1 that was presented in the previous chapter demands that all the records, including the NAPTR records are also centrally managed and stored.

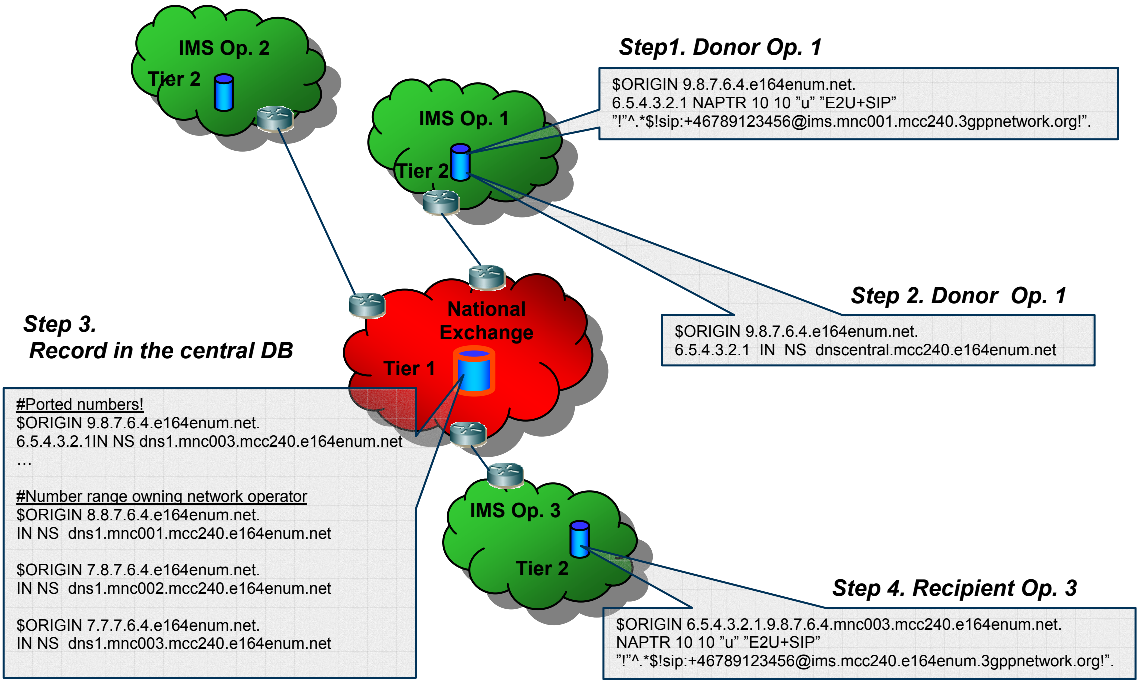
Solution 4 makes some improvements on Solution 1, by storing only a redirection pointer at the centralized database, while the actual NAPTR records are stored in the corresponding operator's network, which gives more control to the actual subscribed operator over the services it provides to its customers. Nevertheless, both Solution 1 and Solution 4 require combined Tier 1 and Tier 2 from the ENUM hierarchy. Such combined database might have a large volume of information, which cannot be managed with the widely used BIND DNS implementation, thus the need to invest in a specialized ENUM/DNS commercial solution [22].

Figure 15 illustrates a proposal solution, based on modification and combination of Solution 3 and Solution 4 described in the previous chapter. The main goal with this modification is to address the concerns of the operators regarding their confidential information, while still keep a centralized mechanism for implementing the MNP. This proposal scenario relies on centralized DB to store *only* the ported numbers of all operators in the country.

Furthermore, it does not store the actual NAPTR records per user, but rather stores a redirecting pointer towards the authoritative for that number ENUM DNS. In case a number has been ported, the donor operator modifies its records, to include a pointer towards the centralized database, which contains further routing information. Effectively, this creates a MNP scenario with redirection at Tier 1 and Tier 2.

In addition, by keeping a pointer at the donor operator's DNS towards the centralized DB, this scenario gives choice to the mobile operators which source to interrogate first when a call is being established. In situations, where the volume of the ported subscribers in a country is relatively low, the operators may safely assume, that the number they are trying to reach is still in its number range owning network, and route the call to it to be terminated. In case the number happens to be ported, then a redirection pointer is returned and new attempt for ENUM resolution occurs.

When the volume of ported numbers reaches a certain threshold, it might be more effective for the operators to assume that a number will be considered ported by default, and the place to look for further routing information will be the centralized MNP database. If there is no record about that particular number in the database, then the number owning operator will be contacted to terminate the call.



Step1. Donor Op. 1

```
$ORIGIN 9.8.7.6.4.e164enum.net.
6.5.4.3.2.1 NAPTR 10 10 ”u” ”E2U+SIP”
”!”^.*$!sip:+46789123456@ims.mnc001.mcc240.3gppnetwork.org!”.
```

Step 2. Donor Op. 1

```
$ORIGIN 9.8.7.6.4.e164enum.net.
6.5.4.3.2.1  IN  NS  dnscentral.mcc240.e164enum.net
```

Step 3.
Record in the central DB

```
#Ported numbers!
$ORIGIN 9.8.7.6.4.e164enum.net.
6.5.4.3.2.1IN NS dns1.mnc003.mcc240.e164enum.net
…

#Number range owning network operator
$ORIGIN 8.8.7.6.4.e164enum.net.
IN NS  dns1.mnc001.mcc240.e164enum.net

$ORIGIN 7.8.7.6.4.e164enum.net.
IN NS  dns1.mnc002.mcc240.e164enum.net

$ORIGIN 7.7.7.6.4.e164enum.net.
IN NS  dns1.mnc003.mcc240.e164enum.net
```

Step 4. Recipient Op. 3

```
$ORIGIN 6.5.4.3.2.1.9.8.7.6.4.mnc003.mcc240.e164enum.net.
NAPTR 10 10 ”u” ”E2U+SIP”
”!”^.*$!sip:+46789123456@ims.mcc240.e164enum.3gppnetwork.org!”.
```

Figure 15. MNP, Centralized NP database, combined with redirection at Tier 2.

The algorithm for the proposed solution is shown on Figure 15. At Step 1, a mobile operator 1 (MO1) has a subscriber, which is provisioned with the corresponding NAPTR record. When this particular subscriber decides to move to another operator, in this case - MO3, the donor operator has to update its records to add pointer towards the centralized DB, shown as Step 2. Nevertheless, this does not make the recipient network dependent on the donor network to start providing services to the ported number. MO3 might initiate change of records at the Tier 1 level independently from MO1. Therefore, in case where the MNP database is interrogated first, the response will correctly point towards the recipient operator. In Step 3, the centralized MNP database is updated to include routing pointer, towards the actual subscribed network – MO3. In step 4, the recipient mobile operator provisions a NAPTR record in its ENUM DNS database with the services available to the ported subscriber. After this step, the porting is completed.

5.4. Discussion of MNP

The MNP solutions present several different challenges to the operator community in a country, particularly those models using a centralized DB.

First interesting aspect is from a commercial point of view. It concerns such details as to who pays for the infrastructure setup, maintenance, and ongoing operation? These are important issues which cannot be ignored.

From a technical point of view, the DNS as an underlying technology is a very well-known system. It is highly developed and not problematic. However, when a configuration of a system on a country level, which needs to be integrated into a bigger, global hierarchy, where different technical constraints or preferences exist, the task is not trivial.

From an operational point of view, the solution must meet the reliability and availability requirements of “telecommunications grade”, which poses high requirements towards the redundancy and back-up capabilities of the network. Furthermore, a reliable interface for query and especially update of the database might be difficult to implement because of the different requirements and capabilities each operator has. A possible solution for this is to implement DNSSec.

From a legislative point of view the problems might occur if there are specific, different requirements in every country regarding the personal data and what can and cannot be included in centralized ENUM DB.

In conclusion, the ENUM DNS solution for providing number portability is future proof, since all services are slowly converging towards the all-IP world. When deployed, the ENUM DNS will make possible to stop the use of an external legacy DB. Nevertheless, in order to be able to provide a complete solution for the number portability, not only for the mobile operators, but to any other operator and service provider, the ENUM DNS infrastructure must be deployed first. Until that time, when the IPX provides its services, there will be necessity to support legacy number portability databases, in order to include not only the mobile operators, but the fixed operators as well.

6. IMS Interworking – Security

6.1. Introduction

This part of the thesis evaluates the potential security threats and possible solutions regarding IMS interworking. Here we assume that the inter-PLMN interconnection will be multiple GPRS Roaming Exchange (GRX) networks connected to each other; with connections between PLMNs and GRXs. Section 6.8 will consider a peer-to-peer scenario, where the inter-PLMN interconnection will be leased lines directly between two IMS operators. The thesis does not attempt to present all the security issues in IMS interworking, but does try to address those issues most relevant to network security threats in the GRX network in a protocol level. Figure 16 shows an overview of two IMS domains exchanging traffic through the GRX network.

The security issues this thesis will focus on are the threats to the traffic flows that two or more mobile operators exchange in the GRX network. Also included is the influence that transit operators have on such traffic flows. Mobile operators, GRX providers, and IPX proxy providers (when GRX has evolved to IPX proxy) are the relevant actors in our consideration of IMS interworking. The thesis lists possible threats to each communications protocol that is exchanged. It will also list preventive measures to protect against these threats. If there are no protections against a specific threat, we will attempt to specify requirements for a suitable prevention mechanism. In this section we will also consider which kind of traffic flows the providers are responsible to secure in the GRX network. Next we will consider what additional attacks or threats will be introduced when the GRX have evolved to IPX proxies and how to prevent these attacks.

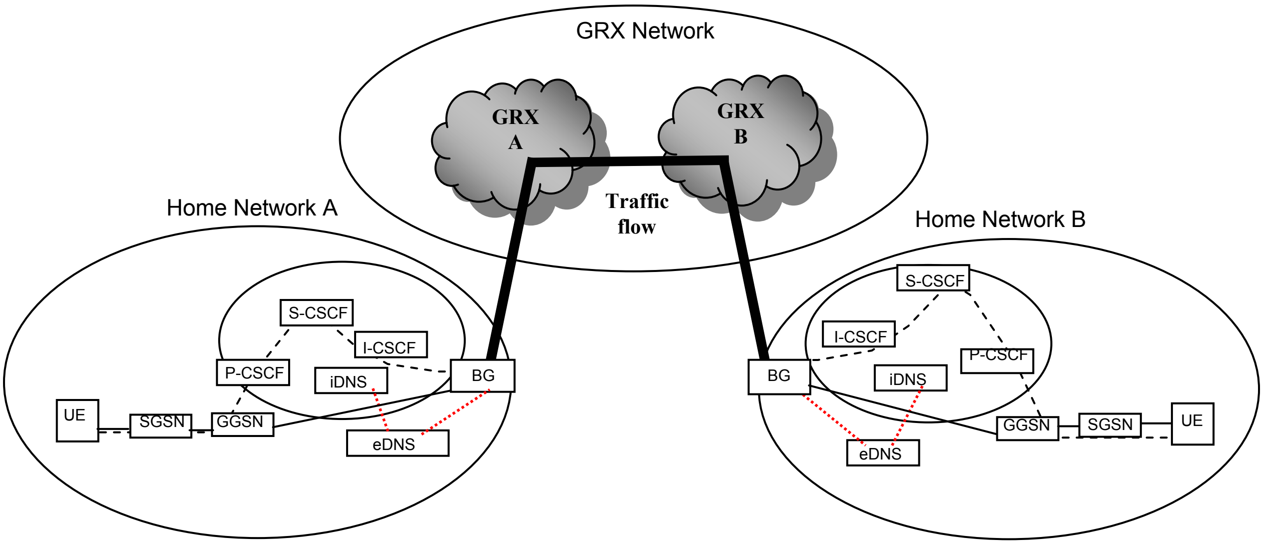


Figure 16. Two mobile IMS domains exchanging traffic through the GRX network

6.2. Interacting parties (providers)

The service providers that are involved in IMS interworking in the GRX network are the mobile operators, the GRX providers, and later on IPX providers when GRX has evolved to utlilize IPX proxies [13]. In addition we have third parties that for example maintain and operate the root Carrier DNS in the GRX network [22].

The mobile operators are responsible for their own traffic when exchanging traffic with other mobile operators. The GRX providers provide the mobile operators with a connection to the GRX network. The mobile operator and the GRX provider will make an agreement of what bandwidth, what kind of traffic will flow, etc will be supported over this connection. The GRX provider is responsible for its connections with the other GRX networks works [13].

If a transit provider hosts a DNS/ENUM server for a mobile operator then both parties should sign a bilateral agreement [22].

6.3. IMS interworking traffic in the GRX network

To be able to analyze possible threats to the IMS interworking traffic within the GRX it is necessary to investigate what types of traffic are exchanged. The exchanged traffic will be listed as protocols below.

- When two mobile IMS operators wish to exchange traffic through the GRX network the two networks will establish a GRE tunnel before exchanging traffic between each other. The actual signaling and media traffic flow to and from the operators' networks will occur within this tunnel. The type of tunnel that will be used in IMS interworking is not standardized at the moment. In the SIP trials in section *4.* Generic Routing Encapsulation (GRE) tunnel was used [42]. We will therefore assume that GRE tunnels will be used. The reason to use GRE tunnels in the trials is that the tunnels were easy to setup and maintain the IP addresses across the GRX network. Private addresses were used in both ends of each operator's network.
- SIP is used in IMS to establish multimedia sessions. (See section *2.1.1* for more detailed information.). The SIP traffic will be carried inside a GRE tunnel.
- DNS is used in the GRX network itself. In addition, Mobile IMS operators will use DNS in many different situations, i.e. to resolve a domain name to an address of an I-CSCF. To route SIP messages or ENUM queries concerning E.164 numbers to find out which terminating network to route to [22].
- To dynamically route IP traffic between GRX providers and mobile operators a routing protocol is needed to exchange routing information between the different networks. The routing protocol that is used is BGP-4 [13].
- The GRX network is also used to transport MMS traffic between operators. The communication protocol that is used is SMTP. GSMA IR.52 does not mention if the SMTP traffic is tunneled between mobile operators' networks [23].
- To be able to synchronize to common time base NTP is used [43]. Due to that the GRX is not connected to the Internet the operator's need to deploy their own NTP servers with separate GPS receivers or atomic clock-based time sources.

IMS interworking may introduce new user plane protocols (such as RTP, SMTP and HTTP) in the future. Thus, the transit providers should not restrict what protocols can be carried inside GRX if traffic is exchanged without tunnels [14].

Operation and maintenance traffic is handled internal in each mobile and transit operator's networks [44].

The traffic and services that exists in IMS interworking scenarios via the GRX can be generalized as follow (see figure 17):

- GRE
- SIP
- RTP
- DNS
- BGP
- SMTP

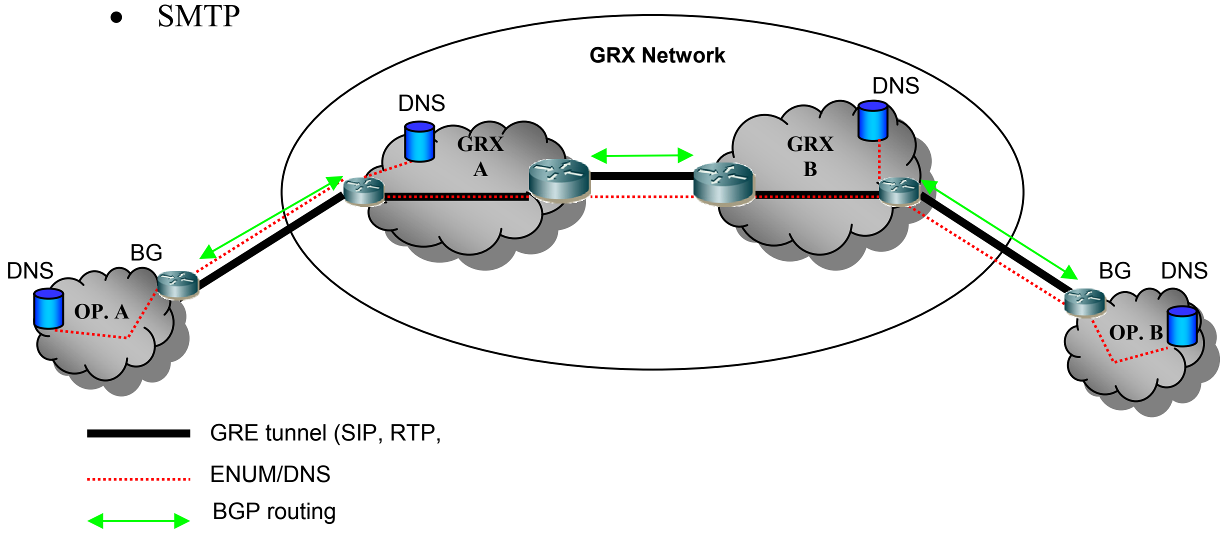


Figure 17 Overview of the protocols that are involved in IMS interworking in the GRX network.

6.4. Possible threats to IMS interworking in the GRX

A security issue that mobile operators will face when connecting their IMS domain to the GRX network is that their traffic will be directly exposed to traffic of other mobile operators and transit providers. Is it possible for a mobile operator to trust all these providers? Note that an important assumption in this paper is that there is no threat inside an operator's network.

The possible attacks or threats in the IP based network GRX are very different compared to the circuit switched (i.e. GSM) based networks. IP based networks are widely known due to the Internet. In comparison, the circuit switched network details are not so known. The protocol SS7 that is used in CS networks is not as well-known in general public as TCP/IP is in IP based networks. As the GRX network expands new providers will connect to the network, hence it will be more difficult to trust all providers. The mobile IMS operators should consider taking countermeasures to possible threats and attacks from the GRX network.

As the mobile IMS operators will compete for the same subscribers the operators can start to be a threat to each other. The purpose of the threat is to make the subscribers to change operator. The action of the threat could be to make disturbance on the competitors' network and services. An attack could be to steal bandwidth from another operator's network. For an example subscribers could experience bad quality of their video calls or experience problems making a regular multimedia call so frequently that the user will change operators. Mobile IMS operators should protect to these kinds of threats. The operators need also to prevent their domain at the network edge so nobody is able to intercept sensitive information about their domain. The prevailing information can be which private network range the operator is using and this information can be found from the SIP headers, URIs that address to internal functions in the home IMS domain like the S-CSCF, BGCF or MGCF [41].

As the GRX-network is an ordinary IP-based transport network it can be exposed to the same security threats as any other IP-based network. Therefore it is possible to apply the same network security concepts and strategies in a GPRS roaming exchange network as applied to other IP-based networks. These concepts or approaches are known as CIA *(Confidentiality, Integrity, and Availability)* [28]. Confidentiality is keeping the message from being seen. So only authorized entities are able to see it. Integrity means preventing a message being tampered with and only allowing authorized entities to modify it. Availability means that authorized users will have their subscribed service when needed. To have a secure network all these aspect need to be addressed [28]. Threats in the mobile operators' GRX network may be unauthorized access to data, unauthorized access to services, attacks on integrity, and denial of services.

This section 6.4 will only list different threats and attacks and not presenting any protections or preventions to these attacks. That will be brought up in the next section 6.5 countermeasures. The possible attacks or threats to CIA in GRX will be divided into groups, where each has a set of potential threats to the communications protocols and services (the protocols were described in section 6.3). We will consider each of these in turn in the following sections.

6.4.1. Confidentiality

6.4.1.1 GRE

If there is no protection or encryption provided by GRE at both ends of the tunnel, the traffic inside will be visible to anyone forwarding or carrying these packets. This makes it possible for someone to eavesdrop the traffic, which could contain confidential information [45].

6.4.1.2 SIP

A GRX provider that has access to the path between two mobile operators could easy capture a subscriber's SIP session and redirect the media traffic or retain confidential information about the users that are participating in the session [46]. This is possible if the SIP signal and the media traffic is tunneled with an unencrypted GRE tunnel or other unencrypted tunnel protocols, see figure 18.

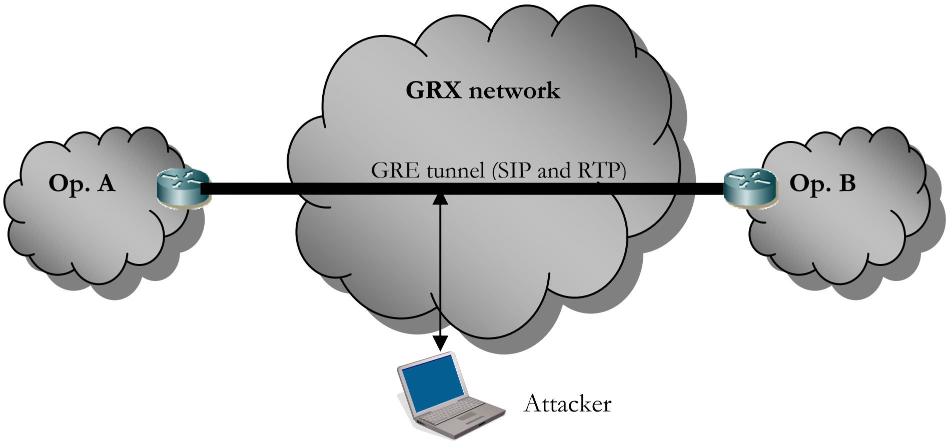


Figure 18. An attacker eavesdrop SIP and RTP traffic in the GRX network

A competitor could eavesdrop the SIP traffic from a path from a mobile operator's network and find out from the sender's operator the domain's topology from the SIP headers field like: Via, Route, Record Route and Service Route etc. From these fields an attacker could find out sensitive URIs addressed to IMS Core function S-CSCF, a list of SIP agents or SIP proxies [41]. This could be commercial sensitive information or a preparation for an attack on the operator's system.

6.4.1.3 DNS

ENUM/DNS queries/replies can contain private information of a mobile customer, i.e. NAPTR records. This DNS reply:

"sip:+467700900123@ims.mnc002.mcc240.3gppnetwork.org"

reveals the customer's network operator. If the ENUM and DNS traffic are not encrypted it can be a threat to confidentiality [22].

6.4.1.4 SMTP

SMTP which is used for MMS interworking has no encryption when interconnecting two MMSCs belonging to different operators through the GRX (See figure 19) [26]. That means it will automatically be a threat to confidentiality [23].

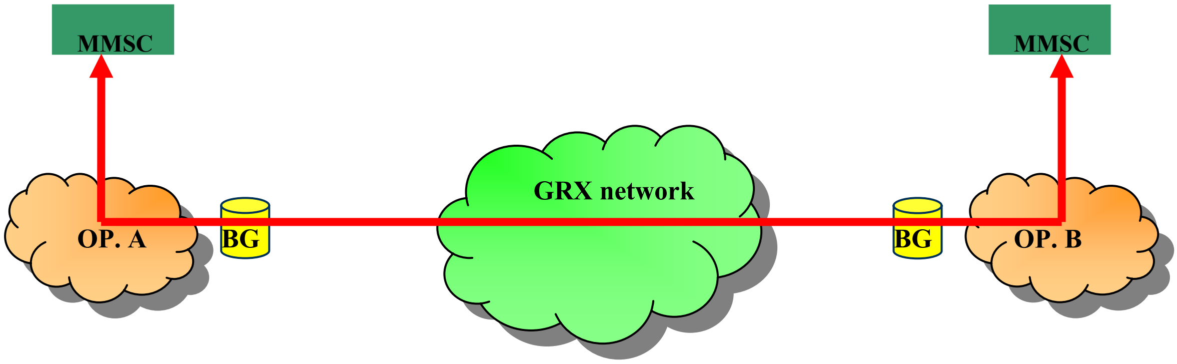


Figure 19. MMS interworking through the GRX network. [22]

6.4.2. Integrity

6.4.2.1 GRE

As mention before the GRE protocol is not encrypted. This means that a bad guy that has access to the GRX can potentially capture the data content (i.e. RTP traffic) and manipulate it despite the fact it is carried inside a GRE tunnel. This could be done with eavesdropping tools.

6.4.2.2 SIP

A hijacked SIP session and redirection of media traffic can threaten the user's integrity as well. SIP itself has no protection for integrity, but there are protocols which can be used which SIP to provide improved security. In addition to eavesdropping upon the media traffic (see figure 18) it is possible to modify or manipulate the media stream. This can easily occur because the signaling and media traffic are by default unprotected. This same threat applies to all kinds of unencrypted traffic, such as DNS queries, NTP syncs, etc. A bad guy could after intercepting the SIP session, modify the SIP header to change the SIP URI of the sender [47], see figure 20.

```
INVITE sip:Alice.Moon@domain.com SIP/2.0
Via: SIP/2.0/UDP ws2.domain2.com:5060:branch=z9hg4bk74gh5
Max-Forwards: 70
From: Bob <sip:Bob.Mars@domain2.com>:tag=9hx4567s1
To: Alice <sip: Alice.Moon@domain.com>
Call-ID: 633655545544545@192.168.0.200.2
Cseq: 1 INVITE
…
```

Figure 20. SIP header fields in an INVITE request where the From field could be modified.

6.4.2.3 DNS

Manipulating of the ENUM/DNS queries/replies could route traffic to the wrong roaming partner, to the wrong user, or render the system unable to route the call at all. These attacks lead to the end mobile customer being able call the user they wish to call.

This kind of attack is known as a DNS Man in the Middle Attacks (DNS Hijacking) [48] and illustrated in figure 21. First the attacker needs to connect to the GRX network so he/she will be able to make a man in the middle attack between an operator's network and a carrier's DNS server. In Step 1 an operator's network makes a DNS/ENUM request via the GRX network. The attacker sniffs the DNS request and intercepts it, this happens in step 2. The attacker sends back, as fast as possible, a false DNS reply to the operator's network. At the same time the valid DNS server sends back the correct reply to the operator's network so there will be a race condition between these two replies (Step 3).

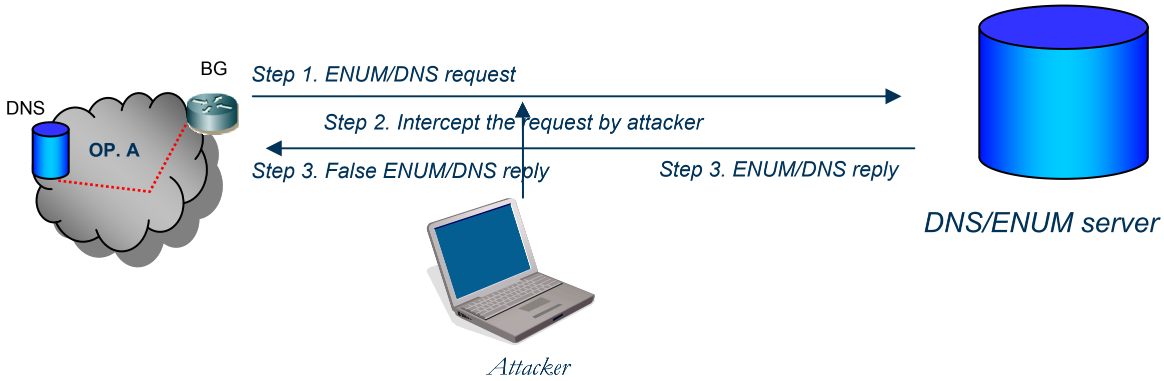


Figure 21. DNS Man in the Middle Attack (DNS Hijacking).

6.4.2.4 SMTP

SMTP is unprotected as described in section 6.4.1.4. This means that an attacker could intercept a MMS message, modify it and resend it, to the (newly) destinated operator [26].

6.4.3. Availability

6.4.3.1 GRE

The node that establishes the GRE tunnel can be exposed to a DoS attack. The purpose of the attack is to send GRE garbage traffic to the node, which will result in dysfunctional nodes. An attacker could hijack a GRE session in the GRX network and insert incorrect data so that nodes will not understand how to handle the corrupted GRE packets. The consequence may be malfunction of the node. The node could be the operator's router connected to the GRX network or one of the operator's BGs.

6.4.3.2 SIP

When SIP is establishing a call the firewall at the border gateway needs to open ports for the media traffic. These ports could either be statically open or opened on-demand. If the operator chooses to use the static solution a bad guy could do a port scan to find open, but unused ports, constituting vulnerabilities of the system. The bad guy could utilize these vulnerabilities to send traffic causing a DoS attack. A DoS attack towards an on-demand firewall could prevent it from dynamically open the media ports for the calls. All SIP aware nodes are potential targets of a possible DoS attack. This is because strong authentication is not used. A simple DoS attack could be based upon flooding of SIP INVITE (figure 22) or SIP SUBSCRIBE messages. Also malformed packets based on SIP can generate DoS attacks [47].

Another threat to availability with SIP is the replay attack. Current implementation of SIP signaling does not have a protection against this threat. A bad guy could collect SIP messages modify and replay them [49], unless the SIP traffic is sent in tunnels.

SIP can be used in DoS attacks against the operator's BG. The attacker sends corrupted SIP packets (figure 23) so that the SIP server behind the BG does not know how to handle all the corrupted/improper packets so much that the server malfunctions [50].

```
INVITE sip:dgen@aegean.gr SIP/2.0
To: Geneiataki Dimitri dgen@aegean.gr
From: Karopoulos Georgios<sip:gkar@aegean.gr>;tag=76341
CSeq: 2 INVITE
Authorization: Digest username="gkar",
realm="195.251.164.23", algorithm="md5",
uri="SIP:195.251.164.23",
nonce="41352a56632c7b3d382b39e0179ca5f98b9fa03b",
response="a6466dce70e7b098d127880584cd57"
Contact: <SIP:195.251.166.73:9384>;>
Content-Type: application/sdp

v=0
o=Tesla 2890844526 IN IP4 lab.high-voltage.org
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP
```

Figure 22. Valid INVITE message [50]

```
INVITE (null)
To: Geneiataki Dimitri dgen@aegean.gr
From: Karopoulos Georgios<sip:gkar@aegean.gr>;tag=76341
CSeq: 2 INVITE
Authorization: Digest username="gkar",
realm="195.251.164.23", algorithm="md5",
uri="SIP:195.251.164.23",
nonce="41352a56632c7b3d382b39e0179ca5f98b9fa03b",
response="a6466dce70e7b098d127880584cd57"Contact: <SIP:195.251.166.73:9384>;>
Content-Type: application/sdp

v=0
o=Tesla 2890844526 IN IP4 lab.high-voltage.org
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Figure 23. Malformed INVITE message [50]

6.4.3.3 DNS

A bad guy that has access to the GRX network could insert false DNS entries into the cache into a Carrier DNS server so that when an operator queries for an ENUM/DNS resolution it may receive a false SIP URI or IP address that may point to the wrong destination network. If these cache entries live a long time, then the result will be unavailability of the requested service. This attack is normally referred to as DNS Cache Poisoning (figure 24). In Step 1 (figure 24) the attacker sends a large of number of requests for opa.net spoofed with different IP source addresses. These requests will go to the name server in the GRX B network. The DNS server does not have the A record, so it forwards the requests to the DNS server in GRX A network where it will find the record, because operator A is connected to this GRX carrier (step 2). The attacker meanwhile sends a large number of false DNS replies with different transaction IDs so some of these replies will be accepted by B's DNS server (step 3). This false record will be placed in the DNS server's cache until the TTL causes the entry to be expired [48].

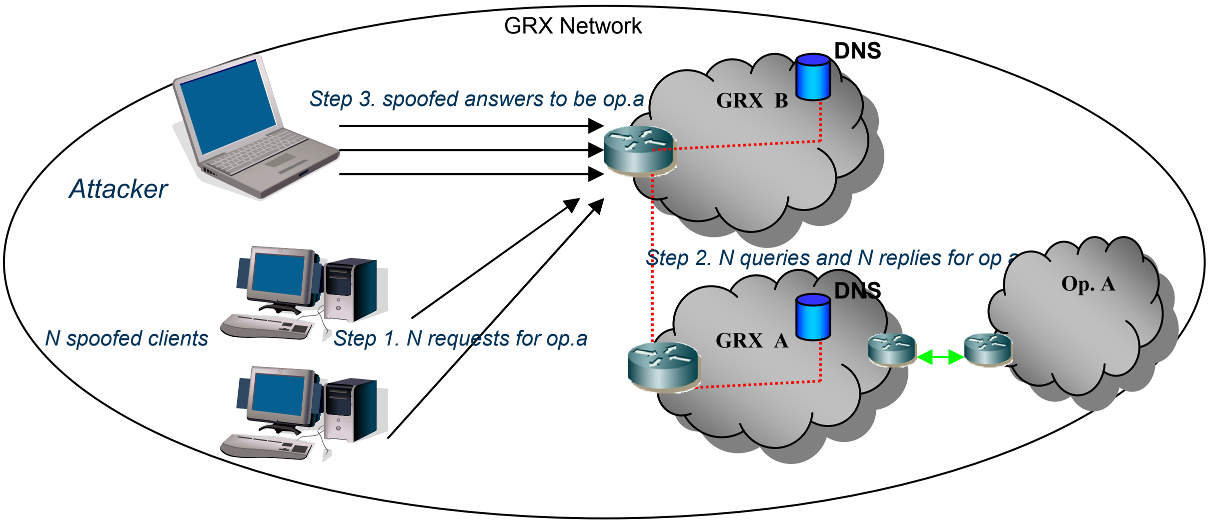

GRX Network
Step 3. spoofed answers to be op.a
Attacker
DNS
GRX B
Step 2. N queries and N replies for op a
Op. A
DNS
GRX A
N spoofed clients
Step 1. N requests for op.a

Figure 24. DNS poison attack in the GRX network

Capturing DNS/ENUM queries/replies and modifying the route information may lead to the end user not being able to make a call to the desired party or not having the requested service.

Denial of service attack on DNS servers will deny the mobile operators' the ability to locate the correct terminating network or hinder other kind of services based upon DNS. This attack is usually called DNS flooding. It works as shown in figure 25. The attacker sends a large number of requests from multiple machines directed to the targeted DNS server. The DNS server will have difficulties to handle that amount of traffic so it will start to work slower and slower, until it will start to deny valid requests [48].

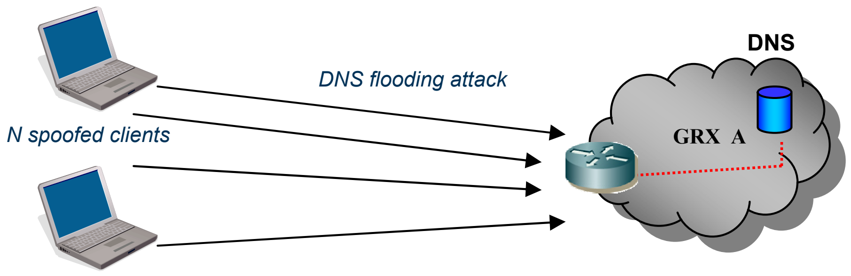


Figure 25. DNS flooding attack in the GRX network

6.4.3.4 SMTP

The lack of authentication of the sender in the SMTP protocol means that the operators' customers can be exposed to SPAM. SPAM consists of messages that are sent to recipients who have not requested it. As SMTP is used for MMS traffic, it is be possible to generate MMS SPAM. MMS SPAM will incur network traffic costs for the destination network (for example, by using bandwidth in the GRX network). MMS SPAM could also be used for DoS attacks to overload the MMSC [26].

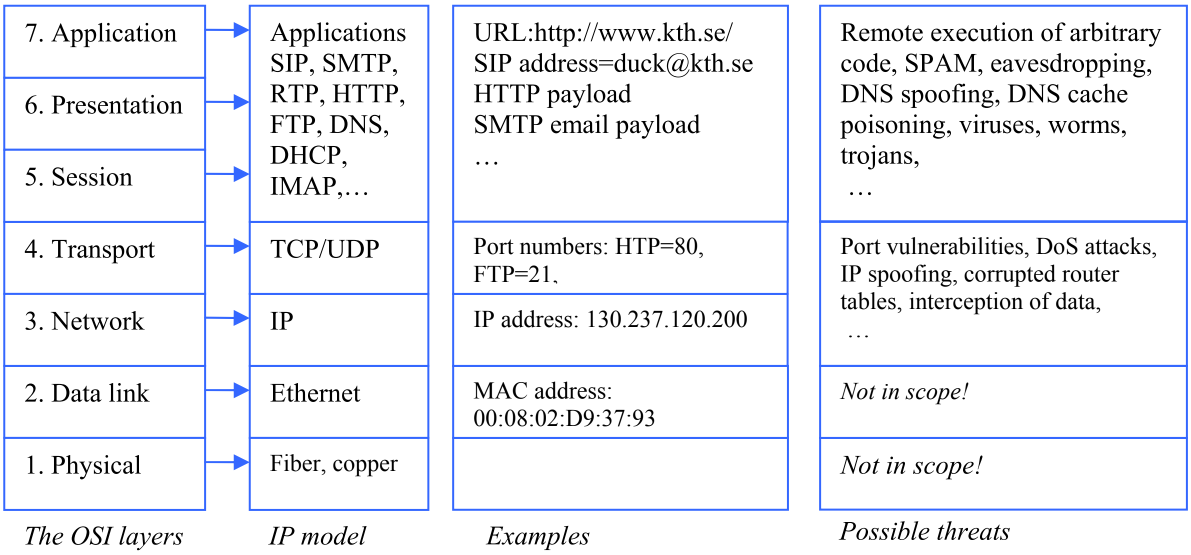
6.4.3.5 BGP

Since BGP uses TCP as its transport protocol and since it is unencrypted a bad guy could intercept the BGP traffic and insert malicious routing information. The purpose of such an attack is to make a mobile operator loose routes to roaming partners [51].

6.4.4. Common threats

A bad mobile operator which is connected to the same GRX provider as another competitive mobile operator could generate garbage traffic to the competitive operator's border gateway to occupy their incoming bandwidth, thus preventing legitimate in traffic and capacity. This is a type of denial of service attack.

An attacker that has access to a mobile operator's network could forge an IP address belonging to another operator and make different attacks upon a third operator so this operator will thinks that the attack is coming from the forged IP address network.



The OSI layers	IP model	Examples	Possible threats
7. Application	Applications SIP, SMTP, RTP, HTTP, FTP, DNS, DHCP, IMAP,…	URL:http://www.kth.se/ SIP address=duck@kth.se HTTP payload SMTP email payload …	Remote execution of arbitrary code, SPAM, eavesdropping, DNS spoofing, DNS cache poisoning, viruses, worms, trojans, …
6. Presentation			
5. Session			
4. Transport	TCP/UDP	Port numbers: HTP=80, FTP=21,	Port vulnerabilities, DoS attacks, IP spoofing, corrupted router tables, interception of data, …
3. Network	IP	IP address: 130.237.120.200	
2. Data link	Ethernet	MAC address: 00:08:02:D9:37:93	*Not in scope!*
1. Physical	Fiber, copper		*Not in scope!*

Figure 26. Overview of possible threats in an OSI layers perspective [27].

6.5. Countermeasures

This section will present different countermeasures in order to protect against threats to the services that were listed in previous section. Some threats may not be important to protect against, because the service may need to be public for some reason. The possible countermeasures will be divided into the same groups as previous chapter; however confidentiality and integrity will be merging into one group. The reason is that some of the countermeasures protect both of the security services.

6.5.1. Confidentiality and integrity

6.5.1.1 GRE

The GRE traffic could be protected with IPSec or similar encrypted tunnel protection (TLS). This prevents threats to both confidentiality and integrity [52].

6.5.1.2 SIP

To provide data confidentiality and integrity in the signaling plane both to and from the BG requires the use of IPSec or similar protection. This serves as a countermeasure against all threats and attacks on the SIP protocol that have been mention in section 6.4.1 and 6.4.2 about SIP [30].

Another encryption protocol that could be used to secure SIP is TLS. This requires use of a connection-oriented protocols such as TCP. TLS can be used when there is no pre-existing trust association between hosts. Another thing TLS demands is to be tightly coupled with a SIP application. One limitations with TLS is that if a UA sends SIP traffic over a proxy server it has no assurance that TLS will be used end-to-end. That is because the transport mechanism are specified on a hop-by-hop basis in SIP. TLS can not use UDP as a transport protocol because it is not a connection-oriented underlying tranport protocol [56]. However, UDP can be carried in IPSec tunnels.

One problem when encrypting entire messages for confidentiality is that network intermediaries (e.g. proxy servers) need to view certain header fields in order to route messages correctly and if these fields are secured with encryption, then the SIP messages will be non-routable. However, S/MIME allows a SIP UA to encrypt the MIME body within SIP, securing these bodies end-to-end without effecting message headers. S/MIME can provide end-to-end confidentiality and intergrity for message bodies. For example S/MIME could encrypt the session description that gives information about where the RTP traffic will flow [36]. One problem with S/MIME is the lack of prevalent public key infrastructure for end users. Which means certificates can not be verified by calling parties, thus making it vulnerable to a man in the middle attack [56].

If SIP is not utilized with IPSec or TLS, then sensitive URI information about a home IMS internal functions like the S-CSCF or BGCF need to be encrypted or removed. However, packets to these functions should not be accepted at the border, since there is no reason for any external packets to be sent to these nodes. Personal information such as the true identity of a user perhaps should not be public. This identity can also be removed before the signaling messages leave the home network, but not if it is an emergency call or due to lawful intercept regulations. All these tasks of hiding confidential information are done at the edge of a domain by the Topology Hiding Interworking Gateway (THIG) [34]. This function is usually implemented in a session border controller (SBC), for more information about the SBC see section 6.6 [41].

6.5.1.3 DNS

One way to protect the DNS traffic in the GRX network from and to a mobile operator would be to utilize IPSec tunnels. This would protect the ENUM traffic with respect to both confidentiality and integrity and while DNS traffic need only integrity protection.

DNSSEC could be used, but it only provides data integrity and not confidentiality [31]. DNSSEC is based on Public key cryptography. The queried DNS server sends back a reply with a signature (see figure 27). The signature is signed with a secret private key and only known by the queried DNS server. The DNS resolver is able to check the signature that comes with the reply to see if it is a valid reply. The resolver does this by checking the signature with The DNS server's public key, which is as its name indicates is public. If it is a valid signature, then the resolver will accept the reply [31].

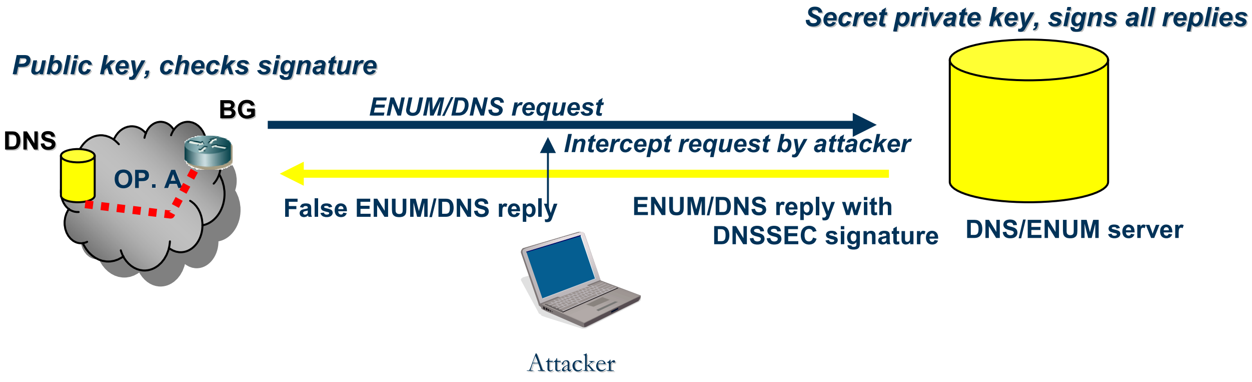

Secret private key, signs all replies
Public key, checks signature
BG
DNS
OP. A
ENUM/DNS request
Intercept request by attacker
False ENUM/DNS reply
ENUM/DNS reply with DNSSEC signature
DNS/ENUM server
Attacker

Figure 26. Countermeasure to man in the middle attack (DNSSEC).

6.5.1.4 SMTP

One way to protect the MMS traffic from confidentiality and integrity are to use IPSec. The only way to provide end-to-end security is if there are no SMTP proxies on the path. An SMTP proxy is used when several operators share a MMSC as a broker [26]. If this is the case hop-by-hop security is the only option [26].

6.5.1.5 Encrypt traffic discussion

3GPP NDS/IP says that IP traffic between two operators shall be protected by Security Gateways [30]. A Security Gateway is an entity placed on the operator's BG and used for securing native IP based protocols. Security Gateways use IPSec tunneling to provide integrity, confidentiality, and replay protection for signaling traffic between operators [30]. According to GSMA:

"Using Security Gateways with GRX can be questioned, since IPSec connections are mandatory between Security Gateways. IPSec tunnels between CSCFs are not needed, if GRX is used, since GRX network by itself provides comparable level of security as IPSec tunnel." [14].

But in an untrusted environment IPSec should be used. However, in the 3GPP document TS 33.210 it says that the signaling traffic should be protected with IPSec in the GRX network [30]. IPSec provides confidentiality, integrity, and authentication across an IP based network [33].

Alternatively, transport layer security (TLS) [55] could be used to encrypt the signaling traffic. Compared to IPSec it is more flexible when it comes to configuring root CAs, when certificates are used. Note that in this thesis we do not focus on what kind of encryption is used.

The SIPS URI could be used when a user wants his/her SIP messages to be secured end-to-end with TLS. SIPS specifies that that SIP messages should be delivered securely [56].

There is an ongoing industry discussion as to how much protection is needed for the user plane traffic. In traditional telephone traffic there was no protection exception for special environments such as military, government, confidential business, …. The problem is that if operators secure the user traffic it could lead to increased cost and power of additional hardware [27]. But without protection it will be easy for eavesdropping of the media plane. The current bottleneck with regard to encrypting the media traffic is that the router at the BG of an operator's network has limits on the amount of IPSec tunnels it can create. Thus it is more important to prioritize the encryption of the signaling plane, than to encrypt some of the media traffic. The mobile operator could put the encryption directly into the end terminal. The user equipment today has sufficient processor performance to make this feasible. The operators are able to take advantage of this to provide a secure end-to-end network which should attract mobile customers. To secure the user traffic between the mobile terminal Secure Real-time Transport Protocol (SRTP) [53] can be used. Another problem with the encryption of media traffic is the authorities' rights to access the media traffic in some circumstances such as in criminal investigations. If the operators encrypt the media traffic in their network, they need to find a way to provide the authorities a means to decrypt the ongoing media session [27]. Of course, if users encrypt their media traffic end-to-end and do not provide the key to the operator, then there is no way for the operator or any authorities to easily decrypt this traffic.

6.5.2. Availability

6.5.2.1 GRE

A solution to protect the node that creates the GRE tunnel could be to implement a firewall with packet filtering at the Boarder Gateway. The filtering should allow GRE traffic only from sources for which the mobile operator has a bilateral agreement. The inspection should be on layer 3 and layer 4. This approach will remove all unwanted GRE traffic from the GRX network. This approach also protects against various DoS attacks.

If an attacker is using GRE to send garbage traffic to deprive the operator of bandwidth a solution could be to trace the traffic back across the GRX and stop this operator from introducing the traffic to the GRX to begin with.

6.5.2.2 SIP

To protect from unknown IP sources the operator's firewall needs to dynamically open media ports when needed to be able to handle incoming and outgoing sessions. This could be implemented by a session border (SBC) controller at the operator's network edge [56]. For more information about the SBC see section 6.6.

A solution to the replay attack is to encrypt sequence messages. The protection is on the application layer. This protection is not necessary needed if an encrypted tunnel, such as IPSec, is used between the pairs of operators communicating through the GRX network, because then the SIP traffic is totally protected with respect to integrity and confidentiality.

To prevent DoS attacks based on SIP traffic at an operator's BG, the BG needs a function that limits the maximum amount of signaling and bandwidth on a specific connection. This functionality is available in a SBC, for more information on the SBC see section 6.6.

6.5.2.3 DNS

DNSSEC could be used as a countermeasure to DNS Cache poisoning [31]. DNSSEC works as described in section 6.5.1.3.

DNS flooding could be prevented through configuration of the operator's DNS server. The configuration should only provide recursive look-ups for only the Carrier DNS provider in the GRX network. This would prevent an intruder from loading a large number of records into the operator's DNS. There is also a protection mechanism that automatically-detects flooding and take measures like auto-blocking this traffic. These prevention systems are based on detecting anomalous traffic patterns [37].

To secure DNS traffic in the GRX network encrypted tunnels, such as IPSec tunnels, could be used. This solution would prevent attacks based upon modifying the replies to produce incorrect destination information.

6.5.2.4 SMTP

One countermeasure to MMS SPAM on an operator-operator basis is to have a charging model, such that the receiving operator must be paid by the sending operator [26]. Another way is to implement sender identification since the receiving operator knows where the SMTP traffic is coming from because of the tunnel between the operators' network. Then the sending operator setting the policies for its subscribers. This option makes it unnecessary to have a charging model at all. Another measure is to introduce SPAM filters at the BG that only allow authorized traffic and that controls the rate with which messages are sent and received [26]. Implementing logging information enables one to be able to analyze an attack [26] either after the fact or to use this pattern to recognize an attack in progress. Additionally, there are protections at the user's device, but that is out of scope in this thesis. But of these the least complex and easiest to implement is sender identification.

6.5.2.5 BGP

An obvious way to prevent mobile operators from loose roaming partners would be to encrypt the BGP datastream between routers. The entities needed to secure BGP could be to use PKI and IPSec. These security entities are used to validate the authenticity and data integrity of BGP updates [40]. An alternative to IPSec is to use a digest algorithm, which means that if the stream is modified then the receiving router should drop it and wait a random time and query again for an updated routing tables. This protection operates in the transport layer and is called TCP MD5 [32]. In this method two or more routers shares a key (see figure 27). This key together with the routing update from one of the routers is used to computer a signed MD5 hash. This hash is transferred with the routing update in clear text to the destinated router. The destination router separates the hash and the routing update message. It takes the routing update with the shared key and calculates a new hash. The router now compares the new hash with the hash the came with the routing update. If the two hashes do not match, it will drop the routing update. If they match it till accept this update and update the routing tables [32].

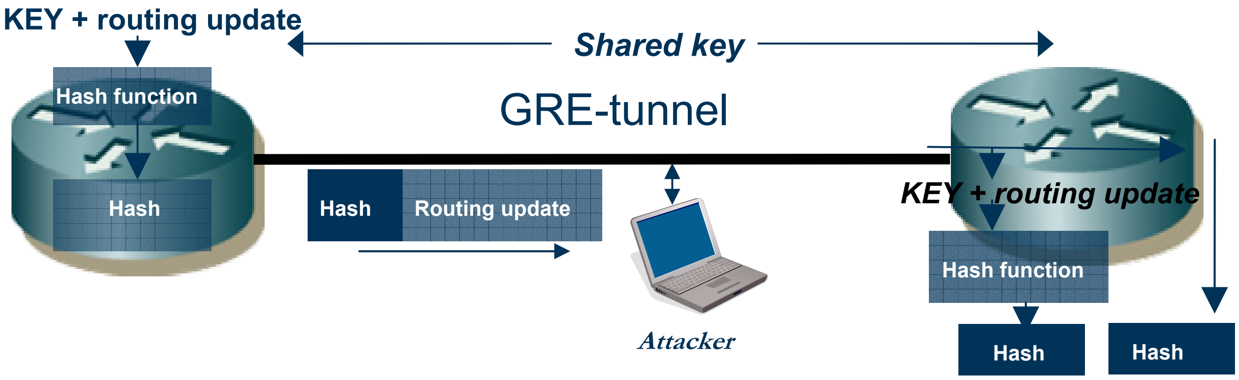


Figure 27. Protection for updating the routing tables in a secure way (MD5).

6.5.3. Common countermeasures

The IMS operators in the GRX network should protect their private network from other PLMN operators with Boarder Gateways. It is almost mandatory that the mobile operators should implement firewalls with packet filtering at their network edge. These firewalls should filter all traffic to/from the mobile operator's network. Such protection prevents several kinds of DoS attacks. Ingress filtering prevents attacks when an intruder makes an attack on a roaming partner with a forged IP address belonging to another operator's network. The mobile operators should make bilateral agreements between each other to clearly define what kinds of traffic and from whom the BG should accept packets, all other packets should be dropped.

It is good if the mobile operators implement a security system that notifies the network administrator when an attacker is trying to break into the operator's system. Such a system is known as Intrusion Detection System (IDS) [54]. The idea is to implement IDS as means of enforcing a security policy in the operator's system. An IDS compares predefined network attack patterns to the current network flow in and out from the operator's network.

To protect against threats to confidentiality, integrity, and availability encrypted tunnels, such as IPSec, are usually used. But there are some drawbacks with IPSec. It is not so scalable in the sense that it becomes problematic to create a large number of operator-to-operator tunnels. Every entity that uses IPSec needs to be configured independently [39].

The OSI layers	*IP model*	*Threats*	*Countermeasures*
7. Application	Applications SIP, SMTP, RTP, HTTP, FTP, DNS, DHCP, IMAP,…	Remote execution of arbitrary code, SPAM, masquerading, eavesdropping, DNS spoofing, DNS cache poisoning, viruses, worms, trojans …	Application inspection FW, deep inspection, system access control, virus protection, S/MIME, Certificates, proxies,…
6. Presentation			
5. Session			
4. Transport	TCP/UDP	Port vulnerabilities, DoS attacks, …	IPSec,TLS/SSL, Stateful inspection FW, tunneling protocol, packet filtering,…
3. Network	IP	IP spoofing	
2. Data link	Ethernet	Not in scope!	*Not in scope!*
1. Physical	Fiber, copper	Not in scope!	*Not in scope!*

Figure 28. Overview of countermeasures to possible threats from an OSI layers perspective [27].

6.6. IMS Session border controller

A Session Border Controller (SBC) has a key role in IMS interworking security. That is why it will be considered separately in this section.

SBC is a SIP aware device that controls and manages multimedia calls at the borders of an operator's network. The device manages both the signaling and the media in and out of the operator's network. The SBC acts as a B2BUA, which means it handles the multimedia calls from both ends of a call. The SBC is constructed in a way that it knows the relationship between the signal and the media plane. The signaling SBC function (I-BCF) manages the access of multimedia calls in and out of the core of IMS. It also modifies the SIP messages. However, the media SBC function (I-BGF) manages the access of the media plane in and out of the operator's network. It provides services for the media, like convert to different CODECs and handles the QoS for different media streams [41]. The I-CSCF node is placed as shown in figure 29, could be implemented in the SBC in some situations. See figure 30 for the SBC architecture.

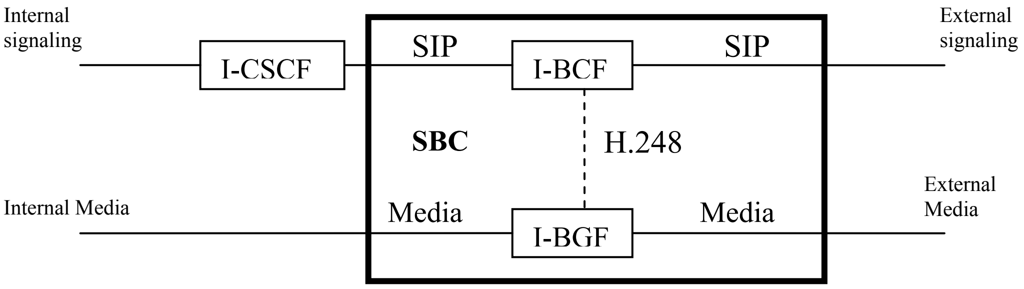


Figure 29. Overview of SBC relationship between signaling and media [41].

The SBC offers a lot of IMS control functions. This section will focus on the security functions that the SBC provides the mobile IMS operators with regard to the GRX network. SBC also provides interoperability and monitoring, but these two features are out of the scope of this thesis. What is also out of scope is the SBC in the access network, where the terminals interwork with the IMS domain. So in this thesis, we will only consider network-to-network security.

The main goal of the security functions that the SBC provides the operator is to secure the SIP and the media traffic in and out from the operator's network. The SBC will act as a filter for these two types of traffic. Some of these security functions are:

- offer Network Address Translator (NAT) for the internal network
- act as a firewall or together with an existing firewall
- provides THIG
- removes corrupted SIP and media packets
- provides call admission control

The SBC together with the firewall, in such a way that rather than statically configuring the firewall the SBC can dynamically open media ports on-demand from the signaling messages. Opening ports on-demand provides much better security than leaving them open and unsecured.

To perform the THIG functionality the SBC rewrites the SIP messages to remove details about the internal network core, such as how the call is routed from the subscriber or remove user information that the subscriber does not want to be made public. Thus the SBC will act as a relay device for both the signaling and the media. The admission control function can be used to reject calls for different reasons. This function also prevents DoS attacks based on the SIP protocol and enforces the bilateral SLA agreements. In this manner only roaming partners will have access to the operator's network. This function also prevents bandwidth theft. All these functions that the SBC should contain do not need to be included in one device or node. The partitioning over one or more nodes depends on the overall system design. A device at the network boundary could contain only one function, that is to enforce access policy rules to limit Denial of Service (DoS) attacks [41].

The session border controller is placed at the operator's border gateway (see figure 30). This means that the SBC is deployed between an external network and the operator's private network. In this thesis the external network is the GRX network and the private network is the operator's own IMS core network.

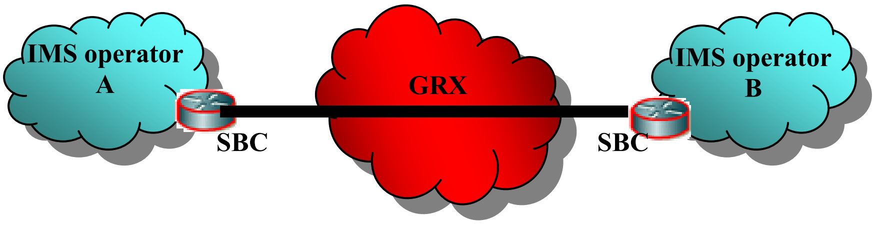


Figure 30. Interworking connection between two mobile IMS domains with SBC.

An important thing to notice is also that the SBC is not a standardized set of functions in IMS. It has evolved to include a number of important functions as issues have arisen during the study of IMS interworking between other IMS domains [41]. Figure 31 shows how the SBC could be implemented in the IMS architecture. The SBC is in the area of NNI EGDE in the figure.

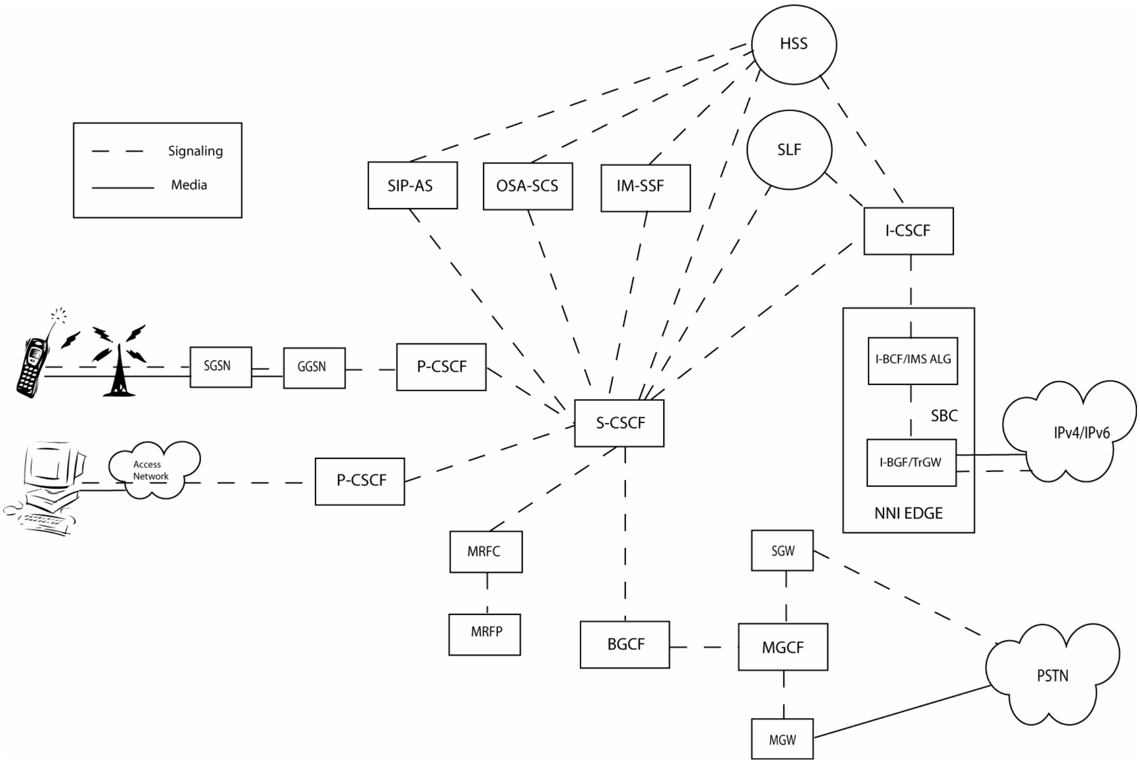


Figure 31. SBC implemented in IMS architecture (NNI EDGE).

6.7. Evolving towards IPX

According to GSMA there is a need for a centralized interconnection of multiple carriers that are interconnected that provides both IP connectivity and for inter-carrier exchange of charging information. This new network will replace the current GRX network it will be known as IPX. These new IPX providers will besides giving access to the inter-carrier network also be able to provide SBC functionalities to the mobile operators (or other customers) within the IPX network (if the operator will fully trust the IPX provider). This new device is known as IPX proxy [41]. IPX proxy should support separation of the user plane and control plane according to the IPX proxy requirements in document IR.34 [13]:

R6 - IPX Proxy shall be able to relay both user plane and control plane. IPX proxy shall also be able to relay only control plane when if so desired, based on contractual arrangement

I.e. user plane can be separated from control plane and routed directly between originating and terminating service providers in some cases

Thus in the GRX network the control plane and the media plane are not separated [13].

The GSMA document IR.34 such as requirements regarding IPX proxy functions. An IPX proxy is a SIP aware proxy such as the SBC. The IPX proxy service providers should be able to provide the mobile IMS operators functionality to protect their domains with firewalls and to hide the operator's IMS core topology, NAT, etc. An IPX proxy could work as a secure multimedia zone where the proxy secures legitimate signaling, multimedia, and maintenance traffic. This approach could create a security fence around an IPX proxy to authenticate traffic to and from the mobile operator's edge devices. Ensuring that only legitimate device can access the IPX network [27]. Most operators will not trust other entities to protect their domains so the operators will probably have their own protection at their BG.

IPX providers inherit the general requirements of the GRX providers. As mention the technical requirements for an IPX proxy are listed in the GSMA document IR.34 [13]. A general security requirement from GSMA [12] is that an IPX proxy shall provide access control and protection against malicious attack, such DoS attack. These general security requirements are listed in GSMA IR.34 as bullets:

R2 - IPX Proxy shall be ablte to handle inter-service provider traffic in a secured and controlled manner. This means that the overall IPX Proxy infrastructure is protected from outsiders.

R8 - IPX Proxy shall be able to verify that the source is who it pretends to be.

Among other requirements for the IPX proxy are routing, user plane support, and security related functions. In this part of our thesis we will concentrate on the requirements for the security area. The most important bullets of the security requirements are between R.49 to R.60, which concern authentication and authorization.

***R49* -** IPX Proxy shall have filtering and routing enforcement capabilities

***R50* -** IPX Proxy shall be able to perform secure NAT traversal as well as firewall traversal for signalling and media, when needed

R51 - IPX Proxy shall support opening pinholes for user plane traffic traversal based on SIP/SDP information

R52 - IPX Proxy shall support closing pinholes used by user plane traffic based on SIP/SDP information

***R53* -** IPX Proxy shall block traffic not related to ongoing SIP sessions

***R54* -** IPX Proxy shall be able to have rate limit / flow control features on control plane as well as on user plane

Including capability for propagation prevention, e.g. prevent problems such as flooding from one network to other connected networks. Flow control can be applied both to control and user plane, on a per operator basis. It shall be possible to configure alarms for the amount of traffic, in order to prevent overloading

***R55* -** IPX Proxy shall support the ability to apply admission control per domain basis

***R56* -** IPX Proxy may support the ability to support maximum admission control limits per domain basis
Helps e.g. preventing DoS attacks by setting a maximum limit of simultaneous

connections

R57 **-** IPX Proxy shall be able to handle policy function across domains
For example bandwidth control & admission control

R58 **-** IPX Proxy shall be able to support user plane policing based on the data rate

R59 **-** IPX Proxy should be able to support external interface(s) towards policy control/admission control function

R60 **-** IPX Proxy shall be able to check that media is what session setup implies
For fraud prevention purposed it is important to be able to check that e.g. session set up as PoC really contains PoC related media instead of something else

Bullets R.28 and R.29 are about protecting the sensitive information about the IMS operator's core:

R28 **-** IPX Proxy shall be able to modify IP addresses in SIP/SDP messages when it is acting as a media proxy

R29 **-** IPX Proxy shall be able to modify SIP headers (fields such as Via, Contact, Record Route, Content-Length) when it is acting as a media proxy

Bullet R.38 is that IPX proxy shall support tunneled (protocols like GRE) and non-tunneled traffic:

R38 **-** IPX Proxy shall be able to support tunneled traffic (e.g. GRE) and non-tunneled traffic, for both control and user planes, including inter-IPX Proxy interface

Control plane & user plane can be in the same tunnel or use separate tunnels.
Control plane & user plane can be also un-tunneled

For more information about the IPX network see section 3.1.2. Figure 32 shows the different kinds of traffic that are exchanged when interworking between operators in the IPX network.

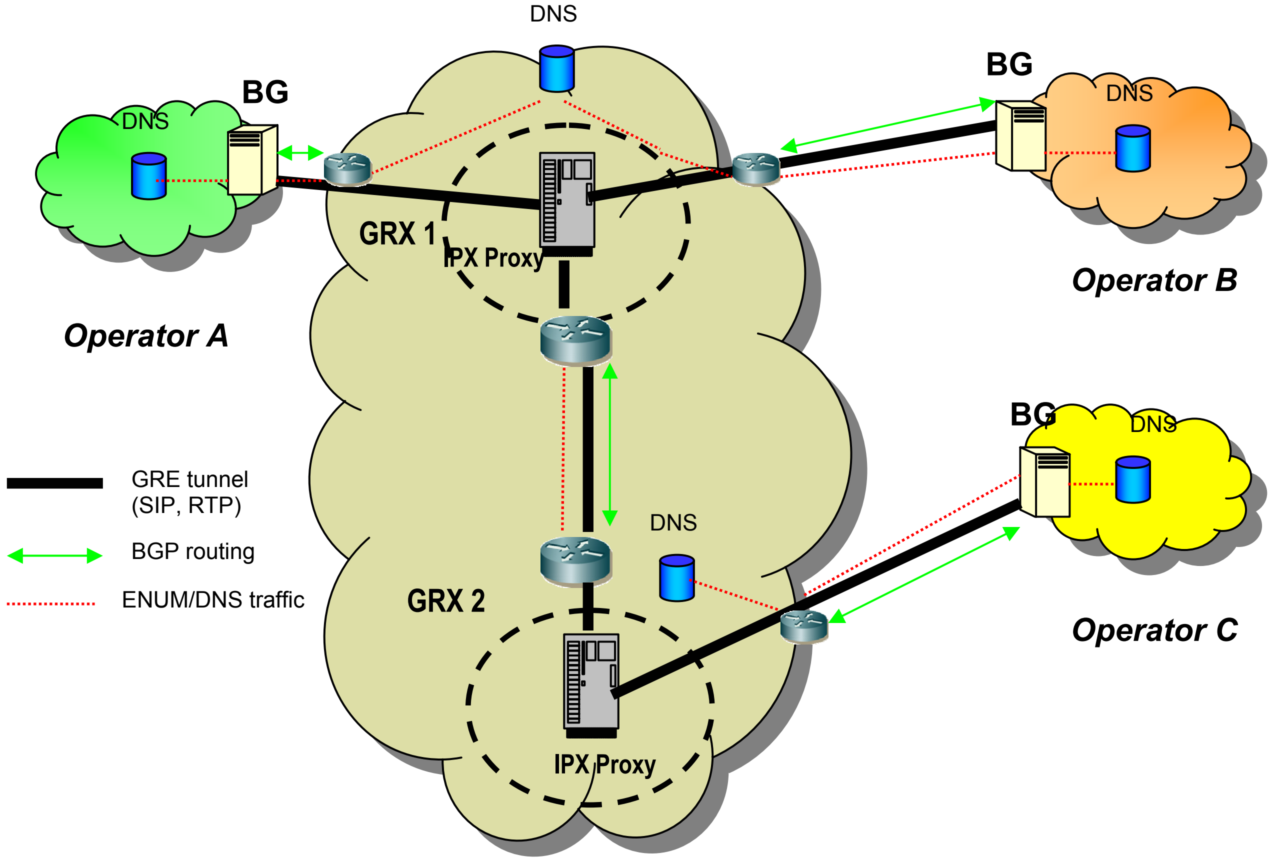


Figure 32. Overview of the protocols that are involved in IMS interworking in the IPX network.

According to the IPX proxy requirements in R.29 in introducing the IPX proxy will make it impossible to use end-to-end security, which would provide confidentiality and message origin authentication when exchanging traffic between operators. Thus hop-by-hop security must be applied. If the operators still want to have end-to-end IPSec there could be a solution where the IPX proxy predefines a path for the IPSec tunnel to pass through. See figure 33 for two IPX-proxies that are interconnected. The IPX proxy itself does not provide any countermeasure to eavesdropping or modifying of traffic between two IPX proxies or between an operator and an IPX proxy if no encryption of the traffic is used and if IPsec encryption is done, then the IPX proxy can not do much more than route packets.

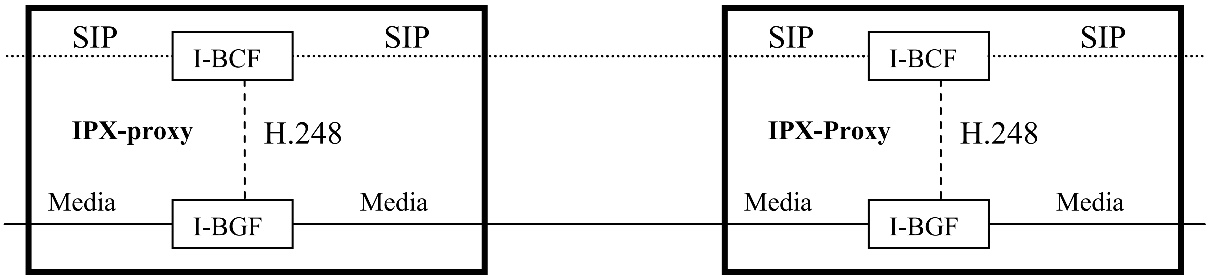


Figure 33. Overview of the architecture over two IPX-proxies interconnected.

SIP does not generally require strong authentication [47]. This means that when two IPX proxies communicate to each other through SIP signaling they will not authenticate each other. It is then possible for an attacker to pretend to be an IPX proxy. This means that the attacker will have access to all SIP messages that flow through between the two IPX proxies, see figure 34.

A countermeasure to IPX impersonation could be to implement an authentication mechanism, so that the two IPX proxies can authenticate each other. The Authentication mechanism could be SIP Authenticated Identity Body (AIB) [66].This will make it difficult for an attacker to act as a valid IPX proxy belonging to the IPX network.

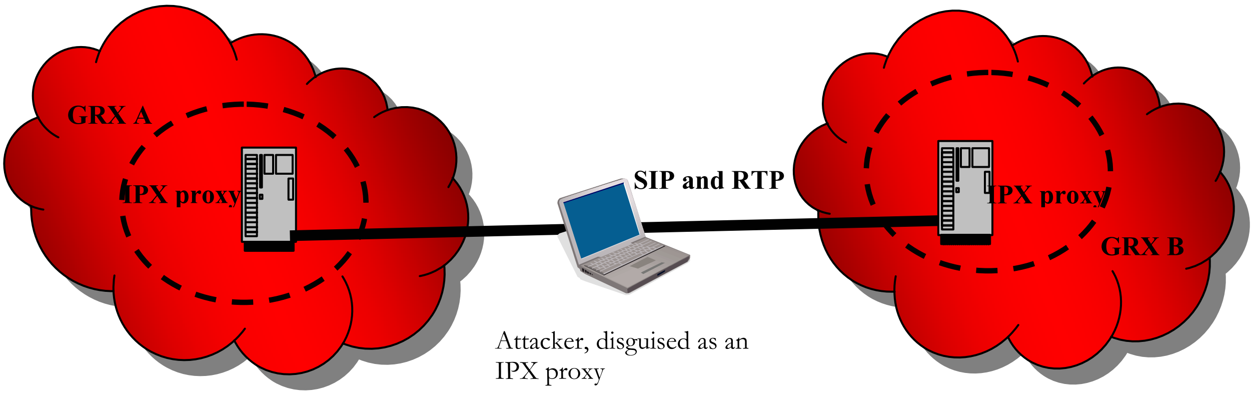


Figure 34. IPX proxy impersonation.

6.7.1. Security of the DNS in the GRX/IP network

The DNS traffic is protected with a firewall at the operator's BG see figure 35. The figure shows the different interaction with an operator's DNS in the GRX/IPX network. The trusted entities are the operator's internal nodes. The untrusted environment is secured by the operator's firewall which is placed at the operator's network edge. The operator's DNS has different views, i.e. external operators have a specific view of the queried operator's DNS. This views has limited rights to access the DNS depending on the source. The operator's DNS is only accessible through the external DNS outside the operator's network. The internal DNS queries other operators' DNS through the external DNS's (eDNS, see figure 35) view.

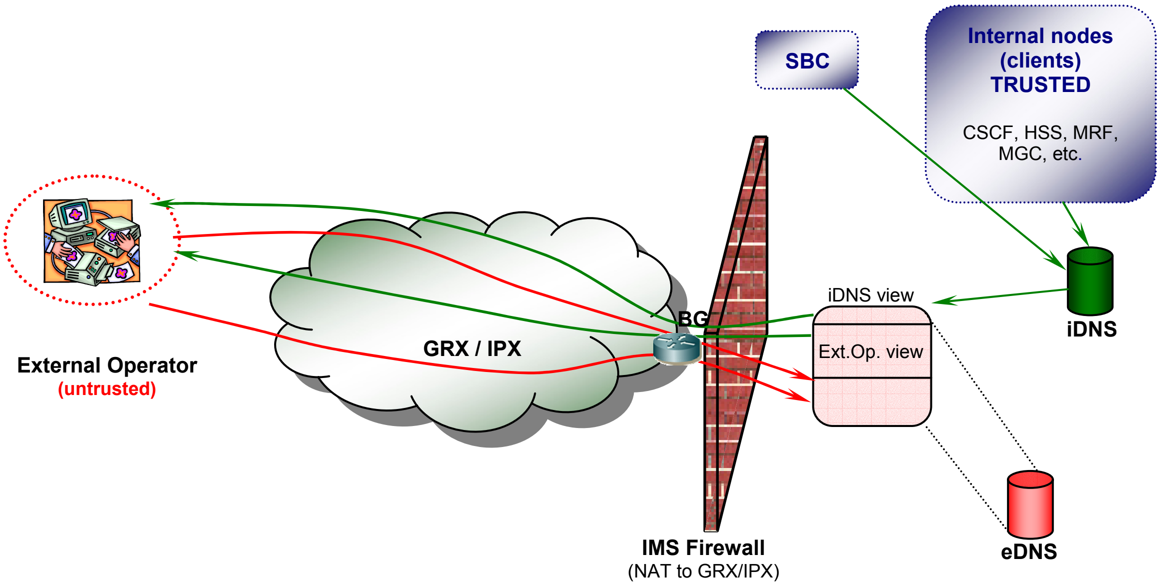


Figure 35. Firewall protection at the BG for the operator's DNS.

6.8. Peer-to-peer scenario

In figure 36 there are two mobile IMS domains exchanging traffic through a leased line (i.e. fiber, copper etc.). It is assumed that that there is no threat inside an operator's network. The traffic exchanged between the mobile IMS domains in the scenario in figure 36 are the control, media, and the DNS traffic. When a direct connection is used a routing protocol is not needed due of feasible of static point-to-point routing. All the traffic that is exchanged is tunneled in a GRE tunnel.

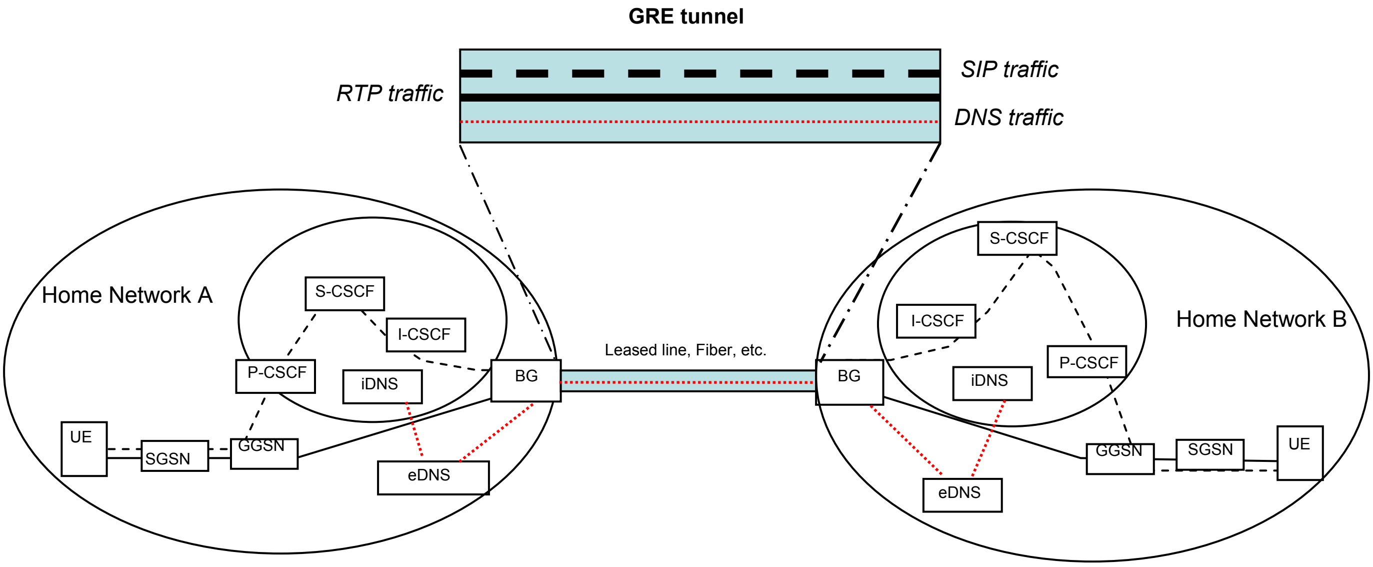


Figure 36. Two mobile IMS domains exchanging traffic through a leased line.

If the operators want to secure confidentiality and intergity encypted tunnel with IPSec is prefered. However, the protection against availability could be to use a firewall at the BG for the GRE and the DNS traffic. The firewall is responsible for controlling in-bound and out-bound network traffic. Protection against threats based on SIP and media traffic could be to implement a SBC at the operator's BG (see section 6.6 for more information about the SBC). It is advisable to implement an IDS as well in the operator's network, see section 6.4.3 for more information about IDS.

7. IMS Interworking – IP protocol versions

7.1. General Interworking model

The IP Multimedia Subsystem Core Network (IMS CN) can inter-work with other IP multimedia networks, based on SIP as defined in RFC 3261 [58]. An IP multimedia network (IP MN) can use either IPv4 or IPv6. Figure 37 illustrates the general model for interworking in this case.

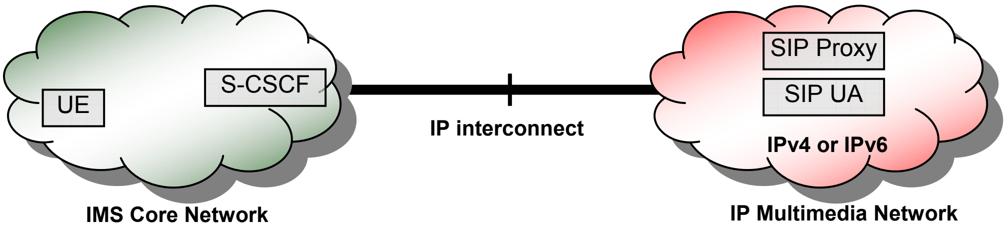


Figure 37. General model for interworking between IMS CN and another IP multimedia network.

The user equipment (UE) uses the CSCF nodes to communicate with the external IP MN. If there is no difference in the IP versions then it could directly contact the SIP UA or the SIP Proxy. Otherwise, IP version interworking is necessary and IMS-ALG and TrGW functionality must be provided. However, these functions might be implemented as parts of other physical nodes in the IMS network.

7.2. Reference model

Figure 38, illustrates the reference architecture for interworking between IMS CN and IP MN.

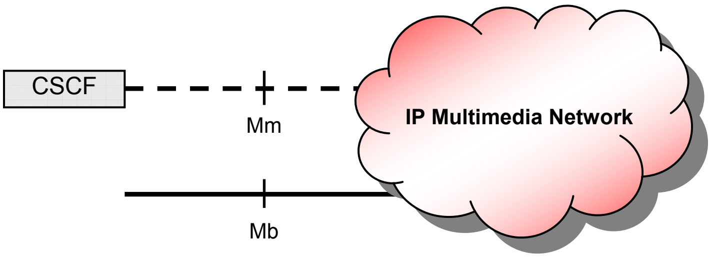


Figure 38. Interworking reference architecture, without IP version interworking
Adapted from [57]

Mm reference point – CSCF and external IP MN utilize SIP, as defined in RFC 3261 [58], as a call control protocol over the Mm interface.

Mb reference point – Defined in 3GPP TS 23.002 [59], this interface is IP based.

The IP MN can utilize the Mb interface to connect to various network nodes, such as user equipment (via GTP tunnel through GGSN), an MRF, or an application server.

Figure 39 shows the reference architecture for interworking between IP MN and IMS CN, when IP version interworking is supported.

The Interconnect Border Control Function (IBCF), which was described in paragraph 3.1.1, earlier in this document, has a central role in the process of IP versions interworking.

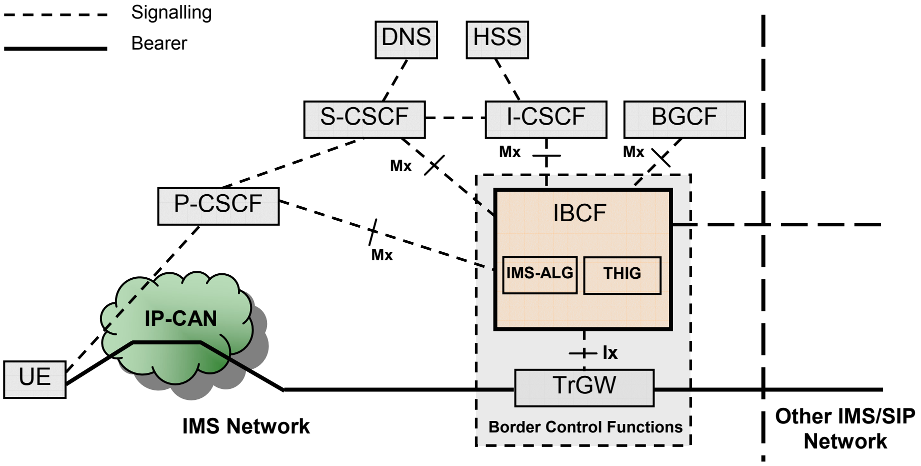


Figure 39. Interworking reference architecture with IP version interworking. Adapted from [57]

The IMS Application level gateway (IMS-ALG) mentioned in chapter 2, provides translation function for both SIP and SDP at the application level. This provides for communication between IPv4 and IPv6 applications. When IMS-ALG functionality is used, the IBCF acts as a B2BUA. The IMS-ALG facilitates the control-plane traffic interworking.

The Topology hiding inter-network gateway, is described in section 2.3, 3.1.1, and 6.5.1, earlier in this document.

The Transition Gateway (TrGW) is a NAT-PT/NAPT-PT. It automatically binds addresses in IPv4 network with addresses in IPv6 network and vice versa. This functionality provides for transparent routing between the two networks, without requiring any changes in the end points. The TrGW facilitates the user-plane traffic interworking.

There are disadvantages of such NAT- and ALG- mechanism. First of all, NAT breaks the end-to-end model of IP, thus the need to rewrite SIP and/or SDP prevents end-to-end security; second, a complex coordination between the ALG responsible for the signaling and the TrGW (NAT) responsible for the media (user) traffic processing is necessary; third – NAT is a single point of failure, since a session must flow through the same NAT from start to end. If the NAT fails, then all ongoing sessions through this NAT will be terminated; and fourth – because of NATs and ALGs networks face scalability challenges [60].

7.3. Interworking at the IBCF

7.3.1. Control-plane

Despite the fact that IMS was designed to be an entirely IPv6 based system, the early deployments of IMS networks are using version 4 of the IP protocol. As mentioned above the IBCF could provide interworking for both control- and user-plane traffic when necessary.

During session setup, when the first SDP offer is received, the AMS-ALG provides the TrGW with the corresponding IPv4 addresses and ports as received in the offer. After that it requests the TrGW to bind IPv6 addresses and port numbers to the received IPv4 addresses and port numbers, in order to provide routing of the traffic from the IPv6 network through the TrGW. When the TrGW responds with the requested information, the IMS-ALG includes the received IPv6 addresses in a new SDP offer and sends it to the interconnecting network.

When the SDP answer comes, IMS-ALG gives the TrGW the received IPv6 addresses and port numbers, and requests it to bind the corresponding IPv4 addresses and port numbers to enable routing of the user-plane traffic. When this is done, the IMS-ALG will send a SDP answer to the IPv4 IMS network.

When the IPv4 network has to terminate a session setup from an IPv6 network, the flow of the messages is similar. When a dialog has been established, it is still possible for both ends to initiate changes of the connection settings. When the session comes to an end, the IMS-ALG should release the session and asks the TrGW to release all bindings related to this particular session.

7.3.2. User-plane

TrGW is responsible for interworking the user-plane traffic. It should use the established bindings between IP addresses and port numbers to modify the messages and secure their transport between the IPv4 and IPv6 networks. It does that, by exchanging the IPv4 address of the outgoing message with the corresponding IPv6 address before forwarding the message to the IPv6 network, and vice versa.

7.4. Implications of the IPv4/IPv6 Interworking

Since the majority of IP networks today are based on the IPv4, if interworking with an IPv6 network is necessary, several aspects of the architecture must be considered in advance. For example, the impact this interworking has on the UEs, the underlying GPRS network, and the IMS CN as well.

7.4.1. UE access to the IMS CN

Before attempting communication with the IMS CN, the UE first has to establish a connection with the IP-CAN; next it must acquire an IP address; and third – to acquire a P-CSCF address.

7.4.1.1 P-CSCF discovery

There are several approaches to solve the P-CSCF discovery [60].

- The address of the P-CSCF could be given to the UE during the PDP context establishment. As part of this process, an IPv4 UE would need to acquire an IPv4 address.
- The P-CSCF address is discovered using DHCP. This means that a UE that supports DHCPv4 will receive from the DHCP server a Fully Qualified Domain Name (FQDN) of the P-CSCF and the address of a DNS, capable of resolving this FQDN.

- Using mechanisms such as SMS, over-the-air programming (OTA), or Open Mobile Alliance (OMA) device management, or some other vendor-specific mechanisms, such as pre-configuration. In this scenario, the P-CSCF address is a FQDN. As with the previous option, the UE must be able to access a DNS capable of resolving this FQDN.

The mechanisms described in third bullet-point above are expected to be the choice for early deployments of IPv4 IMS, since they do not put any additional requirements on the GPRS network.

7.4.1.2 Dual and single stack UE

The number of implemented versions of the IP protocol defines the UE as Single- or Dual-stack; the former running only one version of IP protocol suite, and the latter – simultaneously running two protocol suites. The IMS CN, on the other hand, can be IPv4 only, IPv6 only, or Dual stack. Having that in mind, there are several scenarios of UE connecting to the IMS CN.

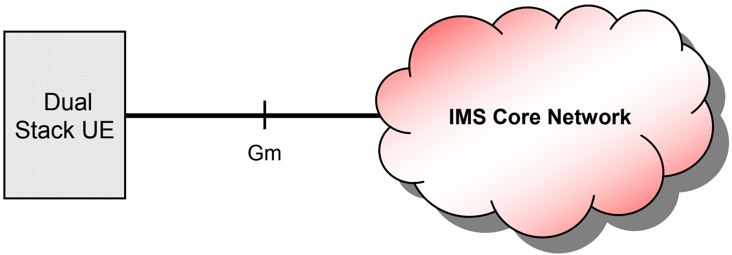


Figure 40. Dual Stack UE, connects to IMS CN. Adapted from [60]

Figure 40, illustrates the case, where UE with support for both IPv4 and IPv6 connects to an IMS core network. In this scenario, there is no way for the UE to know in advance which version of the IP protocol to use to establish a connection to the IMS CN. In such a case, The UE could be pre-configured to use either of the protocol versions.

When the UE is not pre-configured for a specific protocol version, one possible course of action is to attempt a connection using IPv6 and if that fails to resort to IPv4. This approach has the advantage that it provides for easy introduction of an IPv6 IMS CN since the UE would be already capable of establishing dialog using IPv6. On the other hand, for early IPv4 IMS deployments, this scenario would put additional requirements on the UE, which should be avoided.

As it is mentioned in 3GPP TR 23.981 [60], it is important to establish predictable dual stack UE behavior. The following has been recommended in the text:

- A dual stack UE should always attempt to activate an IPv6 PDP context for IMS communication. If that fails, then the UE should try activating an IPv4 PDP context.
- In case of successful IPv6 context activation, the UE should use IPv6 to contact the P-CSCF, whenever possible.

The case where both the UE and the IMS CN support only IPv4 or only IPv6, could be derived from the one describing the Dual Stack scenario.

A scenario where a single stack IPv4 UE attempts to connect to a single stack IPv6 IMS CN is not feasible and cannot be supported with the above described network setup.

7.4.2. Interworking scenarios

Depending on what IP version is supported by the IMS CN and UE, the various access scenarios could be illustrated as follows.

7.4.2.1 IPv4 IMS CN

Figure 41 depicts the scenario where an IPv4 UE or/and a dual stack UE is connected to the IPv4 IMS CN.

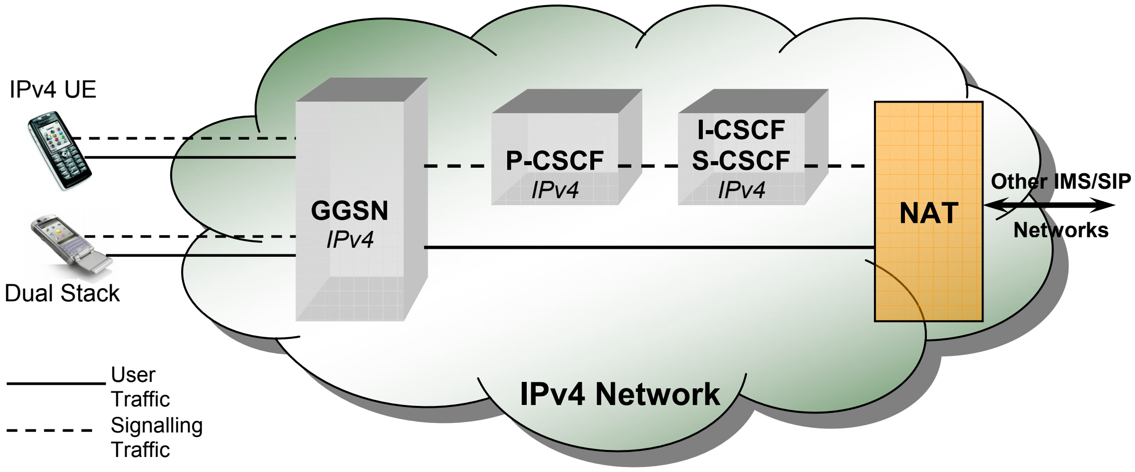


Figure 41. UE access to an IPv4 IMS network, non-roaming

In this scenario, both UE behave as described in paragraph 7.4.1.2. The UE may originate or receive sessions. A NAT might be used in order to connect to external networks.

7.4.2.2. Dual Stack IMS CN

Figure 42 illustrates the scenario where an IPv4 UE, IPv6 UE, or/and a dual stack UE is connected to a Dual Stack IMS CN.

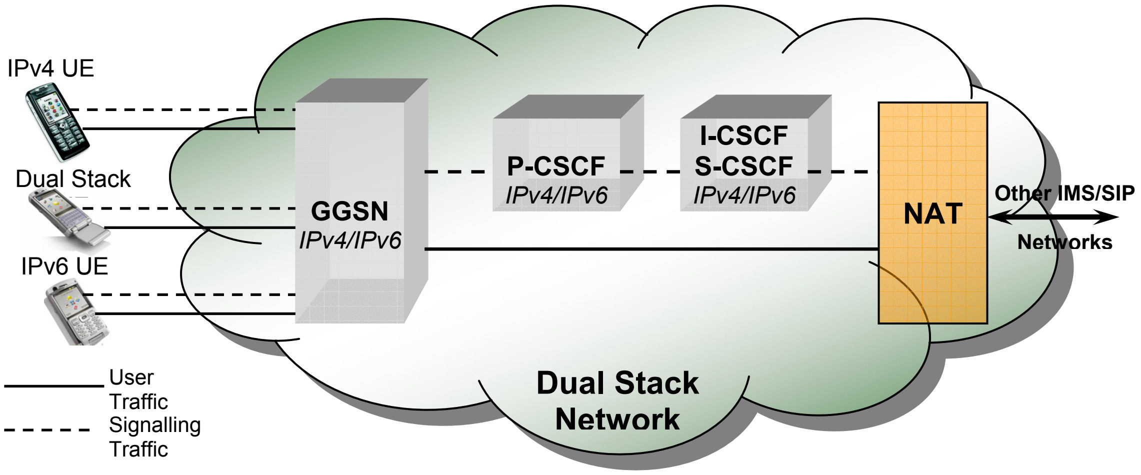


Figure 42. UE access to a Dual Stack IMS network, non-roaming

In this scenario, all UE behave as described in paragraph 7.4.1.2. The UE may originate or terminate sessions. A NAT might be used in order to connect to external networks.

7.4.2.3. IPv6 IMS CN

Figure 43 illustrates the scenario where an IPv6 UE or/and a dual stack UE is connected to the IPv6 IMS CN.

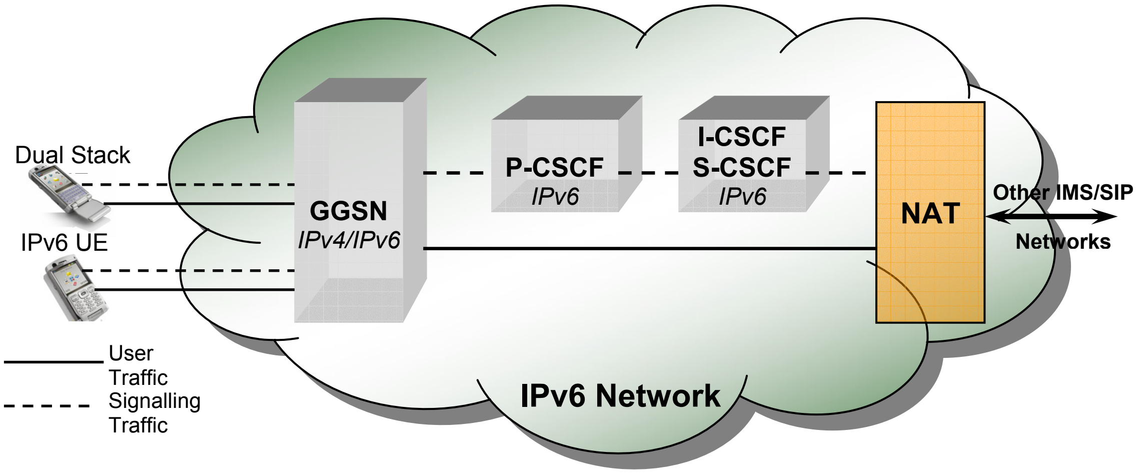


Figure 43. UE access to an IPv6 IMS network, non-roaming

In this scenario, both UE behave as described in paragraph 7.4.1.2. The UE may originate or terminate sessions. A NAT might be used in order to connect to external networks.

As indicated under each of this figures, these are non-roaming scenarios, meaning that the UE is connecting to its Home IMS CN. The roaming scenarios, as well as the GPRS scenarios are not within the scope of this report.

7.4.2.4. End-to-end Scenario

Figure 44, shows one of many possible end-to-end scenarios for IMS IP interworking. In this case, an IPv6 UE belonging to IPv6 IMS CN connects with an IPv4 UE residing in an IPv4 IMS CN. The transit network supports only IPv4.

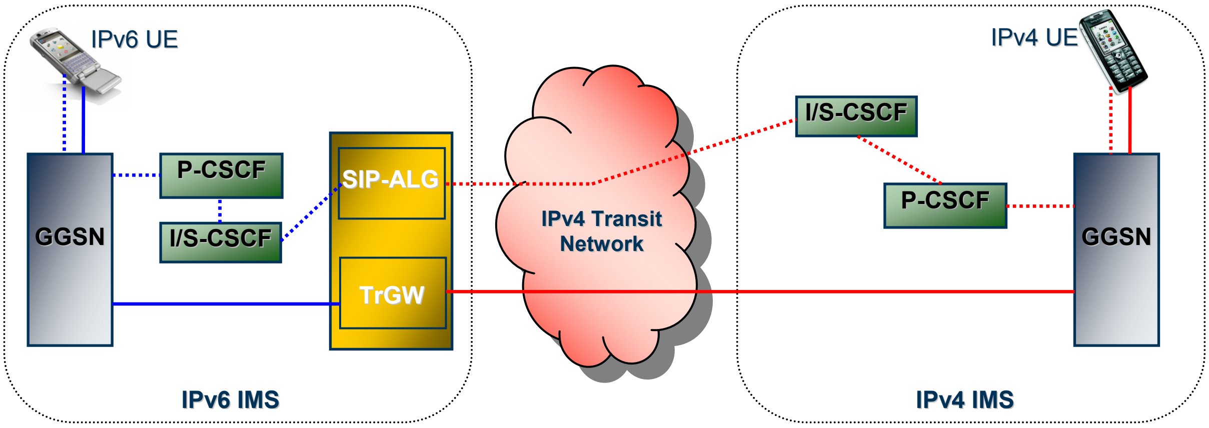


Figure 44. End-to-end IMS IP interworking scenario

As shown in the figure, the IPv6 IMS network shall require SIP-ALG and TrGW functionality at the border of the domain, in order to be able to route traffic through the transit network towards the terminating IPv4 network. As it was said above, this is only one of the possible scenarios, since the end-to-end solution might vary because of the different combinations of deployment scenarios of both the UE end the IMS CN.

For example, if the terminating network in this scenario is also IPv6 capable, then neither of the networks would need SIP-ALG and TrGW deployed at the border of their domains. Instead, the border gateway of each network would use tunneling mechanism to encapsulate the IPv6 packets into IPv4 packets, which would then simply be routed through the transit network. An example of such a case is shown in Figure 45.

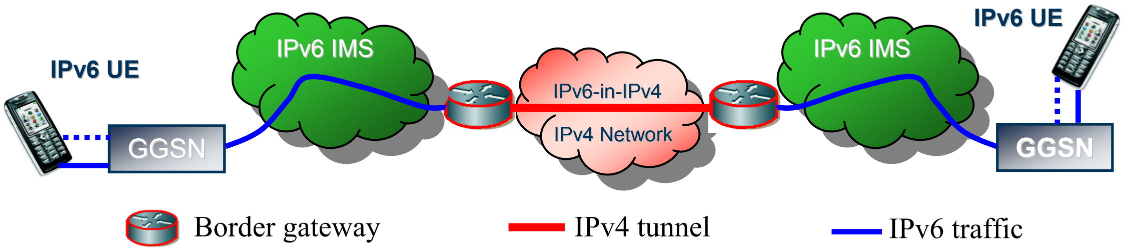


Figure 45. Interconnecting IPv6 IMS CNs, using tunneling mechanism

In this case, the UE activates an IPv6 PDP context with its GGSN. Since the UEs are single stack, the encapsulation of the traffic must be handled in the network, because it requires a node with a dual stack capability. It could be done by any dual-stack node along the path (i.e. the GGSN), or as in the case on figure 45, by the border gateway, which is the preferred scenario. Tunneling, handled by the network, is transparent for the end user, and the entire communication looks like it is native IPv6 traffic.

There are several aspects of the IP version interworking that need to be emphasized.

- Address translation between public and private IPv4 addresses might be necessary, for both signaling and media.
- Address translation between IPv4 and IPv6 addresses might be necessary, for both the signaling and the media.

This could lead to introduction of ALG- and TrGW functionality, as was mentioned before, this should be avoided if possible because of the additional traffic processing, which leads to increased delay and cost. This functionality is necessary only when interworking between IPv4 networks and IPv6 networks. If possible networks should be deployed in such a manner, as to avoid the necessity of NAT functionality when interconnecting.

8. Conclusions

As a result of the work carried out on this thesis project, the following conclusions could be highlighted:

- Peer-to-Peer model is expected to precede the Hub model because of its less complicated technical requirements. The Hub model will take over as the primary model for interworking gradually in time. This assertion coincides with the overall expectation of the telecom industry, as mentioned on several occasions by colleagues and specialist with whom we had discussion on the topic [15][18][19].
- Carrier DNS hierarchy in the GRX/IPX, separated from the Internet DNS will have dominant role in carriers interconnection. Although the Internet has its advantages as an interconnecting network, it is our opinion that service providers and the mobile operators will prefer the GRX/IPX network, because it is perceived as reliable, secure and better suited for the needs of the telecom operators.
- Most likely model for ENUM and MNP would be Centralized MNP database, on a national level (Tier 1). We have studied the theoretical models, as described by the GSM Association, and it is our belief, that this model will have better appeal to the network operators than any other we have studied.
- The IMS operators should use encryption tunnel protocols like IPSec to protect against the security services confidentiality and integrity in the GRX/IPX network. This concerns the control traffic. The media traffic will probably not be encrypted by the operators. The DNS servers in the GRX/IPX network should support DNSSEC to prevent possible attacks to the DNS infrastructure.
- It will be not be possible to use end-to-end security when IPX proxy introduces. This is a big drawback regarding network security. But in the GRX network it is possible to use end-to-end security, because of the absence of proxies.
- Most likely the mobile operators will enhance their security at the border gateway with a Session border Controller and a firewall. This will improve to protect the security service availability.
- To be able to authenticate other IPX proxies in the IPX network a solution could be to use SIP Authenticated Identity Body (AIB).
- Although IMS was designed with IPv6 in mind, the current IMS implementations are mostly IPv4 based. Gradual migration towards IPv6 based networks and services will occur when demand for such a move is noticed. This is likely to be a process, which will occur over long period of time. During this transition period, there will be networks, which support different versions of the IP protocol. This will lead to the need of IP version interworking.
- IP version interworking in IMS is likely to be solved with the introduction of SIP-ALG and TrGW functional entities. Although, these functions could perform IP version interworking, they introduce the NAT/NAPT processing of the traffic which could have negative effect on the service as a whole.

9. Suggested topics for further study

The field of study of this report has been very broad. The report has researched the fields of IMS Interworking models; the DNS functionality and hierarchy in the public Internet, the GRX/IPX network, and the DNS within a PLMN environment; traffic security with respect to known treats, from both the PLMN and GRX/IPX point of view; last but not least, the report looked into the challenging area of IP protocol version interworking.

Each and every of the above mentioned fields is vast and complicated enough, to give inspiration and challenges for further study. The conducted research yielded many interesting results and raised many questions. Some of these are presented below, as suggested topics for further study.

- **IMS interworking models area**

Two main interworking models have been identified and studied. These are the peer-to-peer and the hub models. What could be interesting for further study is the possibility of using the public Internet as a transit network, while addressing the challenges of security, interoperability, and quality of service.

Another area of interest is the evolution towards the IPX. Although this report started to consider the basic requirements that IPX makes, a future study, concentrated on the IPX functionality could be both interesting and very beneficial.

- **DNS hierarchy and Infrastructure ENUM area**

This report has analyzed the current situation and the directions in which the GRX/IPX DNS hierarchy is evolving and the theoretical aspects of an Infrastructure ENUM.

A topic for further study could be a practical test-bed for infrastructure ENUM within the GRX/IPX, with respect to Number Portability and legacy number portability databases.

Another interesting topic that remains open for deeper study is the possibility of simultaneous access to both the Internet DNS and the GRX/IPX DNS trees, with respect to ENUM and number portability.

- **IMS Traffic security area**

The network security regarding the evolution to IPX proxy in the GRX network is a big issue. It needs to be investigated further. The IPX Proxy network needs some kind of authentication mechanism to identify other proxies in the IPX network.

GRX will expand with the addition of new providers, which could introduce new threats to the network.

An intrusion detection system (IDS) in the IMS core could be useful to investigate. When GRX network expands, new protocols will be introduced in the network. IDS could find undetected or suspicious traffic that could harm an operator’s network.

Is it possible to open the GRX network for other Internet providers in a secure way? This is a major question.

- **IP protocol version interworking area**

Although designed with IPv6 in mind, IMS is still in the early deployment phase, and it is still relying on IPv4 protocol for providing services. An interesting area for future study, not touched in this report is the roaming interworking scenarios. Further study of the requirements and the problems that roaming presents is necessary.

References

[1]. John Scourias, *Overview of the Global System for Mobile Communications*, 2006-06-20, <http://www.shoshin.uwaterloo.ca/~jscouria/GSM/1> (1997-10-14)

[2]. Friedhelm Hillebrand, GSM and UMTS: The Creation Of Global Mobile Communication, Wiley, Copyright 2001, 590 pages, ISBN: 9780470843222

[3]. Global mobile Suppliers Association, *Evolution of GSM to 3G/IMT-2000 via GPRS/ EDGE/ WCDMA*, 2006-06-22, <http://www.geekzone.co.nz/content.asp?contentid=2362> (2004-02-20)

[4]. GSM Association, *GSM Roaming*, 2006-06-22, <http://www.gsmworld.com/roaming/index.shtml> (2006-06-22)

[5]. Study by BIPE for Autorité de régulation des telecommunications, *GPRS Roaming*, 2006-06-22, <http://www.arcep.fr/publications/etudes/gprs/ang-syn-gprsjuil03.htm> (July, 2003)

[6]. G. Camarillo and M. A. García-Martin, *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the cellular worlds*, Second edition Wiley, Copyright 2006, 427 pages, ISBN: 470018186

[7]. Wikipedia, *IP Multimedia Subsystem*, 2006-05-15, <http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem#Media_Servers> (2006-06-05)

[8]. Acme Packet, *Session border controllers in converged fixed-mobile IMS/TISPAN architecture*, 2006-06-22, <http://www.acmepacket.com/html/page.asp?PageID=%7B117C0E08-AB1A-4E0E-B0F3-67A453F76E66%7D>

[9]. GSM Association, *GSMA Trials Prove Interoperability of IP Multimedia Services*, 2006-06-09, <http://www.gsmworld.com/news/press_2005/press05_10.shtml> (2005-02-14).

[10].GSM Association, *GSMA Trials in Europe and Asia ensure multimedia services will work across networks*, 2006-06-12, <http://www.gsmworld.com/news/press_2005/press05_26.shtml> (2005-09-28).

[11]. GSM Association, *GSMA Trials to Pave the Way For Global Rollout of Video Share*, 2006-06-12, <http://www.gsmworld.com/news/press_2006/press06_18.shtml> (2006-02-15).

[12]. GSM Association, *Proposal for GRX Evolution*, 2005

[13]. GSM Association, *Inter-PLMN Backbone Guidelines*, PRD IR.34 ver. 3.5.0, October, 2003

[14]. GSM Association, *IMS Roaming & Interworking Guidelines*, IR.65 ver. 3.4, January 2006

[15]. Anders Stegen, interview by Emilio Di Geronimo and Boris Kalaglarski, March 27, 2006, interview 67A, transcript, Ericsson AB, Älvsjö.

[16]. Gert Öster, interview by Emilio Di Geronimo, March 31, 2006, interview 67A, transcript, Ericsson AB, Älvsjö.

[17]. Thomas Edwall, interview by Emilio Di Geronimo and Boris Kalaglarski, April 3, 2006, interview 67A, transcript, Ericsson AB, Älvsjö.

[18]. Hans Nilsson, interview by Emilio Di Geronimo and Boris Kalaglarski, April 4, 2006, interview 67A, transcript, Ericsson AB, Älvsjö.

[19]. Staffan Blau and Per Öberg, interview by Emilio Di Geronimo and Boris Kalaglarski, April 5, 2006, interview 67A, transcript, Ericsson AB, Älvsjö.

[20]. Fredrik Lindholm, interview by Emilio Di Geronimo and Boris Kalaglarski, April 10, 2006, interview 67A, transcript, Ericsson AB, Älvsjö.

[21]. Anders Stegen, interview by Emilio Di Geronimo and Boris Kalaglarski, May 4, 2006, interview 67A, transcript, Ericsson AB, Älvsjö.

[22] GSM Association, *DNS guidelines for operators*, IR.67 ver. 1.2, April 2006

[23] GSM Association*, MMS Interworking Guidelines*, PRD IR.52 ver. 3.1.0, February 2003

[24] P. Fältström and M. Mealling*, The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*, RFC 3761, IETF, April 2004

[25] M. Mealling and R. Daniel, *The Naming Authority Pointer (NAPTR) DNS Resource Record*, RFC 2915, IETF, September 2000

[26] 3GPP TSG SA WG3 Security-S3#31, MMS Security Considerations

[27] Nortel technology Journal 2006-12-11,< http://www.stromcarlson.com/docs/ntj/ntj3.pdf>

[28] Charlie Kaufman, Radia Perlman and Mike Speciner, Network Security: PRIVATE Communication in a PUBLIC World, 2nd Edition Prentice Hall, copyright 2002, 713 pages, ISBN: 0-13-046019-2.

[29] 3GPP TSG SA WG3 Security, February 2002

[30] 3GPP TS 33.210, 3G security; Network Domain Security (NDS); IP network layer security ver. 7.0.0., May, 2005

[31] B. Wellington, Domain Name System Security (DNSSEC) Signing Authority, RFC 3008, IETF, November 2000

[32] A. Heffernan, Protection of BGP Sessions via the TCP MD5 Signature Option, RFC 2385, IETF, August 1998,, <http://www.faqs.org/rfcs/rfc2385.html>

[33] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, IETF, RFC 2401, November 1998

[34] Topology Hiding Inter-working Gateway, 2006-12-11,

<http://www.mpirical.com/companion/IP/Topology_Hiding_Inter-working_Gateway.htm>

[35] J. Peterson, S/MIME Advanced Encryption Standard (AES), RFC 3853, IETF, July 2004

[36] 3GPP, Response to IETF Concerns on SIP and IMS Interoperability, 2006-12-11 <https://www.ietf.org/IESG/LIAISON/SP-020842.htm>(2002-12-01)

[37] Stefano Zanero, Analyzing TCP traffic pattern using self organizing maps, D.E.I.-Politecnico di Milano, 2005

[38] Protect BGP sessions with the TCP MD5 option, 2007-01-07, <http://bgphints.ruud.org/articles/bgp-md5.html>(2004-04-21)

[39] Gary Alterson, Comparing BGP/MPLS and IPSec VPNs, 2002, <http://sans.org/reading_room/whitepapers/vpns/756.php>

[40] Stephen Kent, Charles Lynn, and Karen Seo, Secure Border Gateway Protocol (Secure-BGP), Published in IEEE Journal on Selected Areas in Communications Vol. 18, No.4, April 200, pp. 582-592, <http://www.net-tech.bbn.com/sbgp/IEEE-JSAC-April2000/IEEE-S-BGP.html>

[41] Jonathan Cumming, Session Border Control in IMS: An analysis of the requirements for session Border Control in IMS networks, Data Connection, October 2006

[42] Lecture notes from Anders Stegen, GSMA IOT, September 2005

[43] David L. Mills, Network Time Protocol (Version 3), IETF, RFC 1305, March 1992

[44] IMS IP Connectivity, M-IMS/M-PBN Guidelines, Ericsson AB 2006

[45] D. Farinacci, T. Li, S. Hanks, D. Meyer and P. Traina, Generic Routing Encapsulation (GRE), IETF, RFC 2784, March 2000

[46] Steven M. Bellovin, Lecture notes from Columbia University, computer science AT, 2006-12-09,<http://www.cs.columbia.edu/~smb/classes/f06/l13.pdf>

[47] Mark Collier, Basic Vulnerability Issues for SIP Security, March, 2005, <http://download.securelogix.com/library/SIP_Security030105.pdf>

[48] Attacking the DNS protocol, 2006-12-09, <http://www.rootsecure.net/content/downloads/pdf/sans_attacking_dns_protocol.pdf>, (2003-10-29)

[49] CISCO (white paper), Security in SIP-based networks, 2002

[50] SNOCER, *Low Cost Tools for Secure and Highly Available VoIP Communication Services***,** 2006-12-09, <http://www.snocer.org/Paper/snocer_D2_2.pdf>

[51] Merike Kaeo, Designing Network Security, Second Edition, Cisco Press, 2003, ISBN: 1587051176

[52] Configuring IPSec/GRE with NAT, 2006-12-11, <http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a0080094bff.shtml>, (2006-09-29)

[53] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, the Secure Real-time Transport Protocol (SRTP), IETF, RFC 3711, March 2004

[54] Intrusion detection system, 2007-01-02, <http://en.wikipedia.org/wiki/Intrusion-detection_system>, (2006-12-27)

[55] Transport layer security (TLS), 2007-01-29, <http://en.wikipedia.org/wiki/Transport_Layer_Security>, (2007-01-29)

[56] IMS signaling, Ericsson, LZU 108 6604 R2A, 2006

[57] 3GPP, *Interworking between the IM CN subsystem and IP networks,* TS 29.162 v7.1.1, 2006-03

[58] J. Rosenberg, H. Schulzrine, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, *SIP: Session Initiation Protocol*, IETF, RFC 3261, June 2002

[59] 3GPP, *Network Architecture,* TS 23.002 v7.1.0, 2006-03

[60] 3GPP, *Interworking aspects and migration scenarios for IPv4 based IMS implementations,* TR 23.981 v6.4.0, 2005-09

[61] J. Wiljakka - editor, *Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks*, RFC 4215, IETF, October 2005

[62] ICANN, *Factsheet Root Server Attack on 6th of February*, 2007-03-01, <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>

[63] Internet Architecture Board, *IAB Technical Comment on the Unique DNS Root*, RFC 2826, IETF, May 2000, <http://tools.ietf.org/html/rfc2826>

[64] P. Mockapetris, *Domain names – concepts and facilities*, RFC 1034, IETF, November 1987**,** **<**http://tools.ietf.org/html/rfc1034>

[65] P. Mockapetris, *Domain names – implementation and specification*, RFC 1035, IETF, November 1987**,** **<**http://tools.ietf.org/html/rfc1035>

[66] J. Peterson, Ed, Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format, IETF, RFC 3893, September 2004

COS/CCS 2007-15

www.kth.se